SPONSORED CONTENT | WHITE PAPER

Cybersecurity

膨大で煩雑な ログ管理を 低コストで行うには？

クラウド時代の統合ログ管理/SIEMソリューション「Log360 Cloud」

昨今のビジネス環境においてクラウド活用は、もはや不可逆の潮流だ。これに伴いセキュリティの境界線が曖昧になり攻撃対象領域が拡大したことで、クラウドサービスを含めたあらゆる場所で発生する脅威の兆候を迅速に発見する必要に迫られている。この取り組みの中核となるのが、ログ管理だ。ただし、オンプレミスからクラウドサービスに分散する膨大なログの一元管理の実現は容易ではない。本資料では、この課題を解決すべくゾーホーが提供している統合ログ管理/SIEMソリューション「ManageEngine Log360 Cloud」について解説する。

世界で28万社以上の企業や組織に導入される、ゾーホー「ManageEngine」

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.（本社インド）の日本法人で、IT運用管理製品群「ManageEngine」やクラウドサービス群「Zoho」、それに関連するサポート、コンサルティングを提供している。本資料で紹介するManageEngineシリーズは、世界で28万社以上の企業や組織に導入され、必要十分な機能、リーズナブルな価格、直感的な操作感で日本でも多くの導入実績がある。

CIO

SPONSORED BY ZOHO

Cybersecurity

クラウド化によってログ管理が煩雑に

昨今の悪質かつ巧妙化するサイバー攻撃は、企業に深刻な被害をもたらしている。このリスクを低減させるセキュリティ対策の中心に位置するのがログ管理である。さまざまな機器やシステムから取得するログは、セキュリティインシデントの兆候を捉えるための重要な情報源となる。

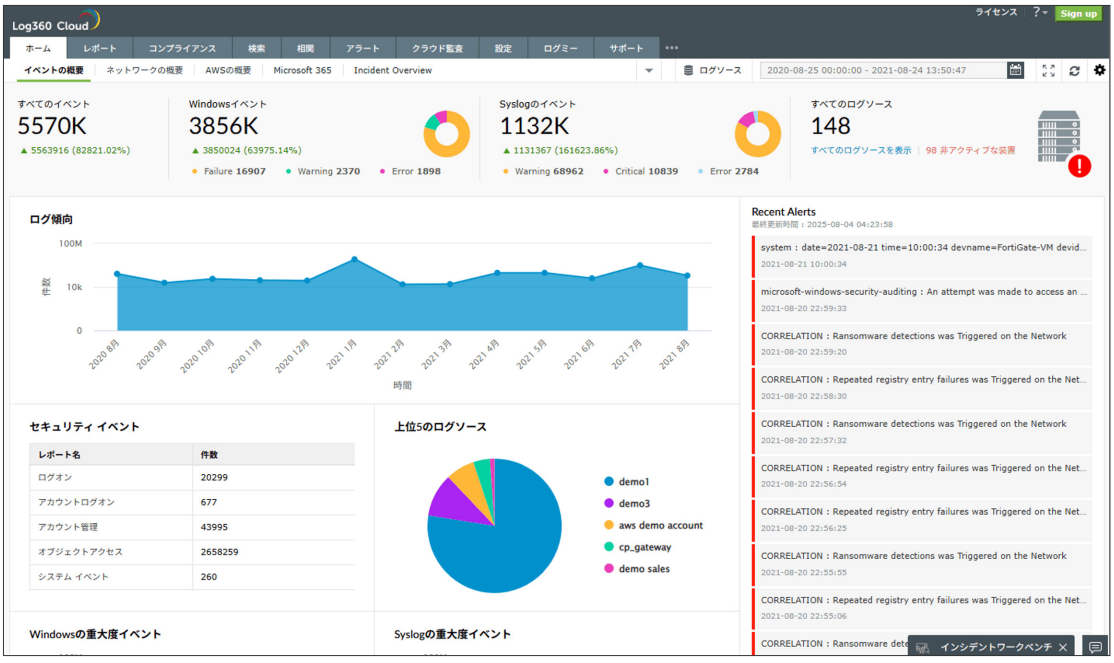
しかし、このログ管理が次第に困難になりつつある。背景にあるのはクラウドサービスの利用拡大だ。クラウドサービスごとに生成されるログは、フォーマットや構造もバラバラであり、これらを一元的に収集し、関連付けて分析することは、非常に困難だ。IT部門の管理者にとって重い負担となり、セキュリティ監視の盲点を生み出す原因にもなりかねない。特に大量のログ収集や分析を手作業に依存している場合、リアルタイムでの脅威検知はほぼ不可能で、インシデント発生後の対応が後手に回るリスクが高まる。

優れたコスト効率、拡張性、UIの「Log360 Cloud」

ログ管理に関する課題を解決すべく、ゾーホーが提供しているのが「ManageEngine Log360 Cloud」（以下、Log360 Cloud）である。オンプレミスから複数のクラウドサービスにまたがるハイブリッド環境のログやイベントを、クラウド上の単一プラットフォームで可視化する統合ログ管理/SIEM（Security Information and Event Management：セキュリティ情報およびイベント管理）ツールだ。

従来のオンプレミス型ログ管理/SIEMと異なり、SaaS型で提供されるLog360 Cloudなら自前のサーバー導入や環境構築は不要だ※。インターネット接続回線とWebブラウザがあればすぐに利用でき、その後のアップデートやメンテナンス作業はすべてゾーホー側で行われるため、IT管理者の負担は最小限に抑えられる。これなら中堅クラスの企業でも、容易に統合ログ管理/SIEMに乗り出すことができる。

※ログ収集用のサーバーが最低1台必要です。



Log360 Cloudのダッシュボード画面

Log360 Cloudは、こうしたコスト効率に加え、拡張性にも優れている。ログ量やユーザー数の増加に柔軟に対応し、必要なリソースを迅速に拡張・縮小することが可能だ。また、後述するログ管理、SIEM、CASB、ダークウェブ監視といった複数の機能を単一プラットフォームから提供することで、各ソリューションを個別に導入・連携させる手間とコストを削減する。

さらに、ManageEngineシリーズ全体に共通する特長として、直感的で使いやすいUIを提供。ITシステムの運用経験が浅い担当者でも容易に操作することができ、セキュリティ監視を効率化する。

ログ管理のための統合的な機能

Log360 Cloudは下記の機能を提供することで、企業におけるセキュリティ監視および対策を強力に支援する。

1.ログの収集・可視化

企業内の多様なシステムからWindowsイベントログ、Syslog、クラウドサービスログ、アプリケーションログなどを収集し、一元的に管理・可視化。収集したログの種別に応じた豊富なレポートテンプレートを提供する。これにより特定のイベント（失敗したログオン試行、重要ファイルへのアクセスなど）や、コンプライアンス違反に合致する情報を簡単に可視化できる。また、強力な検索機能によりキーワード、期間、ログソース、イベントIDなどの条件でログを絞り込み、必要に応じて詳細な情報へとドリルダウンすることで、インシデント調査の時間を大幅に短縮する。

2.相関分析とアラート通知

異なるログソースから収集された複数のイベントを関連付け、あらかじめ定義されたルールに基づいて脅威パターンを検知する。例えば短時間での複数ユーザーによるログイン失敗（ブルートフォース攻撃の兆候）や、特定のサーバーへの異常なアクセスとそれに続くデータ転送といった複合的なイベントを自動的に識別する。さらに最新の脅威インテリジェンスと連携し、ログに含まれる悪意のあるIPアドレスやURLをリアルタイムで特定する。

3.CASB（Cloud Access Security Broker）機能

クラウドサービスへのアクセスを監視し、承認されていないSaaSアプリケーション利用などシャドーITを検知する。また、検知されたシャドーITのリスクレベルをデータ漏えいやコンプライアンス違反などの観点から評価・可視化する。特にリスクが高いと判断されたシャドーITに対しては、サービスへのアクセスをブロックするなどポリシーを適用することも可能だ。

4.コンプライアンスレポート

クレジットカード業界のセキュリティ基準であるPCI-DSSや、ISMS（情報セキュリティマネジメントシステム）の国際規格であるISO27001など、主要なコンプライアンスフレームワークに準拠したレポートを自動生成し、スムーズな監査対応を支援する。

5.アクセス制御・インシデント管理

既存のITSM（IT Service Management）ツールなどチケット管理システムと連携し、Log360 Cloudで検知したインシデントをITSMツールで一元管理できる。これによりインシデント対応のワークフローを効率化し、対応漏れを防止できる。

6.ダークウェブ監視機能

ダークウェブを継続的に監視し、企業のドメインに関連する認証情報や個人情報が公

開されていないかどうか調査する。万一、情報漏えいが検知された場合は、即座にアラートを通知する。これによりパスワードのリセットや、関連アカウントの無効化といった対策を迅速に講じることができる。

組織を守り、ビジネス成長の基盤となるログ管理

事業の維持・成長を考えたとき、クラウド活用は欠かすことができない。その際にLog360 Cloudを活用することは、経営面においてもさまざまなメリットがある。

1点目は、ハイブリッド環境全体の可視化。オンプレミスとクラウドが混在する現在の複雑なIT環境において、Log360 Cloudはすべてのログを一元的に収集・管理できる。これによりログ管理のサイロ化を解消し、組織全体のセキュリティ状況を鳥瞰的に把握することが可能となる。

2点目は、セキュリティインシデントの早期発見・対処。Log360 Cloudが提供する高度な相関分析機能は、潜在的なセキュリティ脅威を早期に発見する上で極めて有効な手段となる。複数のログやイベントを関連付けて分析することで、単体では見過ごされがちな攻撃の兆候や情報流出のリスクを自動的に検知し、アラートを発するのである。これによりラテラルムーブメント（侵入の横展開）や特権アカウントの窃取など、被害が拡大する前に迅速な対処が可能となり、事業への影響を最小限に抑えるサイバーセキュリティの運用体制を確立できる。

3点目は、監査対応・コンプライアンスの強化。GDPR、PCI-DSS、ISO27001など、国内外のさまざまな法規制や業界標準の監査要件に対応したレポートテンプレートをデフォルトで有する。これによりログデータの収集から整理、分析、レポート作成にいたる作業に費やす時間と労力を大幅に削減し、スムーズな監査対応を実現する。さらに継続的なログ監視と記録によりコンプライアンスを強化し、自社の信頼性を高めていく。

4点目は、運用工数・人件費の削減。SaaS型のソリューションであるLog360 Cloudならでは、統合ログ管理/SIEM導入のためのインフラ構築やソフトウェアの設定、その後のパッチ適用、バージョンアップといった煩雑な作業から解放される。これらの運用・保守作業はすべてベンダー側で実施されるため、IT部門やセキュリティチームの運用工数を大幅に削減できる。これにより社内の限られた人的リソースをより戦略的なセキュリティ強化策の検討や、ビジネス価値を生み出すための業務にシフトすることが可能となる。

Log360 Cloudは、オンプレミスとクラウドが混在するハイブリッド環境から発生する複雑かつ膨大なログやイベントを統合し、高度な相関分析を通じてインテリジェンスへと変換することで、一歩先ゆく対策を実現する。また、SaaS型で利用できることで導入・運用負担が軽く、コストを最小限に抑えられる。初めてログ管理に取り組もうという企業、ログ管理に関わるIT部門の負荷を軽減したい企業は、検討してみてはいかがだろうか。