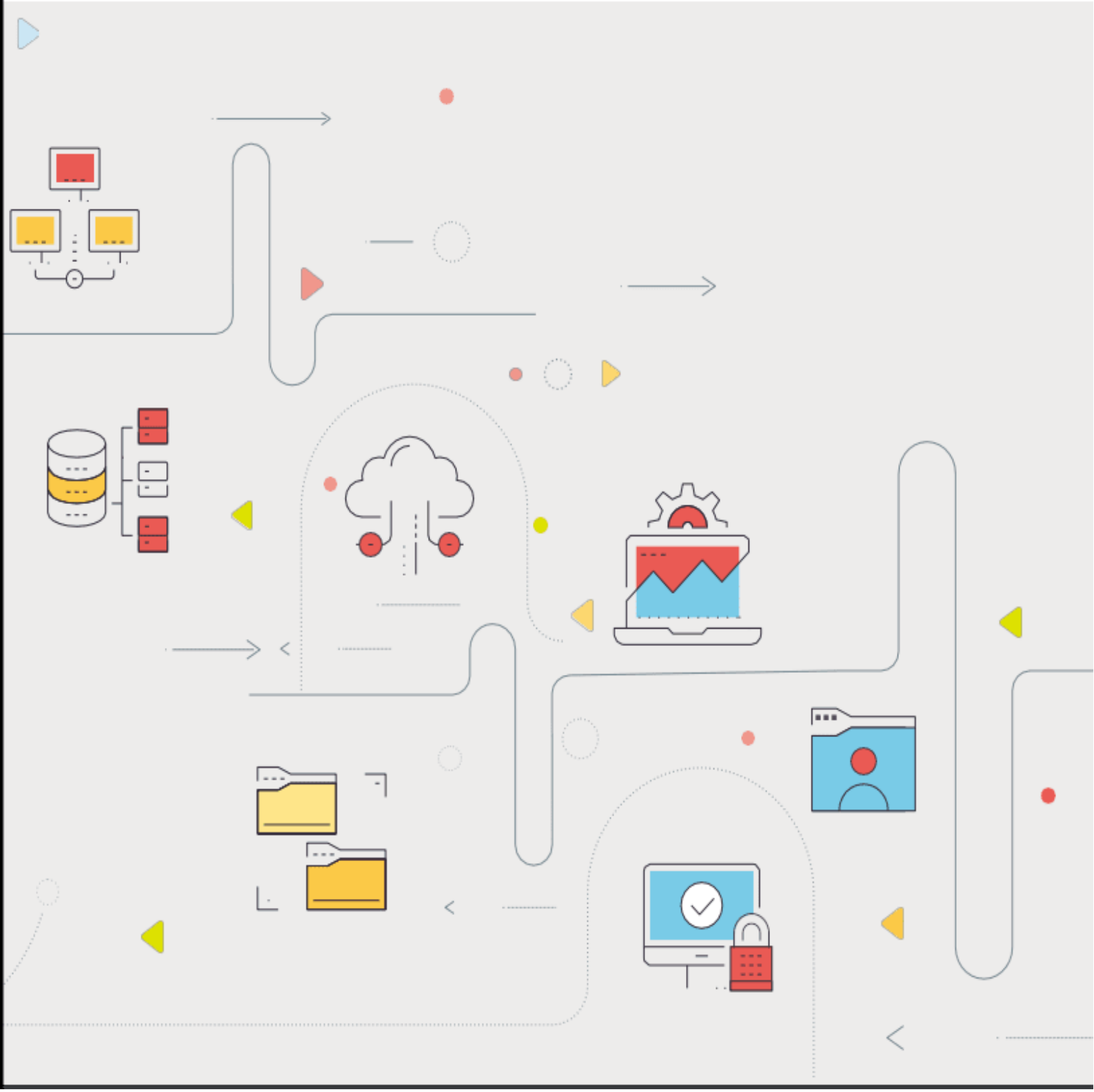


ManageEngine

Log360 Cloud

スタートアップガイド

2024年版

目次

目次 2
はじめに 3
本ガイドの内容 3
著作権 3
注意事項 3
Log360 Cloudの概要 3
プランの概要 3
システム要件 4
ハードウェア要件 4
OS要件 4
ブラウザー要件 4
ポート要件 5
必要な許可設定 5
URLホワイトリスト 7
アカウントの作成およびLog360 Cloudへのアクセス 8
Zohoアカウントを作成済みの場合 8
Zohoアカウントを未作成の場合 8
Log360 Cloudへアクセスする手順 9
Log360 Cloudアカウントを削除する手順 9
ログ収集の開始 10
Windowsログ 10
Syslog 12
クラウドログ 13
その他の設定 15
ログ収集フィルター 15
主要機能の説明 16
レポート 16
検索 17
アラート 18
クラウド監査 19
トラブルシューティング 20
製品ユーザー（技術者） 15
ログ保存期間および検索期間 15
お問い合わせ 21
会社情報 21

はじめに

本ガイドの内容

本ガイドは、ManageEngine Log360 Cloud（以下、Log360 Cloud）を初めて利用する方を対象に、基本的な利用方法および機能説明を記載しています。

著作権

注意事項

本ガイドの内容は、改良のため、予告なく変更することがあります。
ゾーホージャパン株式会社は本ガイドに関しての一切の責任を負いかねます。当社はこのガイドを使用することにより引き起こされた偶発的もしくは間接的な損害についても責任を負いかねます。

Log360 Cloudの概要

Log360 Cloudは、WindowsやSyslog、およびAWSやMicrosoft 365のログを収集・保管できるログ管理クラウドツールです。

プランの概要

Log360 Cloudを利用開始後、Professional（最上位）プランを30日間、無料でご利用いただけます（ATA add-on脅威検知機能は利用できません）。

プランの詳細はこちらをご参照ください。
プランや購入の相談はこちらよりお問い合わせください。

システム要件

Windowsログおよびsyslogを収集するためには、Log360 Cloudエージェント（以下、エージェント）をWindowsデバイスにインストールする必要があります。以下、エージェントをインストールするデバイスの要件を記載します。

ハードウェア要件

- CPU：2.80GHz 64-bit（x64）Xeon® LV processor以上
- RAM：2GB

OS要件

- Windows Server 2022
- Windows Server 2019
- Windows Server 2016
- Windows 11
- Windows 10

ブラウザー要件

- Google Chrome
- Microsoft Edge（Chromium版）
- Mozilla Firefox

*Log360 CloudのUI画面へアクセスする際に使用するブラウザーの要件です。
*解像度は1280x720以上が必要です。
*各ブラウザーの最新バージョンの利用を推奨します。

ポート要件

Log360 Cloudサーバーとの通信に使用するポート

ポート番号	ポート利用内容	通信方向
8080/443 （TCP）	Cloudサーバー通信	エージェント → Cloudサーバー

管理（ログ収集）対象デバイスとの通信に使用するポート

*「Windows/Syslogデバイス」はログ収集対象デバイスを指します。

ポート番号	ポート利用内容	通信方向および詳細
513/514 （UDP）	Syslog受信	Syslogデバイス → エージェント
514 （TCP）	Syslog受信	Syslogデバイス → エージェント
135/445/139 （TCP）	WMI/DCOM/RPC	エージェント → Windowsデバイス ログの収集に使用
49152-65534 （TCP）	WMI/DCOM/RPC	Windowsデバイス → エージェント ログの収集に使用
389	LDAP	ドメインディスカバリーに使用
135/445/139 1024-65535	SMB RPC	ワークグループディスカバリーに使用
139 135/137/138	SMB RPC	イベントソースディスカバリーに使用

必要な許可設定

エージェント関連

アクション	必要な設定
エージェントインストール	● エージェントインストール　Program Files (x86)フォルダーに対してread/write/modify権限をユーザーに付与 ● エージェント自動アップグレード C:\Windows\Tempに対して read/write/modify権限をユーザーに付与
エージェント管理	● レジストリキー「SOFTWARE\Wow6432Node

	\ZOHO Corp\Log360Cloud\ （または） SOFTWARE\ZOHO Corp \Log360Cloud\」に対して access/read/write権限をユーザーに付与

ログ収集

アクション	必要な設定
WMI Log Collection	● ユーザーが以下のグループに所属 ・Event Log Readers ・Distributed COM Users ● ユーザーに以下の許可を付与 ・Enable Account ・Remote Enable ・Read Security ・Execute Methods
Syslog収集	● Syslog受信ポートをファイアウォールで開放
Auto Log Forwarding	● rsyslogまたはsyslogサービスを再起動する権限をユーザーに付与 ● rwパーミッションをrsyslog.confまたはsyslog.confファイルに設定

ディスカバリー

アクション	必要な設定
イベントソースディスカバリー	● レジストリキー「Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipe Servers\winreg」に対してread権限をユーザーに付与 ● Remote registryサービスの起動 ● C:\Windows\System32\winevt\Logsにファイルが存在 ● 管理対象デバイスにて「C$」を有効化
ドメイン	● Active Directoryオブジェクトに対してread権限を

ディスカバリー	ユーザーに付与 ● ADS_SECUREAUTHENTICATIONモードにおけるLDAPクエリの実行権限をユーザーに付与
ワークグループディスカバリー	● ADS_SECUREAUTHENTICATIONモードにおけるWinNTクエリの実行権限をユーザーに付与

URLホワイトリスト

エージェントをインストールするデバイスは、以下のURLにアクセスできる必要があります。

- log360cloud.manageengine.jp
- upload.zoho.jp
- *dms.zoho.jp
- staticdownloads-log360cloud.zohodl.com

JP（日本）以外のデータセンターをご利用の場合はこちらのページをご参照ください。

アカウントの作成およびLog360 Cloudへのアクセス

Log360 Cloudを利用するためには、Zohoアカウントが必要です。

Zohoアカウントを作成済みの場合

サインアップページにアクセス後、「アカウントをお持ちの方はこちら **サインインする**」より作成済みのZohoアカウントを使用してサインインすることで、Log360 Cloudにアクセスできます。

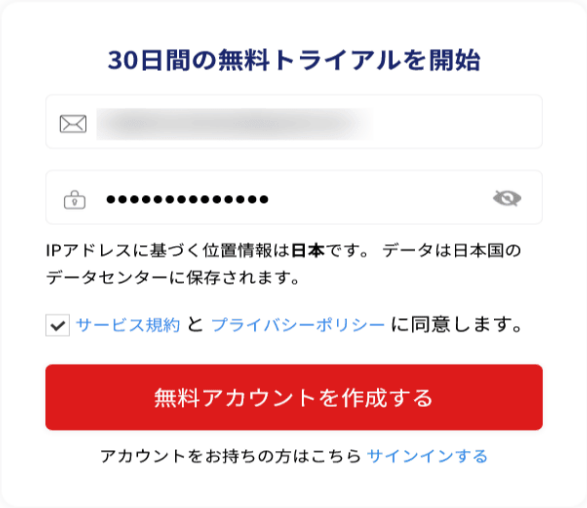
Zohoアカウントを未作成の場合

Zohoのクラウド製品に初めてアクセスする場合は、以下の手順を実施してください。

留意事項

Log360 Cloudが収集するデータを保管するデータセンターのリージョン（日本、米国、EU、オーストラリア、インド）は、アカウント作成時のユーザーの所在地に基づいて自動的に選択されます。

1. サインアップページにアクセス
2. 作成するZohoアカウントに使用するメールアドレスを入力（本アカウントがLog360 Cloudの管理者となります）
3. パスワードを設定
4. サービス規約とプライバシーポリシーを確認後、各チェックボックスにチェックを入れ、「無料アカウントを作成する」をクリック



アカウントが作成され、自動的にLog360 CloudのUI画面が表示されます。

補足事項

サインアップ時にはメールアドレスの認証は求められません。サインアウト後、次回のサインイン時にメールアドレスの認証プロセスの実施を求められます。

Log360 Cloudへアクセスする手順

1. ブラウザーで「https://log360cloud.manageengine.jp/」にアクセス
2. Zohoアカウントでサインイン

Log360 Cloudアカウントを削除する手順

1. Log360 Cloudにサインイン
2. 画面右上の人型アイコン→「マイアカウント」をクリック
3. ページ下部の「Log360 Cloudアカウントを終了」をクリック
4. 解約理由およびキャプチャを入力
5. 「アカウントの解約」をクリック

ログ収集の開始

Windowsログ

Windowsログを収集するためには、Log360 Cloudのエージェント（以下、エージェント）を、システム要件を満たしたWindowsデバイスにインストールする必要があります。手順は以下のとおりです。

エージェントのインストール手順

1. Log360 Cloudに初めてアクセスした後に表示されるページの「エージェントを構成する」をクリック（または、「設定」タブ→「構成」→「ログソースの構成」→「エージェントを管理」→「エージェントをインストール」をクリック）
2. 遷移後のページ内の手順を実施

    a. エージェントのインストーラー（.msi）を取得
    b. エージェントをインストールするWindowsデバイスにて、インストーラーを実行
    c. ウィザードにしたがってインストール（入力するアクセスキーは、Log360 CloudのUI画面より取得）

    エージェントのインストール完了後、エージェントはインストールしたWindowsデバイス自身のWindowsログをLog360 Cloudに転送します。

留意事項

- エージェントは「C:\Program Files (x86)\Log360Cloud_Agent」にインストールされます。
- エージェントのインストール完了後、Windowsサービス「ManageEngine Log360Cloud Agent」が自動的にインストールされ、起動します。本サービスは常に起動させてください。
- エージェントをインストールしたWindowsデバイス以外のWindowsデバイスのWindowsログを収集する場合は、こちらのページを参照し、ログを収集したいWindowsデバイスを既存のエージェントに追加してください。
- エージェントのアンインストール手順はこちらをご参照ください。

エージェントのアンインストール手順

1. エージェントをインストールしたWindowsデバイスにて「コントロールパネル」を起動
2. 「プログラムのアンインストール」をクリック
3. 「ManageEngine Log360Cloud Agent」を右クリック→「アンインストール」をクリック
4. ウィザードにしたがって、アンインストールを実施
5. アンインストール完了後、エージェントのインストールフォルダー「Log360Cloud_Agent」を削除（デフォルトパスは「C:\Program Files (x86)\Log360Cloud_Agent」）

Syslog

Syslogを収集するためには、エージェントをインストールしたWindowsデバイスへSyslogを転送するよう、Syslogデバイスで設定する必要があります（エージェントのインストール方法はこちらを参照）。エージェントは受信したSyslogをLog360 Cloudに転送します。

SyslogデバイスでSyslogを転送する設定は、Syslogデバイスによって異なりますので、デバイスのベンダーにお問い合わせください。以下、設定例を記載します。

Syslog転送設定例

1. rootユーザーとしてログイン
2. /etc/rsyslog.confをvi等で編集
3. 以下のパラメーターを追加

   ***.* @[エージェントのホスト名またはIPアドレス]:[エージェントがsyslog受信に使用するポート番号（デフォルトでは513または514）]**

   パラメーター例
   ***.* @192.168.0.1:513**

4. 設定を保存
5. rsyslogを再起動

クラウドログ

Log360 Cloudは「Amazon Web Services（以下、AWS）」および「Microsoft 365（以下、M365）」のログを収集できます。

Amazon Web Services（AWS）

収集できるログの種類

- AWS CloudTrail
- AWS S3 Access Logs
- AWS ELB Access Logs

設定手順

1. こちらのページを参照し、ログ収集に必要な権限を持つIAMユーザーをAWSで作成
2. Log360 Cloudに初めてアクセスした後に表示されるページの「クラウドアカウントを構成する」をクリック（または、「設定」タブ→「管理者」→「管理」→「アカウント設定」→「クラウドアカウントを構成」→「クラウドアカウントを追加」をクリック）
3. 「クラウドアカウントを選択」にて「AWS」を選択
4. 手順1で作成したユーザー情報を入力
5. 既存のCloudTrailに接続、または、CloudTrailを新規作成して接続
6. 「保存」をクリック

AWS CloudTrail（手順6で追加した以外のCloudTrail）、AWS S3 Access Logs、AWS ELB Access Logsを収集したい場合、こちらのページを参照して追加してください。

Microsoft 365（M365）

収集できるログの種類

- Azure Active Directory
- Exchange Online
- Sharepoint Online
- その他サービス（TeamsやOneDrive）

設定手順

1. Microsoft 365監査ログを有効化（こちらを参照）
2. Log360 Cloudに初めてアクセスした後に表示されるページの「+Configure

Agent」をクリック（または、「設定」タブ→「管理者」→「管理」→「アカウント設定」→「クラウドアカウントを構成」→「クラウドアカウントを追加」をクリック）

3. 「クラウドアカウントを選択」にて「Microsoft 365」を選択
4. Azure ADアプリケーションを構成

自動で設定する場合

a. 画面下部の「ここをクリック」をクリック
b. 「構成」をクリック
c. ポップアップされるMicrosoftのサインイン画面にて、グローバル管理者アカウントでサインイン
d. 「同意する」にチェックを入れ、「承諾」をクリック
e. 「要求されているアクセス許可」内容を確認後、「承諾」をクリック
f. テナント設定が成功した旨のメッセージが表示されることを確認

手動で設定する場合

こちらのページをご参照ください。

その他の設定

ログ収集フィルター

必要なログのみを収集することで、ログ容量を節約できます（詳細はこちらを参照）。

製品ユーザー（技術者）

Log360 Cloudにアクセスできるユーザー（技術者）を追加できます（詳細はこちらを参照）。

ログ保存期間および検索期間

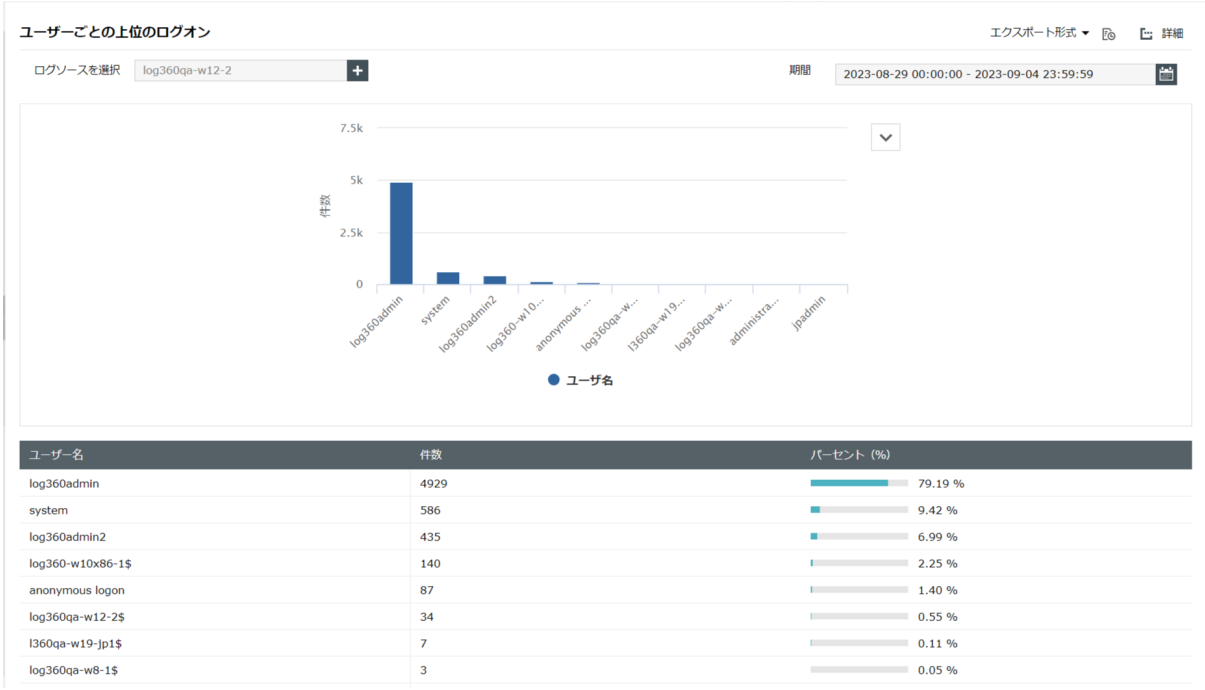
Log360 Cloudが収集したログを保存する期間、および、Log360 Cloudにて収集したログを検索できる期間を設定できます（詳細はこちらを参照）。

主要機能の説明

レポート

Windows、Unix、ネットワークデバイスやクラウドログといったあらゆるログに関するレポートを生成できます。生成されるレポートでは、誰がいつ何を実行したなどの詳細を確認できます。生成したレポートのエクスポートも可能です（さらなる詳細はこちらを参照）。

レポート例）ユーザー別のログオン状況

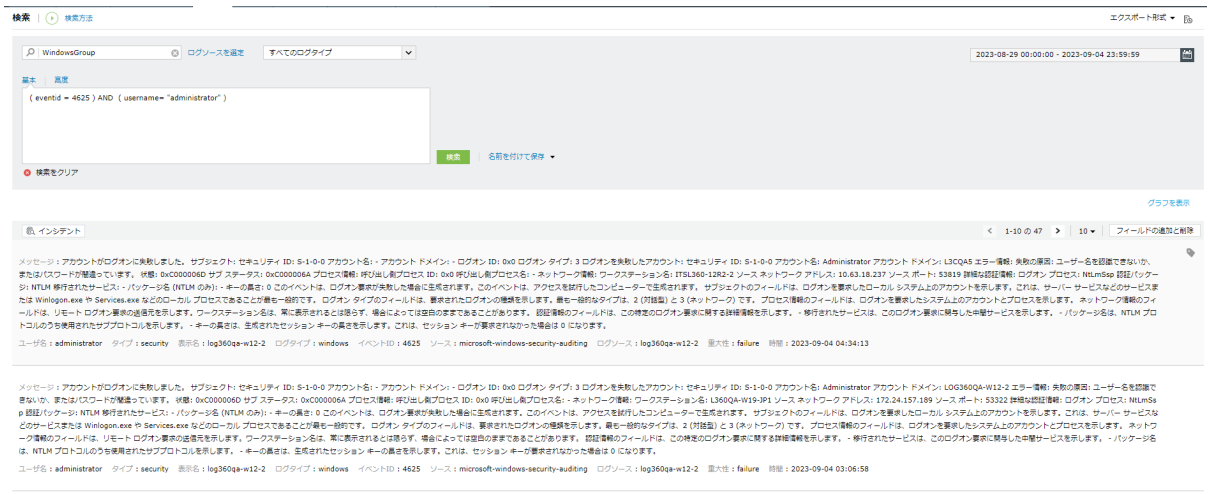


ユーザー名	件数	パーセント (%)
log360admin	4929	79.19 %
system	586	9.42 %
log360admin2	435	6.99 %
log360-w10x86-1$	140	2.25 %
anonymous logon	87	1.40 %
log360qa-w12-2$	34	0.55 %
l360qa-w19-jp1$	7	0.11 %
log360qa-w8-1$	3	0.05 %

検索

クエリ入力や期間で条件指定することで収集したログを検索できます。クエリを入力するのではなく、ログの項目（イベントIDやユーザー名）および値をUI上で指定することもでき、より直感的な操作が可能です（さらなる詳細はこちらを参照）。

検索例）ユーザーadministratorのログオン失敗（イベントID：4625）



アラート

特定のログを収集した際にアラートを発生させることができます。ログに含まれるイベントIDやユーザー名、リモートIPアドレスといった条件を指定したアラートを設定できます（さらなる詳細はこちらを参照）。

アラート例）「administratorのログオン失敗」、「禁止アプリへのアクセス」

クラウド監査

クラウドアクセスセキュリティブローカー（CASB）機能を使用することで、組織で利用しているクラウドサービスの使用状況の監査や、禁止アプリへのアクセスブロックを実施できます（さらなる詳細はこちらを参照）。

クラウド監査）ダッシュボードで必要な情報を取得できます。

トラブルシューティング

こちらのページをご参照ください。

お問い合わせ

価格、お見積りなど営業に関するお問い合わせ
https://www.manageengine.jp/purchase/

評価版ご利用中のお客様向け技術サポート
https://www.manageengine.jp/support/trail.html

保守サポート契約締結のお客様向け技術サポート
https://www.manageengine.jp/support/purchased.html

その他製品に関するお問い合わせ
https://www.manageengine.jp/contact.html

会社情報

ゾーホージャパン株式会社ManageEngine事業部
〒220-0012
神奈川県横浜市西区みなとみらい3丁目6番1号 みなとみらいセンタービル13階

ホームページ：https://www.manageengine.jp/
Log360 Cloud製品ページ：https://www.manageengine.jp/products/Log360_Cloud/