

## 統合ログ管理ソフト EventLog Analyzer、セキュリティ機能を強化

TLS のログ収集に対応して組織の PCI DSS 準拠を支援

ゾーホージャパン株式会社（代表取締役：迫 洋一郎、本社：横浜市、以下、ゾーホージャパン）は、イベントログや Syslog をはじめ任意のテキスト形式のログを取り込むことで、統合ログ管理/簡易 SIEM（Security Information and Event Management）として活用できるソフトウェア「ManageEngine EventLog Analyzer（マネージエンジン イベントログ アナライザー、以下、EventLog Analyzer）」の最新版「ビルド 11070」を、2017 年 10 月 3 日より正式に提供開始しました。

- ・ 統合ログ管理ソフト/簡易 SIEM「EventLog Analyzer」Web サイト  
[https://www.manageengine.jp/products/EventLog\\_Analyzer/](https://www.manageengine.jp/products/EventLog_Analyzer/)

### 【新機能】

EventLog Analyzer は従来、クレジットカード会員のカード情報や取引情報を安全に守るために策定された、クレジットカード事業者およびその加盟店向けの国際セキュリティ基準「PCI DSS（Payment Card Industry Data Security Standard）」に準拠するための機能（主に要件 10 に関連する内容）を複数提供してきました（※）。

※参考：ManageEngine の PCI DSS 対応ソリューションページ

[https://www.manageengine.jp/solutions/pci\\_dss/lp/](https://www.manageengine.jp/solutions/pci_dss/lp/)

この度リリースした EventLog Analyzer の最新版「ビルド 11070」では、TLS ※1（最新版 1.2 を含む）を使用したログ収集をサポートする事で、PCI DSS 準拠の要件 2.2.3、2.3、4.1 に関連する市場のログ管理ニーズへ応えました ※2。なお、PCI DSS については、2020 年に開催される東京オリンピックに向け、経済産業省から実行計画が公開され、国内の EC 加盟店は 2018 年 3 月末までの準拠（もしくはクレジットカード情報の非保持化）が求められています。

※1 TLS（Transport Layer Security）：インターネットなどのコンピュータネットワークにおいてセキュリティを要求される通信を行うためのプロトコル（通信手順）の一つ。TLS の元となったプロトコルが SSL（Secure Sockets Layer）であるため、SSL と呼ばれることも多い。

※2 PCI DSS に準拠する組織は、2018 年 6 月 30 日までに SSL および初期 TLS から安全な TLS へ移行する事が求められています。

この他、最新版「ビルド 11070」では、組織の業務時間外（深夜や定休日等）に発生した重要操作をアラートとして通知する機能を新たに追加し、セキュリティログの管理機能を強化しました。ManageEngine では、今後も使いやすいさとコストパフォーマンスのバランスが取れた製品を提供し、日本市場のセキュリティレベル底上げに貢献します。

The screenshot shows the EventLog Analyzer web interface. The top navigation bar includes links for Home, Reports, Configuration, Alerts, Correlation, Settings, Log Me, and Reports. The left sidebar contains a search bar and a list of alert categories: All Alerts, My Alerts, Recently Viewed Alerts, Unassigned Alerts, Important Alerts, Profile Alerts, and Alert Settings. The main content area displays a list of alerts. At the top of the alert list is a 'Severity' gauge. The alert list has columns for Status, Time, Host, Severity, Owner, Log Source, and Message. The first alert is from 'mihiro-thinkpad.ad...' with a severity of 'High' and status 'Open'. The message describes a Microsoft Windows Security-Auditing event where a user failed to log on.

ステータス	時刻	ホスト	重要度	オーナー	ログ収集ステータス	メッセージ
Open	Sep 22 2017 09:41:08	mihiro-thinkpad.ad...	High	-	Open	Microsoft Windows Security-Auditing アカウントがログオンに失敗しました。サブジェクト: セキ23リチ (ID: 51-10-0 アカウント名: アカウント ドメイン: ログオン ID: 0x0 ログオン タイプ: 3 ログオンに失敗したアカウント: セキ23リチ (ID: 51-10-0 アカウント名: DEMO-ELA5 アカウント ドメイン: ME-DEVELOP エラーの種類: 失敗の原因: ユーザー名を認識できないか、またはパスワードが間違っています。 (状態: 0x00000064) プロセスの種類: 呼び出し元のプロセス ID: 0x0 呼び出し元のプロセス名: ネットワークの種類: ワークステーション名: DEMO-ELA5 ソース ネットワーク アドレス: 192.168.83.25 ソース ポート: 52154 詳細な説明の種類: ログオン プロセス: NtLmSsp 認証の種類: NTLM 移行されたサビス: バナージ名 (NTLM のみ): キーの長さ: 0 このイベントは、ログオン要求が失敗したときに生成されます。このイベントは、アクティブな認証プロセスで生成されます。サブジェクトのフィールドは、ログオンを要求したローカルシステム上のアカウントを示します。これは、サーバーサービスなどのリモートまたは Winlogon.exe や Services.exe などローカルプロセスであることが最も一般的です。ログオン タイプのフィールドは、要求されたログオンの種類を示します。最も一般的なタイプは、2 (対話型) と 3 (ネットワーク) です。プロセスの種類は、ログオンを要求したシステム上のアカウントと一致を示します。ネットワークの種類は、リモートログオン要求の送信元を示します。ワークステーション名は、常に表示されることはありません。場合によっては匿名のままであることがあります。認証の種類は、この特定のログオン要求に関する詳細な説明を示します。移行されたサビスは、このログオン要求に関連する中間サビスを示します。バナージ名は、NTLM プロトコルの使用されたサブプロトコルを示します。キーの長さは、生成されたセッションキーの長さを示します。これは、セッションキーが要求された場合のみ表示されます。
Open	Sep 22 2017 09:41:08	MIHIRO-THINKPAD	High	-	Open	Microsoft Windows Security-Auditing アカウントがログオンに失敗しました。サブジェクト: セキ23リチ (ID: 51-10-0 アカウント名: アカウント ドメイン: ログオン ID: 0x0 ログオン タイプ: 3 ログオンに失敗したアカウント: セキ23リチ (ID: 51-10-0 アカウント名: DEMO-ELA5 アカウント ドメイン: ME-DEVELOP エラーの種類: 失敗の原因: ユーザー名を認識できないか、またはパスワードが間違っています。 (状態: 0x00000064) プロセスの種類: 呼び出し元のプロセス ID: 0x0 呼び出し元のプロセス名: ネットワークの種類: ワークステーション名: DEMO-ELA5 ソース ネットワーク アドレス: 192.168.83.25 ソース ポート: 52154 詳細な説明の種類: ログオン プロセス: NtLmSsp 認証の種類: NTLM 移行されたサビス: バナージ名 (NTLM のみ): キーの長さ: 0 このイベントは、ログオン要求が失敗したときに生成されます。このイベントは、アクティブな認証プロセスで生成されます。サブジェクトのフィールドは、ログオンを要求したローカルシステム上のアカウントを示します。これは、サーバーサービスなどのリモートまたは Winlogon.exe や Services.exe などローカルプロセスであることが最も一般的です。ログオン タイプのフィールドは、要求されたログオンの種類を示します。最も一般的なタイプは、2 (対話型) と 3 (ネットワーク) です。プロセスの種類は、ログオンを要求したシステム上のアカウントと一致を示します。ネットワークの種類は、リモートログオン要求の送信元を示します。ワークステーション名は、常に表示されることはありません。場合によっては匿名のままであることがあります。認証の種類は、この特定のログオン要求に関する詳細な説明を示します。移行されたサビスは、このログオン要求に関連する中間サビスを示します。バナージ名は、NTLM プロトコルの使用されたサブプロトコルを示します。キーの長さは、生成されたセッションキーの長さを示します。これは、セッションキーが要求された場合のみ表示されます。
Open	Sep 22 2017 09:39:03	MIHIRO-THINKPAD	High	-	Open	Microsoft Windows Security-Auditing 警告的な資格情報を使用してログオンが実行されました。サブジェクト: セキ23リチ (ID: 51-5-21-930237310-1041266944-3528606667-3707 アカウント名: mihiro.meida アカウント ドメイン: ADVENTNET ログオン ID: 0xA09BA ログオン GUID: (00000000-0000-0000-0000-000000000000) 資格情報を使用したアカウント: アカウント名: administrator アカウント ドメイン: meshch ログオン GUID: (00000000-0000-0000-0000-000000000000) ターゲット サーバー: ターゲット サーバー名: mwin2016 meshch.local 接続の種類: mwin2016 meshch.local プロセスの種類: プロセス ID: 0x4 プロセス名: ネットワークの種類: ネットワーク アドレス: 192.168.83.191 ポート: 445 このイベントは、プロセッサアカウントの資格情報を明示的に指定して、そのアカウントへのログオンを実行した場合に生成されます。これは、スケジュール タスクなどのバッチ タイプ構成で、または RUNAS コマンドの使用時に発生するものも一般的です。
Open	Sep 22 2017 09:39:03	mihiro-thinkpad.ad...	High	-	Open	Microsoft Windows Security-Auditing 警告的な資格情報を使用してログオンが実行されました。サブジェクト: セキ23リチ (ID: 51-5-21-930237310-1041266944-3528606667-3707 アカウント名: mihiro.meida アカウント ドメイン: ADVENTNET ログオン ID: 0xA09BA ログオン GUID: (00000000-0000-0000-0000-000000000000) 資格情報を使用したアカウント: アカウント名: administrator アカウント ドメイン: meshch ログオン GUID: (00000000-0000-0000-0000-000000000000) ターゲット サーバー: ターゲット サーバー名: mwin2016 meshch.local 接続の種類: mwin2016 meshch.local プロセスの種類: プロセス ID: 0x4 プロセス名: ネットワークの種類: ネットワーク アドレス: 192.168.83.191 ポート: 445 このイベントは、プロセッサアカウントの資格情報を明示的に指定して、そのアカウントへのログオンを実行した場合に生成されます。これは、スケジュール タスクなどのバッチ タイプ構成で、または RUNAS コマンドの使用時に発生するものも一般的です。
Open	Sep 22 2017 09:38:30	MIHIRO-THINKPAD	High	-	Open	Microsoft Windows Security-Auditing 警告的な資格情報を使用してログオンが実行されました。サブジェクト: セキ23リチ (ID: 51-5-21-930237310-1041266944-3528606667-3707 アカウント名: mihiro.meida アカウント ドメイン: ADVENTNET ログオン ID: 0xA09BA ログオン GUID: (00000000-0000-0000-0000-000000000000) 資格情報を使用したアカウント: アカウント名: administrator アカウント ドメイン: ela-demo ログオン GUID: (00000000-0000-0000-0000-000000000000) ターゲット サーバー: ターゲット サーバー名: demo-ela.me-develop.local 接続の種類: demo-ela.me-develop.local プロセスの種類: プロセス ID: 0x4 プロセス名: ネットワークの種類: ネットワーク アドレス: 192.168.83.25 ポート: 445 このイベントは、プロセッサアカウントの資格情報を明示的に指定して、そのアカウントへのログオンを実行した場合に生成されます。これは、スケジュール タスクなどのバッチ タイプ構成で、または RUNAS コマンドの使用時に発生するものも一般的です。

### <EventLog Analyzer : アラート機能画面>

EventLog Analyzer 最新版「ビルド 11070」その他の主な新機能は、以下のページで確認できます。

- 「EventLog Analyzer」リリース情報／新機能の紹介

[https://www.manageengine.jp/products/EventLog\\_Analyzer/release-note.html](https://www.manageengine.jp/products/EventLog_Analyzer/release-note.html)

## 【EventLog Analyzer の価格および評価版ダウンロード】

「EventLog Analyzer」では、30 日間無料で全機能を利用でき、技術サポートも受けられる「評価版」を提供しています。評価版は、以下のリンクよりダウンロードできます。なお、「EventLog Analyzer」の有料版ライセンス料金については、以下の価格ページで確認できます。

- 「EventLog Analyzer」の評価版ダウンロード

[https://www.manageengine.jp/products/EventLog\\_Analyzer/download.html](https://www.manageengine.jp/products/EventLog_Analyzer/download.html)

- ・ 「EventLog Analyzer」の価格情報ページ

[https://www.manageengine.jp/products/EventLog\\_Analyzer/pricing.html](https://www.manageengine.jp/products/EventLog_Analyzer/pricing.html)

## EventLog Analyzer について

EventLog Analyzer は、低コストで利用できる統合ログ管理ソフトウェア/簡易 SIEM です。Windows イベントログ、Syslog の相関分析に活用できる他、任意の text 形式ログを取り込んでログフォーマットの定義付けを行い、相関検索に活用できます。既に全世界で 5,300 社以上に利用され、国内でも金融・大手企業、官公庁等、幅広い業種の導入実績があります。



### EventLog Analyzer

[https://www.manageengine.jp/products/EventLog\\_Analyzer/](https://www.manageengine.jp/products/EventLog_Analyzer/)

## ManageEngine について

ManageEngine は、ゾーホージャパン株式会社が提供するネットワークや IT サービス、セキュリティ、デスクトップ・ノート PC、ビジネスアプリケーションなどを管理する製品・サービス群です。

必要十分な機能に限定、かつ、直感的な操作が可能な画面設計により、短期間での導入が可能であり、その後の運用フェーズにおいても手間がかからず、よりシンプルな IT 運用管理を実現します。

また、中堅・中小企業でも導入しやすいリーズナブルな価格で、これまで大手 IT ベンダーが提供する複雑で高額なツールを利用していた企業や、ツールを自社開発していた組織にも採用されてきました。現在では、日本国内の一般企業、官公庁や自治体などへ、4,000 ライセンスを超える販売実績があり、安心して使える製品・サービスです。

最大で 29 言語に対応する製品・サービスは、北米、欧州をはじめ、南米、中東、アジアなど世界で 12 万社以上の企業や組織が導入し、企業・組織の IT 運用管理のシンプル化、グローバル化に貢献しています。



<https://www.manageengine.jp/>

## ゾーホージャパン株式会社について

ゾーホージャパン株式会社は、ワールドワイドで事業を展開する Zoho Corporation Pvt Ltd が開発/製造したネットワーク管理開発ツールや企業向け IT 運用管理ツール、企業向けクラウドサービスを日本市場に提供すると同時に関連するサポート、コンサルティングなども提供しています。

ネットワーク管理開発ツール「WebNMS」は、シスコシステムズ、エリクソン、アルカテル・ルーセント、モトローラなど世界 2 万 5 千社の有力企業で採用され、ネットワーク管理の OEM 市場でデファクト・スタンダードとして認知されています。

また、WebNMS のノウハウや経験を生かして開発された企業向け IT 運用管理ツール群「ManageEngine」は、世界 12 万社を超える顧客実績を誇り、国内でも販売本数を伸ばしています。

その他、業務改善/生産性向上を支援する企業向けクラウドサービス群「Zoho」は、世界で 2500 万人を超えるユーザーに利用されています。



<http://www.zoho.co.jp/>

## お問い合わせ先

本ニュースリリースに関するお問い合わせ：

ゾーホージャパン株式会社 ManageEngine & WebNMS 事業部 マーケティングチーム

TEL：045-319-4613 E-mail: [jp-memarketing@zohocorp.com](mailto:jp-memarketing@zohocorp.com)

※本資料に掲載されている製品、会社などの固有名詞は各社の商号、商標または登録商標です。®マーク、TM マークは省略しています。