

SPAMTEQ™ とは?メールセキュリティ

スパムの問題は無くなることはありません。大量の未承諾広告メッセージ送信を目的とし、リソースを使い尽くす「アフィリエイトスパム」から、今日ではサイバー犯罪者が Eメールを利用してターゲットを絞ったマルウェアやランサムウェアを配信する在り方へと進化してきました。データを盗み、詐欺を行い、ネットワークを不正利用しようと狙っています。サイバー犯罪者は量と速度に依存するため、インターネット上の生きた情報源から得た Spamhaus のリアルタイム脅威インテリジェンスは、お客様にとって最善の防御となります。

世界の Eメールの
90%はスパムメールです



スパムのトレンド



Hailstorm

1つの IP アドレスから
大量・高速



Snowshoe

複数の IP アドレスから
少量・低速

スパムの運業者

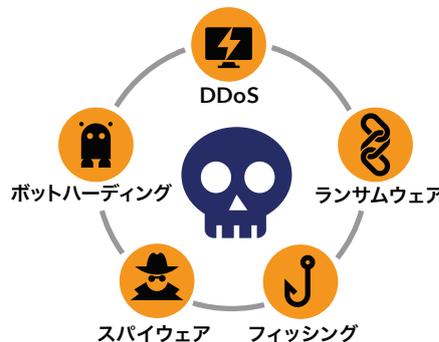


エイリアス、アドレス、リダイレクト、サーバーの所在地、ドメインまた DNS 設定で追跡すると**100のスパム業者**のうちアメリカとヨーロッパだけで**80%**を占めています

現在活動中のスパム業者を持つ上位10ヶ国
Spamhaus 調べ



スパムは単なる迷惑メールではありません



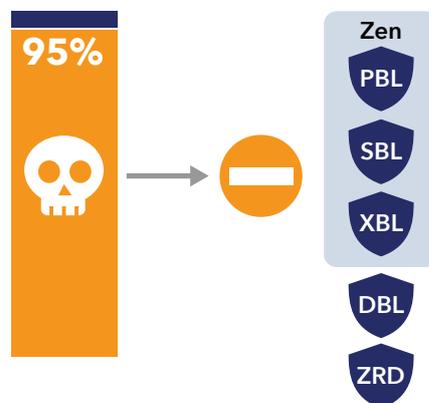
少なくとも
40%のサイバーセキュリティ脅威がEメールから来ていると考えられています

プロアクティブな防御

Spamhaus のデータフィードサービスは、実際の脅威となる前にスパムをブロックするために必要な情報を提供します。

- Zen PBL** ポリシーブロックリスト (Policy Block List)
Eメールを送るべきでないエンドユーザーのデバイス
例: スマートテレビ、家庭用ルーター
- SBL** Spamhaus ブロックリスト (Spamhaus Block List)
未承諾 Eメールの配信に関係している IP アドレスの範囲
- XBL** eXploits ブロックリスト (eXploits Block List)
マルウェア、ウォーム等に感染またはポットネットに制御されているデバイス
- DBL** ドメインブロックリスト (Domain Block List)
スパム業者を識別するドメインベースの情報
- ZRD** ゼロレピュテーションドメイン (Zero Reputation Domain)
レピュテーションが確立されるまで、新しいドメインを 24 時間ブロックします。

Spamhaus は 3,000,000,000 個以上の
メールボックスを日々守っています



95%以上のスパムが、メールサーバーに到達する前にSMTP 接続時に阻止されます

リアルタイムの脅威インテリジェンスの目標は誤判定をゼロにすることです