

Cloudmark Sender Intelligence:ネットワーク・エッジで高度なセキュリティを実現

機能と利点

スパム送信元をグローバルに識別

Cloudmark のユーザからは、各 IP アドレスから受信したメッセージの数やスパムまたは正規メッセージの分類など、受信メッセージに関する価値ある統計情報が報告されます。Cloudmark Sender Intelligence(CSI)では、世界各国の 100 社以上のサービス・プロバイダと 35,000 社の企業から送られてくるこれらの包括的なデータを利用して解析を行い、スパム送信元を識別する仕組みになっています。

攻撃と脅威を完全に追跡

CSI では、Global Threat Network を使用して送信者の行動を追跡し、評価スコアを調整します。その際、Global Threat Network は、大規模および小規模の攻撃のほか、複数の送信者から次々と仕掛けられる攻撃を追跡するのに必要な情報を CSI に供給する役割を果たします。

トラフィックをユーザ別に解析

Cloudmark のセキュリティ運用タスク・フォース・チームは、トラフィックをユーザ別に手動で解析して、CSI による自動解析を補完し、将来起こり得る攻撃を確実に防止します。

リアルタイムの解析

CSI では、Cloudmark の Global Threat Network からのフィードバックを利用して、トラフィック・パターン、フィードバック、フィンガープリント関連統計情報を解析し、送信者の評価スコアをほぼリアルタイムに算出し調整することができます。

保護機能を動的に更新

CSI では、データをリアルタイムに更新する仕組みになっているため、ユーザはアップデートを数分以内にダウンロードすることができます。従来のテクノロジーでは、アップデートのダウンロードに 30 分以上の時間がかかると同時に、メッセージごとにインターネット・クエリが発行されることが多いため、スパム送信者に悪用される遅延を招く恐れがあります。

サービス・プロバイダの多くは、スパム攻撃に対する第一段階の防御策としてプロトコル・レベルのフィルタリングを採用しています。しかし、現在ではスパム、フィッシング、ウィルスの攻撃が複雑化しているため、メッセージング・トラフィックを自動的にかつきめ細かくフィルタリングできる方法を探し求めているサービス・プロバイダが規模の大小を問わず増えています。また、従来の DNSBL はこうしたポリシーの基本的なレベルを把握する際に有効な手段となりますが、評価データを利用してプロトコル・フィルタリングを効率的に制御できる、より包括的な方法が必要とされているのが現状です。Cloudmark Sender Intelligence™ (CSI) は、従来の送信者評価サービスに新たなセキュリティ層を追加し、スパム、フィッシング、マルウェアの攻撃を阻止する包括的な送信者評価サービスです。この CSI サービスでは、グローバルなデータ・セットと、サービス・プロバイダのユーザから送られてくる特別なフィードバック情報を連携させ、専門家の手動の解析によって CSI の自動解析を補完することにより、サービス・プロバイダのインフラを襲う現在および将来の攻撃を確実に防止します。CSI のデータをエッジ・メール転送エージェント (MTA) などのネットワーク境界機器に組み込めば、メッセージング・インフラのセキュリティも確保できます。

CSI では、送信者の特徴を正確に表すプロファイルを、様々なデータ・ソースを解析して作成することができます。また、8 億 5,000 万個以上のメールボックスと、数百万のハニーポット・ソースで構成される巨大な Global Threat Network™ のほか、Cloudmark 独自の様々な送信者識別システムとサードパーティのデータを利用して、送信者を評価できるだけでなく分類することも可能となっています。これらの送信者識別システムには、ニュース・レターの送信者を識別する Newsletter Sender Logic、公開メールフォワードを識別する Mail Forwarders Identification、サービス・プロバイダの動的 IP アドレス範囲に特定の IP が含まれていることを確認する役割を果たす Dynamic Space Analysis などがあります。なお、CSI は送信者の評価、総数計算、分類に必要な詳細かつ正確なプロファイルを作成して、きめ細かいポリシーを策定し、検出精度の向上が図れる高度な解析機能もサポートしています。また、ネットワークとセキュリティに関する幅広く高度なノウハウを持つ当社の専門家が展開する CSI では、他の送信者評価サービスで検出不可能な送信者も識別し、従来のサービスで見逃していたメッセージのうち半分をフィルタリングできます。

Cloudmark の特長

送信者を迅速かつ正確に識別

大半の送信者評価サービスでは、トラフィック・パターンの統計情報のみを利用してしています。これは、評価を確実に行うには有効かもしれませんが、受動的な方法であるため遅延を招き、新種のスパムの攻撃に脆弱になってしまいます。しかも、ボットネットを増殖させると同時に、動的 IP を利用してスパムを生産する攻撃者が増えているため、トラフィック・パターンの解析だけではもはや不十分です。

一方、CSI では、フィンガープリント関連統計情報のほか、Cloudmark 独自のデータ・ソース、ユーザやハニーポットからのフィードバック情報を利用して、スパム送信者と正当な送信者を迅速に識別し、脆弱な「すき間」をふさぎます。また、ゼロ・アワー攻撃を受けた場合には、適切なトラフィック・パターンの統計が出る前に、スパム・メッセージと正規のメッセージに含まれる様々なフィンガープリントの相関関係を解析し、不審な行動を確実に検出します。

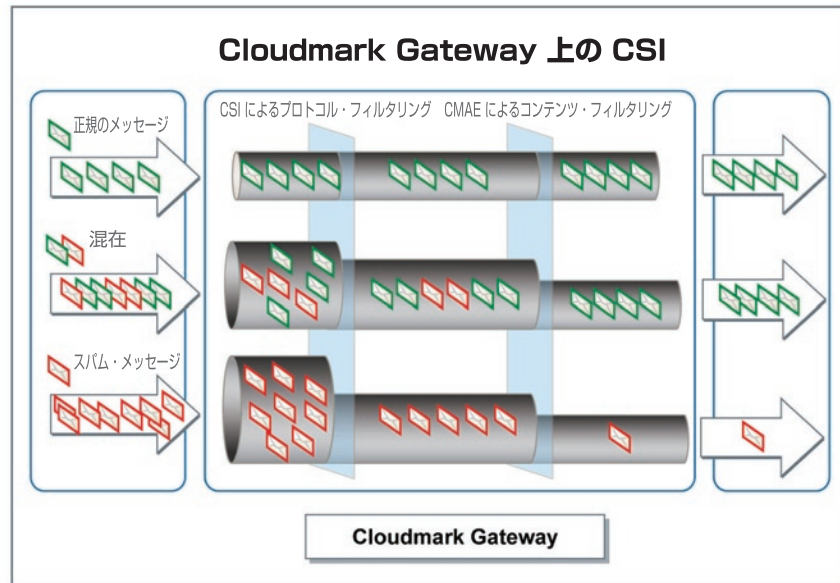
標的型攻撃を阻止できる唯一のサービス

Cloudmark の Security Operations Center は、サービス・プロバイダのデータに焦点を絞り、独自の方法で標的型攻撃を阻止することができる多数の電子メール・セキュリティ専門家を擁しています。この専門家チームは、サービス・プロバイダ固有の環境に仕掛けられる攻撃を未然に防止する対策を講じ、IP 評価データのベース・レベルを解析しただけでは得られない成果を上げています。こうした実績を持つ Security Operations Center を運営する当社の CSI は、標的型攻撃を阻止できる唯一の送信者評価サービスです。

Cloudmark Gateway とシームレスに統合された CSI

Cloudmark Gateway では、CSI の送信者評価データに基づいて、特定の送信者にポリシーを自動的に適用します。Cloudmark Gateway は接続要求を受けると、最初に CSI のローカル・コピーを検索し、送信者評価などのデータを CSI から受信します。次に、この送信者に適したポリシーを適用し、設定済みの処理を行います。通常、評価スコアの低い送信者には十分な帯域幅を割り当てますが、評価スコアの低い送信者に対しては帯域幅を制限します。

このように、送信者評価に基づいて接続を完全に制御できるため、ネットワークに侵入する悪意のあるコンテンツをきめ細かくブロックすることができます。また、CSI とシームレスに統合された Cloudmark Gateway では、IP アドレス単位だけでなく、共通の評価スコアや評価特性を共有する IP アドレス・グループ単位で抑制することも可能です。



Cloudmark Gateway では、CSI の送信者評価データを利用してトラフィックを制御する仕組みになっています。この CSI を導入すれば、悪意のある送信者からの接続は切断し、疑わしい送信者からの接続は抑制し、さらに正当な送信者からの接続は遅延なく許可するといったように、法令や社内ポリシーに準拠したインテリジェントな接続およびフロー制御を実現できます。



詳細は www.cloudmark.com をご覧ください。

<p>日本事業所 クラウドマーク ジャパン 〒107-0052 東京都港区赤坂 4-13-5 赤坂オフィスハイツ 131 電話：03-6277-8816 Fax: 03-6277-8829 電子メール：japan@cloudmark.com</p>	<p>北米事業所 Cloudmark, Inc. (本社) 128 King Street, 2nd Floor San Francisco, CA 94107 USA 電話：+1-415-543-1220 Fax: +1-415-543-1233</p>
--	--