【プレスリリース】

マカフィー株式会社
2018 年 4 月 9 日

マカフィー、セキュリティ運用ソリューションを強化

SIEM のアーキテクチャー刷新と機械学習による高度な分析で早期発見、早期対応を支援

マカフィー株式会社（本社：東京都渋谷区、代表取締役社長：山野修）は、本日、高度なサイバーセキュリティの脅威に対し、迅速な対応を可能にするセキュリティ運用機能を強化した「Enterprise Security Manager（McAfee ESM 11）」、及び「McAfee Behavioral Analytics」を発表しました。

SIEM の最新版「Enterprise Security Manager（McAfee ESM 11）」は、拡張性、パフォーマンス、高速検索、そして連携機能の強化を目的として最適化された新しいデータ アーキテクチャーを活用しています。本日より日本市場で提供を開始する「McAfee Behavioral Analytics」は機械学習を活用し、導入や運用負担を軽減しながら検知率を向上し、セキュリティ運用チームをサポートします。より高度化・巧妙化するサイバー脅威に対抗するために、テクノロジーの積極活用によって限られたリソースで早期発見と早期対応の実現を支援します。

強化された最新の SIEM を基盤とした運用に加え、「McAfee Behavioral Analytics」の高度な分析機能を活用することで、セキュリティ運用チームによるデータの収集、解析、共有を効率化し、テクノロジーによる運用支援の進化を加速させることができます。その結果、セキュリティ運用チームは、セキュリティ イベントから実用的な洞察を導き出し、巧妙な脅威を迅速に検知し、確実に対応することが可能になります。

今回、「McAfee ESM 11」、「McAfee Behavioral Analytics」に搭載・強化された機能は以下のとおりです。

McAfee ESM 11 の新機能:

- **柔軟なデータ アーキテクチャー**
  McAfee ESM 11 の中核を成すオープンで拡張性の高いデータ バス アーキテクチャーの採用により、大量のセキュリティ イベントを効率よく処理できるようになりました。セキュリティ運用者や脅威ハンターは大量のセキュリティ イベントを対象に、インシデントの調査やコンプライアンスのためのデータ保全を柔軟かつ効率よく行えるとともに、大量のデータを必要とする分析プラットフォームとの連携も向上します。
- **拡張可能な取り込みと検索パフォーマンス**
  McAfee ESM 11 のアーキテクチャーでは、大量データの保存だけでなく数十億件規模の大量のイベントを対象に検索し素早く調査が行えます。必要に応じて、McAfee ESM にアプライアンスや仮想マシンを追加し、パフォーマンスを高めたり、冗長性を向上させることができます。

McAfee Behavioral Analytics:

- **機械学習による脅威の特定**
  ビッグデータ セキュリティ分析と機械学習を活用し、複雑な設定や前提となる特別な知識を必要とせずに、組織内のセキュリティ脅威を発見できるようになります。
- **脅威の優先付け**
  McAfee Behavioral Analytics は、数十億件規模の大量のセキュリティ イベントを数百種類の異常に分類した上で、更に優先対応すべきリスクの高い脅威を可視化します。

米国マカフィーのセキュリティ分析担当バイス プレジデントであるジェイソン・ロールストン（Jason Rolleston）は、「今日の脅威動向に対応するために企業が懸命な努力を重ねるなか、人とテクノロジーの連携に対する必要性がかつてないほどに高まっています。セキュリティ人材不足の状況で優秀な人材の十分な確保は難しく、企業は高度な分析機能や機械学習を用いたソリューションで組織の生産性を強化しなければなりません。セキュリティ運用チームは、新しいソリューションが持つ能力やスピードを人間の知見と融合させることで、運用のスピード、品質、効果、そして効率性をさらに向上させることが可能になるのです」と述べています。

マカフィーは、2017年12月にガートナーが発行した「セキュリティ情報・イベント管理（SIEM）に関するマジック クアドラント」において、7年連続でリーダーに選出されています。[1]

【提供開始時期について】

- Enterprise Security Manager（McAfee ESM 11）は現在利用可能 です。
- McAfee Behavioral Analytics は 4 月 9 日より提供を開始いたします。

【関連情報】

- 関連 Web サイト：インテリジェントなセキュリティオペレーション
- レポート：攻撃の阻止に必要なのはスキルかテクノロジーか？
- 2017 Gartner Magic Quadrant for Security Information and Event Management, Dec. 2017

[1] Gartner, Magic Quadrant for Security Information and Event Management、著者: ケリーM.カヴァナー（Kelly M. Kavanagh）、トビー・ブッサ（Toby Bussa）、 2017 年 12 月 4 日初版
*マカフィーは、過去にインテル セキュリティおよび NitroSecurity として本レポートにおいて選出されています。

マカフィーについて
マカフィーはデバイスからクラウドまでを保護するサイバーセキュリティ企業です。業界、製品、組織、そして個人の垣根を超えて共に力を合わせることで実現するより安全な世界を目指し、マカフィーは企業、そして個人向けのセキュリティ ソリューションを提供しています。詳細は http://www.mcafee.com/jp/ をご覧ください。