# セキュリティ脅威のランドスケープ

## 2018年下半期

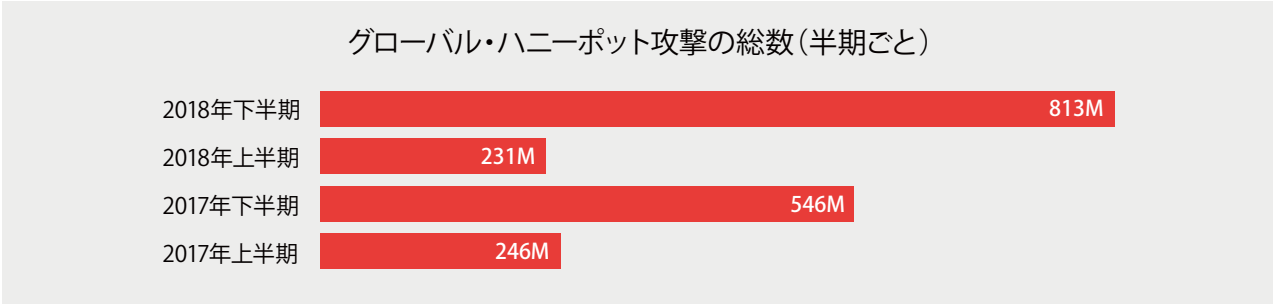
エフセキュアのハニーポットのグローバルネットワークによる
攻撃トラフィックの可視化

2018年3月

F-Secure

# 攻撃トラフィックが4倍に増加

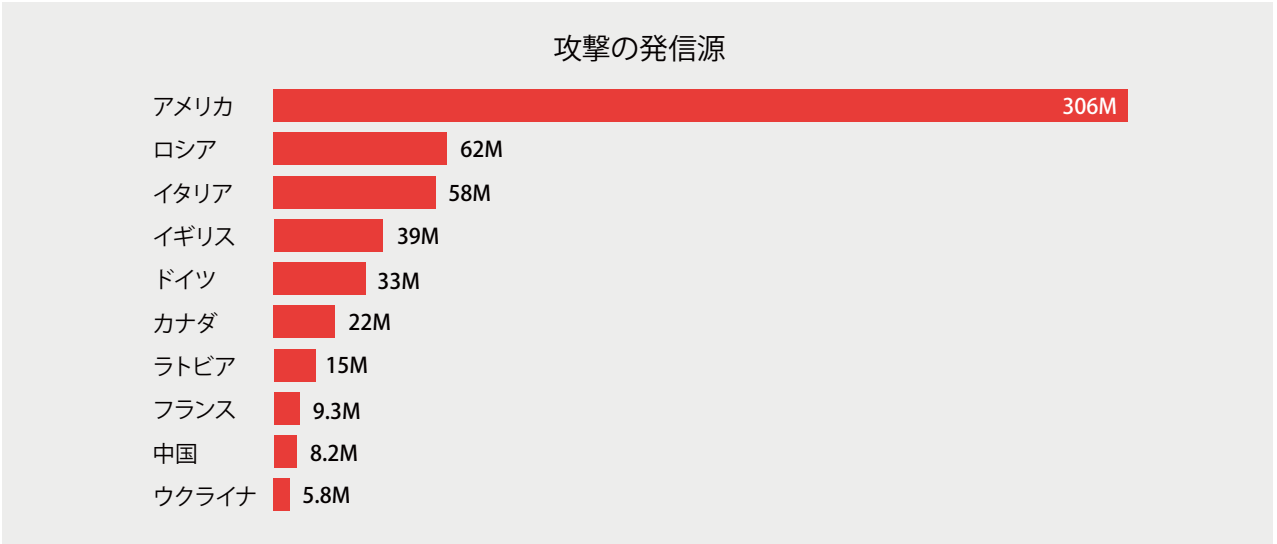
2018年下半期の当社のハニーポットのグローバルネットワークから得られた統計データによると、サイバースペース上の犯罪者の活動は活発だったようです。当社の記録では、この期間中の攻撃と偵察トラフィックの量が、2018年の上半期に比べて4倍に急増していました。
攻撃トラフィックはTelnetプロトコル上で最も多く観測されました。これは、IoTデバイスの利用数が増加しているためと考えられます。次によく見られたのは、SSH、SMB、SMTPプロトコル上の攻撃トラフィックで、Webサーバのセキュリティ侵害はTelnetに次ぐ主要な攻撃ベクターでした。米国およびロシアのIPアドレス・スペースを発信元とする攻撃が多数を占め、イタリアと英国がそれに続いていました。




当社では、過去数年間に渡り半年ごとにハニーポットのグローバルネットワーク、または、攻撃者を惹きつけ、行動を監視する目的で構築されたデコイサーバへの攻撃トラフィックに関するレポートを発表しています。当社のハニーポットは、SMB、SSH、HTTPなどの一般的なサービスをエミュレートしており、これらのハニーポットによって観測されるトラフィックは、攻撃ランドスケープ全体に対して高レベルのトレンドを示しています。
例えば、2017年のWannaCryとNotPetyaの発生後は、それまでは正常だったSMBポート445でのトラフィック量が急増しました。（SMBトラフィック量はその後も高いレベルで推移しています。）

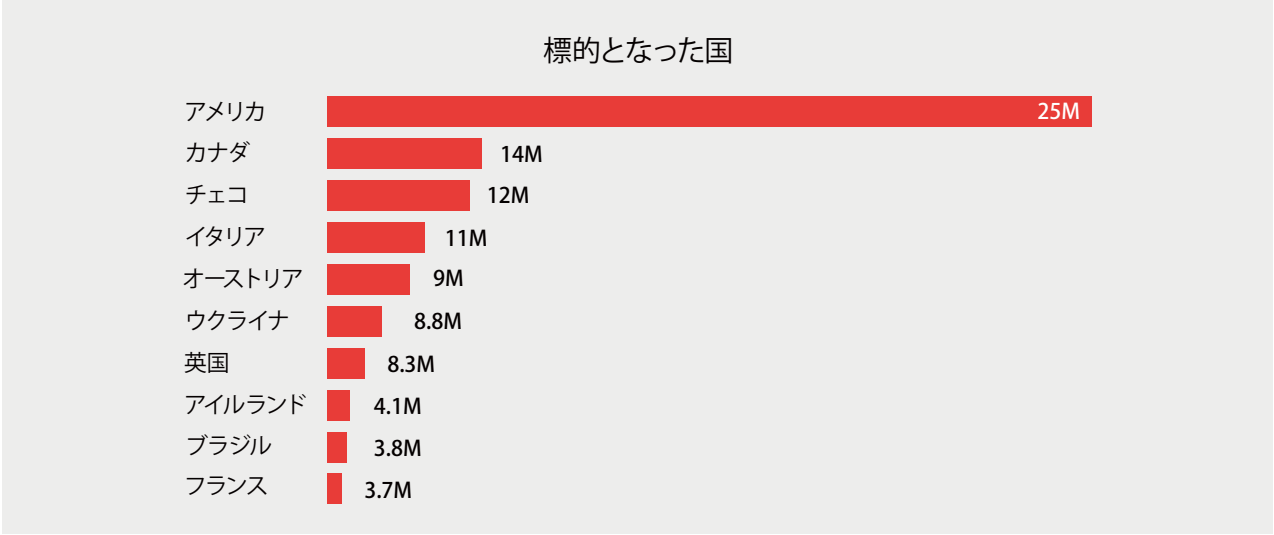
## 国別順位

常に興味深い情報である、どの国からIPアドレス・スペース攻撃が行われたのか、またどの国に攻撃が仕掛けられたのかを見てみます。



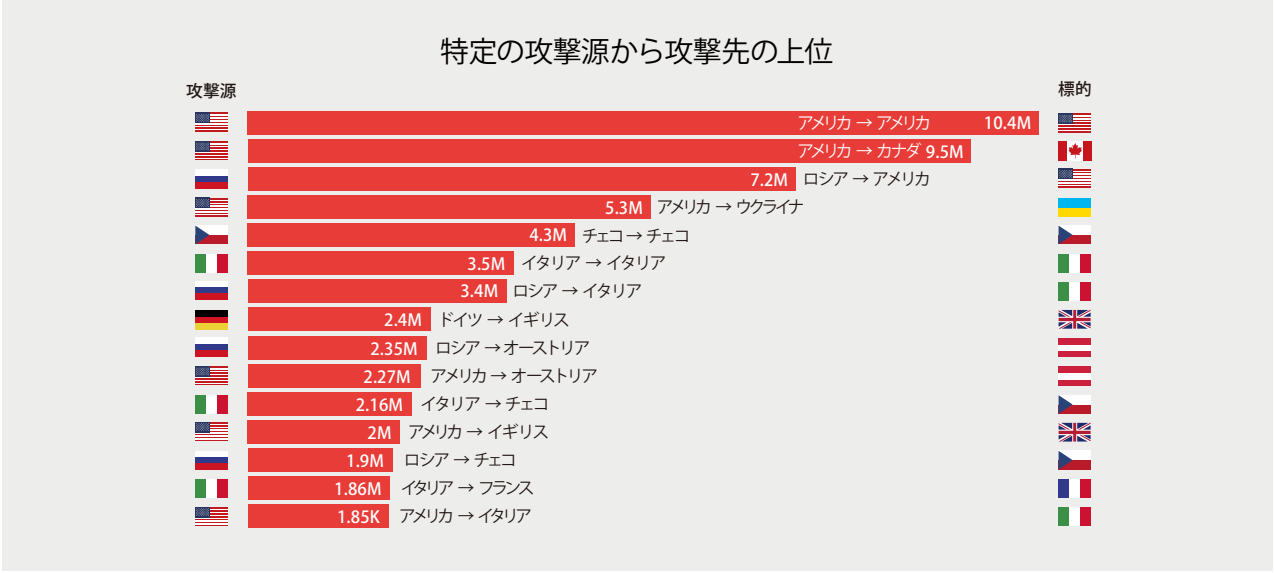
米国のIPアドレス・スペースを発信元とする攻撃トラフィックがこの期間中で最大シェアを占めており、かなり離れてロシアが続いています。言うまでもなく、サイバー犯罪者は検出を回避するためにプロキシを介して攻撃をルーティングするため、攻撃が実際にその国で行われているかどうかを特定する方法はありません。彼らは、法執行機関からの捕捉を回避するため、さまざまな地域に存在するVPN、TOR、侵害されたマシンやインフラを利用して攻撃している可能性があります。

さらに、発信源リストは、これらの攻撃が国家関与による活動であることを意味するものでもありません。大部分の攻撃の背後にある動機はおそらく金銭的なものであり、DDoS攻撃を仕掛けてマルウェアなどを送信する一般的なサイバー犯罪者によって引き起こされているものだと考えられます。
一方、攻撃先についてはより確実に特定することが可能であり、攻撃者にとって最も魅力的に映る国がリストアップされています。



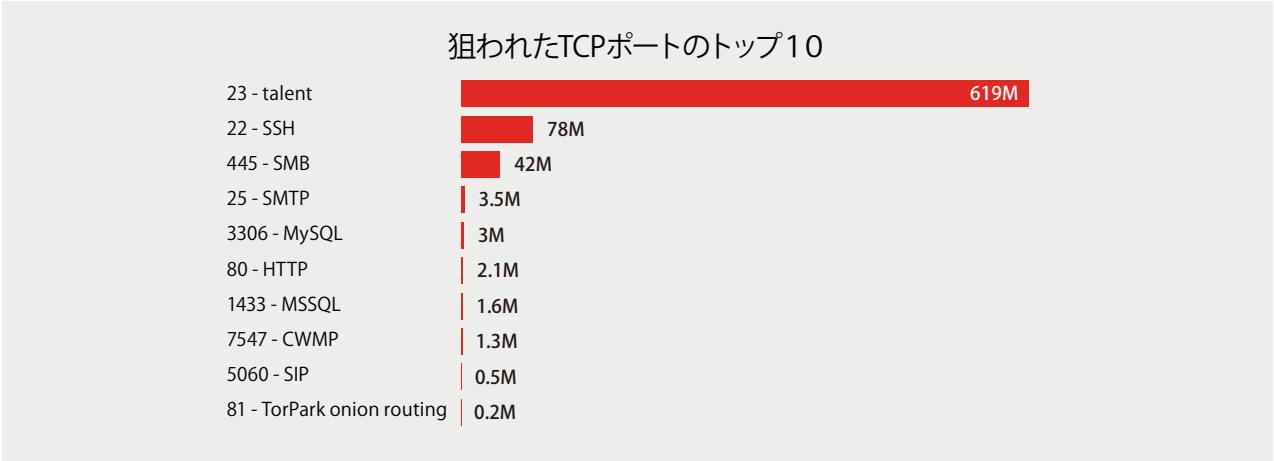

サイバー犯罪者のイメージについて質問すると、皆がフードを被った犯罪者が机に向かって攻撃を実行している姿を想像するかもしれません。しかし実体はかなり異なっています。当社のハニーポットの観測では、人間がマニュアルで攻撃している割合は、0.1%程度しかありませんでした。つまり、攻撃トラフィックの99.9%は、ボット、マルウェア、その他の自動化されたツールからのものです。もちろん、これらのツールを開発して設定しているのは人間ですが、何億という膨大な数の攻撃は自動化されてこそ可能になっています。

攻撃は、あらゆる種類のネットワークに接続されたコンピューティングデバイスからもたらされている可能性があります。脆弱なコンピュータ、スマートウォッチ、あるいはIoT歯ブラシでさえも、スキャンされ攻撃トラフィックの発信元になる恐れがあるのです。




興味深いことに、英国は攻撃源のリストでは上位にありますが、「特定の攻撃源から攻撃先の上位」リストの攻撃源国としては登場していません。前回の調査と同様に、英国からの攻撃は広範囲の国に向けられており、一国あたりの攻撃数はそれほど多くはないことが見てとれます。また、英国の最大の標的は米国で、攻撃の回数は85,000件を記録しています。これも前回の調査と同じですが、英国からの主要なプローブのターゲットはSMBポートで攻撃の99%に達しています。

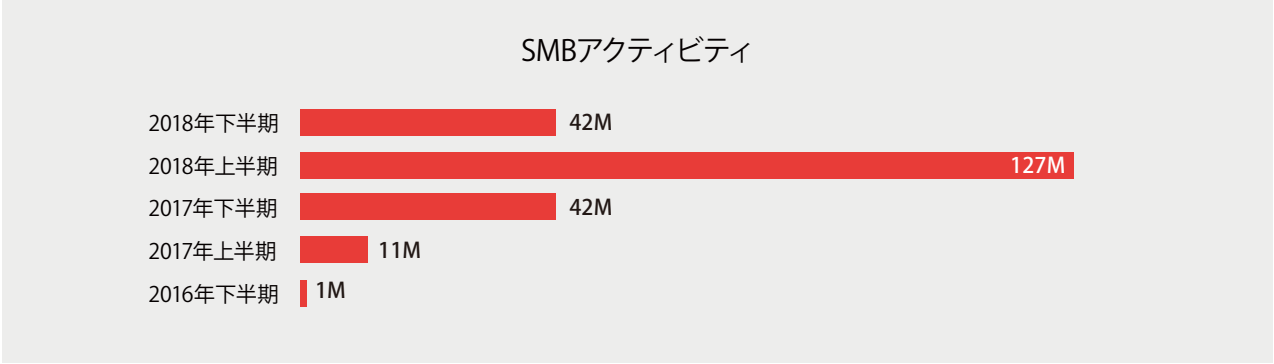
## ポートとプロトコル




2018年7月から12月にかけて、圧倒的多数（83%）の攻撃トラフィックがTelnetで使用されているTCPポート23上を流れたことが分かりました。実は、この期間の早い時期に当社のハニーポットのTelnet部分を調整しました。これによって、当社サーバがTelnet攻撃をより良く認識可能になったことがこの数字に反映されています。しかし、この急増の原因はそれだけではありません。デフォルトのユーザ名とパスワードの組み合わせを使用しているIoTデバイスがあまりにも多く存在し、攻撃者にとって格好の餌食になっているという事実も大きく影響しています。

Telnetを介した攻撃活動の大部分は、ボットネットの一部として悪用されているインターネット接続デバイスの「Thingbot」（モノのボット）の存在に関連しています。私たちは昨年12月下旬に、激烈かつ集中的なTelnetキャンペーンを観測しました。おそらく、このホリデーシーズンには多くの人が気もそぞろになり自宅を離れて旅行するために、サイバー犯罪者は攻撃する最高のタイミングだと捉えていると考えられます。

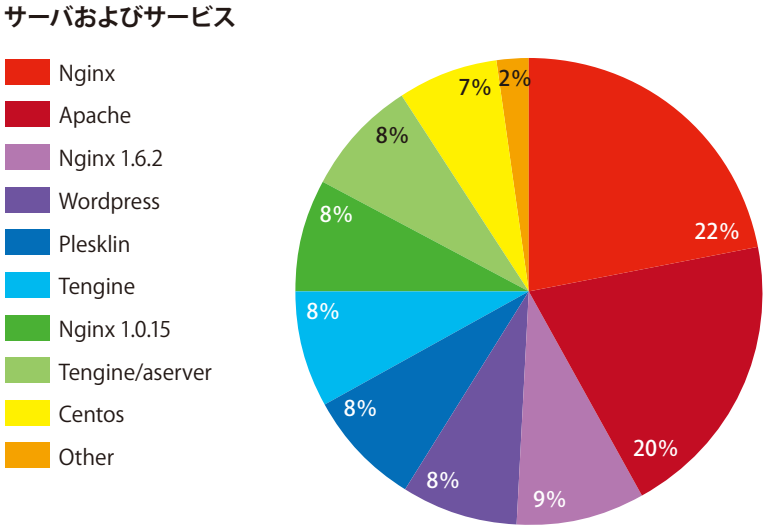
ポート23の次は、ポート22（SSHに関連し、リモートログインも試行される）が、標的とされたポートの第2位でした。SMBを標的にした攻撃でポート445が第3位 に入りましたが、前年同期からは減少しています。2018年前半には、ポート445を介した攻撃は1億2,700万件に急上昇していました。2017年のWannaCryとNotPetya攻撃の以前は、SMB攻撃のトラフィックは極めてわずかで、上位20にもリストされていませんでした。




SMTP、すなわちEメール攻撃トラフィックは4位でした。これは、おそらくマルウェアとスパムによる攻撃であり12月に報告されています。第5位はMySQLトラフィックで、データ侵害の企てと関連していると考えられます。MySQLはWordpress、Drupal、Joomlaなどのコンテンツ管理システムのユーザに大変人気があります。リストのさらに下位には、CWMPプロトコルがあります。これは、モデム、ゲートウェイ、ルーター、VoIP電話、およびセットトップボックスなどのエンドユーザデバイスのリモート管理に使用されるTR-069プロトコル（既知のエクスプロイト）と関連しています。

## サーバとサービス

当社のWebトポロジマッピングツールであるF-Secure Riddlerを使用して、最も一般的なWebベースの攻撃源であるサーバとサービスに狙いを定めて調査することができました。このリストのトップにはNginx、Apache、Wordpressが挙がっています。これらは攻撃者によって危険にさらされ悪用されることがよくあります。IoTに続いて、ハニーポットでしばしば見られる攻撃ベクターの1つがWebサーバの侵害です。



## 資格情報の悪用

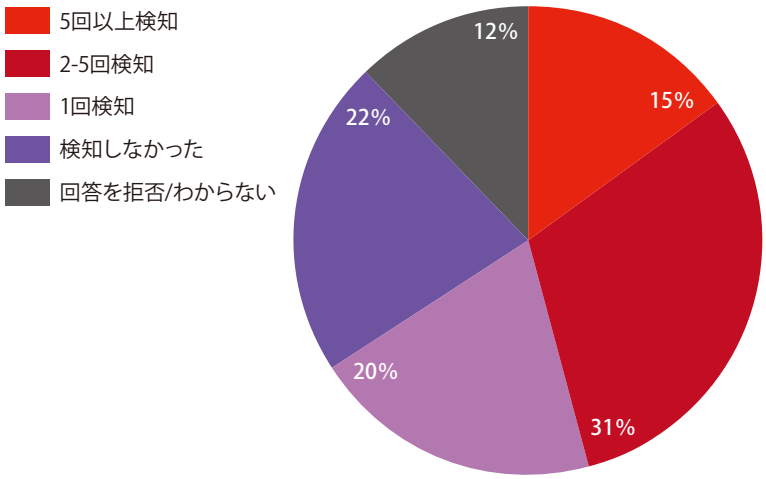
ハニーポットサービスに侵入しようとするときに攻撃者が使用するユーザ名とパスワードの上位は劇的に変わることはありません（"root"と"admin"は常に上位にリストされています）。しかし、今期での興味深い点は、2位と6位のパスワードがDahua社製IoTカメラと中国製H.264デジタルビデオレコーダーのデフォルトパスワードだったということです。

| 試されたユーザ名のトップ10 | 試されたパスワードのトップ10 |
|---|---|
| root | admin |
| admin | vizxv |
| shell\x00 | root |
| guest | default |
| default | 123456 |
| shell | xc3511 |
| enable\x00 | 12345 |
| supervisor | taZz@23495859 |
| support | 1001chin |
| user | 1234 |

## 企業の環境

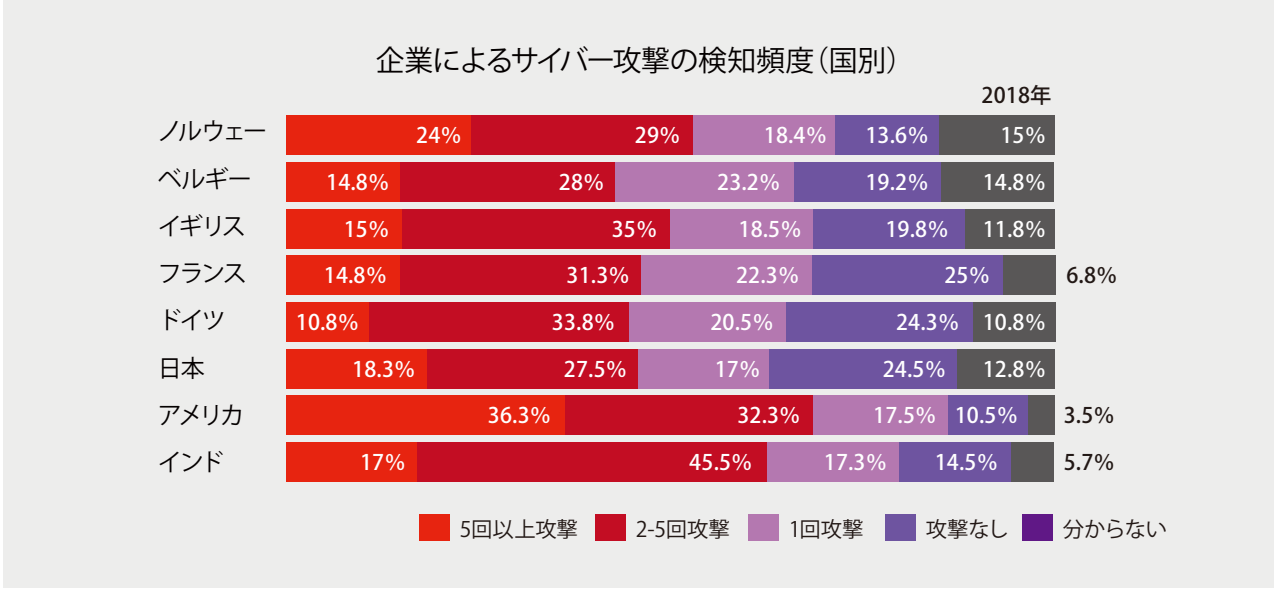
企業は外部の脅威ランドスケープからどのような影響を受けているのでしょうか？ITの意志決定者とインフルエンサーに過去1年間における日和見的攻撃と標的型サイバー攻撃の両方に対する検出状況について質問しました。回答者の3分の2は、少なくとも1つの攻撃を検出したと答え、22%が攻撃をまったく検出しなかったと答えました。また、12%は回答が分からないか拒否しました。

**過去1年間に攻撃を検知した回数**




企業規模が大きくなるほどより多くの攻撃を検出する可能性が高く、5件以上の攻撃を検出している企業のうち、従業員数が5,000人以上の企業が20%であるのに対して、200～500人の企業は10%に過ぎません。また、攻撃をまったく検出していない企業は大規模になるほど少なくなり、従業員数が5,000人以上の企業では16%が検出数ゼロと回答しているのに対して、500人未満の企業ではその割合は28%に増加します。

攻撃をまったく検出していないと回答している企業は、フランス、ドイツ、日本に多く、一方で5件以上検出している企業は、北欧と米国に多いことが分かりました。インドの企業のほぼ半数が2～5件の攻撃を検出していますが、他の国では、およそ3分の2の企業が2～5件と回答しています。




全世界の3分の1弱の企業が何らかの検出と対応のソリューションを使用していると回答しています。

## 結論

当社が長年にわたってハニーポットへの攻撃トラフィックを追跡してきた経験から学んだ教訓は、いくらうわべが変わっても本質は変わらないということです。犯罪者は次々と新たな戦術を繰り出します。IoTデバイスを侵害して最大のボットネットを構成し、SMBワームを拡散してランサムウェアを蔓延させ、Eメールスパムを送信し、Webサービスを標的にします。結局は簡単に金もうけをするために、これからも戦術を変え続けることでしょう。

最善の防御策も変わりはありません。人、プロセス、およびテクノロジーを含む包括的なセキュリティプログラムを組み込むことです。

**攻撃対象領域を限定する：**ネットワーク、ソフトウェア、およびハードウェアの複雑性を緩和します。どのシステムやサービスを使用しているのかを認識し、不要なものを削除します。

**従業員の関心を高める：**情報セキュリティの概念を教育し、ベストプラクティスにしたがうよう指導します。人々が従うべきプロセスと手順を導入します。

**多階層の技術を採用する：**セキュリティは階層構造で機能します。予測、予防、検出、および対応の技術を組み合わせたアプローチを実践しましょう。

# 私たちエフセキュアには、他社が見ていないものが見えています

## エフセキュアについて

エフセキュアは、他のどの企業よりもサイバーセキュリティを知っています。エフセキュアは30年間に渡ってサイバーセキュリティの革新を主導し、何万もの企業や何百万人もの人々を守ってきました。エフセキュアは、エンドポイント保護と検出とレスポンスにおける卓越した経験を元に、高度なサイバー攻撃やデータ侵害から幅広い脅威に至るまで、企業と消費者を保護します。エフセキュアの洗練されたテクノロジーは、世界的に著名なセキュリティラボの専門知識と機械学習を組み合わせ、ライブセキュリティという高度なアプローチを可能にします。エフセキュアのセキュリティ専門家は、欧州において他のどの企業よりも多くのサイバー犯罪の現場調査に参加しており、その製品は200を超えるブロードバンドおよびモバイル事業者、そして数千社のパートナーによって世界中で販売されています。

エフセキュアは1988年に設立され、NASDAQ OMX Helsinki Ltd.に上場しています。

**エフセキュア株式会社**
〒105-0004 東京都港区新橋2丁目2番9号 KDX新橋ビル2階
Tel: 03-4578-7710 / E-mail : japan@f-secure.co.jp
https://www.f-secure.com/
2019.03 JP

F-Secure