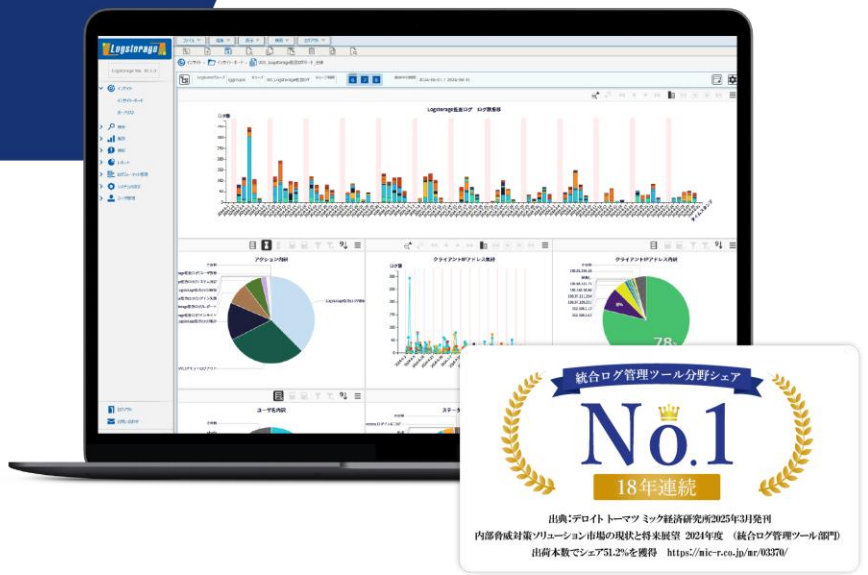
Logstorage VER.10

統合ログ管理システム「ログストレージ」

Logstorage Microsoft 365 連携パック
参考資料



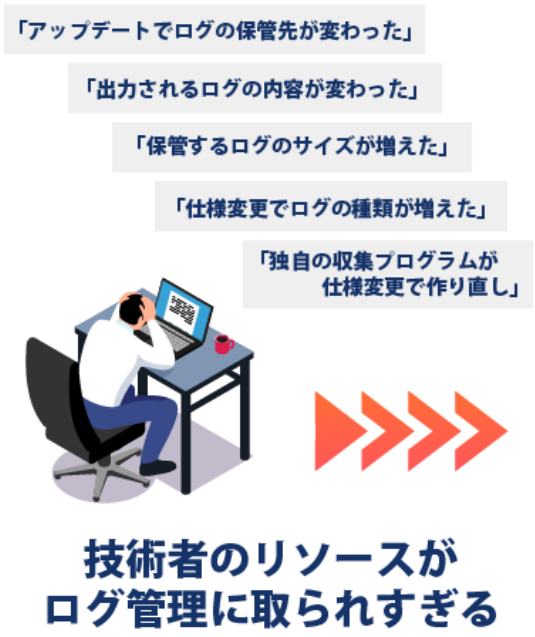
Infoscience
インフォサイエンス株式会社　Infoscience Corporation　www.infoscience.co.jp
プロダクト事業部　Product division　https://logstorage.com　info@logstorage.com　／　Tel: 03-5427-3503　／　Fax: 03-5427-3889

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

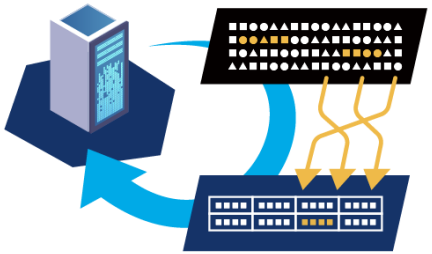
Logstorage 連携パックには、専用のログ収集モジュール・ログフォーマット定義ファイル・分析テンプレートが含まれます。

ログ収集モジュール

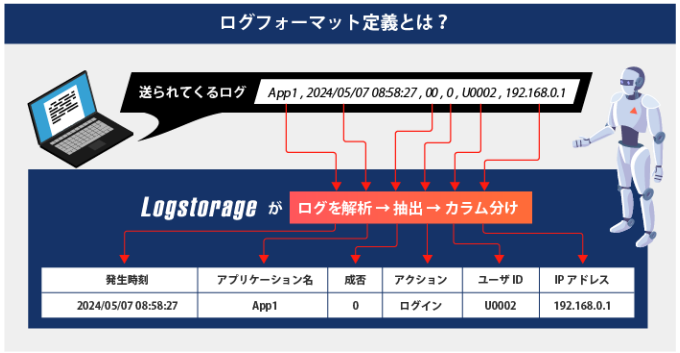
製品ごとにログの出力方法や出力先は異なります。各製品のログにあわせたログ収集モジュールをご用意しております。

※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



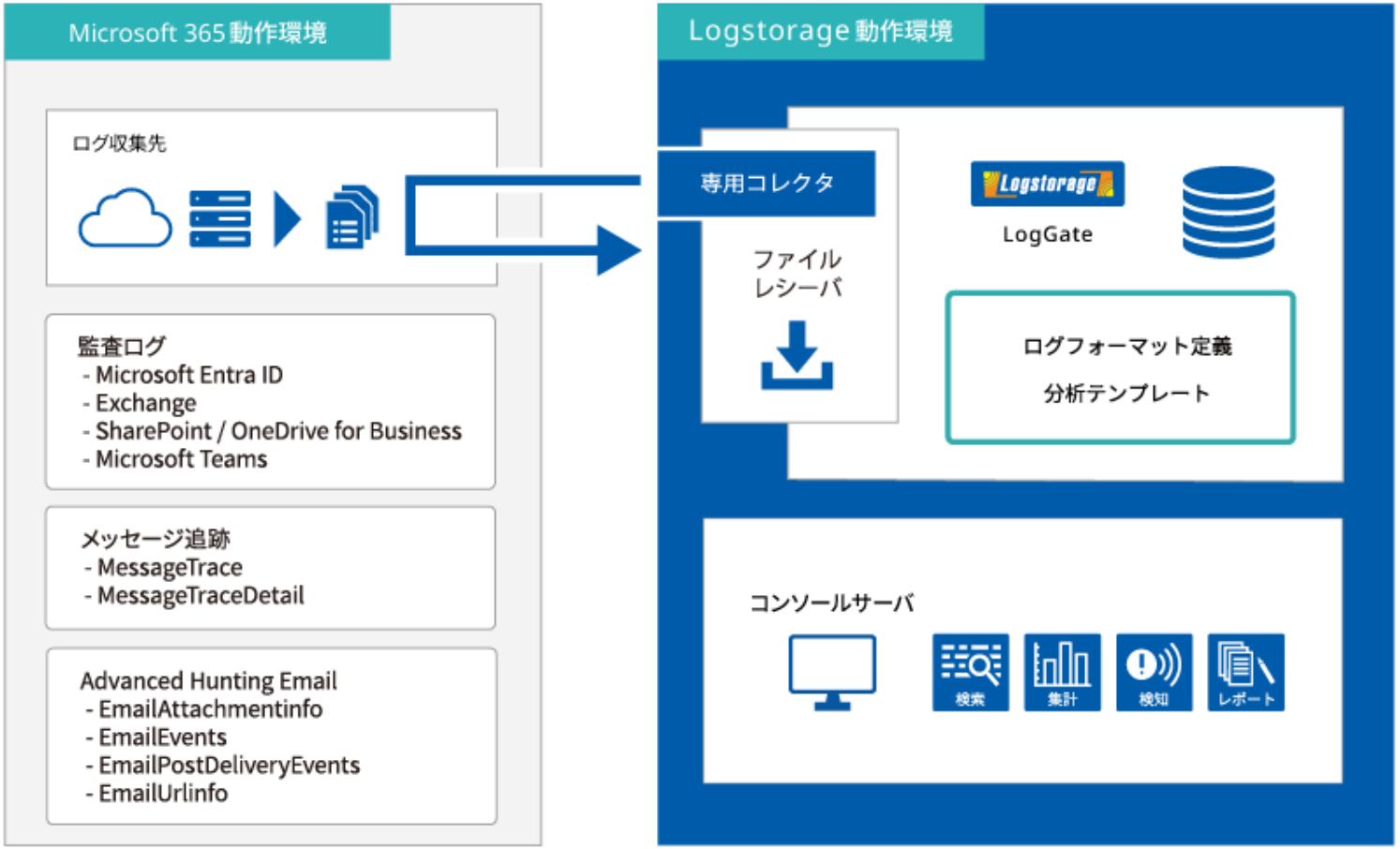
連携している製品のログフォーマット（並び順や表示の仕方）を分析し、ログを項目ごとに抽出します。



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



監査ログ・テンプレート一覧

検索-1

Logstorage Microsoft 365 連携パック 監査ログ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	概要
Microsoft 365 Exchange メールの削除	メール削除のアクティビティを検索します。
Microsoft 365 Exchange メールボックスの転送設定	メール転送設定のアクティビティを検索します。
Microsoft 365 Exchange メールボックスへのサインイン	メールボックスへのサインインのアクティビティを検索します。
Microsoft 365 Exchange メールボックスアクティビティ	「メールボックスアクティビティ」に含まれるアクティビティを検索します。
Microsoft 365 Exchange 全ログ検索	Exchange の全てのアクティビティを検索します。
Microsoft 365 Exchange 受信トレイのルール設定	受信トレイのルール作成、変更のアクティビティを検索します。
Microsoft 365 Exchange 管理アクティビティ	「管理アクティビティ」に含まれるアクティビティを検索します。
Microsoft 365 Microsoft Entra ID アプリケーション管理アクティビティ	「アプリケーション管理アクティビティ」に含まれるアクティビティを検索します。
Microsoft 365 Microsoft Entra ID グループ管理アクティビティ	「グループ管理アクティビティ」に含まれるアクティビティを検索します。
Microsoft 365 Microsoft Entra ID ディレクトリ管理アクティビティ	「ディレクトリ管理アクティビティ」に含まれるアクティビティを検索します。
Microsoft 365 Microsoft Entra ID ユーザー管理アクティビティ	「ユーザー管理アクティビティ」に含まれるアクティビティを検索します。
Microsoft 365 Microsoft Entra ID ログイン	ログイン成功、失敗のアクティビティを検索します。
Microsoft 365 Microsoft Entra ID ロール管理アクティビティ	「ロール管理アクティビティ」に含まれるアクティビティを検索します。
Microsoft 365 Microsoft Entra ID 全ログ検索	Microsoft Entra ID の全てのアクティビティを検索します。
Microsoft 365 Microsoft Teams Teamsのアクティビティ	「Teamsのアクティビティ」に含まれるアクティビティを検索します。
Microsoft 365 Microsoft Teams Teamsへのサインイン	Teamsへのサインインのアクティビティを検索します。
Microsoft 365 Microsoft Teams コネクターの作成、変更、削除	コネクターの作成、変更、削除のアクティビティを検索します。
Microsoft 365 Microsoft Teams チャネルの作成、削除	チャネルの作成、削除のアクティビティを検索します。
Microsoft 365 Microsoft Teams チームの作成、削除	チームの作成、削除のアクティビティを検索します。
Microsoft 365 Microsoft Teams プライベートチャネルの作成	プライベートチャネル作成のアクティビティを検索します。
Microsoft 365 Microsoft Teams メンバーの追加、削除	メンバーの追加、削除のアクティビティを検索します。
Microsoft 365 Microsoft Teams 全ログ検索	Microsoft Teams の全てのアクティビティを検索します。
Microsoft 365 Microsoft Teams 組織設定の変更	組織設定変更のアクティビティを検索します。

監査ログ・テンプレート一覧

検索-2

検索条件テンプレート名	概要
Microsoft 365 OneDrive for Business ファイルとページのアクティビティ	「ファイルとページのアクティビティ」に含まれるアクティビティを検索します。
Microsoft 365 OneDrive for Business フォルダーのアクティビティ	「フォルダーのアクティビティ」に含まれるアクティビティを検索します。
Microsoft 365 OneDrive for Business マルウェアの検出	マルウェア検出のアクティビティを検索します。
Microsoft 365 OneDrive for Business 全ログ検索	OneDrive for Business の全てのアクティビティを検索します。
Microsoft 365 OneDrive for Business 共有とアクセス要求のアクティビティ	「共有とアクセス要求のアクティビティ」に含まれるアクティビティを検索します。
Microsoft 365 OneDrive for Business 同期アクティビティ	「同期アクティビティ」に含まれるアクティビティを検索します。
Microsoft 365 Quarantine エクスポートされた検疫メッセージ	「エクスポートされた検疫メッセージ」に含まれるアクティビティを検索します。
Microsoft 365 Quarantine プレビューされた検疫メッセージ	「プレビューされた検疫メッセージ」に含まれるアクティビティを検索します。
Microsoft 365 Quarantine リリース要求検疫メッセージ	「リリース要求検疫メッセージ」に含まれるアクティビティを検索します。
Microsoft 365 Quarantine 全ログ検索	Quarantine の全てのアクティビティを検索します。
Microsoft 365 Quarantine 削除された検疫メッセージ	「削除された検疫メッセージ」に含まれるアクティビティを検索します。
Microsoft 365 Quarantine 検疫メッセージのリリース要求が拒否されました	「検疫メッセージのリリース要求が拒否されました」に含まれるアクティビティを検索します。
Microsoft 365 Quarantine 表示された検疫メッセージのヘッダー	「表示された検疫メッセージのヘッダー」に含まれるアクティビティを検索します。
Microsoft 365 Quarantine 解放された検疫メッセージ	「解放された検疫メッセージ」に含まれるアクティビティを検索します。

監査ログ・テンプレート一覧

検索-3

検索条件テンプレート名	概要
Microsoft 365 SharePoint SharePointリストのアクティビティ	「SharePointリストのアクティビティ」に含まれるアクティビティを検索します。
Microsoft 365 SharePoint サイト権限のアクティビティ	「サイト権限のアクティビティ」に含まれるアクティビティを検索します。
Microsoft 365 SharePoint サイト管理アクティビティ	「サイト管理アクティビティ」に含まれるアクティビティを検索します。
Microsoft 365 SharePoint ファイルとページのアクティビティ	「ファイルとページのアクティビティ」に含まれるアクティビティを検索します。
Microsoft 365 SharePoint フォルダーのアクティビティ	「フォルダーのアクティビティ」に含まれるアクティビティを検索します。
Microsoft 365 SharePoint マルウェアの検出	マルウェア検出のアクティビティを検索します。
Microsoft 365 SharePoint 全ログ検索	SharePoint の全てのアクティビティを検索します。
Microsoft 365 SharePoint 共有とアクセス要求のアクティビティ	「共有とアクセス要求のアクティビティ」に含まれるアクティビティを検索します。
Microsoft 365 SharePoint 同期アクティビティ	「同期アクティビティ」に含まれるアクティビティを検索します。
Microsoft 365 Threat Intelligence Advanced Threat Protection 関連の脅威を検知	「Advanced Threat Protection 関連の脅威を検知」を含むアクティビティを検索します。
Microsoft 365 Threat Intelligence 全ログ検索	ThreatIntelligence の全てのアクティビティを検索します。
Microsoft 365 Threat Intelligence 脅威のあるメールを検知	「脅威のあるメールを検知」を含むアクティビティを検索します。
Microsoft 365 Threat Intelligence 脅威のある URL をクリック	「脅威のある URL をクリック」を含むアクティビティを検索します。
Microsoft 365 全ログ検索	Microsoft 365 の全てのアクティビティを検索します。

監査ログ・テンプレート一覧

集計-1

Logstorage Microsoft 365 連携パック 監査ログ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
Microsoft 365 SharePoint アクセス頻度の高いフォルダー・ファイル	アクセス頻度の高いフォルダー・ファイルを集計します。
Microsoft 365 SharePoint アップロードの頻度が高いユーザー	アップロードの頻度が高いユーザーを集計します。
Microsoft 365 SharePoint ダウンロードの頻度が高いユーザー	ダウンロードの頻度が高いユーザーを集計します。
Microsoft 365 SharePoint 業務時間外にファイルアクセスしたユーザー	業務時間外にファイルアクセスしたユーザーを集計します。
Microsoft 365 SharePoint 組織外からアクセスされたフォルダー・ファイル	組織外からアクセスされたフォルダー・ファイルを集計します。
Microsoft 365 Threat Intelligence Advanced Threat Protection 関連の脅威を検知	Advanced Threat Protection 関連の脅威を検知のアクティビティを集計します。
Microsoft 365 Threat Intelligence 脅威のある URL をクリック	脅威のある URL をクリックのアクティビティを集計します。
Microsoft 365 Threat Intelligence 脅威のあるメールを検知	脅威のあるメールを検知のアクティビティを集計します。
Microsoft 365 業務時間外にアクセスしたユーザー	業務時間外に Microsoft 365 にアクセスしたユーザーを集計します。
Microsoft 365 SharePoint アクセス頻度の高いフォルダー・ファイル	アクセス頻度の高いフォルダー・ファイルを集計します。
Microsoft 365 SharePoint アップロードの頻度が高いユーザー	アップロードの頻度が高いユーザーを集計します。
Microsoft 365 SharePoint ダウンロードの頻度が高いユーザー	ダウンロードの頻度が高いユーザーを集計します。
Microsoft 365 SharePoint 業務時間外にファイルアクセスしたユーザー	業務時間外にファイルアクセスしたユーザーを集計します。
Microsoft 365 SharePoint 組織外からアクセスされたフォルダー・ファイル	組織外からアクセスされたフォルダー・ファイルを集計します。
Microsoft 365 Threat Intelligence Advanced Threat Protection 関連の脅威を検知	Advanced Threat Protection 関連の脅威を検知のアクティビティを集計します。
Microsoft 365 Threat Intelligence 脅威のある URL をクリック	脅威のある URL をクリックのアクティビティを集計します。
Microsoft 365 Threat Intelligence 脅威のあるメールを検知	脅威のあるメールを検知のアクティビティを集計します。
Microsoft 365 業務時間外にアクセスしたユーザー	業務時間外に Microsoft 365 にアクセスしたユーザーを集計します。

監査ログ・テンプレート一覧

集計-2

集計条件テンプレート名	概要
Microsoft 365 Exchange メールボックスへのサインイン	メールボックスへのサインインのアクティビティを集計します。
Microsoft 365 Microsoft Entra ID ログイン失敗	ログイン失敗のアクティビティを集計します。
Microsoft 365 Microsoft Entra ID ログイン成功	ログイン成功のアクティビティを集計します。
Microsoft 365 Microsoft Teams Teamsへのサインイン	Teamsへのサインインのアクティビティを集計します。
Microsoft 365 OneDrive for Business アクセス頻度の高いフォルダー・ファイル	アクセス頻度の高いフォルダー・ファイルを集計します。
Microsoft 365 OneDrive for Business アップロードの頻度が高いユーザー	アップロードの頻度が高いユーザーを集計します。
Microsoft 365 OneDrive for Business ダウンロードの頻度が高いユーザー	ダウンロードの頻度が高いユーザーを集計します。
Microsoft 365 OneDrive for Business 業務時間外にファイルアクセスしたユーザー	業務時間外にファイルアクセスしたユーザーを集計します。
Microsoft 365 OneDrive for Business 組織外からアクセスされたフォルダー・ファイル	組織外からアクセスされたフォルダー・ファイルを集計します。
Microsoft 365 Quarantine エクスポートされた検疫メッセージ	エクスポートされた検疫メッセージのアクティビティを集計します。
Microsoft 365 Quarantine プレビューされた検疫メッセージ	プレビューされた検疫メッセージのアクティビティを集計します。
Microsoft 365 Quarantine リリース要求検疫メッセージ	リリース要求検疫メッセージのアクティビティを集計します。
Microsoft 365 Quarantine 削除された検疫メッセージ	削除された検疫メッセージのアクティビティを集計します。
Microsoft 365 Quarantine 検疫メッセージのリリース要求が拒否されました	検疫メッセージのリリース要求が拒否されましたのアクティビティを集計します。
Microsoft 365 Quarantine 表示された検疫メッセージのヘッダー	表示された検疫メッセージのヘッダーのアクティビティを集計します。
Microsoft 365 Quarantine 解放された検疫メッセージ	解放された検疫メッセージのアクティビティを集計します。

監査ログ・テンプレート一覧

レポート-1

Logstorage Microsoft 365 連携パック 監査ログ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
Microsoft 365 Exchange メールボックスの転送設定	検索条件「メールボックスの転送設定」を指定してレポート出力します。
Microsoft 365 Exchange メールボックスへのサインイン	集計条件「メールボックスへのサインイン」を指定してレポート出力します。
Microsoft 365 Microsoft Entra ID グループ、ユーザー管理アクティビティ	検索条件「グループ管理アクティビティ」と「ユーザー管理アクティビティ」を指定してレポート出力します。
Microsoft 365 Microsoft Entra ID ログイン失敗	集計条件「ログイン失敗」を指定してレポート出力します。
Microsoft 365 Microsoft Entra ID ログイン成功	集計条件「ログイン成功」を指定してレポート出力します。
Microsoft 365 Microsoft Teams Teamsへのサインイン	集計条件「Teamsへのサインイン」を指定してレポート出力します。
Microsoft 365 Microsoft Teams チャネルの作成、削除	検索条件「チャネルの作成、削除」を指定してレポート出力します。
Microsoft 365 Microsoft Teams チームの作成、削除	検索条件「チームの作成、削除」を指定してレポート出力します。
Microsoft 365 Microsoft Teams メンバーの追加、削除	検索条件「メンバーの追加、削除」を指定してレポート出力します。
Microsoft 365 Microsoft Teams 組織設定の変更	検索条件「組織設定の変更」を指定してレポート出力します。
Microsoft 365 OneDrive for Business アクセス頻度の高いフォルダー・ファイル	集計条件「アクセス頻度の高いフォルダー・ファイル(OneDrive)」を指定してレポート出力します。
Microsoft 365 OneDrive for Business アップロードの頻度が高いユーザー	集計条件「アップロードの頻度が高いユーザー(OneDrive)」を指定してレポート出力します。
Microsoft 365 OneDrive for Business ダウンロードの頻度が高いユーザー	集計条件「ダウンロードの頻度が高いユーザー(OneDrive)」を指定してレポート出力します。
Microsoft 365 OneDrive for Business マルウェアの検出	検索条件「マルウェアの検出(OneDrive)」を指定してレポート出力します。
Microsoft 365 OneDrive for Business 業務時間外にファイルアクセスしたユーザー	集計条件「業務時間外にファイルアクセスしたユーザー(OneDrive)」を指定してレポート出力します。
Microsoft 365 OneDrive for Business 組織外からアクセスされたフォルダー・ファイル	集計条件「組織外からアクセスされたフォルダー・ファイル(OneDrive)」を指定してレポート出力します。

監査ログ・テンプレート一覧

レポート-2

レポート条件テンプレート名	概要
Microsoft 365 Quarantine エクスポートされた検疫メッセージ	集計条件「エクスポートされた検疫メッセージ」を指定してレポート出力します。
Microsoft 365 Quarantine プレビューされた検疫メッセージ	集計条件「プレビューされた検疫メッセージ」を指定してレポート出力します。
Microsoft 365 Quarantine リリース要求検疫メッセージ	集計条件「リリース要求検疫メッセージ」を指定してレポート出力します。
Microsoft 365 Quarantine 削除された検疫メッセージ	集計条件「削除された検疫メッセージ」を指定してレポート出力します。
Microsoft 365 Quarantine 検疫メッセージのリリース要求が拒否されました	集計条件「検疫メッセージのリリース要求が拒否されました」を指定してレポート出力します。
Microsoft 365 Quarantine 表示された検疫メッセージのヘッダー	集計条件「表示された検疫メッセージのヘッダー」を指定してレポート出力します。
Microsoft 365 Quarantine 解放された検疫メッセージ	集計条件「解放された検疫メッセージ」を指定してレポート出力します。
Microsoft 365 SharePoint アクセス頻度の高いフォルダー・ファイル	集計条件「アクセス頻度の高いフォルダー・ファイル(SharePoint)」を指定してレポート出力します。
Microsoft 365 SharePoint アップロードの頻度が高いユーザー	集計条件「アップロードの頻度が高いユーザー(SharePoint)」を指定してレポート出力します。
Microsoft 365 SharePoint ダウンロードの頻度が高いユーザー	集計条件「ダウンロードの頻度が高いユーザー(SharePoint)」を指定してレポート出力します。
Microsoft 365 SharePoint マルウェアの検出	検索条件「マルウェアの検出(SharePoint)」を指定してレポート出力します。
Microsoft 365 SharePoint 業務時間外にファイルアクセスしたユーザー	集計条件「業務時間外にファイルアクセスしたユーザー(SharePoint)」を指定してレポート出力します。
Microsoft 365 SharePoint 組織外からアクセスされたフォルダー・ファイル	集計条件「組織外からアクセスされたフォルダー・ファイル(SharePoint)」を指定してレポート出力します。
Microsoft 365 Threat Intelligence Advanced Threat Protection 関連の脅威を検知	集計条件「Advanced Threat Protection 関連の脅威を検知」を指定してレポート出力します。
Microsoft 365 Threat Intelligence 脅威のある URL をクリック	集計条件「脅威のある URL をクリック」を指定してレポート出力します。
Microsoft 365 Threat Intelligence 脅威のあるメールを検知	集計条件「脅威のあるメールを検知」を指定してレポート出力します。
Microsoft 365 業務時間外にアクセスしたユーザー	集計条件「Microsoft 365 業務時間外にアクセスしたユーザー」を指定してレポート出力します。

メッセージ追跡ログ・テンプレート一覧

検索

Logstorage Microsoft 365 連携パック メッセージ追跡ログ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	概要
Microsoft 365 メッセージ追跡	メッセージ追跡 に関する情報を検索します。
Microsoft 365 メッセージ追跡	詳細メッセージ追跡詳細 に関する情報を検索します。
Microsoft 365 メッセージ追跡（サマリ情報＋詳細情報）	特定のメッセージトレースIDに紐づく、 MessageTrace と MessageTraceDetail に関する情報を検索します。

メッセージ追跡ログ・テンプレート一覧

集計 レポート

Logstorage Microsoft 365 連携パック メッセージ追跡ログの集計及び、レポートテンプレートは以下の通りです。

集計・レポート条件テンプレート名	概要
Microsoft 365 Exchangeメールサイズ集計（日別）	日別のメールサイズを集計・レポートします。
Microsoft 365 Exchangeメールサイズ集計（時間別）	時間別のメールサイズを集計・レポートします。
Microsoft 365 Exchangeメールステータス集計	日別のメールステータスを集計・レポートします。
Microsoft 365 Exchangeメール件数 TOP20（受信者別）	受信メールアドレス毎のメール件数が多いデータを抽出します。既定値は20件で設定しています。
Microsoft 365 Exchangeメール件数 TOP20（送信者別）	送信メールアドレス毎のメール件数が多いデータを抽出します。既定値は20件で設定しています。
Microsoft 365 Exchangeメール件数集計（日別）	日別のメール件数を集計・レポートします。
Microsoft 365 Exchangeメール件数集計（時間別）	時間別のメール件数を集計・レポートします。
Microsoft 365 Exchangeメール受信者一覧	受信メールアドレス毎のメール件数を集計・レポートします。
Microsoft 365 Exchangeメール送信者一覧	送信メールアドレス毎のメール件数を集計・レポートします。
Microsoft 365 Exchange組織外の宛先へのメール送信	組織外の宛先へのメール送信件数を集計・レポートします。
Microsoft 365 Exchange組織外の差出人からのメール受信	組織外の差出人からのメール受信件数を集計・レポートします。

Advanced Hunting Emailログ・テンプレート一覧

検索

Logstorage Microsoft 365 連携パック Advanced Hunting Emailログ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	概要
Microsoft 365 AdvHunting Email EmailAttachmentInfo スキーマ 全ログ検索	EmailAttachmentInfo スキーマの全てのログを検索します。
Microsoft 365 AdvHunting Email EmailEvents スキーマ 全ログ検索	EmailEvents スキーマの全てのログを検索します。
Microsoft 365 AdvHunting Email EmailPostDeliveryEvents スキーマ 全ログ検索	EmailPostDeliveryEvents スキーマの全てのログを検索します。
Microsoft 365 AdvHunting Email EmailUrlInfo スキーマ 全ログ検索	EmailUrlInfo スキーマの全てのログを検索します。
Microsoft 365 AdvHunting Email 共通	特定のネットワークメッセージIDに紐づく、 AdvHunting Email の各ログを検索します。

Advanced Hunting Emailログ・テンプレート一覧 集計 レポート

Logstorage Microsoft 365 連携パック Advanced Hunting Emailログの集計及びレポートテンプレートは以下の通りです。

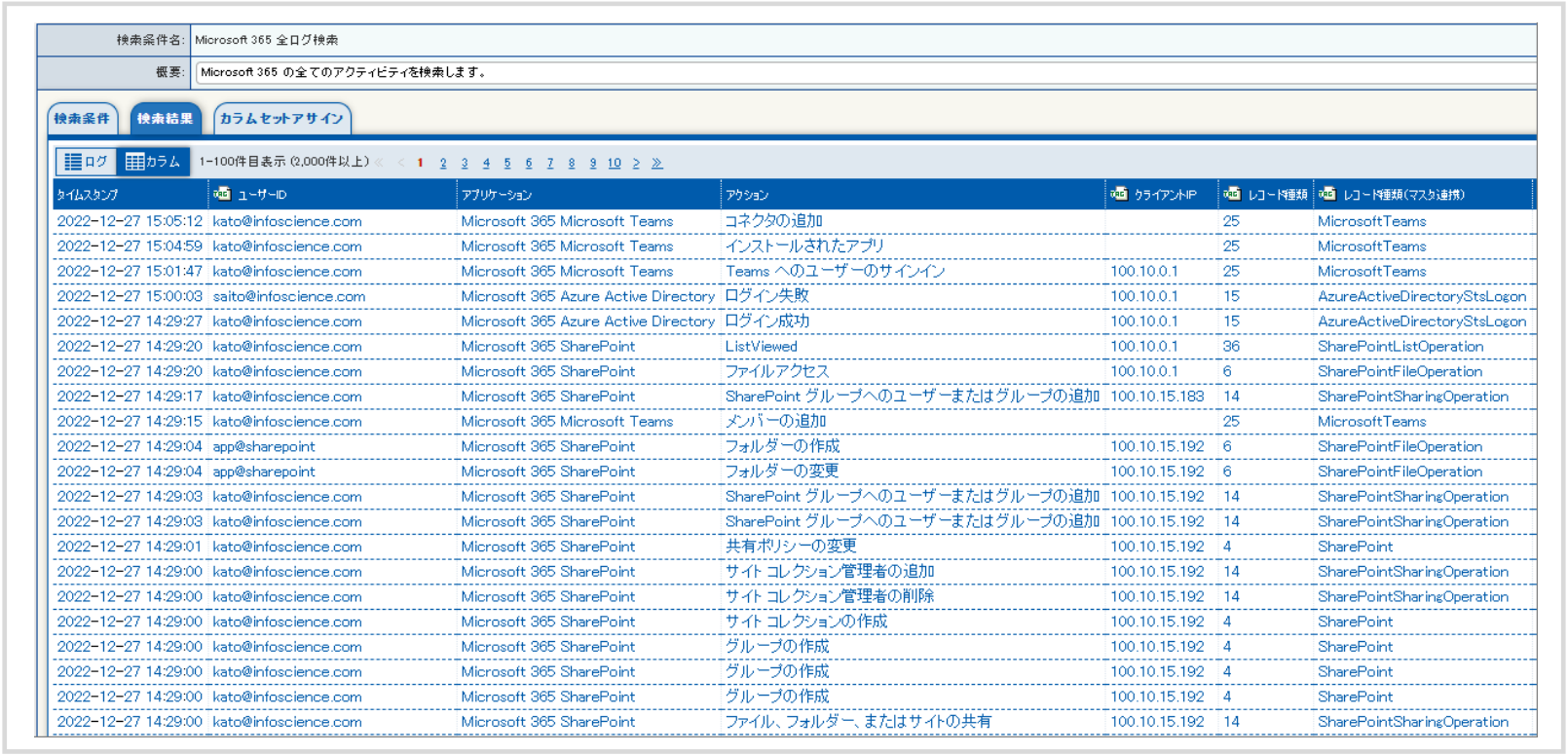
集計・レポート条件テンプレート名	概要
Microsoft 365 AdvHunting Email URLドメイン件数集計（日別）	EmailUrlInfo の日別のURLドメイン件数を集計・レポートします。
Microsoft 365 AdvHunting Email URLドメイン件数集計（時間別）	EmailUrlInfo の時間別のURLドメイン件数を集計・レポートします。
Microsoft 365 AdvHunting Email イベント件数集計（日別）	EmailEvents の日別のイベント件数を集計・レポートします。
Microsoft 365 AdvHunting Email イベント件数集計（時間別）	EmailEvents の時間別のイベント件数を集計・レポートします。
Microsoft 365 AdvHunting Email 添付ファイルサイズ集計（日別）	EmailAttachmentInfo の日別の添付ファイルサイズを集計・レポートします。
Microsoft 365 AdvHunting Email 添付ファイルサイズ集計（時間別）	EmailAttachmentInfo の時間別の添付ファイルサイズを集計・レポートします。
Microsoft 365 AdvHunting Email 脅威判定集計	EmailEvents の脅威判定を集計・レポートします。
Microsoft 365 AdvHunting Email 自社ドメイン外の宛先へのメール件数集計	EmailEvents の自社ドメイン外の宛先へのメール件数を集計・レポートします。抽出条件の「@infoscience¥.co¥.jp」は自ドメインに変更してください。
Microsoft 365 AdvHunting Email 自社ドメイン外の差出人（エンベロープFrom）からのメール件数集計	EmailEvents の自社ドメイン外の差出人からのメール件数を集計・レポートします。抽出条件の「@infoscience¥.co¥.jp」は自ドメインに変更してください。
Microsoft 365 AdvHunting Email 自社ドメイン外の差出人（ヘッダーFrom）からのメール件数集計	EmailEvents の自社ドメイン外の差出人からのメール件数を集計・レポートします。抽出条件の「@infoscience¥.co¥.jp」は自ドメインに変更してください。
Microsoft 365 AdvHunting Email 認証結果集計	EmailEvents の認証結果を集計・レポートします。
Microsoft 365 AdvHunting Email 送信者別／URL件数集計（日別）	EmailEvents の日別のメール内URL件数を集計・レポートします。
Microsoft 365 AdvHunting Email 送信者別／URL件数集計（時間別）	EmailEvents の時間別のメール内URL件数を集計・レポートします。
Microsoft 365 AdvHunting Email 送信者別／添付ファイル件数集計（日別）	EmailEvents の日別の添付ファイル件数を集計・レポートします。
Microsoft 365 AdvHunting Email 送信者別／添付ファイル件数集計（時間別）	EmailEvents の時間別の添付ファイル件数を集計・レポートします。
Microsoft 365 AdvHunting Email 送信者別／添付ファイル名件数集計（日別）	EmailAttachmentInfo の日別の添付ファイル件数を集計・レポートします。
Microsoft 365 AdvHunting Email 送信者別／添付ファイル名件数集計（時間別）	EmailAttachmentInfo の時間別の添付ファイル件数を集計・レポートします。

検索例 1

Microsoft 365のドキュメントを参考にテンプレート条件を作成しています。

各テンプレート条件を用いて、集めたログを容易に可視化・分析することができます。

< 監査ログ >



検索条件名: Microsoft 365 全ログ検索

概要: Microsoft 365 の全てのアクティビティを検索します。

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 ≥ ≫

タイムスタンプ	ユーザーID	アプリケーション	アクション	クライアントIP	レコード種類	レコード種類(マスタ連携)
2022-12-27 15:05:12	kato@infoscience.com	Microsoft 365 Microsoft Teams	コネクタの追加		25	MicrosoftTeams
2022-12-27 15:04:59	kato@infoscience.com	Microsoft 365 Microsoft Teams	インストールされたアプリ		25	MicrosoftTeams
2022-12-27 15:01:47	kato@infoscience.com	Microsoft 365 Microsoft Teams	Teams へのユーザーのサインイン	100.10.0.1	25	MicrosoftTeams
2022-12-27 15:00:03	saito@infoscience.com	Microsoft 365 Azure Active Directory	ログイン失敗	100.10.0.1	15	AzureActiveDirectoryStsLogon
2022-12-27 14:29:27	kato@infoscience.com	Microsoft 365 Azure Active Directory	ログイン成功	100.10.0.1	15	AzureActiveDirectoryStsLogon
2022-12-27 14:29:20	kato@infoscience.com	Microsoft 365 SharePoint	ListViewed	100.10.0.1	36	SharePointListOperation
2022-12-27 14:29:20	kato@infoscience.com	Microsoft 365 SharePoint	ファイルアクセス	100.10.0.1	6	SharePointFileOperation
2022-12-27 14:29:17	kato@infoscience.com	Microsoft 365 SharePoint	SharePoint グループへのユーザーまたはグループの追加	100.10.15.183	14	SharePointSharingOperation
2022-12-27 14:29:15	kato@infoscience.com	Microsoft 365 Microsoft Teams	メンバーの追加		25	MicrosoftTeams
2022-12-27 14:29:04	app@sharepoint	Microsoft 365 SharePoint	フォルダーの作成	100.10.15.192	6	SharePointFileOperation
2022-12-27 14:29:04	app@sharepoint	Microsoft 365 SharePoint	フォルダーの変更	100.10.15.192	6	SharePointFileOperation
2022-12-27 14:29:03	kato@infoscience.com	Microsoft 365 SharePoint	SharePoint グループへのユーザーまたはグループの追加	100.10.15.192	14	SharePointSharingOperation
2022-12-27 14:29:03	kato@infoscience.com	Microsoft 365 SharePoint	SharePoint グループへのユーザーまたはグループの追加	100.10.15.192	14	SharePointSharingOperation
2022-12-27 14:29:01	kato@infoscience.com	Microsoft 365 SharePoint	共有ポリシーの変更	100.10.15.192	4	SharePoint
2022-12-27 14:29:00	kato@infoscience.com	Microsoft 365 SharePoint	サイト コレクション管理者の追加	100.10.15.192	14	SharePointSharingOperation
2022-12-27 14:29:00	kato@infoscience.com	Microsoft 365 SharePoint	サイト コレクション管理者の削除	100.10.15.192	14	SharePointSharingOperation
2022-12-27 14:29:00	kato@infoscience.com	Microsoft 365 SharePoint	サイト コレクションの作成	100.10.15.192	4	SharePoint
2022-12-27 14:29:00	kato@infoscience.com	Microsoft 365 SharePoint	グループの作成	100.10.15.192	4	SharePoint
2022-12-27 14:29:00	kato@infoscience.com	Microsoft 365 SharePoint	グループの作成	100.10.15.192	4	SharePoint
2022-12-27 14:29:00	kato@infoscience.com	Microsoft 365 SharePoint	グループの作成	100.10.15.192	4	SharePoint
2022-12-27 14:29:00	kato@infoscience.com	Microsoft 365 SharePoint	ファイル、フォルダー、またはサイトの共有	100.10.15.192	14	SharePointSharingOperation

監査ログの各項目の詳細は、マイクロソフト社のドキュメント
(https://docs.microsoft.com/ja-jp/microsoft-365/compliance/detailed-properties-in-the-office-365-audit-log?view=o365-worldwide) でご確認ください。

検索例 2

< メッセージ追跡 (MessageTrace) >

検索条件名: Microsoft 365 メッセージ追跡

概要:

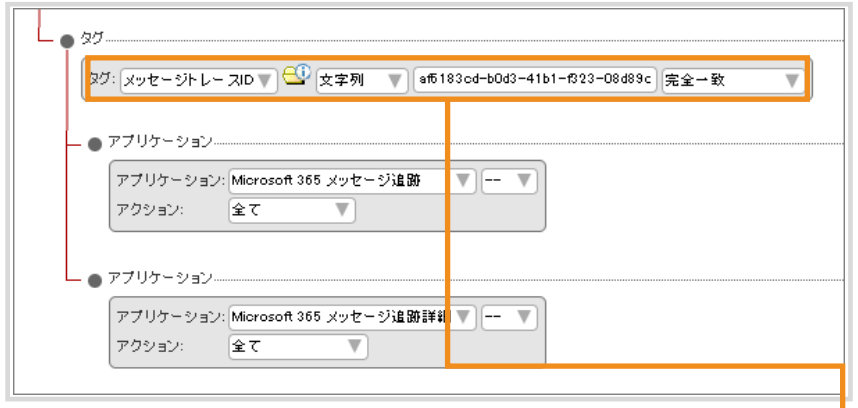
検索条件 | 検索結果 | カラムセットアサイン

ログ | カラム　1-19件目表示 (全19件)

タイムスタンプ	差出人アドレス	宛先アドレス	件名	アクション	送信元IP	送信先IP	サイズ
2022-12-10 11:48:48	ito@infoscience.com	kitagawa2@infoscience.co.jp	○○案件:打ち合わせの日程調整	Delivered	100.10.0.1	100.10.133.132	18200
2022-12-10 10:48:17	ito@infoscience.com	sato@abc.com	○○案件:打ち合わせの日程調整	Delivered	100.10.0.1	100.10.133.132	2922015
2022-12-10 10:19:16	ito@infoscience.com	sato@abc.com	○○案件:打ち合わせの日程調整	Delivered	100.10.0.1	100.10.225.24	17697
2022-12-10 10:14:19	MicrosoftExchange329exxx@infoscience.com	ito@infoscience.com	配信不能: ○○案件:打ち合わせの日程調整	Delivered	null	null	40152
2022-12-10 10:14:18	ito@infoscience.com	kitagawa@infoscience2.co.jp	○○案件:打ち合わせの日程調整	Failed	100.10.0.1	null	13477
2022-12-10 10:07:24	MicrosoftExchange329exxx@infoscience.com	ito@infoscience.com	配信不能: ○○案件:打ち合わせの日程調整	Delivered	null	null	59885
2022-12-10 10:07:23	ito@infoscience.com	kato@infoscience.com	○○案件:打ち合わせの日程調整	Failed	100.10.0.1	null	13315
2022-12-09 11:14:30	MicrosoftExchange329exxx@infoscience.com	kato@infoscience.com	配信不能: 情報共有ミーティング (2022年12月)	Resolved	null	null	90052
2022-12-09 11:14:30	MicrosoftExchange329exxx@infoscience.com	kato-11@gmail.com	配信不能: 情報共有ミーティング (2022年12月)	Failed	null	null	90052
2022-12-09 11:14:30	sample@microsoft.com	kikuchi@infoscience.com	情報共有ミーティング (2022年12月)	Delivered	100.10.131.137	null	36470
2022-12-09 11:14:30	sample@microsoft.com	ito@infoscience.com	情報共有ミーティング (2022年12月)	Delivered	100.10.131.137	null	36470
2022-12-09 11:14:29	sample@microsoft.com	kato@infoscience.com	情報共有ミーティング (2022年12月)	Resolved	100.10.131.137	null	51910
2022-12-09 11:14:29	sample@microsoft.com	kato-11@gmail.com	情報共有ミーティング (2022年12月)	Failed	100.10.131.137	null	51910
2022-12-09 11:11:01	noreply@email.teams.microsoft.com	ito@infoscience.com	Microsoft Teams の「Microsoft」にゲストとして追加されています	Delivered	100.10.75.88	null	48274
2022-12-09 11:10:59	noreply@email.teams.microsoft.com	kikuchi@infoscience.com	Microsoft Teams の「Microsoft」にゲストとして追加されています	Delivered	100.10.243.74	null	48446
2022-12-09 11:10:57	MicrosoftExchange329exxx@infoscience.com	kato@infoscience.com	Undeliverable: Microsoft Teams のチームに追加されています	Resolved	null	null	102117
2022-12-09 11:10:57	MicrosoftExchange329exxx@infoscience.com	kato-11@gmail.com	Undeliverable: Microsoft Teams のチームに追加されています	Failed	null	null	102117
2022-12-09 11:10:55	noreply@email.teams.microsoft.com	kato@infoscience.com	Microsoft Teams のチームに追加されています	Resolved	100.10.92.44	null	71662
2022-12-09 11:10:55	noreply@email.teams.microsoft.com	kato-11@gmail.com	Microsoft Teams のチームに追加されています	Failed	100.10.92.44	null	71662

検索例 3

< メッセージ追跡・メッセージ追跡詳細 (MessageTrace, MessageTraceDetail) >



メッセージトレースIDを用いて、
横串検索をすることができます。

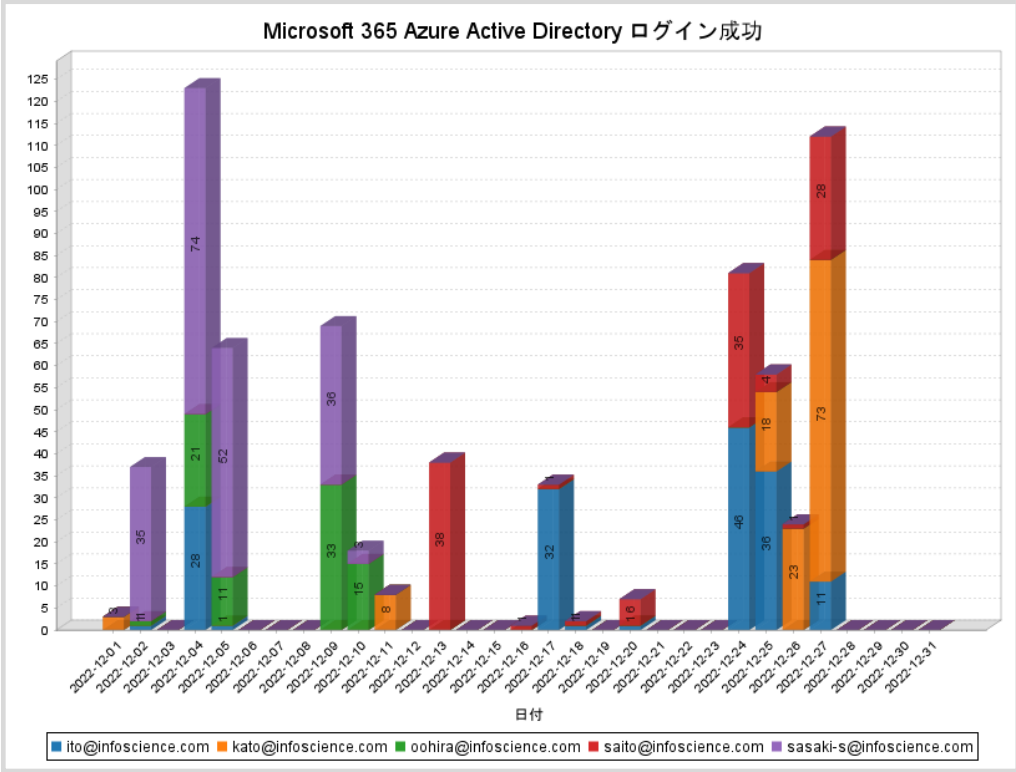
< メッセージ追跡 (MessageTrace) 取得項目 >
Organization, MessageId, MessageTraceId, Received, SenderAddress, RecipientAddress, Subject, Status, ToIP, FromIP, Size

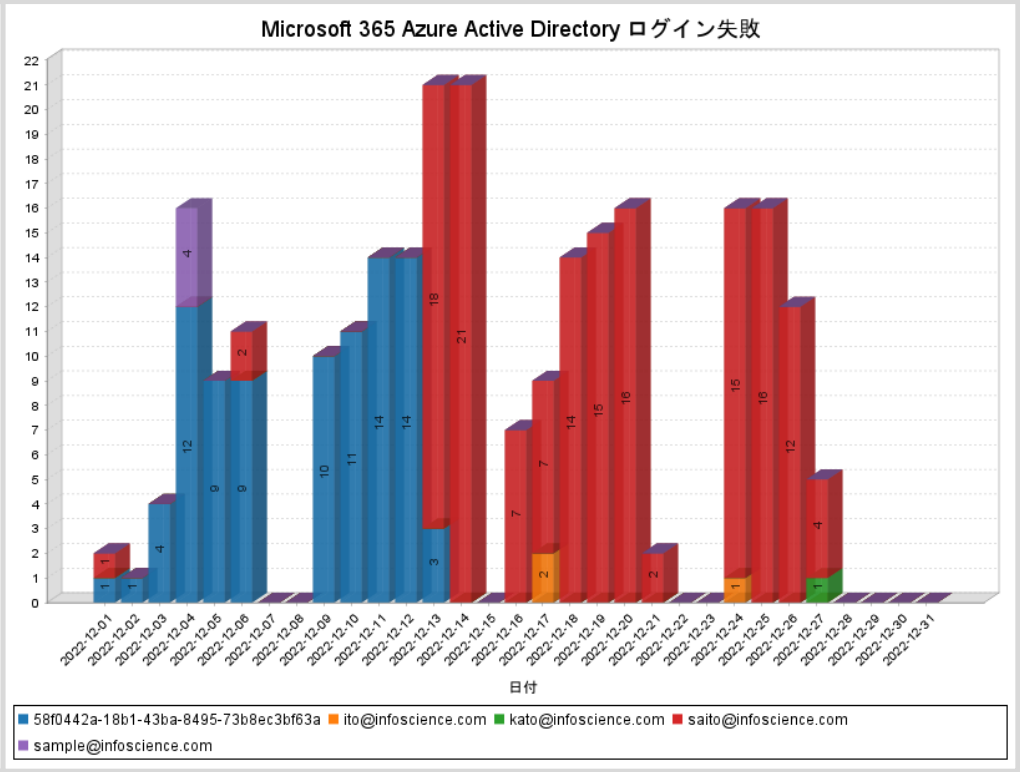
< メッセージ追跡詳細 (MessageTraceDetail) 取得項目 >
Organization, MessageId, MessageTraceId, Date, Event, Action, Detail, Data

詳細は、マイクロソフト社のドキュメント (https://docs.microsoft.com/ja-jp/exchange/monitoring/trace-an-email-message/message-trace-modern-eac) で確認ください。

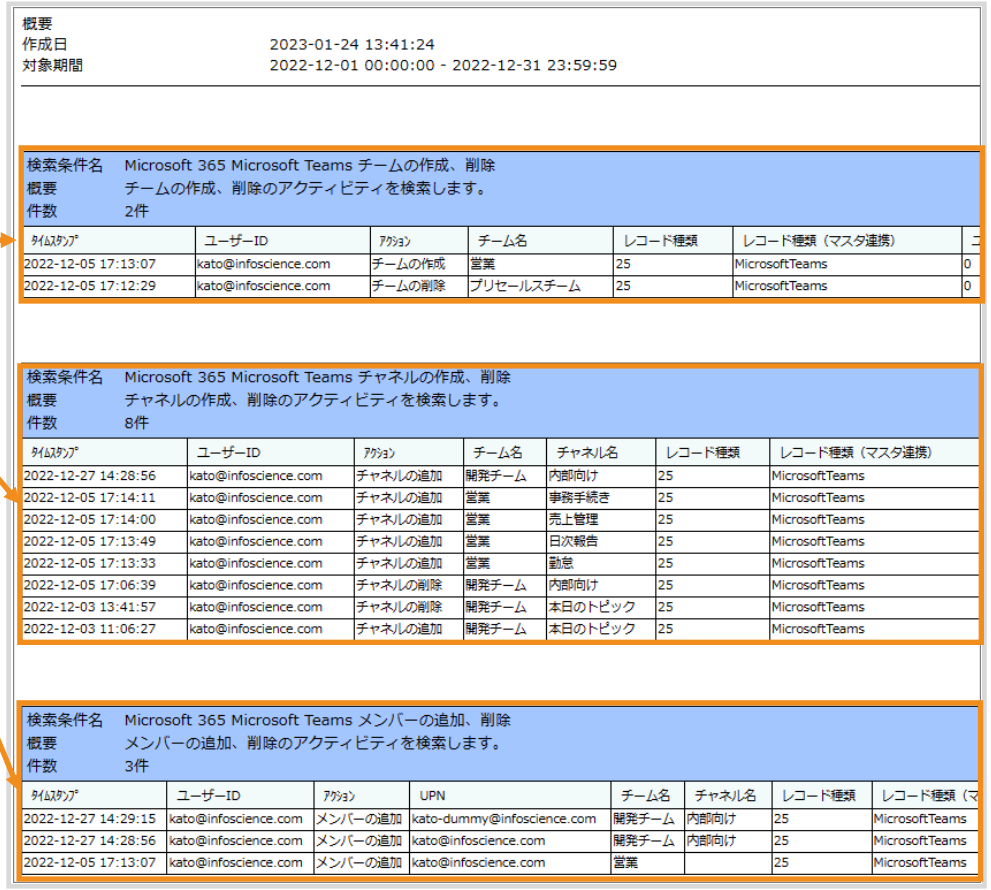
レポート例 1

Microsoft 365のログイン履歴で、
Microsoft 365の利用状況や不審なアクセスがないことを確認できます。





レポート例 2



概要
作成日 2023-01-24 13:41:24
対象期間 2022-12-01 00:00:00 - 2022-12-31 23:59:59

検索条件名 Microsoft 365 Microsoft Teams チームの作成、削除
概要 チームの作成、削除のアクティビティを検索します。
件数 2件

ﾀｲﾑｽﾀﾝﾌﾟ	ユーザーID	ｱｸｼｮﾝ	チーム名	レコード種類	レコード種類（マスタ連携）	ニ
2022-12-05 17:13:07	kato@infoscience.com	チームの作成	営業	25	MicrosoftTeams	0
2022-12-05 17:12:29	kato@infoscience.com	チームの削除	プリセールスチーム	25	MicrosoftTeams	0

検索条件名 Microsoft 365 Microsoft Teams チャネルの作成、削除
概要 チャネルの作成、削除のアクティビティを検索します。
件数 8件

ﾀｲﾑｽﾀﾝﾌﾟ	ユーザーID	ｱｸｼｮﾝ	チーム名	チャネル名	レコード種類	レコード種類（マスタ連携）
2022-12-27 14:28:56	kato@infoscience.com	チャネルの追加	開発チーム	内部向け	25	MicrosoftTeams
2022-12-05 17:14:11	kato@infoscience.com	チャネルの追加	営業	事務手続き	25	MicrosoftTeams
2022-12-05 17:14:00	kato@infoscience.com	チャネルの追加	営業	売上管理	25	MicrosoftTeams
2022-12-05 17:13:49	kato@infoscience.com	チャネルの追加	営業	日次報告	25	MicrosoftTeams
2022-12-05 17:13:33	kato@infoscience.com	チャネルの追加	営業	勤怠	25	MicrosoftTeams
2022-12-05 17:06:39	kato@infoscience.com	チャネルの削除	開発チーム	内部向け	25	MicrosoftTeams
2022-12-03 13:41:57	kato@infoscience.com	チャネルの削除	開発チーム	本日のトピック	25	MicrosoftTeams
2022-12-03 11:06:27	kato@infoscience.com	チャネルの追加	開発チーム	本日のトピック	25	MicrosoftTeams

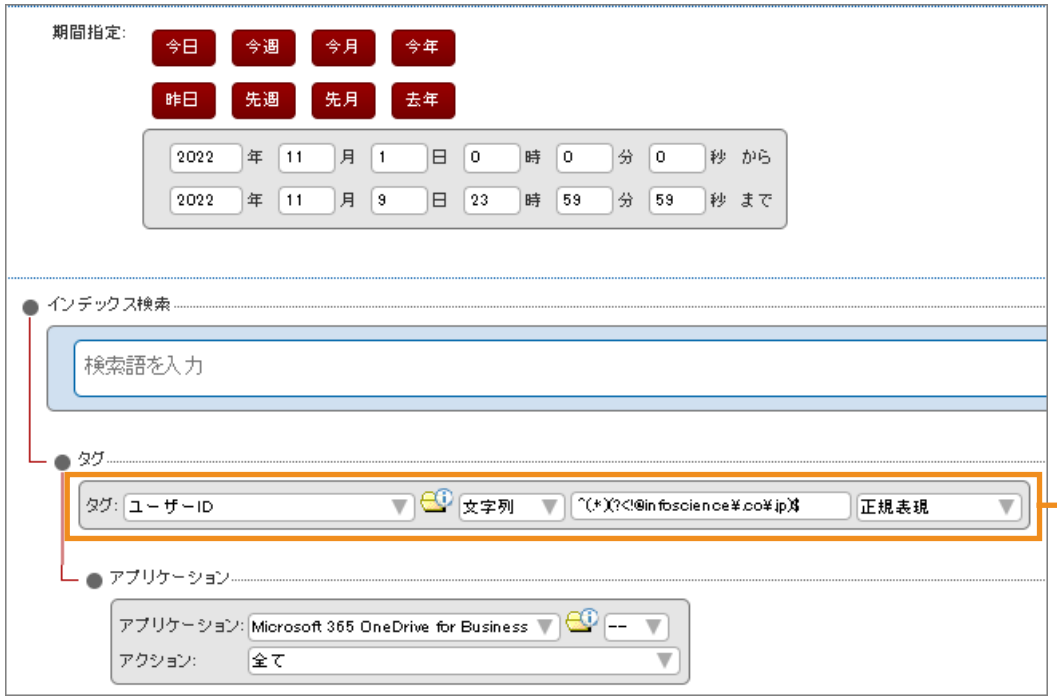
検索条件名 Microsoft 365 Microsoft Teams メンバーの追加、削除
概要 メンバーの追加、削除のアクティビティを検索します。
件数 3件

ﾀｲﾑｽﾀﾝﾌﾟ	ユーザーID	ｱｸｼｮﾝ	UPN	チーム名	チャネル名	レコード種類	レコード種類（マ
2022-12-27 14:29:15	kato@infoscience.com	メンバーの追加	kato-dummy@infoscience.com	開発チーム	内部向け	25	MicrosoftTeams
2022-12-27 14:28:56	kato@infoscience.com	メンバーの追加	kato@infoscience.com	開発チーム	内部向け	25	MicrosoftTeams
2022-12-05 17:13:07	kato@infoscience.com	メンバーの追加	kato@infoscience.com	営業		25	MicrosoftTeams

監査したい条件を複数設定し、

定期的にレポート出力することができます。

レポート例３



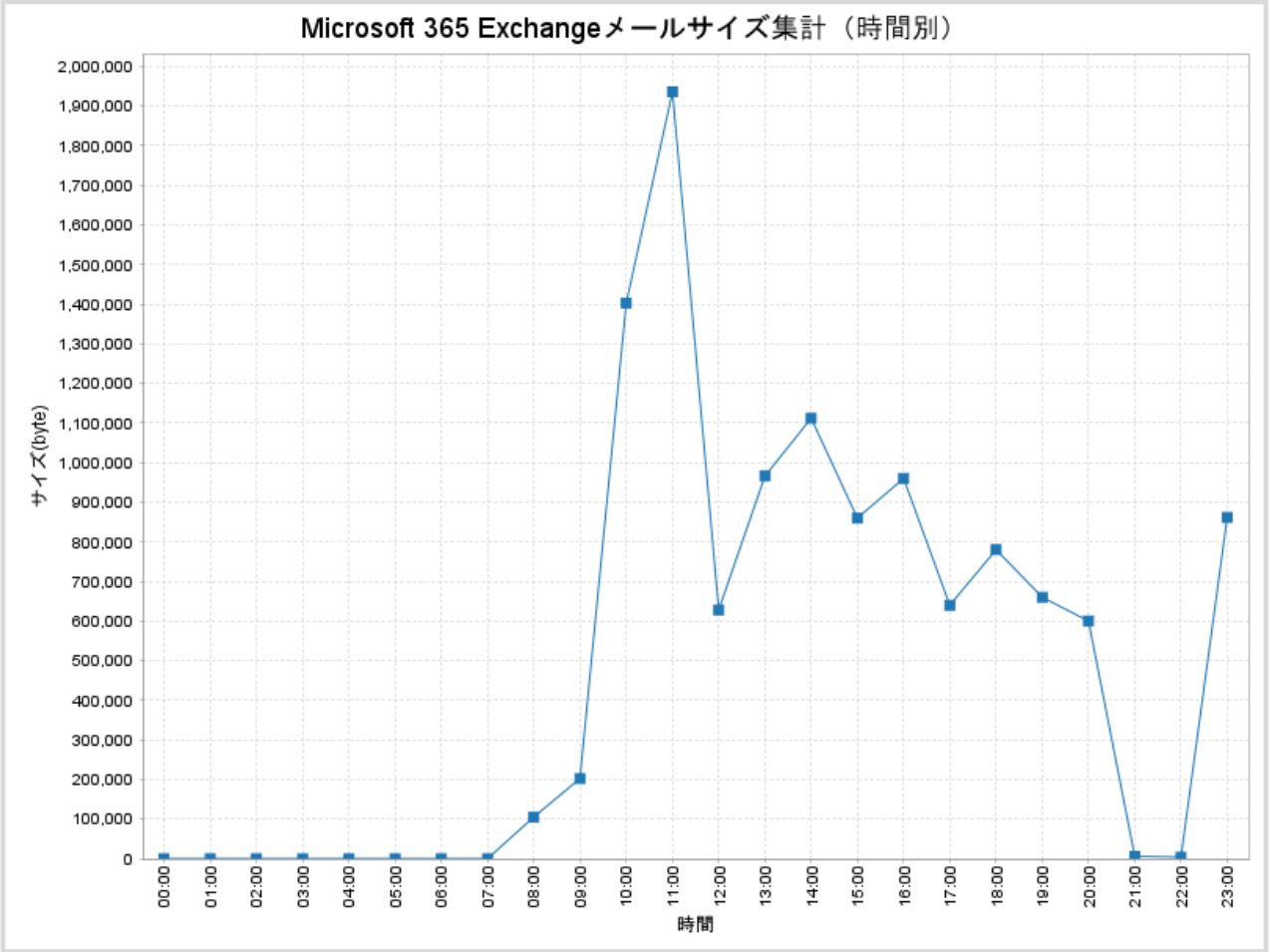
日付	ファイル名	ユーザー	件数
2022-11-02	20211201_○○案件打ち合わせ議事録.doc	hayashi@bbb.com	1
		kimura@aaa.com	1
		maeda@bbb.com	2
		miyata@bbb.com	1
		sakata@bbb.com	1
		suzuki@aaa.com	2
	□△Q A表.doc	sakata@bbb.com	1
	△△Q A表.doc	sakata@bbb.com	1
	○△Q A表.doc	sakata@bbb.com	1
2022-11-06	社内規定.doc	to@infoscience.com	116
2022-11-09	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
		kiyota@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
総合計			149

組織外のユーザーからアクセスされた
フォルダ・ファイルの一覧を確認できます。

レポート例 4

時間別のメールサイズを可視化、表やグラフ（棒グラフ、折れ線グラフ等）で出力できます。

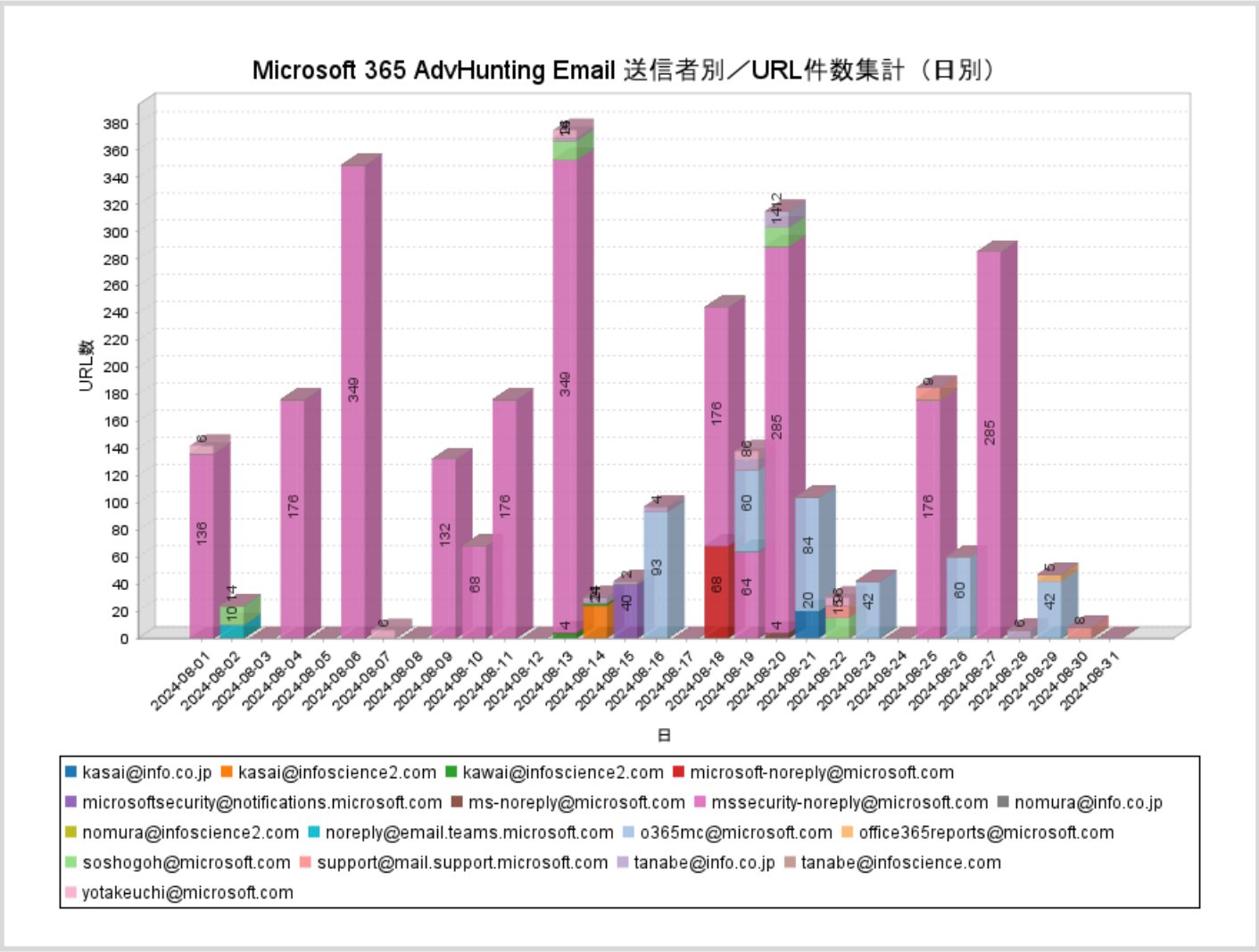
時間	サイズ(byte) 合計
2022-11-21 00	0
2022-11-21 01	0
2022-11-21 02	0
2022-11-21 03	0
2022-11-21 04	0
2022-11-21 05	0
2022-11-21 06	0
2022-11-21 07	0
2022-11-21 08	105098
2022-11-21 09	202466
2022-11-21 10	1402466
2022-11-21 11	1936284
2022-11-21 12	628064
2022-11-21 13	965976
2022-11-21 14	1112114
2022-11-21 15	860000
2022-11-21 16	960000
2022-11-21 17	640000
2022-11-21 18	780000
2022-11-21 19	660000
2022-11-21 20	600000
2022-11-21 21	6000
2022-11-21 22	4000
2022-11-21 23	861668



レポート例 5

日	脅威種類	脅威名	検出方法	信頼レベル	メールアクション	メールアクションポリシー	件数
2024-09-02	Malware	O97M/Casdet!rfn	{"Malware":["Antimalware engine"]}		Send to quarantine	Anti-malware	1
	Phish		{"Phish":["URL detonation reputation"]}	{"Phish":"High"}	Send to quarantine	Others	3
	Phish, Spam		{"Phish":["URL detonation reputation"],"Spam":["General filter"]}	{"Phish":"High","Spam":"Normal"}	Send to quarantine	Others	3
	Spam		{"Spam":["General filter"]}	{"Spam":"Normal"}	Move to junk mail folder	Antispam	2
2024-09-10	Malware	MSIL/AgentTesla.RDCB!MTB	{"Malware":["Antimalware engine"]}		Others	Others	1
					Send to quarantine	Anti-malware	1
		O97M/CVE-2017-11882.RVCK!MTB	{"Malware":["Antimalware engine"]}		Send to quarantine	Anti-malware	1
		O97M/Casdet!rfn	{"Malware":["Antimalware engine"]}		Send to quarantine	Anti-malware	1
		Win32/AgentTesla.SKAV	{"Malware":["Antimalware engine"]}		Others	Others	1
					Send to quarantine	Anti-malware	1
		Win32/Leonem	{"Malware":["Antimalware engine"]}		Others	Others	2
					Send to quarantine	Anti-malware	2
		Win32/SuspPEInArcEmail.A	{"Malware":["Antimalware engine"]}		Others	Others	1
					Send to quarantine	Anti-malware	1
		Win32/Vigorf.A	{"Malware":["Antimalware engine"]}		Others	Others	1
					Send to quarantine	Anti-malware	1
	Malware, Phish	HTML/Msphish.GB!MTB	{"Malware":["Antimalware engine"],"Phish":["URL detonation reputation"]}	{"Phish":"High"}	Send to quarantine	Anti-malware	1
	Malware, Spam		{"Malware":["URL detonation reputation"],"Spam":["Mixed analysis detection"]}	{"Spam":"Normal"}	Send to quarantine	Anti-malware	1
	Phish	Phish_HTML_MacLer_A	{"Phish":["File detonation"]}	{"Phish":"High"}	Send to quarantine	Others	2
	Phish, Spam	Phish_HTML_DynamicLogo_B	{"Phish":["File detonation"],"Spam":["Mixed analysis detection"]}	{"Phish":"High","Spam":"Normal"}	Send to quarantine	Others	1
2024-09-11	Malware	O97M/CVE-2017-11882.RVCK!MTB	{"Malware":["Antimalware engine"]}		Send to quarantine	Anti-malware	1
		PowerShell/GuLoader.RVA!MTB	{"Malware":["Antimalware engine"]}		Others	Others	1
					Send to quarantine	Anti-malware	1
		Win32/Babatex.B	{"Malware":["Antimalware engine"]}		Others	Others	1
					Send to quarantine	Anti-malware	1
	Phish		{"Phish":["URL detonation reputation"]}	{"Phish":"High"}	Send to quarantine	Others	2
	Spam		{"Spam":["URL malicious reputation"]}	{"Spam":"High"}	Send to quarantine	Antispam high-confidence spam	1
2024-09-12	Malware	O97M/Casdet!rfn	{"Malware":["Antimalware engine"]}		Send to quarantine	Anti-malware	1
		Win32/Leonem	{"Malware":["Antimalware engine"]}		Send to quarantine	Anti-malware	1
	Phish		{"Phish":["URL detonation reputation"]}	{"Phish":"High"}	Send to quarantine	Others	1
2024-09-13	Malware	O97M/CVE-2017-11882.RVCK!MTB	{"Malware":["Antimalware engine"]}		Send to quarantine	Anti-malware	2
		Script/Malgent!MSR	{"Malware":["Antimalware engine"]}		Others	Others	1
					Send to quarantine	Anti-malware	1
		Win32/Babatex.B	{"Malware":["Antimalware engine"]}		Others	Others	1
					Send to quarantine	Anti-malware	1
	Phish		{"Phish":["URL detonation reputation"]}	{"Phish":"High"}	Send to quarantine	Others	1
総合計							46

レポート例 6



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