ホワイトペーパー

McAfee
An Intel Company

レピュテーション：効果的な脅威保護の基盤

目次

エグゼクティブサマリー 3
背景 3
危険なビヘイビアの検出 4
脅威のダイナミクス 5
グレーのエンティティ 6
信頼の構築 7
レピュテーションの威力 8
Global Threat Intelligenceの流れ 9
結論 9
著者について 11
McAfee Labs™について 11
マカフィーについて 11

エグゼクティブサマリー

レピュテーションシステムは、病気を診断する医師から金融商品を評価する数学の専門家まで、さまざまな分野で長年、状態の評価と意思決定に使用されてきました。オンラインコミュニティと e コマースの黎明期から、プロバイダーとユーザーは Web 経由で商品、サービスおよび情報を取引する関係者のレピュテーションを測定する方法を模索してきました。多様なデバイスでオンラインツールにアクセスして、同僚や友人、あるいは赤の他人とオンラインで対話するユーザーが増えた今、レピュテーション算出ツールはサイバーセキュリティにとって、これまで以上に重要になっています。レピュテーションによって身元と整合性が保証されれば、インターネットをベースに個人で、または業務で安心して重要な取引が行えます。

この文書は、セキュリティの意思決定者にインターネットセキュリティのための効果的なレピュテーションシステムに関する情報を提供し、その知識を短期的なセキュリティポリシーと長期的な戦略で活用してもらうことを目的としています。この文書では以下について説明します。

- 動的な脅威とエンティティの現在の状態をリアルタイムで反映するレピュテーションの必要性
- 「完全な悪意」と「完全な善意」の間のグレーゾーンに存在するレピュテーションの考え方と静的なブラックリストやホワイトリストの保護の対比
- レピュテーション信頼性を高める 4 つの要素（データの量、データの長さ、データの信頼性および 4 つのうちで最も重要とされる幅広いデータの相関関係）

レピュテーションサービスでは、脅威の発信元を特定し、適正であるかどうかを判断します。つまり、特定のIPアドレス、Webサイトまたはメール名の会社と取引があるかどうかを確認し、もしあれば、その取引先が信頼できるかどうか判断します。大規模な脅威のインテリジェントシステムでは、数千万のエンドポイントと数百万のサーバーからのデータを分析します。

—Chris Christiansen 氏（IDC）

オンラインコミュニティとeコマースの黎明期から、プロバイダーとユーザーはWeb経由で商品、サービスおよび情報を取引する関係者のレピュテーションを測定する方法を模索してきました。そのニーズによって、軽量級のコミュニティによる投票から重量級の認証機関や認可プログラムまで、サードパーティの多様な「信頼性」モデルが生み出されました。これらのモデルでは、さまざまな方法でレピュテーションが使用されています。現在、レピュテーションベースのシステムに対するニーズが最も高いのは、ネットワーク侵入やマルウェアなど、オンラインの脅威を特定および防止するサイバーセキュリティの分野だと言われています。

背景

*4 月 30 日午前 9 時 56 分、ユーザーが動画を投稿したり、検索または視聴できる Web サイト、www.multimedia***.com が新しく登録され、オンラインで公開されました。この Web サイトは新たに登録された 160 ドメインのグループに含まれ、McAfee Global Threat Intelligence のセンサーネットワークとデータフィードによって特定されました。これらのドメインの多くはメディア共有サイトの悪用を目的にしながら、善意を装っていました。それでも、当社がシステムのレピュテーションを「高リスク」に変更する手がかりが 1 つありました。それは、何だったのでしょうか。*

Wikipedia ではレピュテーションを「人、人の集まり、または組織に対するエンティティのグループの一定の基準に基づいた評価（専門的には社会的評価）」と定義しています [1]。マカフィーではファイルから送信者や Web サイトまで、インターネット上に存在するエンティティのレピュテーションを長年処理しているため、その間に当社の定義は拡大され、それ以上の要素が含まれるようになりました。

まず、レピュテーションは動的かつ一時的なものです。たとえば、善意の Web サイトがマルウェアに感染し、その後、すぐに駆除される場合があります。このような場合、コンテンツを修正したら、レピュテーションもすぐに修正する必要があります。また、レピュテーションでは「完全な善意」や「完全な悪意」と評価されることはほとんどなく、大半はその中間のグレーゾーンに位置するため、レピュテーションとポリシーを組み合わせてセキュリティ上の対応を判断します。また、レピュテーションを算出する場合、信頼性は必要不可欠です。信頼性とは、この場合、信頼区間または計算の信頼性を意味します。分析で考慮するデータポイントと評価基準が多ければ多いほど、レピュテーションの正確性も向上します。信頼性を向上させる要素には、データの量、データの長さ、データの信頼性およびデータの幅広い相関関係の 4 つがあります。

1「レピュテーション」（Wikipedia、http://en.wikipedia.org/wiki/Reputation）

マカフィーでは、ビヘイビア、特徴、当社が経験したエンティティのビヘイビアの比較をベースにした詳細な評価システムを使用して、インターネット上の数億のエンティティ（ファイル、Webサイト、Webドメイン、メッセージ、DNSサーバー、ネットワーク接続）のレピュテーションを算出しています。当社が使用するさまざまなデータの中には、テレメトリデータも含まれます。マルウェア対策のクライアント、Webやメールのゲートウェイ、ファイアウォールなどのマカフィー製品は、世界中に数千万単位で配置され、クラウドベースの分析エンジンのセンサーとして毎日数十億のクエリを処理しています。たとえば、ネットワーク接続のレピュテーションでは、IPアドレスの寿命、使用しているポートとプロトコル、ネットワークアクティビティと予測されるビヘイビアの基準値の比較、攻撃の履歴、他の既知のIPとの関係など、数千の属性やビヘイビアを確認します。

危険なビヘイビアの検出

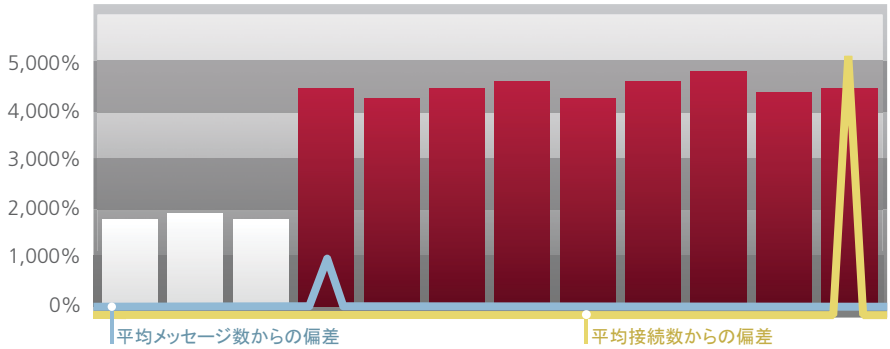

図 1：マカフィーのレピュテーションシステムでは IP アドレスの危険なビヘイビアなどが監視され、そこからお客様に送信されるメッセージがプロアクティブにブロックされます。

上記の図1は、当社のシステムによって分散型サービス拒否攻撃が予測される異常なビヘイビアが検出され、そのレピュテーションが変更されたインスタンスを示しています。青い線はIPアドレスの平均メッセージ数からの逸脱を示しています。グラフの最初の3分の1で発生したメッセージの逸脱によって、接続のレピュテーションスコア（垂直のバー）が上がり、「未検証」（グレー）から「高リスク」（赤）に変更されています。実際に攻撃が実行された場合、IPアドレスの平均接続数（黄色の線）からの逸脱によって示され、この「高リスク」のレピュテーションスコアがマカフィー製品に通知され、お客様を保護するためにそのメッセージがブロックされます。

レピュテーションはすべてのセキュリティシステムにとって、単なる重要なコンポーネントではなく、必須のコンポーネントです。脅威の動きは速すぎたり、目立たなかったりするため、シグネチャベースの保護やブラックリストなど、従来の手法に頼ることはできません。脅威の目的が可能な限り多くのコンピューターを攻撃することである場合、シグネチャが作成されて配置されるよりはるかに早く拡散します。また、ブラックリストソリューションはレピュテーションスコアでは識別される微妙な差異が識別されません。急速に拡散する脅威が存在する一方で、標的を絞った脅威の中には、検出されないように影響を最小限に抑えて、微小な目的を達成するものもあります。このような極端な攻撃（およびその中間に位置する攻撃）に対抗するには、エンティティに関する総合的な情報をベースにリアルタイムでレピュテーションを算出し、そのレピュテーションに基づいてアクションを実行するシステムが必要だということにセキュリティ専門家とベンダーは気づいています。

オペレーションオーロラは2009年後半から2010年前半にかけて、Googleをはじめとする20社以上の企業を攻撃しましたが、この攻撃では特定の個人を標的にしていました。攻撃者は検出が困難な高度な技術を使用して、標的とするユーザーのマシンにアクセスし、そこから、会社の重要な情報や知的財産にアクセスしました。検出を巧妙に回避するオペレーションオーロラのような脅威には、たとえば、ユーザーに疑われないようマルウェアに感染したWebサイトへおびきだすために、一時的に悪用したIPアドレスから送信されたメールなど、関連するエンティティが少数ながらあり、そのレピュテーションは一瞬のうちに変更されます。マカフィーではこのようなレピュテーションの変更を利用して、不正なアクティビティを自動的に検出および防止して、重要なユーザー、資産、情報を保護しています。

脅威のダイナミクス

急速に変化するインターネットの脅威には、そのダイナミズムを考慮したレピュテーションシステムが必要です。エンティティに関する情報量が増えたら、その情報を使用して、エンティティのレピュテーションを継続的に変更する必要があります。たとえば、コンピューターがトロイの木馬に感染して、スパムを送信するボットネットに利用された後、短時間で駆除されて安全な状態に戻ったとします。この場合、低リスクから高リスク、そしてまた低リスクへと、コンピューターの状態はわずか数分で元に戻っています。レピュテーションシステムは、このようなコンピューターの変化をすばやく検知して、その状態を正確に反映できなければ効果的とは言えません（図 2 参照）。

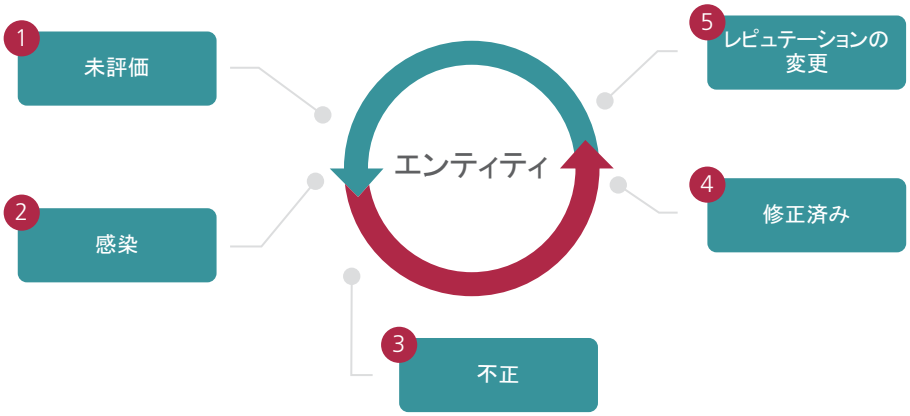

図 2：効果的なレピュテーションシステムでは、エンティティの状態が短時間で変化しても認識されます。

クエリとその応答は、レピュテーションスコアの重要なデータです。効果的なレピュテーションシステムは適切に設定された数百万の製品で構成され、ローカルの製品がトリガされると、これらの製品によってレピュテーションシステムにクエリが送信され、システムの応答を利用してローカルのアクションを判断するというフィードバックループを形成しています。また、エンティティのレピュテーションは、クエリと応答の量と頻度によっても変更されます。たとえば、新しい IP アドレスがオンラインで使用され、そのアドレスで十分な量のメッセージが送信されると、世界中に配置されたメールゲートウェイからそのメッセージに関するクエリがレピュテーションシステムに送信され、システムによってその IP はスパムを送信している可能性が高いと判断され、その接続のレピュテーションが変更されます。同様に、感染したエンティティの駆除が終わると、レピュテーションシステムには駆除後の状態が反映されます。

データポイントが追加されるたびにレピュテーションシステムは自動的に変更されます。そのため、マルウェアのテストやネットワーク攻撃の「ドライラン」を実行したサイバー犯罪者は、気づかないうちにその活動をシステムに警告することになります。効果的なレピュテーションシステムの前では、サイバー犯罪者はマルウェアのテストを途中で断念するか、ツールをテストせずに攻撃するか、いずれかを選択せざるをえません。いずれにしても、犯罪者が不利な状況に追い込まれることに変わりありません。

当社は急速に拡散する脅威から潜行型の脅威まで、あらゆるサイバーセキュリティ製品を取り扱っているため、優れたレピュテーションシステムによって効率的にデータを収集して、大量のデータを迅速に分析し、その結果を即時、世界中のコンピューターに配布する必要があります。この 3 つのうち 1 つか 2 つの次元が最適化されたコンピューターシステムは世界には数多くありますが、3 つのすべてに対応したシステムはほんのわずかです。

グレーのエンティティ

*www.multimedia***.com などのドメインが悪意であることを知る手がかりとは何だったのでしょうか。それは、ドメインのビヘイビアと予測の比較です。たとえば、そのメディア共有サイトのドメインの中には、一般的なメディア共有サイトのトラフィックパターンと異なるドメインがありました。正常なドメインもありましたが、ホスティングドメインに似たドメインもありました。このようなモデルは通常、トラフィックを転送して、スパムを送信する IP アドレスをわかりにくくしたり、マルウェア実行ファイルやボットネット制御の指示、個人情報のフィッシングに使用されます。また、突然、異なる IP アドレスに変更されたドメインもありましたが、これは Fast Flux と呼ばれ、検出を逃れるために使用されます。そのほかに、IP アドレス間を同時に移動するドメインもありましたが、ビヘイビアが同時に起こる場合は、それらのドメインが単一のエンティティに操作されていることを示しています。このようなビヘイビアが確認されると、当社のシステムでは、そのドメインのレピュテーションは「高リスク」に格下げされます。*

レピュテーションシステムはブラックリストとホワイトリストの技術とは異なります。前者が「善意」と「悪意」の間のグレーゾーンを扱うのに対し、後者は静的で、管理者が一定間隔で追加と削除を行います。一方、レピュテーションはシステムが新しいエンティティを「学習」するたびに変更されるため、本質的に動的です。エンティティが多数存在し、それらのレピュテーションが動的であれば、100% 正確に見極めることはほとんど不可能です。システムのスキャンを終えて、善意であるか悪意であるか判断する頃には状態は変化しています。レピュテーションシステムを使用すると、セキュリティ製品の一瞬の判断で常に最良の回答が得られるようになります。このような不確実性が存在する場合、レピュテーションシステムを使用しないと、脅威のブロックに過不足が生じます。効果的なレピュテーションシステムでは、たとえば、ブラックリストよりも誤認識の少ない動的なレピュテーションが導き出されるため、管理者はより正確な情報を使用できます。そのため、グレーゾーンが問題になる場合でも、動的なレピュテーションスコアによってポリシーを遵守できます（図 3 参照）。

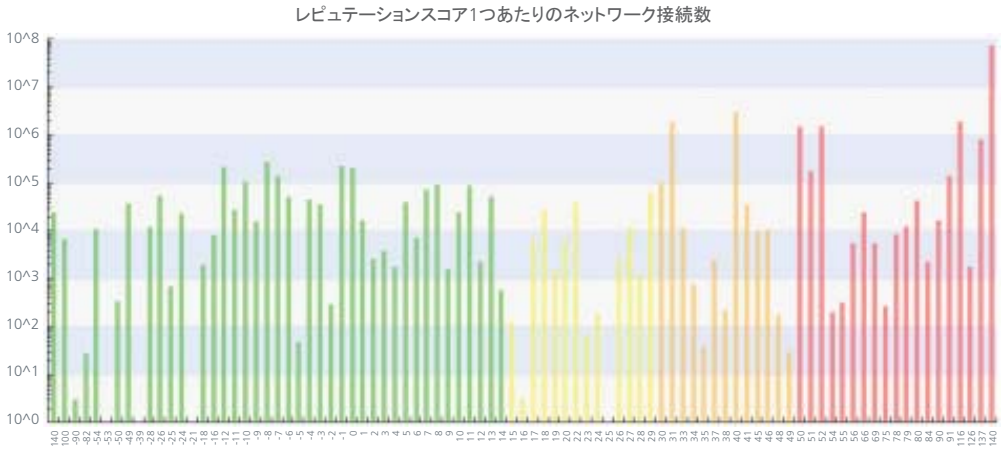

図 3:このグラフはマカフィーのレピュテーションスコアシステムの詳細さを示しています。連続体（x 軸）のレピュテーションスコアのそれぞれに対して追跡するネットワーク接続を示しています。y軸は対数尺度で示していますが、ある時点における各レピュテーションの接続数です。接続のリスクレベルをスコアによって、緑（低い）、黄色（未検証）、オレンジ（中程度）、赤（高い）で色分けしています。

ファイルのブロックやネットワーク通信の抑制など、セキュリティ関連の対応が必要かどうかを判断する要素はいくつかあります。それには、組織のリスクプロファイル、生産性の要件、誤認識の許容範囲、資産の重要性、代替のセキュリティ対策が含まれます。レピュテーションシステムでは一貫した客観的な評価が可能になり、意思決定者は組織に固有のリスクと特質評価に基づいてポリシーを設定できます。そのため、インフラストラクチャーではポリシーに従って自動的にアクションが実行されます。

信頼の構築

当社は白か黒かが明確なエンティティよりも、グレーのエンティティを扱うことが多いため、レピュテーションの信頼性レベルを高めることは重要です。セキュリティの専門家やその組織が可能性に基づいて動的なポリシーを策定する場合、レピュテーションスコアが重視されます。そのため、レピュテーションシステムのスコアには、最高レベルの信頼性が求められます。また、スコアを算出するときに考慮する次元が増えれば増えるほど、信頼性は高くなります。

医療の診断と比べてみましょう。医師は患者の病気をどのようにして診断するのでしょうか。一連の手順に従いますが、それぞれの手順は仮説を検証すること、または、仮説が正しいという確信を深めることのいずれかを目標にしています。医師は患者に症状を尋ねてから熱を測ります。この2つの行為によって、問題の概要を把握します。そして、その情報を新しいデータ、たとえば血圧などと関連付けることで、医師は仮説に対する確信を深めます。確信を深めるために、10以上の症状（次元）を確認する場合もありますが、実際にはそれだけでは不十分で、それらの症状を相互に関連付けてはじめて、医師は診断が正しいことを確信できます。また、この例えを一歩進めると、医師は予測することもできます。ある患者を診断した後、10分間に同じ症状の患者10人が診察室を訪れたら、1つの診断を他の患者にも適用できます。さらに、次の患者が現れる前に病気を予防するための行動を起こすこともできます。

同様に、サイバーセキュリティのレピュテーションシステムにとっても、多次元でデータの相関関係を示すことは重要です。複数の次元で相関関係を示すことにより、信頼性が向上することを説明するため、図4では、不正な（赤）IPアドレスと正当な（緑）IPアドレスを使用した3つのグラフを並べています。最初のグラフでは、単一の次元であるメッセージの量とIPを示しています。このグラフでは、両者の違いがわかりにくいため、間に線を入れています。2番目のグラフでは、2番目の次元であるIPアドレスの持続性（IPアドレスが継続して存在すること）を示していますが、それによって、データの区別が明確になり、データポイントが属するグループをより正確に判断できます。3番目のグラフでは、3番目の次元であるIPアドレスの受信者の幅を示していますが、データの微妙な差異がより明確になり、IPは簡単に識別できるクラスタで表示されるため、予測はより正確になります。当社の実際の分析では、1000以上の次元に基づいてデータを評価し、レピュテーションスコアの信頼性レベルを向上させています。

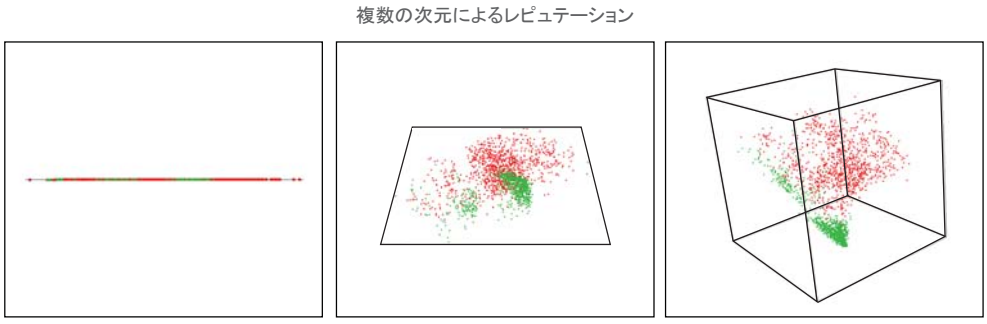

図 4：レピュテーションスコアに次元を追加すると、スコアの信頼性レベルが向上します。

多次元のレピュテーション分析を効果的に行うには、幅広いソースから必要なデータを十分に収集する必要があります。マカフィーでは、クラウドベースの情報の基盤として世界中に配置された当社製品からデータを収集して、レピュテーションシステムにフィードしています。テレメトリデータは効果的なレピュテーションシステムの基盤となりますが、信頼性レベルを設定するため、以下でも使用されます。

- **データの量**：受信したクエリがシステム全体に影響するデータポイントになる場合、データが多いほどレピュテーションスコアの信頼性は高くなります。望遠鏡のレンズもデータ量（光）が増えれば増えるほど、天体を詳細に見ることができます。マカフィーでは、クラウドベースのインテリジェントシステムで毎日数十億のクエリを受信しているため、脅威のアクティビティを迅速に検出し、優れた正確性で特定することができます。
- **データの長さ**：長期間データを収集すると、システムが成熟します。成熟したレピュテーションシステムでは、同一または類似のエンティティの過去のビヘイビアに基づいて、確かな基準を策定して予測に使用できます。それによって、異常を検出できるだけでなく、認識済みのパターンに基づいて攻撃を特定できます。
- **データの信頼性**：レピュテーションシステムにとって、データの信頼性は重要です。大量のデータ収集と自動化されたデータ分析の手法によって、ユーザーの共謀など、感染源を知る機会が提供されます。レピュテーションシステムには、受信するデータを認証し、ソースの信頼性を変更するメカニズムが必要です。データソースの場所、設定および過去のビヘイビアなどの要素は、レピュテーション算出におけるそのソースのデータの比重に大きく影響します。
- **データの相関関係**：レピュテーションシステムにとって最も重要なのは、あらゆる脅威媒体を網羅した幅広いソースからテレメトリデータを収集して関連付ける機能です。マカフィーでは、エンドポイントのマルウェア対策、Web とメールのゲートウェイ、境界のファイアウォール、侵入防止システムなど、当社の幅広い製品を活用して、ファイル、Web、メール、ネットワーク、アプリケーションなど、あらゆる側面から脅威を検出しています。データの相関関係を構築できれば、脅威を全方向から確認できるため、ジグソーパズルのすべてのピースを手に入れたことになります。

レピュテーションの威力

あらゆる脅威媒体からテレメトリデータを収集できると、脅威に対する理解が深まり、脅威に関係するすべてのエンティティのレピュテーションの正確性が大幅に向上します。図 5 では、マカフィーが 1 つの脅威媒体から収集したテレメトリデータを使用して、他の脅威媒体の脅威を特定し、そのレピュテーションシステムを更新してお客様を保護するまでを示しています。当社のレピュテーションシステムには、マルウェア、Web の脅威、ネットワーク接続、メールメッセージなどに関する情報を求めて、世界中のセンサーからクエリが送信されます。たとえば、当社のマルウェア対策クライアントからは、ファイルのハッシュ（フィンガープリント）をベースにしたファイルレピュテーションのクエリが送信されます。クエリの数、頻度および地理的分布によって、当社はマルウェアのファルがない場合でも高レベルの信頼性を維持しています。当社のレピュテーションシステムがスコアを返すと、マルウェア対策のクライアントソフトウェアによって該当するファイルのブロックや検疫が実行されます。たとえば、未知の IP アドレスのメール送信者が、同じハッシュのファイルを添付したメールを当社のメールゲートウェイの 1 つを経由してユーザーに送信したとします。その場合、ゲートウェイから当社のクラウドにクエリが送信され、それがマルウェアであると確認されるとそのメッセージはブロックされます。当社のシステムでは、ハッシュのファイルをホストする Web サイトがデータベースで検索され、その Web サイトのレピュテーションと関連するネットワーク接続が「高リスク」に変更され、マルウェアのファイルが回収されて処理されます。また、当社のマルウェア対策クライアントでは、メールおよび Web のゲートウェイ、ファイウォールによってレピュテーションシステムにクエリが送信され、使用された媒体を問わずその脅威がブロックされます。

Global Threat Intelligenceの流れ

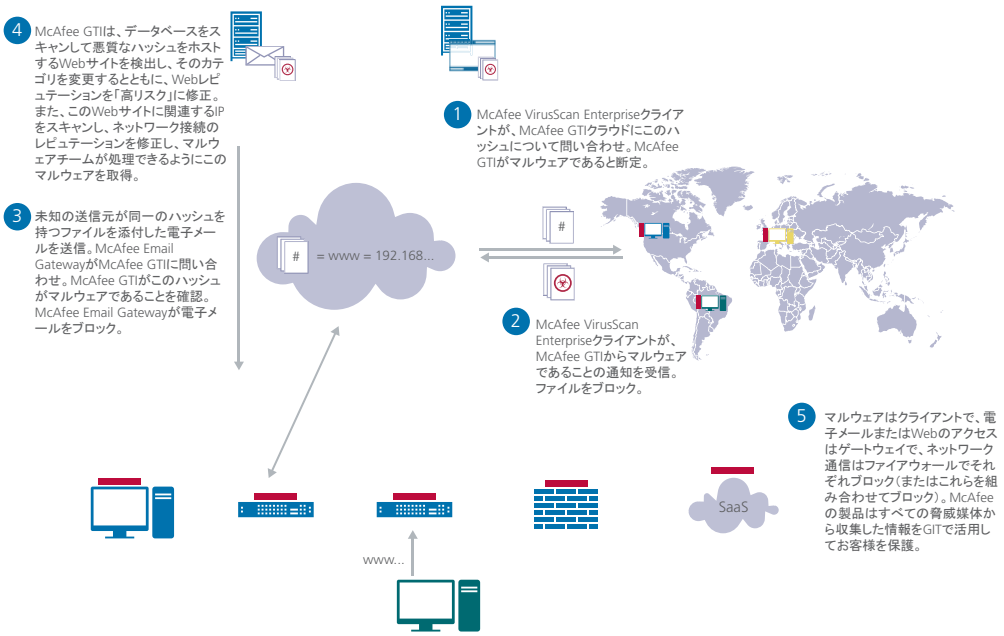

図 5：脅威の媒体問わず、マカフィー製品ではクラウドベースのインテリジェンスにクエリが送信され、新しい脅威は損害を与える前に阻止されます。

結論

*結局、www.multimedia***.com と他の 159 の疑わしいドメインは、Zeus ベースの拡散型フィッシング攻撃を目的としていました。Zeus はパスワードを盗むトロイの木馬の作成で有名なアプリケーションです。不正なドメインは、実際にはログイン情報を盗むためのフィッシングサイトでした。当社はこのドメインに「関係する」多くのエンティティを調査しました。IP をホストするドメイン、そのドメイン内の URL が埋め込まれたリンク、そのドメインでホストするマルウェアファイルなどです。これらのエンティティを分析し、システムでそのレピュテーションを「高リスク」に変更したため、企業と消費者の環境にローカルでインストールされたマカフィー製品によって、その脅威は配信方法にかかわらず、完全に阻止されました。*

現在のサイバーセキュリティには洗練された高度な保護が必要とされ、優れたレピュテーションシステムはそのような保護にとって必須の要素です。レピュテーションベースのセキュリティは新しい概念ではありませんが、急速に拡散するウィルス、ターゲットを絞った潜伏型の IP の悪用、またはその中間に位置する攻撃など、脅威の数は急増しています。このような課題を解決するには、客観的で一貫性のあるセキュリティの枠組みによって、動的なエンティティの状態を把握および評価する必要があります。テレメトリデータの相関関係に基づいてエンティティの状態を優れた信頼性で示す情報は、包括的な保護を提供する上で必要不可欠です。

レピュテーションの算出

マカフィーのクラウドベースのレピュテーションシステムでは、次の方法でインターネット上のエンティティのレピュテーションを算出しています。このレピュテーションを当社製品のポリシーと組み合わせて使用すると、セキュリティ専門家は組織のリスクとビジネスニーズに基づいて的確な意思決定が行えます。

ファイルレピュテーション: マカフィーのクラウドベースのシステムでは、毎日約20億のファイルレピュテーションのクエリ(ファイルのハッシュ使用)を受信し、ファイルがマルウェアである可能性を示すスコアを返しています。そのスコアは、マカフィーのクラウドに問い合わせたセンサーから収集した情報や、McAfee Labs™の研究者と自動化ツールが実行した分析だけでなく、Web、メールおよびネットワークの脅威データからの媒体の相関関係に関する情報もベースにしています。マカフィーのローカルのマルウェア対策エンジンでは、エンドポイントのマルウェア対策やゲートウェイなどのソリューションの一部として導入されている場合でも、ローカルポリシーに基づいた処理(ブロック、検疫、無視など)の判断にはこのスコアが使用されます。

Webレピュテーション: マカフィーのクラウドベースのシステムでは、毎日80億のWebレピュテーションのクエリを受信し、URL、WebドメインまたはDNSサーバーが不正(フィッシングサイト、マルウェアに感染など)である可能性を示すスコアを返しています。そのスコアは、マカフィーのクラウドに問い合わせたセンサーから収集した情報や、McAfee Labsの研究者と自動化ツールが実行した分析だけでなく、ファイル、メールおよびネットワークの脅威データからの媒体の相関関係に関する情報もベースにしています。McAfee Web Gatewayなど、マカフィーのローカル製品では、このスコアをローカルのエンジンと組み合わせて、ローカルポリシーをベースに対応が判断されます。マカフィーではURLのレピュテーションをだけでなく、ドメイン、関連するIPアドレス、DNSサーバーのレピュテーションも算出しています。

メッセージレピュテーション: マカフィーでは毎日2.6億のメールクエリを受信し、メッセージコンテンツ(個人情報になる内容とは異なります)のフィンガープリントを採取し、さまざまな次元で分析しています。メッセージレピュテーションでは、スパム送信パターンなどの要素とIPの動作を組み合わせて、問題のメッセージが不正なメッセージ(スパム、マルウェアなど)である可能性が判断されます。そのスコアは、マカフィーのクラウドに問い合わせたセンサーから収集した情報や、McAfee Labsの研究者と自動化ツールが実行した分析だけでなく、ファイル、Webおよびネットワークの脅威データからの媒体の相関関係に関する情報もベースにしています。メールゲートウェイなど、マカフィーのローカル製品では、ローカルポリシーをベースにした対応の判断にこのスコアが使用されます。

ネットワーク接続のレピュテーション: マカフィーは、550億のIPアドレスとネットワークポートからデータを収集し、数百兆にのぼる一意のビューを提供します。また、ポート、宛先、プロトコル、インバウンド/アウトバウンド接続要求を含むネットワークトラフィックに関するデータに基づいて、レピュテーションスコアを計算します。そのスコアには、ネットワーク接続が脅威となる可能性(ボットネット制御に関連付けられた接続など)が反映されます。そのスコアは、マカフィーのクラウドに問い合わせたセンサーから収集した情報や、McAfee Labsの研究者と自動化ツールが実行した分析だけでなく、ファイル、Webおよびネットワークの脅威データからの媒体の相関関係に関する情報もベースにしています。ファイアウォールや侵入防止システムなど、マカフィー製品では、ローカルポリシーをベースにした対応の判断にこのスコアが使用されます。

McAfee Labs™について

McAfee Labs は、世界各地に存在する McAfee の研究機関で、マルウェア、Web、メール、ネットワークなどに対する脅威を研究・調査し、脆弱性の報告を行っています。McAfee Labs は、世界各地に数百万台のセンサーを配備し、クラウド型サービスの McAfee Global Threat Intelligence™により情報収集を行っています。世界 30 か国に存在する McAfee Labs には、様々な分野を専門とする 500 名の研究者が在籍し、企業や一般のユーザーを保護するため、リアルタイムの脅威検出、アプリケーションの脆弱性特定、リスクの相関分析、迅速な問題解決に努めています。

マカフィーについて

マカフィーは、インテルコーポレーション（NASDAQ：INTC）の完全子会社であり、企業、官公庁・自治体、個人ユーザーが安全にインターネットの恩恵を享受できるよう、世界中のシステム、ネットワーク、モバイルデバイスを守るプロアクティブで定評あるセキュリティソリューションやサービスを提供しています。マカフィーは、Security Connected 戦略、セキュリティにハードウェアを活用した革新的なアプローチ、また独自の Global Threat Intelligence により、常に全力でお客様の安全を守ります。詳しくは、http://www.mcafee.com/jp/ をご覧ください。マカフィーでは、セキュリティに関する様々な研究成果や調査結果を web 上で公開しています。詳しくは下記ページをご覧ください。

http://www.mcafee.com/japan/security/publication.asp

McAfee
An Intel Company

マカフィー株式会社
www.mcafee.com/jp

●製品、サービスに関するお問い合わせは下記へ

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エスト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　〒460-0002　愛知県名古屋市中区丸の内3-20-17 中外東京海上ビルディング3F
TEL：052-954-9551(代)　FAX：052-954-9552

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)　FAX：092-287-9675