ソリューション概要

脅威情報を効果的に利用する方法

犯罪者は様々な手法でインフラに侵入し、重要なデータ資産やシステムに攻撃を仕掛けてきます。ITセキュリティが受信するアラートは氷山の一角にすぎません。最近の標的型攻撃は一連の流れで実行されています。この攻撃チェーンは、偵察、脆弱性のスキャン、侵入、重要なデータの取得という段階から構成されています。

セキュリティ アナリストはこの事実を十分に認識しています。攻撃の手口と動機を特定するために脅威情報を利用し、高度脅威を検出して適切な修復作業を行い、今後の攻撃に備えています。しかし、特定のシステムの状態が把握できなかったり、データ量が多すぎて有益な情報を取得できないことも少なくありません。SANS Instituteの調査『Who's Using Cyberthreat Intelligence and How?』（サイバー脅威インテリジェンスの利用状況）によると、すべての情報源から脅威情報を収集して活用していると答えた回答者は全体の11.9%に過ぎず、イベントとIoCを関連付けて全体の状況を把握しているのはわずか8.8%でした[1]。

Forresterが最近公開したレポートによると、北米とヨーロッパにある大企業の77%は、脅威情報の有効活用を最優先課題に挙げています[2]。サイバー脅威インテリジェンスの利用により、特定の地域、業界、企業を狙うサイバー攻撃を早期に認識し、対策を講じることが可能になりますが、ITセキュリティの担当者は次のような課題に直面しています。

- 外部と内部の情報源から脅威情報をどのように収集するか
- データを相関分析し、リスクの優先度をどのように設定するか
- 異なるベンダーのセキュリティ対策を利用している環境で脅威情報をどのように配信するか
- 適切な対応を迅速に行うために、ITインフラの可視化をどのように強化するか

フォレンジックだけでなくSIEM分析の向上に役立つ情報を収集するには、脅威情報の収集、分析、要約、管理を自動的に行うオープンな統合アーキテクチャが必要です。

intel Security

新たな脅威の出現で変わる脅威情報に対するアプローチ

サイバー攻撃の量は増え続け、複雑さだけでなく精度も増しています。これまでの手法では脅威を防ぐことはできません。脅威情報に対するアプローチも変える必要があります。標的型攻撃の調査は決して簡単な作業ではありません。攻撃者の振る舞いは常に変化しています。グローバルやローカルで利用可能な脅威情報は多様化し、データ形式も統一されていません。このような脅威データをセキュリティ オペレーション センター（SOC）で集約し、選別することは、さらに難しい作業となっています。

大規模な環境では異なるベンダーのソリューションが混在しているのが普通です。組織全体でイベント データを共有し、可視化するのは簡単なことではありません。Gartnerのレポート『Technology Overview for Threat Intelligence Platforms』（脅威情報プラットフォームの技術概要）にあるように、脅威情報の共有が進まない現状はサイバー犯罪者にとって非常に都合のよい状況です。増え続ける脅威と攻撃を防ぐには、脅威情報の共有が重要になります[3]。

しかし、脅威情報の共有ですべてが解決されるわけではありません。情報が増えれば分析者の負担も増加します。多くのセキュリティ チームは、大量のデータから標的型攻撃の兆候を検出するため、膨大なセキュリティ イベントと不審なファイルを手動で分析しています（図1を参照）。脅威の詳細を把握できない状態で攻撃の封じ込めを行うようなアプローチでは、徹底した対応を迅速に行うことは不可能です。2014年にIntel Securityが公開した調査報告『When Minutes Count』（迅速な対応）にあるように、数分以内に攻撃を検出できると答えた回答者は全体の25%にも達していません[4]。

「セキュリティ インフラの構築に複数のテクノロジ ベンダーが必要でした。このため、顧客の様々な要件を管理し、常に変化する脅威状況に対応できるパートナーを探していました。このニーズを満たしていたのがマカフィーです。マカフィーのソリューションから受信するセキュリティ情報は最先端のビジネスを継続する上で重要な役割を果たしています。」

—Anurana Saluja
CISO兼情報セキュリティ担当
バイスプレジデント
Sutherland Global Services

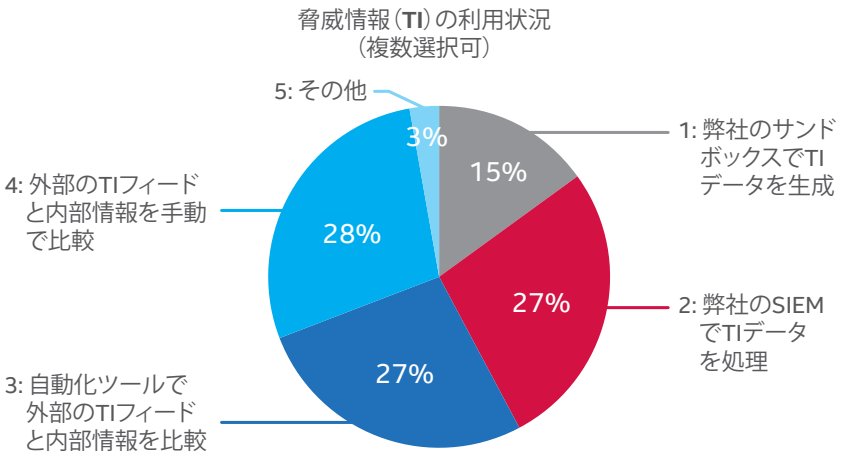

図 1. Intel SecurityがBlackHat 2015で実施した調査結果。外部の脅威情報と内部の脅威情報の比較を手動で行っているユーザーも少なくありません。

脅威情報の効果的な利用

脅威情報を基に検出と修復を行うには、Webサイトに公開されている不正なIPアドレスを週に1回SIEM ウォッチリスト テーブルにインポートするだけでは不十分です。短時間で拡散するステルス型の脅威を未然に防ぐには、脅威情報をリアルタイムで収集し、攻撃に関連するすべての情報（手口や攻撃範囲など）を関連付けて分析する必要があります。大企業のSOCは、環境に影響を及ぼす攻撃の全貌を把握するため、脅威情報を有効に活用できる方法を模索しています。大量のデータから有効な情報を選別して相関分析を行い、優先度に応じて対応するだけでなく、特定の業界、地域、企業に関連する脅威も識別しなければなりません。現在発生している可能性がある攻撃だけでなく、過去のセキュリティ イベント データを使用した傾向分析も必要です。Forresterが指摘しているように、攻撃の75%は発生から24時間以内に拡散しています。脅威情報を効果的に活用し、情報の共有速度と攻撃の拡散速度のギャップを埋める必要があります[5]。

Intel Securityの統合アーキテクチャ

Intel Securityが提供する統合プラットフォームでは、すべてのコンポーネントが脅威情報を利用しています。グローバルの脅威情報だけでなく、ローカルでも脅威情報を収集し、ITインフラ全体でリアルタイムに共有しています。また、セキュリティ情報とイベントを管理し、適切な保護機能を自動的に配布しています。

脅威情報の要件	McAfee® Threat Intelligence Exchange	McAfee Advanced Threat Defense	McAfee Enterprise Security Manager	McAfee Global Threat Intelligence
外部情報源からの脅威情報の収集	STIX、McAfee Global Threat Intelligence（McAfee GTI）のインポート、VirusTotal	McAfee GTIのインポート	McAfee GTI、TAXII/STIXのインポート、McAfee Enterprise Security Manager経由でのHTTP脅威情報のフィード	複数のCyber Threat Alliance/パートナーと公開情報から脅威情報を収集し、集約。数百万台のセンサーを使用し、顧客に配備されたIntel Security製品（エンドポイント、Web、メール、ネットワーク侵入防止（IPS）、ファイアウォール機器など）から脅威情報を抽出。
内部の脅威情報の収集	McAfee VirusScan®、McAfee Application Control、McAfee Web Gateway、McAfee Advanced Threat Defense、McAfee Enterprise Security Managerからサンプルを収集。McAfee Data Exchange Layer経由で情報を送信する他社製品からもサンプルを収集。	McAfee Threat Intelligence Exchangeまたはネットワーク経由で受信したサンプル ファイルを分析	STIX/TAXIIまたはMcAfee Data Exchange Layer経由	
ローカルでの脅威情報の取得	不審なファイルのインシデントを記録し、最初の接点や感染経路をデータベースに登録	マルウェアの解析でローカルの脅威情報を生成。McAfee Data Exchange Layer経由またはSTIX形式のAPIとして配信。	イベントを関連付け、脅威情報のウォッチリスト、レポート、ビューを作成	
セキュリティ対策への脅威情報の配信	McAfee Data Exchange Layer経由	McAfee Data Exchange Layerまたは製品API経由	McAfee Data Exchange Layer、製品API、スクリプト統合経由	McAfee Web Gateway、McAfee Enterprise Security Manager、McAfeeエンドポイント ソリューションなど、様々なIntel Security製品に統合
脅威情報の可視化と収集	McAfee Threat Intelligence Exchangeのダッシュボード	レポート	コンテンツ パックまたはカスタム生成で提供されるダッシュボード、ビュー、レポート	McAfee Threat Center、四半期ごとのMcAfee脅威レポート

表 1. Intel Securityの脅威情報統合プラットフォーム

取得・分析・配信

McAfee Global Threat Intelligence

脅威情報の統合プラットフォームでまず必要になるのがMcAfee Global Threat Intelligence（McAfee GTI）です。このソリューションはIntel Security製品に完全に統合され、クラウド ベースの包括的なレピュテーション サービスをリアルタイムで提供します。これにより、ファイル、Web、メッセージ、ネットワークなど、すべての経路でサイバー脅威を迅速に阻止できます。McAfee GTIは、McAfee Labsが世界各地に配備している数百万台のセンサー、調査パートナー、Cyber Threat Allianceなど、複数の情報源から入手した脅威データに基づいて数十億のファイル、URL、ドメイン、IPアドレスのレピュテーション スコアを提供します。McAfee GTIは高品質な関連情報を提供するので、正確なリスク アドバイスに基づいて的確な判断を行い、ブロック、駆除、許可を制御できます。

McAfee Enterprise Security Manager

McAfee Enterprise Security Manager（SIEM）は脅威情報の分析を行い、検討事項と分析結果を提供します。このソリューションは脅威情報のアクション ハブとして機能します。状況を可視化し、状態を確認できるので、標的型攻撃を迅速に検出し、問題を修復できます。この高度なデータ管理システムは、大量のコンテキスト データをリアルタイムで保管し、処理できるように設計されています。

McAfee Enterprise Security Managerは、すべてのシステム、データベース、ネットワーク、アプリケーションからアクティビティとイベント データを収集します。また、FS-ISAC（Financial Services Information Sharing and Analysis Center）などの業界団体によって定義されたSTIX（Structured Threat Information eXpression）/TAXII（Trusted Automated eXchange of Indicator Information）やCyboxなどの標準フォーマットでグローバル脅威フィードをインポートし、脅威情報を処理できます。これらの情報から高度な分析を行い、有益な情報を分かりやすい形式で出力します。新たに発生する脅威をリアルタイム ビューで確認するだけなく、過去のセキュリティ情報も利用できます。過去の状況から脅威の流行やパターンを分析したり、ウォッチリストを自動的に作成してイベントの発生や再発を検知できます。不正であることが確認されているイベントに対する感度を強化することで、攻撃チェーンの各段階で不正なアクティビティとパターンの検知能力を強化し、優先度に応じた対策が可能になります。

図 2. McAfee GTIビュー

Cyber Threat Alliance

Cyber Threat Allianceでは、参加メンバーとその顧客を脅威から保護するため、メンバー間で脅威情報を共有しています。Intel Securityは、このグループの設立メンバーで、脅威データを共有する最も効果的な方法を開発しています。メンバー間のコラボレーションを推進し、洗練されたサイバー犯罪者との戦いに貢献しています。

McAfee GTIとMcAfee Enterprise Security Managerにより、McAfee Labsの調査結果を利用して企業のセキュリティ監視を強化できます。常に更新されるMcAfee GTIフィードを利用することで、状況認識能力が向上します。たとえば、不審または不正なIPとの通信を迅速に検出し、社内で現在または以前にこのようなIPと通信を行っているホストを特定できます。

McAfee Threat Intelligence Exchange
統合された脅威情報エコシステムの3番目のコンポーネントは、ファイル レピュテーション情報の収集とセキュリティ インフラ全体での共有を担うMcAfee Threat Intelligence Exchangeです。McAfee Threat Intelligence ExchangeはMcAfee GTIからの脅威情報、STIXファイル、McAfee Enterprise Security Managerからの脅威情報フィードを受信し、エンドポイント、アプリケーション制御、モバイル デバイス、データセンター、サンドボックスから情報を受信します。Intel Securityのソリューションだけでなく、他のベンダーのソリューションからも情報を取得します。インフラのすべてのポイントからデータを収集するので、環境にのみ存在する脅威（標的型攻撃など）を確認できます。ファイルのレピュテーション情報は、McAfee Threat Intelligence Exchangeに接続しているすべての製品とソリューションにMcAfee Data Exchange Layer経由で送信され、エコシステム全体ですぐに共有されます。たとえば、McAfee Threat Intelligence Exchangeが不正な実行ファイルに関する情報を送信すると、McAfee Data Loss PreventionはMcAfee Data Exchange Layer経由でこの情報を受信し、重要なファイルに対する実行ファイルのアクセスを監視します。

ファイル レピュテーション、データの分類、アプリケーションの整合性、ユーザー コンテキスト データなどの脅威データがMcAfee Data Exchange Layer経由で送信され、McAfee Data Exchange Layerファブリックに統合されている製品間で共有されます。どの製品またはソリューションでもMcAfee Data Exchange Layerに統合し、システムに公開する情報や取得する情報を設定できます。

McAfee Threat Intelligence ExchangeはIntel Securityの高度なサンドボックス ソリューションであるMcAfee Advanced Threat Defenseと緊密に連携しています。このソリューションは、McAfee Threat Intelligence Exchangeにマルウェアの分析データをフィードします。不正なファイルであることが判明すると、McAfee Threat Intelligenceは接続しているすべてのシステムにMcAfee Data Exchange Layer経由で最新のファイル レピュテーションを送信します。この逆の処理も行われます。McAfee Threat Intelligence Exchangeが有効になっているエンドポイントがレピュテーション不明のファイルを検出すると、このファイルをMcAfee Advanced Threat Defenseに送信して解析し、アウトバンドでのペイロード配信を阻止します。この2つの製品により、新たに発生する脅威を自動的に検出し、阻止できます。検出された攻撃の情報は環境全体に配信されるので、被害が拡大する前にサイバー攻撃チェーンを断ち切ることができます。

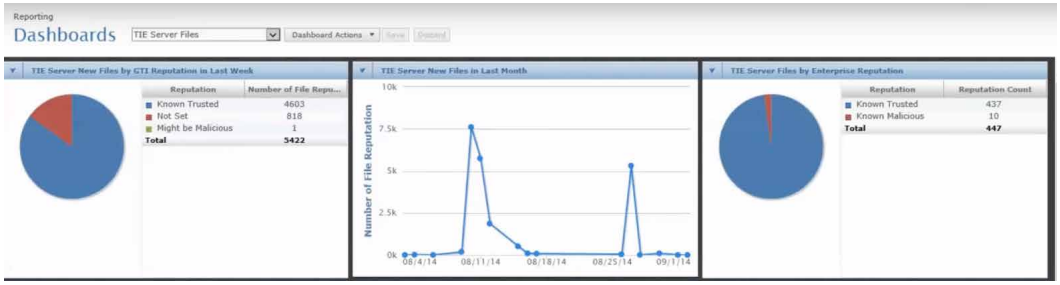

図 3. McAfee Threat Intelligence Exchangeのダッシュボード

McAfee Threat Intelligence Exchangeを使用すると、エンドポイント、ゲートウェイ、ネットワーク、データセンターを保護するソリューションの間でセキュリティ情報をリアルタイムに交換し、適応型の脅威検出と対応が可能になります。ローカルで収集された情報とグローバルの脅威情報が統合され、複数のセキュリティ対策が1つのソリューションのように機能します。

サイバー攻撃チェーンの切断
不明なマルウェアの最初の接点がどこであっても、感染が発生すると、接続している環境全体でただちに情報が更新されます。McAfee Advanced Threat Defenseが不正なファイルと判断すると、McAfee Threat Intelligence ExchangeがMcAfee Data Exchange Layer経由で組織内のすべてのセキュリティ対策に最新のレピュテーション情報を送信し、McAfee Threat Intelligence Exchangeが有効になっているゲートウェイがインフラへの脅威の侵入を阻止します。このように、組織内のすべてのセキュリティ対策で脅威情報が共有されるので、攻撃チェーンを自動的に切断し、被害の拡大を防ぐことができます。

要約と適用: 正確な検出と的確な判断

収集された脅威データはすべてMcAfee Enterprise Security Managerで管理されます。McAfee GTI、McAfee Threat Intelligence Exchangeのフィード、STIX/TAXII形式の侵害兆候（IoC）とイベント データが関連付けられ、ネットワーク上で不正な対象や不審なドメインと通信を行っているノードをすぐに特定できます。また、履歴データからの特定も可能です。脅威管理ダッシュボードには、収集された脅威兆候、情報源からのフィード、兆候のヒット率だけでなく、重要な侵害兆候（IoC）の詳細が分かりやすい表現で表示されます。

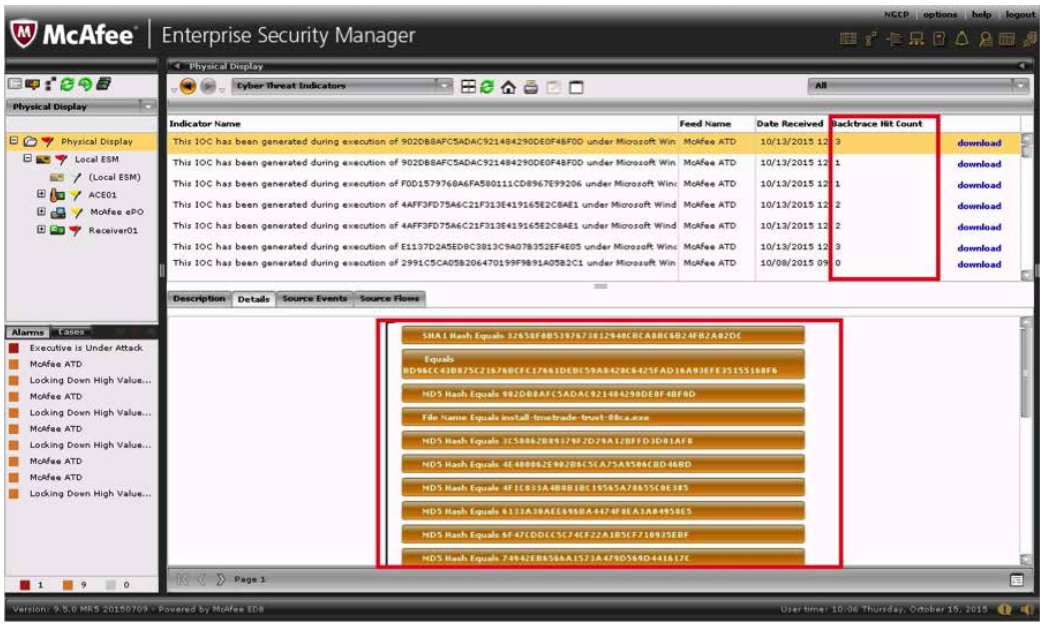

図 4. McAfee Enterprise Security Managerに表示されたサイバー脅威インジケーター、バックトレース率、IoCの詳細

通常、相関ルールの設定は手動で行う面倒な作業ですが、Intel SecurityのSIEMシステムと他の脅威情報ツールを使用すると、このような手間を省くことができます。たとえば、セキュリティ アナリストは受信した脅威情報を分かりやすい形式で直接確認できるので、新たな脅威の詳細をすぐに把握できます。受信した脅威情報はリアルタイムまたは相関ルールによって自動的に処理されるため、進行中の不正なアクティビティや新たな脅威の検出にかかる時間を短縮できます。アラーム ビューでコンテキスト情報を見ながらIT環境全体で報告された脅威を確認し、的確な判断を行うことができるので、標的型攻撃をより正確かつ迅速に検出できます。

攻撃者はITインフラに短時間で侵入するために手口を頻繁に変えています。McAfee Enterprise Security Managerは、常に最新の情報を利用できるように、取得したすべての脅威情報を定期的に更新しています。たとえば、削除された指令サーバーをクリーンアップし、不正なレピュテーション スコアが低くなったWebサイトを自動的に消去して誤検知を防ぎ、セキュリティ担当者が実際の脅威を追跡できるようにします。

Intel Securityの以下の製品は、STIX形式の脅威情報に対応しています。

- McAfee Threat Intelligence Exchange
- McAfee Advanced Threat Detection
- McAfee Enterprise Security Manager

まとめ

Intel Securityの脅威情報統合プラットフォームは、脅威情報の収集、選択、管理を自動的に行います。手動による操作を排除し、脅威検出の精度を向上させます。これにより、ビジネスに対する被害を防ぎます。セキュリティ システム エコシステム全体で不正なアクティビティが可視化されるので、現在の標的型攻撃の被害を食い止めるだけでなく、今後発生する攻撃を未然に防ぐことができます。

詳細情報

Intel Securityの脅威情報統合プラットフォームを構成する製品の詳細については、次のサイトをご覧ください。

- **McAfee Global Threat Intelligence**
- **McAfee Threat Intelligence Exchange**
- **McAfee Advanced Threat Defense**
- **McAfee Enterprise Security Manager**
- **McAfee Enterprise Security ManagerでTAXIIフィードを使用する方法**

1. https://www.sans.org/reading-room/whitepapers/analyst/who-039-s-cyberthreat-intelligence-how-35767
2. https://www.forrester.com/The+State+Of+The+Cyberthreat+Intelligence+Market/fulltext/-/E-RES123011
3. https://www.gartner.com/doc/2941522/technology-overview-threat-intelligence-platforms
4. http://www.mcafee.com/jp/resources/reports/rp-when-minutes-count.pdf
5. https://www.rsaconference.com/writable/presentations/file_upload/cxo-t08r-threat-intelligence-is-like-three-day-potty-training.pdf

62161brf_threat-intel_1015

McAfee. Part of Intel Security.
マカフィー株式会社
東京本社　〒150-0043 東京都渋谷区道玄坂 1- 12- 1 渋谷マークシティウェスト 20F TEL 03-5428-1100（代）FAX 03-5428-1480
西日本支店　〒530- 0003 大阪府大阪市北区堂島 2-2-2 近鉄堂島ビル 18F TEL 06-6344-1511（代）FAX 06-6344-1517
名古屋営業所　〒450-0002 愛知県名古屋市中村区名駅 4-6-17 名古屋ビルディング 13F TEL 052-551-6233（代）FAX 052-551-6236
福岡営業所　〒810- 0801 福岡県福岡市博多区中洲 5-3-8 アクア博多 5F TEL 092-287-9674（代）
www.intelsecurity.com