radware

グローバルアプリケーション＆ネットワーク セキュリティーレポート　2014-2015年

Table of Contents

エグゼクティブサマリー

01

「歯ごたえのある」(C.H.E.W.)ことを証明したサイバー攻撃

2013年8月、米国本土防衛及び国土安全保障担当の元国防次官補であるポール・ストックトン (Paul Stockton) 博士が、米国の配電網の内部に存在するいくつかの脆弱性など、各公益企業が直面しているサイバーセキュリティーの問題に関するパネルディスカッションに参加しました。博士は、コンピューターネットワークへの侵入により配電網が相当期間にわたって停止した場合、重大なライフライン インフラストラクチャーが機能しなくなるであろうと強く主張しました。病院、輸送機関、食品や医薬品の物流インフラストラクチャーについては、一時的な損害であっても、公共の衛生や安全が脅かされる可能性があります。

つまり、エネルギー源だけでなく、国の重要なインフラストラクチャーにかかわるすべての組織で準備ができているかどうかを理解することが重要です。公益企業や医療機関、航空会社、食糧生産者は、このような障害から市民を防御する準備ができているでしょうか。このシナリオが起きる可能性はあるのでしょうか。実行すべきミティゲーション (緩和) 手順とは何でしょうか。そしてその緊急度はどの程度でしょうか。

サイバー攻撃の観点から見ると、2014年は、電気、電力、医療、および金融サービスをはじめ、多くの業界にとって転機の年でした。中でも電力業界は、概して脆弱性の考え方に抵抗してきました。それは、インターネットと発電装置間の「エアーギャップ」制御や、業界固有のSCADA IPプロトコルを多く利用しているためです。

しかし、今年、電力業界は、通常のサービスの提供に対する脅威とリスクが増加していることをついに認めなければならなくなりました。例えば、電力業界は最近、大きく報道された「Energetic Bear」マルウェアレポートを含め、数多くの攻撃の犠牲となりました。

かつて「免疫性がある」と言われていた他の業界がサイバー攻撃の危険に晒され始めたことにより、電力業界の認識も生まれてきました。金融サービス業界は、暗号化プロトコルの脆弱性（BASH脆弱性など）を悪用した猛攻撃を受けました。ボストン小児病院は、ハクティビストの標的となった最初の医療機関です。

脅威は実世界で発生します。
問題は複雑です。しかし、警笛はすでに鳴っています。私たちは、大惨事を招かないよう有意義な行動を起こす必要があります。

ますます多くの業界が複雑な脅威に晒されるようになった今こそ、「C.H.E.W」を再考するよい時期です。「C.H.E.W」とは、サイバーセキュリティーに関して米国大統領の特別顧問を務めたリチャード・クラーク（Richard Clarke）氏が発案した用語であり、サイバー攻撃リスクの起源を分類し、説明するものです。

- **C**ybercrime（サイバー犯罪）ー他人を攻撃し、その試みから金銭的利益を得ることを第一の動機とする考え。
- **H**acktivism （ハクティビズム）ーイデオロギーの相違を動機とする攻撃。この攻撃が最も重視することは、 金銭的利益ではなく、特定の行動または「発言」を促したり、思いとどまらせたりすることです。
- **E**spionage （ネットスパイ）ー他の組織の情報を取得し、政治上、金融上、資本主義上、または市場のシェアを獲得すること、あるいは他の形で情報を活用することを追及する単純な動機。
- **W**ar (Cyber) （サイバー戦争）ー敵対者の権力の中枢に対して、サイバー攻撃によって国民国家的な脅威または国家を超えた脅威を与える考え。攻撃の標的としては、非軍事的な重要インフラストラクチャーや金融サービス、または従来の標的（軍産複合体など）が考えられます。

このような厄介な動機を前にすれば、平均的な小規模企業（地方の電力会社など）が多方面にわたってどれだけ危険に晒されるかということが明らかになります。このような公益企業は、サービス料金の値上げに反対する顧客から攻撃を浴びせられることがあります。発電方法を容認しないハクティビストから狙われることもあります。あるいは、国の配電網インフラストラクチャーに存在する弱いリンク部分を悪用しようとする、国外の諜報員の犠牲になることもあります。

脅威は、組織の規模に関係なくあらゆる組織を襲います。前もって準備することは、困難なことですが必要なことです。Stuxnet、Night Dragon、Shamoon、Dragonfly、Energetic Bearなどの脅威が、すでに世界中の重要インフラストラクチャーを標的としています。これらは、私たちが過去に経験したことを思い出させるものであると同時に、今後何が起きるかを告げるものでもあります。

脅威は実世界で発生します。問題は複雑です。しかし、警笛はすでに鳴っています。私たちは、生活を脅かす大惨事を招かないよう、有意義な行動を起こす必要があります。

本レポートの目的は、事業を悩ます脅威を組織自体が検知してミティゲートできるよう、実用的な情報を提供することです。本レポートは2つの役割を果たします。それは、セキュリティー専門家が容易に参照できるリソースガイドとしての役割と、組織が最新の攻撃トレンドおよび技術から組織自体を防御するために導入できる機能提案としての役割です。

最も重要な調査結果

ラドウェアの2014年度版「グローバルアプリケーション&ネットワーク セキュリティーレポート」では、2014年の「セキュリティーに関する業界調査」の調査結果と分析の概要、ラドウェアの緊急対策チーム（ERT）が最前線でサイバー攻撃に対抗した経験、世界中の様々な業界の経営幹部レベルに対する初の定性的調査から得られた洞察について説明します。

本レポートは、セキュリティーコミュニティー全体にメリットをもたらすことを目的として作成されたものであり、2014年のサイバー攻撃をビジネス面と技術面の両方から包括的かつ客観的にレビューし、組織が2015年のサイバー攻撃に対する計画を策定する際に考慮すべきベストプラクティスを提示します。また、サイバーアタックの背後に潜む「動機」を理解するためのフレームワーク（一見混沌としたように見える脅威を整然と評価するための方法）も示します。

2014年に起きたセキュリティーの変化は？

2014年はセキュリティー業界にとって転機の年でした。サイバー攻撃は、量、期間、複雑さ、および標的の面で転換点に至りました。注目を集める最新のサイバー攻撃はマスコミ報道に常に取り上げられ、攻撃に関する大量の記事があふれました。ただし、本レポートでは、非常に物騒な毎夜のニュース放送よりもはるかに恐ろしい全体像を示します。サイバーの脅威はますます増大し、新しい標的に向けて拡大しています。技術的な「トリックの袋」（あらゆる手段を詰め込んだ袋）はこれまでになく大きくなり、ハッカーは新しい（かつ恐ろしい）方法を使用して「トリック」を組み合わせます。定石通りにセキュリティープログラムを実施している組織も不意を突かれる可能性があります。

長期化し、連続的になった攻撃

2014年の「セキュリティーに関する業界調査」によると、最も多く報告された攻撃継続時間は1か月でした（回答者の約15%）。ただし、標的とされた組織は、主な攻撃の19%を「一定」の攻撃と見なしています。これは、2011、2012、2013年の調査と大きく異なります。1週間および1か月におよぶ攻撃は多く報告されましたが、一定攻撃を受けたと報告した組織は6%以下でした。

このトレンドは、攻撃がない状態を通常状態とみなす、インシデントレスポンスに関する従来の概念に異議を唱えるものです。またこれはセキュリティーギャップを露出しています。休みなく続く攻撃キャンペーンに効果的に対抗できた期間を尋ねた質問では、52%の回答者が、そのような攻撃キャンペーンに対抗できたのは1日以内であったと答えています。最後に、攻撃サイズを依然として重視する専門家もいますが、ラドウェアは、攻撃サイズを、犯罪で使用する拳銃の色のような属性だと考えます。攻撃の洗練度が増すにつれ、サイズだけでは効果にそれほど影響が及ばなくなってきました。

脅威に対する免疫力は誰も持っていない

ボストン小児病院のケーススタディーに示されるとおり、脅威は拡大しており、様々な業界、組織サイズ、技術展開が標的とされるようになってきました。2014年のRing of Fireでは、4つの業界（教育、ゲーミングサイト、医療、ホスティングおよびISP）が灼熱の中央部に近づいています。（管理されたサービスプロバイダーにとってセキュリティーがますます複雑かつ重要になってきた理由については、ServerCentralのケーススタディーを参照）。金融サービスが「高」から「中」のリスクに移動しましたが、従来のほとんどの業界は同じリスクレベルにとどまっています。

新しいトレンドがゲームのルールを変える

今年のレポートでは、情報セキュリティーにとって非常に破壊的だと思われる3つのトレンドを特定しました。それは、クラウドへの継続的な移行（およびそれに伴う企業ITの解体）、モノのインターネット（Internet of Thngs: IoT）の登場、そしてSDN（Software-Defined Network）への動きです。

ハイブリッドソリューションの普及

2014年の「セキュリティーに関する業界調査」では、回答者の3分の1以上（36%）がカスタマー構内設備（CPE）およびクラウドソリューションと共にハイブリッドソリューションをすでに使用しており、6%がハイブリッドソリューションの実装を計画していることが示されました。興味深いことは、ほぼ半数（48%）が2015年までにハイブリッド防御を採用することが示されたことです。

ありがたくない名誉に輝くインターネットパイプとリフレクター攻撃

ラドウェアの2014年調査から、インターネットパイプが、障害点として増加しただけでなく、ナンバーワンの障害点としての栄誉を得たことがわかりました。一方、ハッカーは、あらゆるプロトコルを通り抜けて、次の大規模なリフレクター攻撃に向けてインターネットパイプを使用するかどうか、さらにどのように使用するかを判断しているように思われます。つまり、リフレクター攻撃は、2014年のDDoSに関する唯一最大の「頭痛の種」です。

より洗練されたヘッドレスブラウザーとDDoS攻撃

攻撃側は1回の攻撃で複数の技術を組み合わせるようになりました。これにより、攻撃側は、防御ラインを通過し、サーバー側の脆弱性を悪用して、サーバー側のリソースに負担をかけることができます。このような攻撃には、匿名化やなりすまし、断片化、暗号化、動的パラメーター、検知回避とエンコード、パラメーター汚染、広範な機能の悪用などがあります。

DDoSがトップを維持するも、唯一の懸念事項ではない

サイバー攻撃は過去4年のトレンドを維持し、ネットワークレベルの攻撃とアプリケーションレベルの攻撃に均等に分かれました。最も多く挙げられた脅威の種類はDDoSでしたが（46%）、他との差はあまりありませんでした。僅差で次に続くのは、不正アクセス（41%）と、APT攻撃（Advanced Persistent Threat）（39%）です。しかし、依然として、すべての脅威の種類が相応に示されており、脅威を取り巻く環境は、各組織の業界やビジネス面での懸念によって異なるようです。

経営幹部レベルにとってのセキュリティーの問題

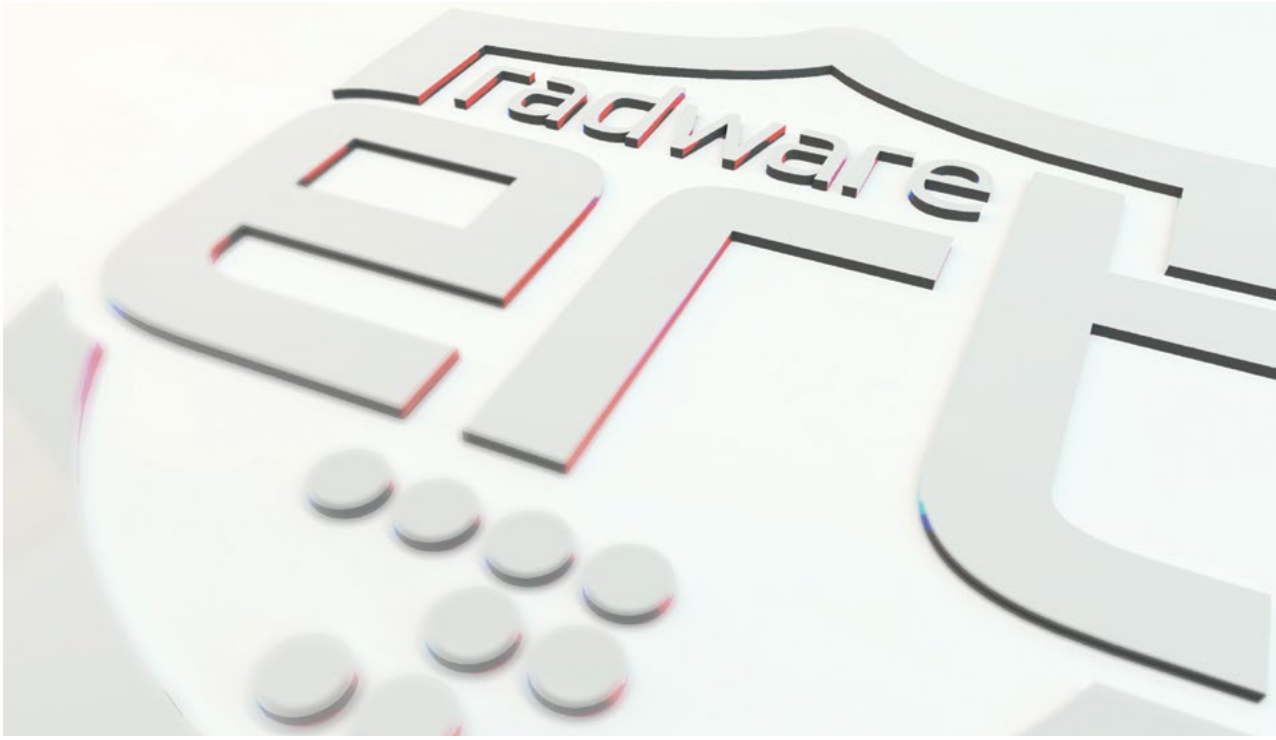
ラドウェアの定性的調査によると、幹部の4分の3近くが、現在、セキュリティー脅威がCEOまたは役員レベルでの懸念事項になっていると答えています。トップトレンドについては、幹部の3分の1以上がクラウドとBYODを挙げました。幹部は、これらを組織のセキュリティーリスクを高めるものと考えています。また、幹部の4分の1以上がIoTを選択しました。SDNを挙げたのは5分の1以下です。

予算が問題となる場合があるが、投資を続ける組織

サイバー攻撃の予防とミティゲーションに対して、あらゆる規模の組織が苦労しながら資金を調達し、費用を確保しています。過去12か月に組織がサイバー脅威に対応してリソースをどのように展開したかを尋ねた質問には、回答者の半数以上がセキュリティーに関するプロセス、プロトコル、または職務を変更したと答え、半数近くが新技術または専門的な技術に投資したと答えました。

2014年のレポートは、マクロITのトレンドによりセキュリティーの有効性が解消されていく中で、セキュリティー攻撃がいかに複雑になっているかということを明らかにしています。ラドウェアの研究では、セキュリティー攻撃の動機、方法、および有効性が増加傾向にあることが確認されており、進化する脅威に迅速に適応するための敏捷性を高める必要があることが強調されています。

02 調査の方法および情報源



この調査では直接取得したデータに基づく統計調査に最前線での経験を加え、セキュリティーコミュニティーの育成に役立つ可能性のあるトレンドを特定しています。このレポートの情報源は次のとおりです。

セキュリティーに関する業界調査

定量的なデータソースとして、「セキュリティーに関する業界調査」を使用しています。これは、ラドウェアが330名の回答者に行ったものです。この調査は、サイバー攻撃に対する計画策定時およびサイバー攻撃への対抗時に組織が直面した問題に関して、特定のベンダーに偏らない客観的な情報を収集することを目的として作成されたもので、世界中の様々な組織に送られました。

サンプル企業の39%は、年間収入が5億米国ドルを超える大規模組織です。調査は、合計23の業界を対象としており、回答企業の多くは、電気通信/インターネット/クラウドサービスプロバイダー（20.42%）、金融サービス（13.15%）、コンピューター関連の製品またはサービス（12.11%）、製造/生産/物流（6.57%）に属しています。約40%の組織が世界中でビジネスを展開しています。

セキュリティー担当エグゼクティブを対象とした調査

業界調査に加えて、ラドウェアは、セキュリティー部門の最高責任者を各組織から1名ずつ、合計11名選出し、サイバー攻撃を受けた経験に関して、詳細なインタビューを実施しました。

ラドウェアの緊急対策チーム（ERT：Emergency Response Team）によるケーススタディー

ラドウェアのERTは、攻撃を積極的に監視しリアルタイムでミティゲートする、専門のセキュリティーコンサルタントグループであり、サイバー攻撃や大量のマルウェアでお困りのお客様に24時間365日のセキュリティーサービスを提供しています。ラドウェアのERTメンバーは、サイバー攻撃への「第一応答者」として、業界でも特に顕著なハッキング事象に対処した広範な経験を積んでおり、社内のセキュリティーチームでは対応したことがないような攻撃を軽減するための情報や専門知識を提供しています。レポート全体を通じて、ERTチームが最前線でサイバー攻撃にどのように対抗したかが示されており、単独の調査や学問的研究よりも詳細なフォレンジック分析が得られます。

03 サイバー攻撃のRing of Fire

サイバー攻撃のRing of Fire[1]は、業界内の組織が攻撃にさらされる可能性に基づき、その業界をマッピングしたものです。Ring of Fireは、5つのリスクレベルを反映しており、赤い中央部分に近い組織ほど、DoS/DDOS攻撃やその他のサイバー攻撃にさらされる可能性が高くなるだけでなく、それらの攻撃にさらされる頻度も高くなる可能性があります。

図1のサイバー攻撃のRing of Fireには、10個の業界が含まれています。赤の矢印は、昨年のレポートから位置が変わった業界を示しています。これは、サイバー攻撃の総数のほかに、サイバー攻撃の頻度や強度が2014年に増加したことを意味します。いくつかの業界は一貫した脅威レベルにさらされています。一方、実際に「高」から「中」のリスクに移動したのは、1つの業界（金融サービス）だけです。4つの業界（教育、ゲーミングサイト、医療、ホスティングおよびISP）はRing of Fireの中央部に近づきました。

企業がRing of Fireの中央部に進むにつれて、サイバー攻撃を受けやすくなり、セキュリティーギャップが生じます。

通常、変化はリスクを伴います。業界がサイバー攻撃のRing of Fireの中央部に近づくと、その業界の企業は攻撃の標的となる可能性が高まります。ミティゲーションの仮定が依然としてサークル内の以前の位置、つまり、異なるリスクレベルに合わせられている場合、サイバー攻撃を受けてデータセンターの停止を招く可能性は劇的に高まります。赤い矢印が付いている業界内の組織は、新しいリスクレベルに適合するよう、迅速にミティゲーションソリューションの調整を行う必要があります。

1 現在の脅威の環境をより反映したものにするため、2013年のDoS/DDoS Ring of Fireから名称を変更しました。

⚠⚠⚠ 攻撃対象の危険性が「高」の業種

ゲームサイト

長年にわたってサイバー攻撃の標的となってきたゲーミングサイトは、速度低下や停止に対して非常に敏感な業界です。また、ゲームサイトは、特定のプレイヤーがゲームに負けたりクリアできなかったときの金銭的損失に激怒した場合も脆弱になります。彼らが復讐を企てる場合、自由に使えるもの（多くの場合DDoS攻撃）によって、サイトに猛攻撃を加える可能性があります。

2014年、ラドウェアのERTの経験から、攻撃期間が長くなっただけでなく、攻撃が「卑劣になった」ことが示されています。ほぼ確実に言えることは、これらの事件が、腹を立てた1人によるものではないということです。このような持続的な攻撃は、攻撃的にサボタージュを行う人、脅された攻撃者、あるいは容量の大きいその他の実体によると考えられます。

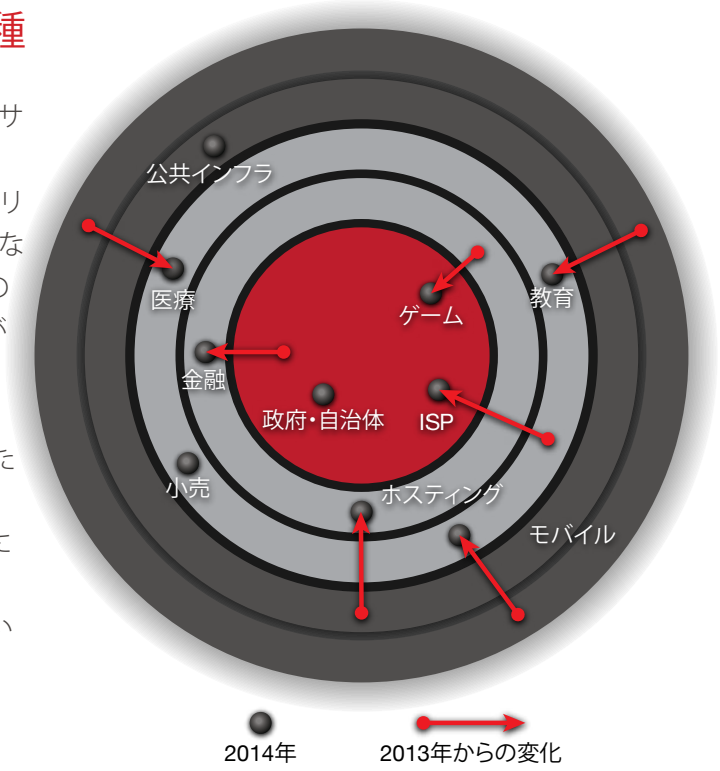


図1：サイバー攻撃のRing of Fire

政府機関

政府機関は、サイバー攻撃とDDoSの脅威にさらされる可能性が常に高く、今後もそれらの脅威に常にさらされると考えられます。ウクライナ・ロシア紛争、香港の抗議活動、ミズーリ州ファーガソンでの射殺事件、イスラエル・パレスチナ紛争を含め、2014年に発生した出来事により、関連する政府や連邦機関は差し迫った危険にさらされました。

幸いにも、政府は高リスクエンティティとしての長い歴史があり、比較的適切に防御されています。現在、政府が抱えている主な課題は、攻撃側に遅れずについていくことと、そして、他の政府によって遂行またはサポートされる「APTグレード」の攻撃に準備することです。

ISPおよびホスティング業者

ISPおよびホスティング業界の企業にとって、2014年はリフレクター攻撃の年でした。攻撃は、古いDNSベクトルに加えて、NTP、Chargen、SSDP（UPnP）などの新しいベクトルも対象としました。また、このトレンドにより、10～50Gの範囲で攻撃の量と数が劇的に増加しました。2014年、このような攻撃は常習的に行われるようになりました。これらの攻撃は、増幅技術を使用して容易に生成できるためです。このトレンドによって特に激しく攻撃されたのはISPです。ISPは長い間、その顧客を対象とした、現在も継続している低レベルの攻撃に対処してきましたが、ほとんどの場合、その事象についてそれほど心配する必要はありませんでした。しかし、現在、そのリスクは大幅に高くなりました。ISPの顧客ではなく、ISP自体を標的とすることで、攻撃は大規模になり、その潜在的な影響も大きくなりました。

予想していなかった対象（医療や教育）へのリスクが増加しています。ゲーミング、ホスティング、ISP企業に対する攻撃の可能性も過熱してきました。

⚠⚠ 攻撃対象の危険性が「中」の業種

教育

教育組織では、「犬が宿題を食べちゃった」（学生の言い訳）の現代版としてサイバー攻撃が使用されるようになり、リスクが過熱しています。学生は課題の時間を稼ぐために攻撃を開始します。また、特定の講師や管理者と衝突した後、ハクティビストのスタイルで地区や大学を標的とします。多くの教育システムは、巨大な相互接続ネットワークに依存し、多くの学校が1つのプラットフォームにつながれていますが、この事実は、リスクを高めるだけです。

また、米国のK-12学区では、サイバー攻撃が収入源に脅威を与える可能性があることが確認されました。これは、連邦の資金が、重要な試験結果などの情報のタイムリーな電子提出に依存するためです。2014年、多くの学区で資金調達の遅れが生じました。サイバー攻撃によってデータの提出が妨げられたためです。

金融サービス

ここ数年はアクション満載の年でした。2011年には、株式取引所への攻撃、2012〜2013年にかけてはOpAbabilでの米国銀行への攻撃がありました。しかし、その後、2014年は比較的に「静かな」年でした。前年までの経験から、銀行などの金融機関は防御を強化し、比較的に堅実な位置を維持しています。

ただし、金融組織が多方面からの攻撃のリスクを依然として抱えていることは間違いありません。国有企業ではなくても、銀行は国の象徴としての役割を果たします。一部の国では、銀行は、国の重要インフラストラクチャーの金銭的部分を提供しているほか、資本主義を象徴する役割も果たしています。このすべてが、大きな注目を集める、つまりサイバー攻撃を引き付ける要因となります。

医療

ハクティビストによるボストン小児病院（BCH）への攻撃によって、健全な機関、あるいは論争を引き起こしそうにない機関であっても激しいサイバー攻撃の標的となりえることが明らかになりました。2014年のこの攻撃を通じて、ラドウェアのERTは、病院に対してサイバー攻撃が何を実行できるかを直接目撃しました。そして、私たちは、他の多くのサイバー攻撃が何をできるのかということに気づきました。病院が攻撃されると、生命が危険にさらされるのです。当然のことながら、BCHのケースによって、セキュリティーの現場担当者間だけでなく、医学界の中でも議論が活性化しました。

BCHの事件は簡単に片づけられない、簡単に片づけるべきではないとラドウェアは考えています。この事件は、現在すべての病院にリスクがあることを示す明確なメッセージです。

小売り業

小売り業界は安定を維持しており、攻撃を受ける可能性は中程度です。小売業者の場合、脅威の発生源は通常、競争相手、不満を持つユーザー、金銭的利益を目的とする、賠償金に関する策略を専門とするハッカー、そしてリテーラーを特定の理由と結びつけるハクティビストです。

モバイル

スマートフォンの登場以前、モバイルデバイスは高リスクのサイバー脅威の対象ではありませんでした。今でも、モバイルユーザーはDDoS攻撃に対して特に脆弱ではありません。しかし、「モバイル」デバイスは、現在スマートフォンだけでなく、ラップトップに接続するモバイルルーターや、他のリモート/携帯端末も含まれます。この理由だけで、脅威が「低」から「中」に上昇しました。一方、DDoS攻撃は目的を達成するための手段であることに注意が必要です。例えば、モバイル装置は、セキュリティーサービスによって他の種類の攻撃ベクトルから防御されている場合があります。DDoS攻撃がセキュリティーサービスを中断させることで、モバイルデバイスやユーザーに影響を及ぼすことができるのです。

⚠ 攻撃対象の危険性が「低」の業種

公共企業

2013年から2014年にかけて、公益企業の脅威の環境に根本的な変化はありませんでした。このような企業は、核となるネットワーク機能を、分離したネットワークセグメント内に維持しています。通常、これは、DDoS攻撃から保護されていることを意味します。しかし、過去に行われた、これらの企業の公開サイトへの攻撃や侵入の試み、および他の既知のインシデントによって、これらのネットワークへのDDoS攻撃が実際には可能であることが証明されました。そのため、攻撃の可能性が高まっており、DDoS攻撃が成功すると、その潜在的な影響によって非常に高いリスクが生じます。この要因の1つとして、サイバー戦争の脅威の高まりが挙げられます。

04 サイバー攻撃に関するビジネス面の懸念

サイバー攻撃に関して、組織が最も恐れている影響は何でしょうか。組織はサイバー攻撃による財務上の潜在的影響をどのように定量化し、どのような種類のソリューションを使用してそのインシデントをミティゲートしているのでしょうか。ラドウェアは、3年間にわたるこれまでの調査に基づき、セキュリティーリーダーに対する調査を再度実施し、サイバー攻撃に関連するビジネス面の懸念を把握しました。

攻撃の動機のほとんどが不明

理由の中で圧倒的なトップ（約70%）を占めたのは「不明」でした。ほとんどの組織にとって、サイバー攻撃の動機は謎に包まれたままです。「政治的理由/ハクティビズム」（34%）が4年連続で2位を維持し、「ライバル企業による妨害」（27%）が3位となりました。リストのその他の項目は、「不満を持つユーザーによる妨害」および「金銭の要求」です。

経験したサイバー攻撃の背後にある動機は？

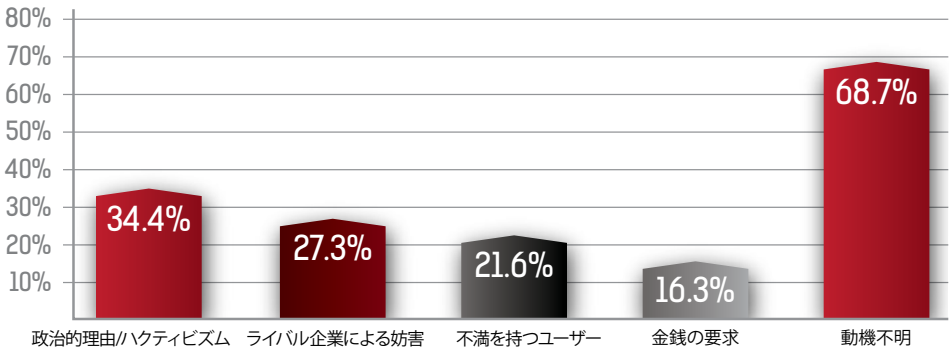


図2：サイバー攻撃の背後にある動機

この調査結果について最も警戒すべき点は、サイバー攻撃の理由として「不明」が「既知」のカテゴリを依然として上回っていることです。基本的に、組織は、組織への犯行の理由について見当がついていません。つまり、将来の攻撃に備えることが難しく、攻撃を訴追しても逃げられてしまいます。

最も危険な脅威

今年の「セキュリティーに関する業界調査」では、どの種類のサイバー攻撃が回答者の組織に最大の被害を与えるかを尋ねました。半数近くの回答者がDDoS攻撃を挙げました。最も多く挙げられた脅威の種類はDDoSでしたが（46%）、他との差はあまりありませんでした。

僅差で次に続くのは、不正アクセス（41%）と、APT（Advanced Persistent Threat）攻撃（39%）です。しかし、依然として、すべての脅威の種類が相応に示されており、脅威を取り巻く環境は、各組織の業界やビジネス面での懸念によって異なることが示唆されます。

組織に最も損害を与えると考えられるサイバー攻撃は？

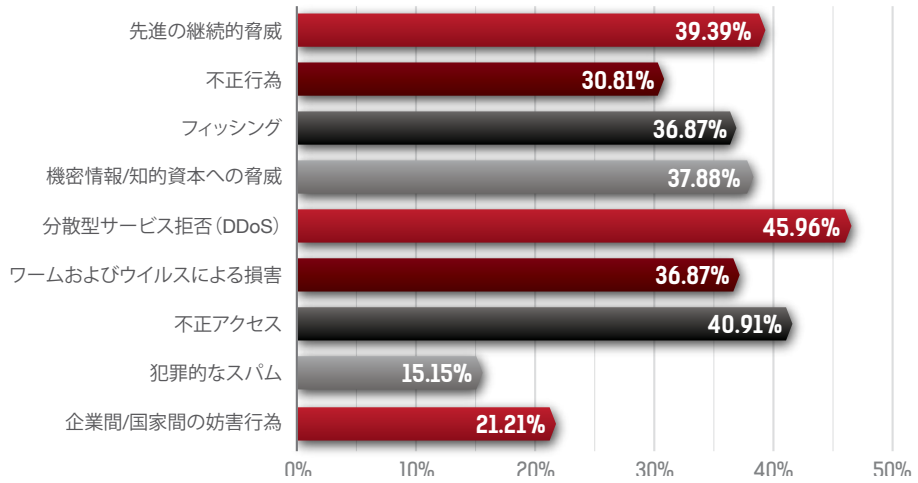


図3：事業に最も損害を与える攻撃

限界点を見つける

調査では、昨年経験したサイバー攻撃の平均継続時間についても尋ねてみました。回答の中で最も多かった継続時間は1時間でした（回答者の41%以上）。しかし、14%近くが平均3時間と回答し、10%近くが攻撃は平均して1か月続いたと回答しています。

経験したセキュリティー脅威の平均時間は？

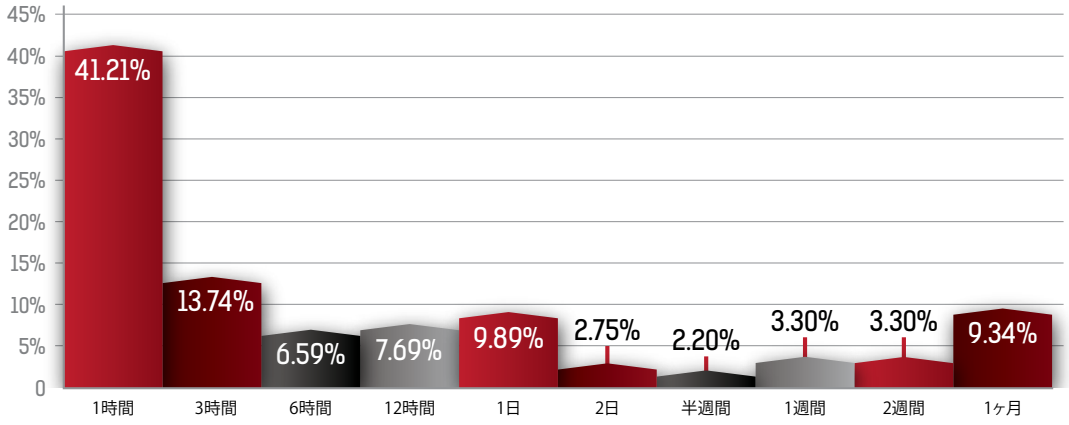


図4：セキュリティー脅威の平均的な継続時間

2014年に経験した最長のセキュリティー脅威についても尋ねてみました。回答の中で最も多かった継続時間は1か月でした（回答者の約15%）。一方で、回答者の14%近くは、経験した最長の脅威はわずか1時間であったと回答しており、13%以上が、脅威の最長継続時間は3時間であったと回答しています。

経験した最も長かったセキュリティー脅威は?

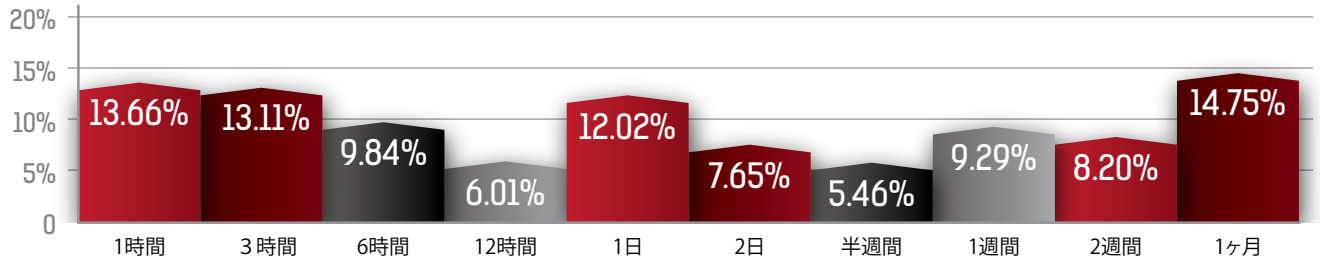


図5:最長のセキュリティー脅威

休みなく続く攻撃キャンペーンに効果的に対抗できた期間についても尋ねてみました。このような攻撃キャンペーンに対抗できた期間として最も多かった回答(約52%)は1日以内でした。しかし、回答者の約35%は、1週間以上におよぶ攻撃キャンペーンに耐える準備ができていると考えています。また、回答者の17%が、1か月におよぶ攻撃キャンペーンにも対抗できると答えています。

休みなく続く攻撃キャンペーンにどれだけの期間効果的に対抗できますか?

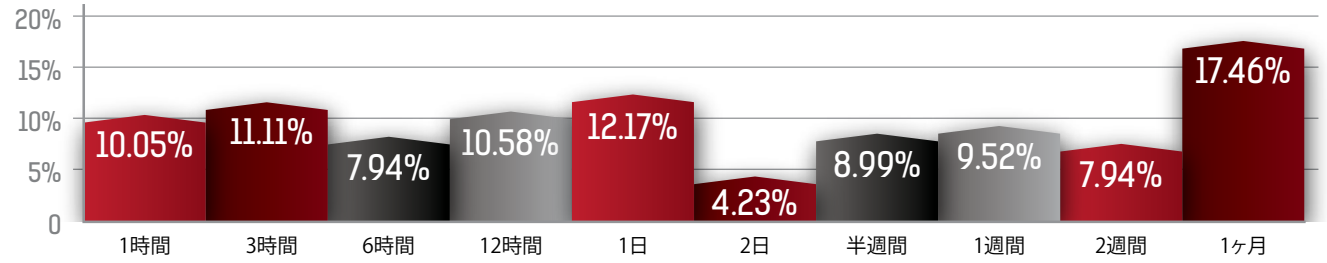


図6:休みなく続く攻撃キャンペーンに効果的に対抗できる期間

最も差し迫った問題

2013年の「セキュリティーに関する業界調査」において、サイバー攻撃に対するビジネス面での懸念に関して最も多かった回答は、「評判の喪失」と「内部組織への影響/生産性の損失」でした。今年の調査で最も多く挙げられた懸念は、「評判の喪失」と「収益の損失」でした。

組織がサイバー攻撃を受けた場合にビジネス面で最も懸念されることは何ですか?

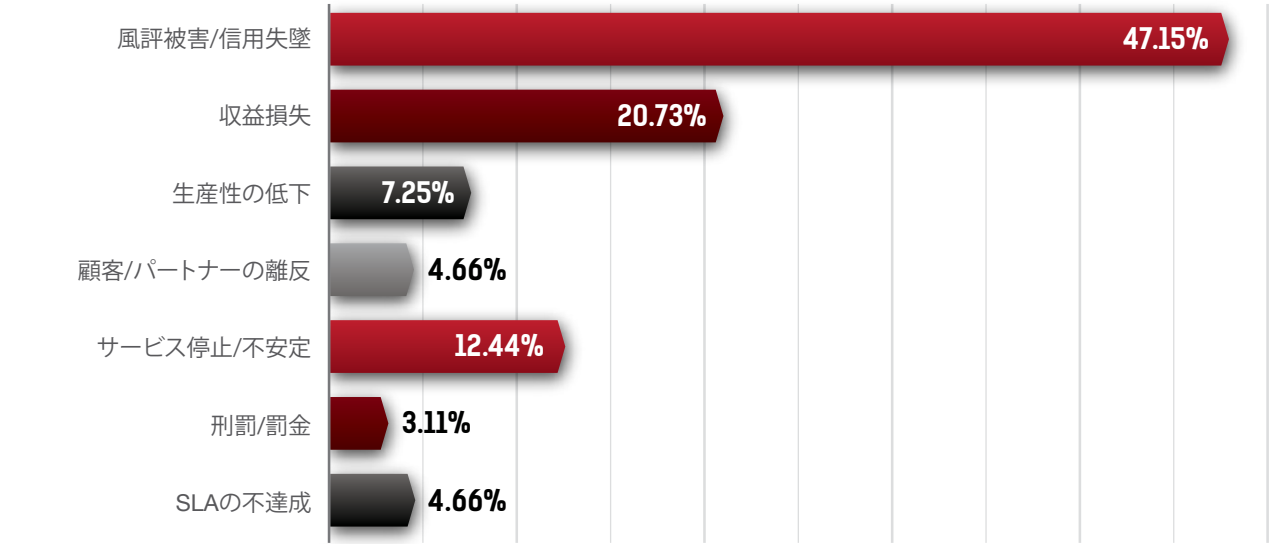


図7:サイバー攻撃によるビジネス面での懸念

予算割当と計画

「セキュリティーに関する業界調査」において、過去12か月に組織がサイバー脅威に対応してリソースをどのように展開したかについて尋ねました。回答者の半数以上が、セキュリティーに関するプロセス、プロトコル、または職務を変更したと答え、半数近くが新技術または専門的な技術に投資したと答えました。

過去12か月に組織はサイバー脅威にどのように対応しましたか？

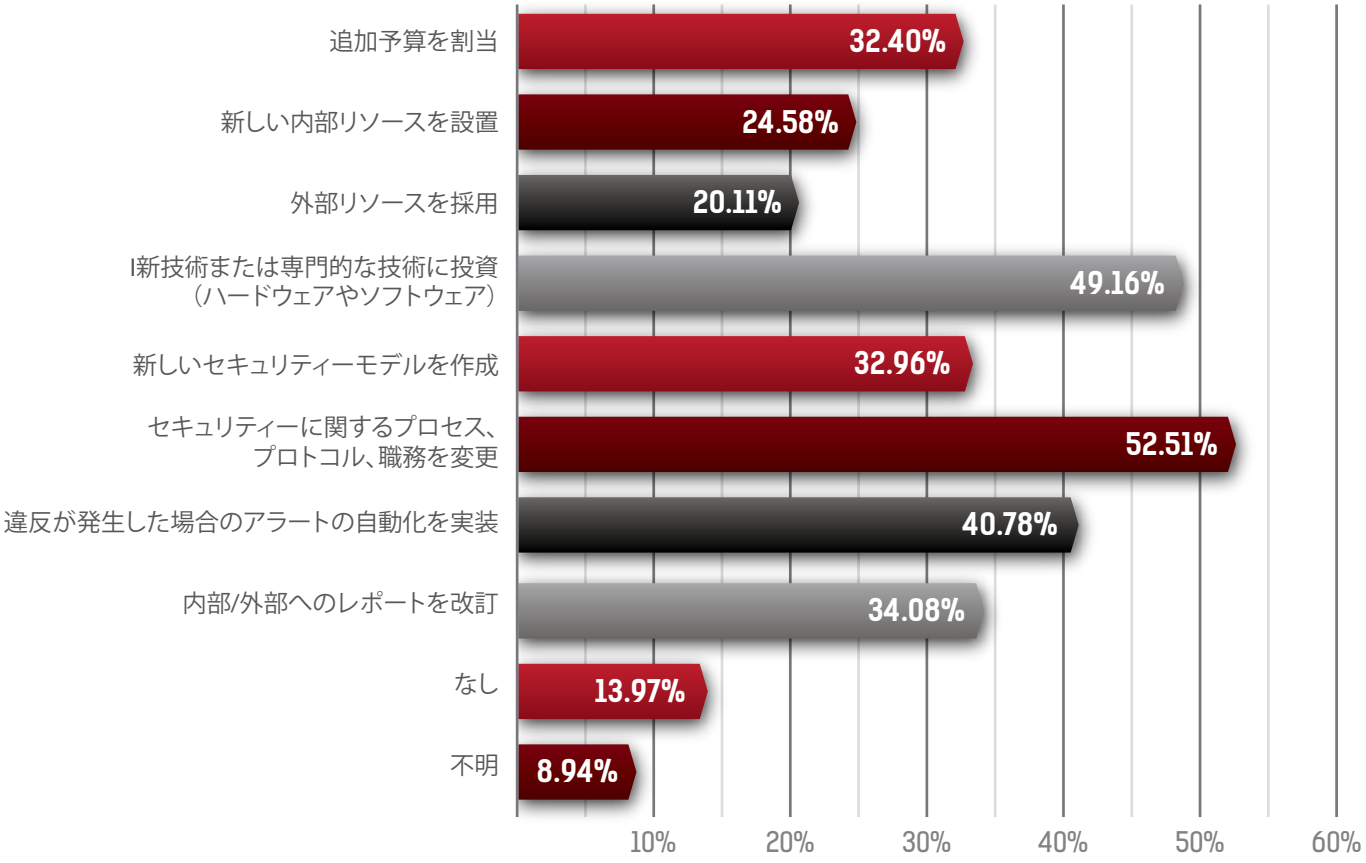


図8：サイバー脅威への対応

サイバー攻撃に対するハイブリッド防御

2014年は、回答者の3分の1以上（36%）がカスタマー構内設備（CPE）およびクラウドソリューションと共にハイブリッドソリューションをすでに使用しており、6%がハイブリッドソリューションの実装を計画していることが示されました。興味深いことは、半数近く（48%）が2015年までにハイブリッド防御を採用すると回答していることです。このトレンドは、ハイブリッドの方法が最適であるというラドウェアの長期にわたる見解と一致します。これは、市場でもアナリスト界でも継続的に勢いを得ている考え方です。

この理由は明白で、他にクラウドを防御する方法がなく、クラウドのミティゲーションが必須であるためです。一方、低レートの攻撃がクラウド防御のレーダーに気付かれないように飛んでいるため、オンプレミスのミティゲーションが必須になります。代表的な例として、SSLベースのトラフィックがあります。これは、復号化（このプロセスは組織内で行われます）されて初めて有意義な処理が可能になります。組織は、依然として、組織の証明書をクラウドプロバイダーにエクスポートできていません。

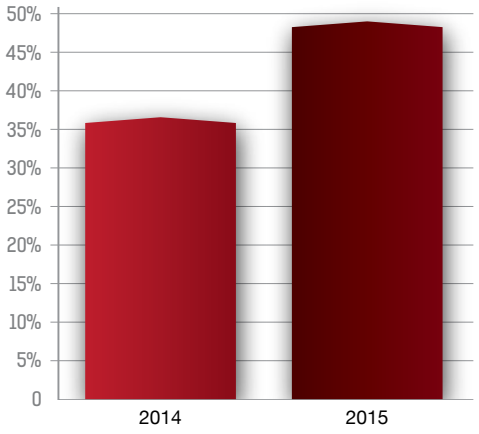
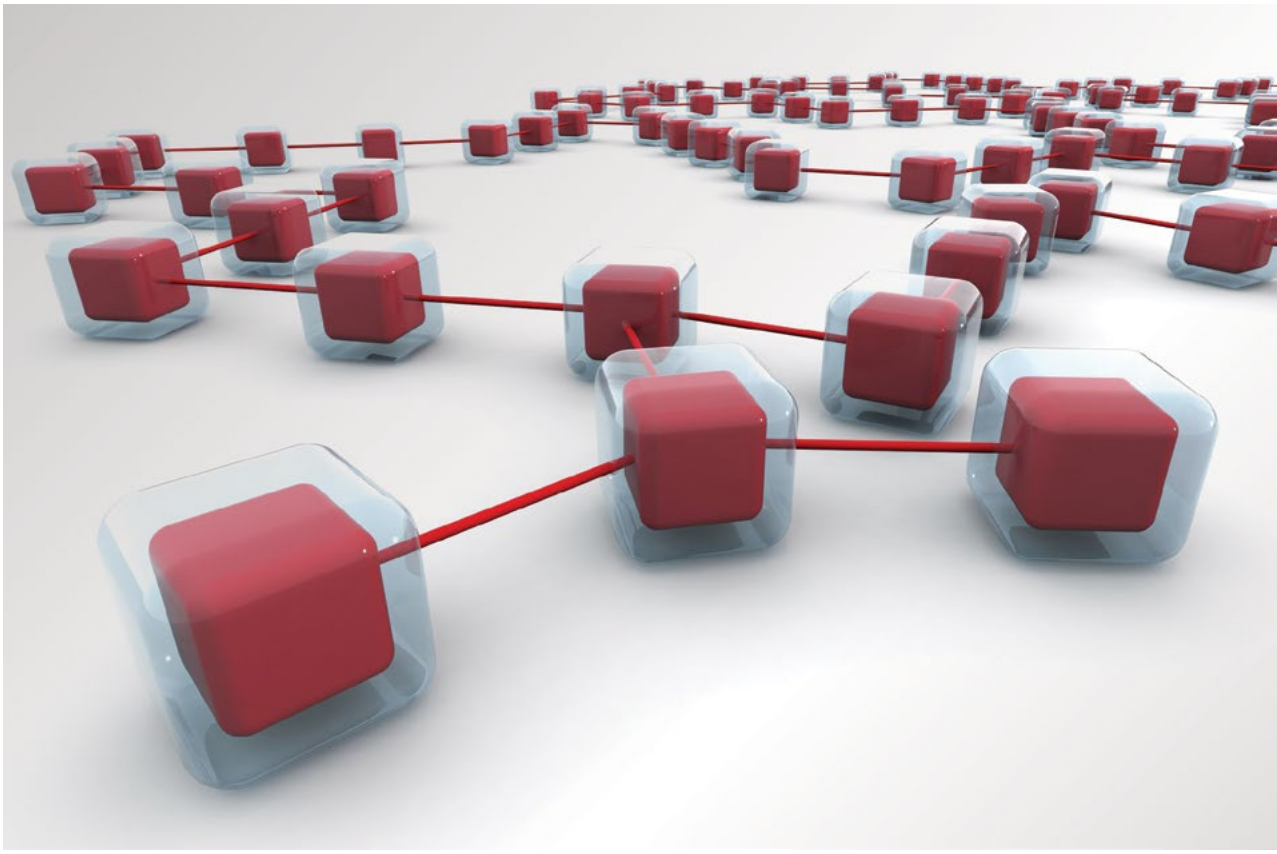


図9：ハイブリッドセキュリティーソリューションを現在使用している、および使用する予定がある組織

05 攻撃状況

攻撃ベクトルを取り巻く環境



ラドウェアのERTと今年の「セキュリティーに関する業界調査」の回答に基づき、本章では、2014年に流行した様々な攻撃ベクトルについてレビューします。

アプリケーション攻撃とネットワーク攻撃の割合

今年度版セキュリティーレポートにおいて、ラドウェアは、ネットワークのDDoS攻撃とアプリケーションのDDoS攻撃は均衡を保っており、今後も保っていくという見解を維持しています。これは、攻撃側の「関心」が、複数分野を組み合わせた攻撃にあるためです。例えば、相当程度の攻撃はもちろん、控えめな攻撃であっても、HTTPフラッド、UDPフラッド、SYNフラッド、スローレートの攻撃が含まれている可能性があります。つまり、新しい「トレンド」が生まれても、より強力な動因が残っているため、この状況の均衡が保たれるのです。

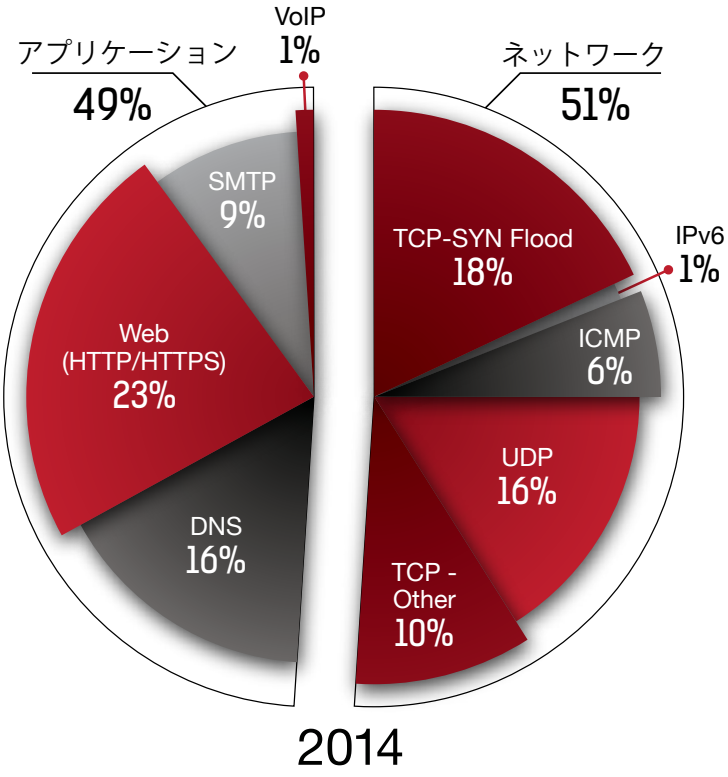


図10：ネットワーク攻撃とアプリケーション攻撃の割合 - 2014

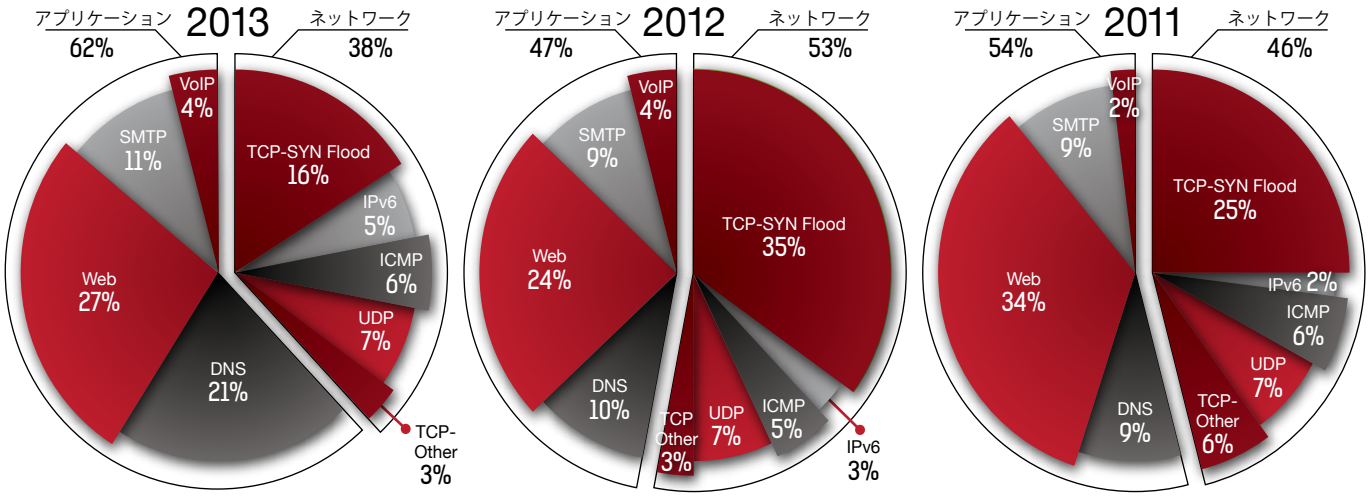


図11：年ごとの様々なサイバー攻撃ベクトル

驚くことではないかもしれませんが、2014年の結果は、ネットワークを標的とした攻撃が51%、アプリケーションを標的とした攻撃が49%と、均等に分かれました。2013年と比較すると、DNS攻撃は21%から16%に減少しました。2013年は、増幅リフレクター攻撃のほとんどがDNSを標的とするものでしたが、2014年はNTPとChargenがこのシーンに登場しました。その結果、2013年は7%であったUDP攻撃が2014年は16%に増加しました。一方、Web攻撃は依然として、最もよく見られる1つの攻撃ベクトルでした。Webベース攻撃の4分の3がHTTPを標的とする攻撃であり、4分の1がHTTPS攻撃です。

Web攻撃は依然として、最もよく見られる1つの攻撃ベクトルでした。Webベース攻撃の4分の3がHTTPを標的とする攻撃であり、4分の1がHTTPS攻撃です。

2014年、複数ベクトルの攻撃が「標準」に

2014年は、ほぼすべての攻撃キャンペーンが複数の攻撃ベクトルで構成されており、そのすべてのベクトルを見つけ出すことが難しいほどでした。1回の攻撃キャンペーンの攻撃ベクトル数が2014年にどれほど増加したかを評価することは、多くの意味で関心の的ではなくなりました。複数の攻撃ベクトルを持つ攻撃キャンペーンが一般的になったため、1つの攻撃ベクトルで攻撃キャンペーンを仕掛けるほうがはるかに珍しいものになりました。

- SYNフラッド攻撃
- UDPフラッド攻撃
- DNSフラッド攻撃
- HTTPアプリケーションフラッド攻撃
- SSLフラッド攻撃

とはいえ、攻撃をミティゲートしたERTの経験から、今年と昨年とではベクトルが異なることが示されました。これは、単に、攻撃キャンペーンが長期化したためです。これまでは、ほとんどの攻撃ベクトルが攻撃の初日に確認されましたが、現在は、防御側は毎日異なるミティゲーション作業を実行する必要があります。1つの攻撃ベクトルをミティゲートするたびに、翌日には新しい難題が待ち受けていることが判明するためです。

専門家でない人は、DDoSはそれ自体によって攻撃ベクトルになっていると考えるかもしれませんが、DDoSの分野に十分に精通している専門家は、攻撃ベクトルには数十、さらには数百もの亜種が存在し、その攻撃が新しい亜種を実際に創作していることを知っています。例として、ERTが2014年に発見したTsunami SYNフラッド攻撃を挙げてみましょう。この攻撃ベクトルは従来のSYNフラッドに基づいたものですが、この亜種のパケットは、データのない従来のTCP SYNパケットではありません。代わりに、攻撃は、各SYNパケットに約1,000バイトのデータを埋め込みます。興味深いこと

に、RFCはこのような使用を拒否しません。攻撃側にとって、このベクトルはボリューメトリック フラッドをTCPプロトコル上に送信できるため魅力的です。

「新しい」ベクトルのもう1つの例は、攻撃が攻撃を開始するタイムリーな方法に表されます。2014年、ラドウェアのERTは、攻撃が高レートのSYNフラッドを1分間生成し、15分停止した後、同じパターンを再開するという攻撃キャンペーンを数多く確認しました。また、他のケースでは、組織が非常に大きなボリューメトリックUDPフラッドに3分間晒され、沈黙の1時間を過ごした後、別のバーストに晒されるということもありました。確かに、2014年以前にも「バースト」攻撃はありました。しかし、これが多用されたことと、攻撃を同期する（短い時間で大量のフラッドを生成する）能力により、2014年、この攻撃は非常に目立つようになりました。現在は、多くの組織がDDoSに対する防御を備えていますが、攻撃側は、一定攻撃よりもバースト攻撃の効果が高くなる可能性があることに気づきました。セキュリティー対策が完全に効果を発揮するまで数分かかる場合がありますが、攻撃側はそれを都合よく利用することを学習したのです。

攻撃の強度と継続時間の増加

ラドウェアでは、攻撃の測定に、3つの軸に基づく一貫した公式を使用します。3つの軸とは、攻撃継続時間、攻撃ベクトル数、攻撃ベクトルの洗練度です。この公式により「DDoSスコア」が求められます。このスコアは、攻撃が進化し、攻撃の期間がどれだけ長くなり、規模がどれだけ大きくなり、洗練度がどれだけ増したかを示すのに役立ちます。これは、2014年の全く新しいトレンドというわけではありません。実際に、2013年および2012年の結果では、攻撃の複雑さと攻撃ベクトルの数が増し、さらに攻撃継続時間も長くなっていることが示されています。2014年の変化としては、攻撃継続時間が長くなり、超大型の攻撃が一般的になりました。

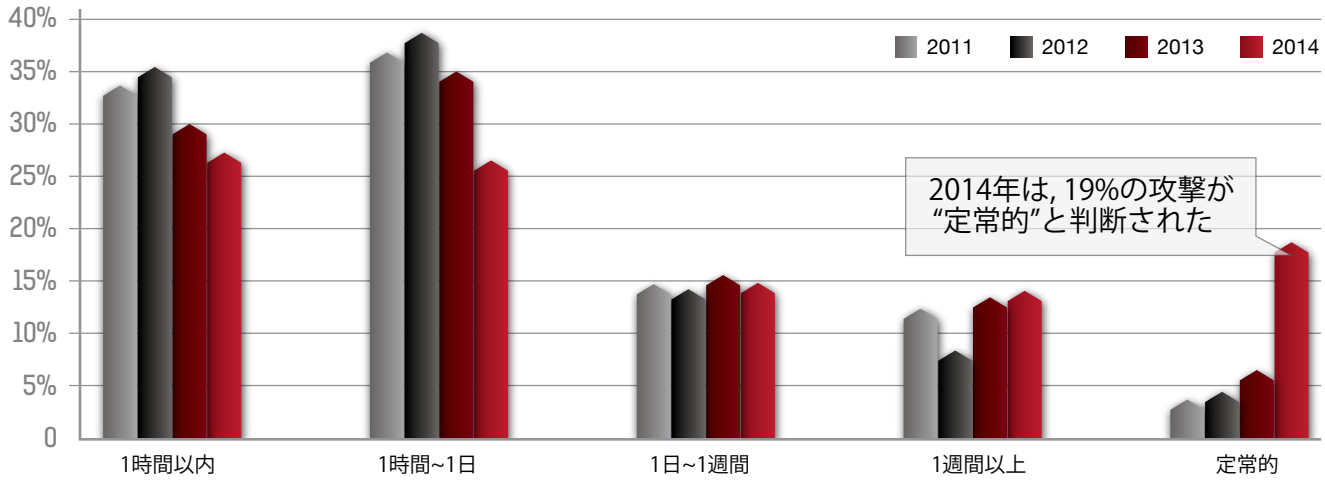


図12：年ごとの攻撃継続時間

2014年、ラドウェアのERTの多くのお客様が非常に長い攻撃を経験しました。調査結果にもこの経験が反映されており、報告された主な攻撃の19%が、標的となった組織によって「定常的な」攻撃と見なされています。これまでも（2013、2012、2011年）、1週間および1か月におよぶ攻撃は多く報告されましたが、定常的攻撃を受けたことを報告した組織は6%未満でした。

ラドウェアは、10Gbps～100Gbpsの攻撃を「超大型」とみなしています。注目を集めている事例に基づき、このような攻撃は長い間一般的であったと推論する人もいますが、実際には、つい最近（2013年や2012年）まで極めて稀でした。結局のところ、多くの組織は1Gbpsの攻撃にも耐えることができません。これ以上大きくする理由は何なのでしょうか。

しかし、2014年の経験や調査データから、状況が変わりつつあることが示されました。ラドウェアのERTは、超大型攻撃を毎日のように確認したことを報告しています。また、この攻撃はあらゆる種類の組織を標的としていることも報告しています。ラドウェアは、攻撃の期間が長くなり、規模が大きくなったのは、洗練度が増した（つまり、「壁のひび割れ」を狙い撃ちする欲望が突然強くなった）からではなく、攻撃側がいつでも自由に使える「向上した」技術、すなわちリフレクター攻撃によってもたらされたものと考えます。リフレクター攻撃を使用すると、超大型攻撃の生成だけでなく、その攻撃を長期間持続させることも比較的容易になります。

攻撃サイズ：サイズは問題になるか

セキュリティー部門の最高責任者の多くは、巨大な100Gbpsの範囲での攻撃に対する準備を行うことを重視しています。しかし、このような攻撃に過度に集中すると、近視眼的になる恐れがあり危険です。DDoS脅威の複雑さを見落としてしまうのです。実際には、より複雑な脅威の状況に準備すべきです。例えば、パイプ側よりも大きな帯域幅消費型攻撃、アプリケーション攻撃（帯域幅の観点では目立たないが特定の重要リソースを標的とすることができる）、「低くてスロー（Low & Slow）」な攻撃（レーダーに気付かれずに実行でき、帯域幅だけでは検知されにくい）などです。

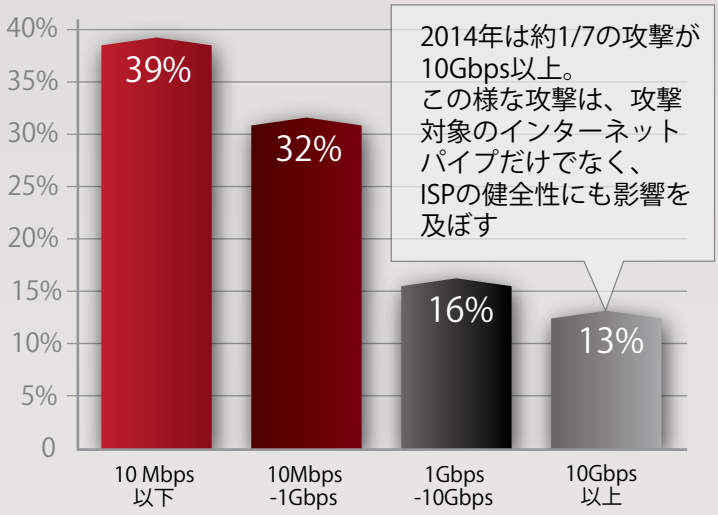


図13：サーバー攻撃の帯域幅

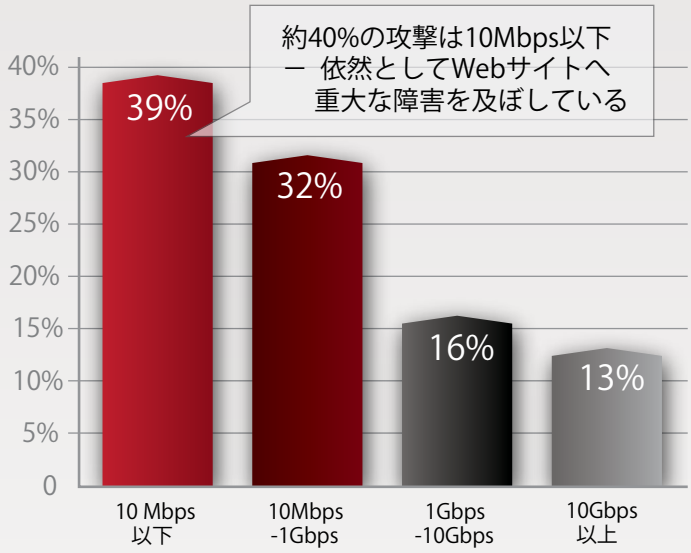


図14：サーバー攻撃の帯域幅

06

より洗練されたヘッドレスブラウザーとDDoS攻撃

HTTPプロトコル経由でアクセス可能なWebアプリケーションは、サービス拒否（DoS）攻撃と分散型サービス拒否（DDoS）攻撃のミティゲーションに関して様々な問題に直面します。組織が専用のDDoS対策ソリューションを導入して適応しているため、攻撃側も同様に適応しています。本章では、HTTPレイヤーでの攻撃の進化においてキーとなるマイルストーンについてレビューし、ヘッドレスブラウザーから脅威がどのように洗練度を増していったかについて説明します。

サービス拒否攻撃は、Webアプリケーションの多層アーキテクチャー内にある様々な要素を標的とすることができます。例えば、WebサーバーがHTTPプロトコル自体を処理する方法、WebサーバーのCPU、ストレージリソース、データベースや他のエンティティとの通信などが標的となる場合があります。DoS攻撃の目的は、Webアプリケーションの限られたリソースを枯渇させることで、ユーザー体験にダメージを与えたり、Webサイトを停止させたりすることです。

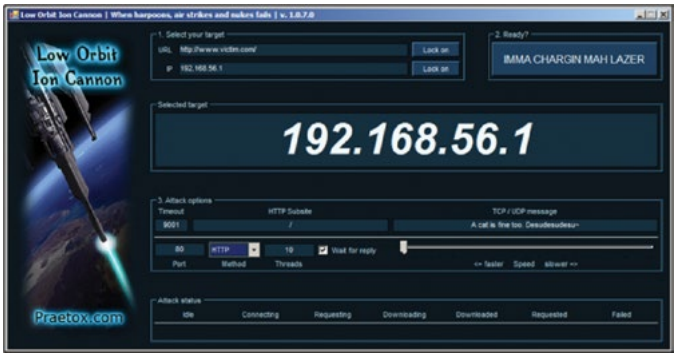


図15：LOICサービス拒否ツール

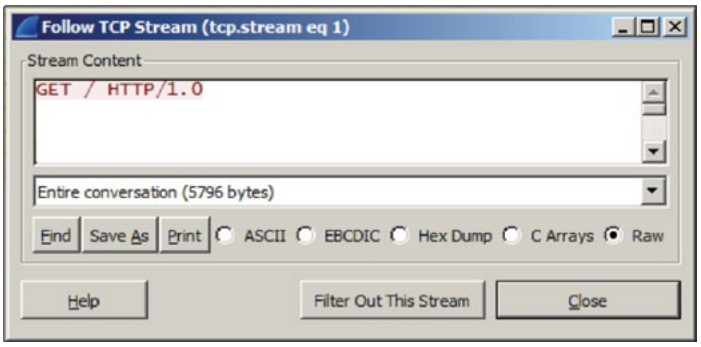


図16：LOICで生成されたHTTP GETリクエスト

例えば、HTTP GETフラッドはよくある攻撃です。この攻撃で、攻撃側は複数のHTTP GETリクエストを生成し、Webサーバーやデータベースの接続プール、帯域幅、さらにはCPUに負荷をかけます。Low Orbit Ion Cannon（LOIC）は、簡単なHTTP GETリクエストを素早く生成するサービス拒否ツールです。

GETリクエストを詳しく見ると、HTTPヘッダーのない最小限のGETメソッドが送信されていることがわかります。

ミティゲーションと適応のサイクル

DDoS対策ソリューションは、受信トラフィックを検査し、HTTPリクエストにHTTPヘッダー（有効なユーザーエージェントやホストヘッダーなど）が含まれているかどうかをチェックすることで、素早く対応しました。ヘッダーがない場合、またはヘッダーが無効な場合、DDoS対策ソリューションは、そのトラフィックに悪意があるとみなし、トラフィックをWebアプリケーションに渡しません。

攻撃側はミティゲーションを分析し、有効なヘッダーをHTTP GETリクエストに追加することで適応しました。また、静的なシグネチャの検出を回避するため、High Orbit Ion Cannon（HOIC）などの一部のツールには、ユーザー提供の有効なヘッダーリストに基づいて様々なヘッダーの組み合わせを送信するオプションが含まれています。

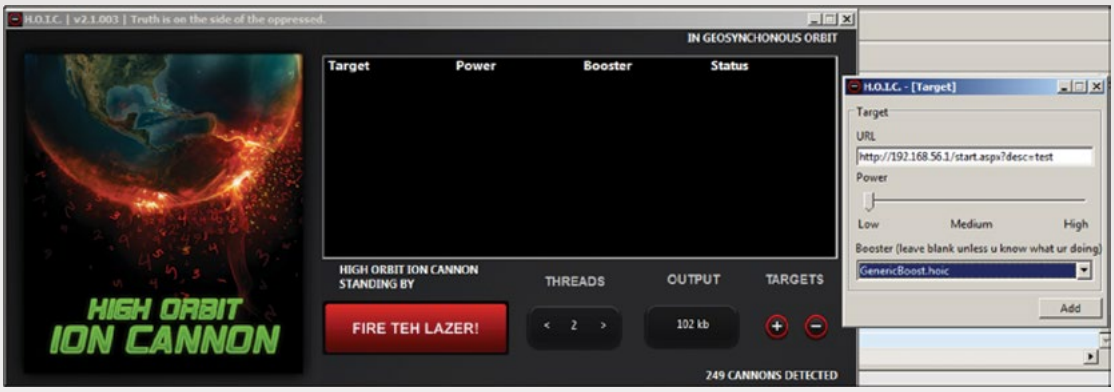


図17：HOICサービス拒否ツール

ツールは、RefererとUser-Agentのヘッダーに変化を付けます。

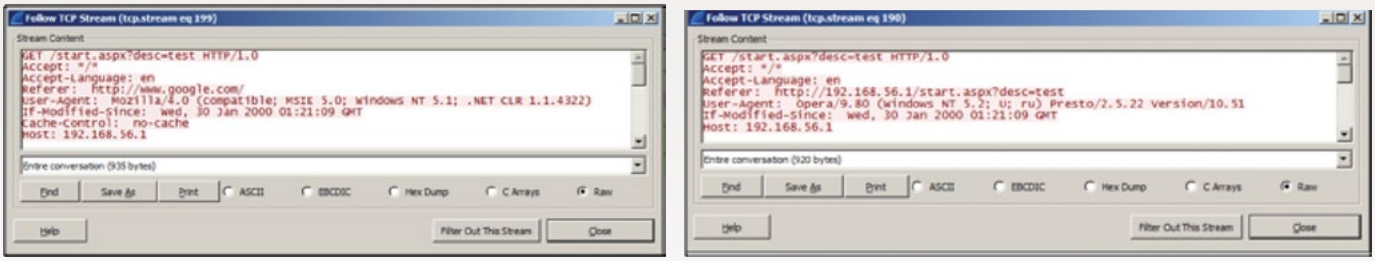


図18：HOICによるRefererヘッダーとUser-Agentヘッダーの変化

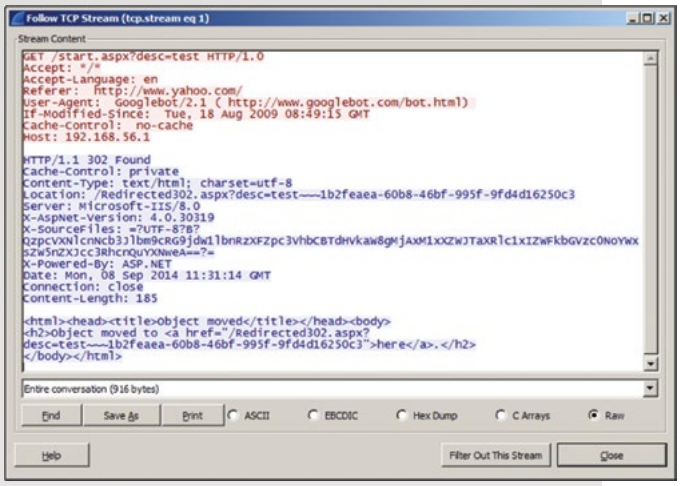


図19：HOICで生成されたHTTPが302リダイレクトのチャレンジに失敗

図20：Cookieチャレンジを処理するためのURLレトリーバーツール

この段階で、DDoS対策ソリューションは、トラフィックをサーバーに渡す前に別の簡単な安全機能を使用しました。DDoS対策ソリューションは、受信したリクエストに対してCAPTCHAチャレンジを表示します。ただし、この方法はユーザー体験に悪影響を与えたため、結局は特別な場合のみに限定されています。

そこで、DDoSソリューションは新しい方法を取る必要がありました。実際のユーザーが使用するツール（Webブラウザー）の動作を使用して、実際のユーザーと自動化されたトラフィックを区別する方法です。ブラウザーの動作から、HTTPチャレンジを発行して疑わしいトラフィックを検出する新しいメカニズムが提供されるようになりました。

初期のHTTPチャレンジ

対応すべき最初のHTTPチャレンジは、302 HTTPレスポンスコードです。このコードは、HTTPレスポンスに示されたリダイレクトに従ってWebアプリケーション上の目的のリソースにアクセスするようクライアントに指示します。簡易スクリプトおよび専用のDDoSツールは、特定のタスク向けに設計されたプログラムです。そのため、これらはリダイレクトに従わず、Webアプリケーションにアクセスしません。これらのスクリプトとツールを拡張し、ブラウザーと同様にあらゆるHTTPレスポンスを処理することはできますが、これは攻撃側の観点からは価値がありません。

HOICで生成されたHTTPフラッドは、302 HTTPリダイレクトに従いません。

第2世代のHTTPチャレンジ

もう1つの重要なチャレンジは、クライアント側のHTTP Cookieの処理でした。DDoS対策ソリューションは、HTTP Cookieを確立するようクライアントに指示します。また、以降のリクエストに有効なHTTP Cookieが含まれているかどうかをチェックします。

攻撃側はもう一度、302 HTTPとCookieチャレンジに適応するための新しい技術を開発しました。そのため、攻撃側は、これらのチャレンジを処理できる利用可能なURLレトリーバーツールを導入しました（curl、wgetなど）。

第3世代のHTTPチャレンジ

この時点までに、防御側は、正当なユーザーからのトラフィックとURLレトリーバーからのトラフィック（前述のcurl、wgetなど）を区別するための新しい技術を考案する必要がありました。

レスポンスに設定された新しいHTTPチャレンジは、動的なJavaScriptチャレンジでした。このチャレンジで、クライアントはJavaScriptコードを自動的に解析し、新しいリクエストをサーバーに送信します。このリクエストには、JavaScriptコードを解析して実行できたことを示す指示マーカーが付けられます。

JavaScriptコードの解析機能は、標準のURL取得に固有のものではありません。したがって、接続ストリームはこのチャレンジで終了します。

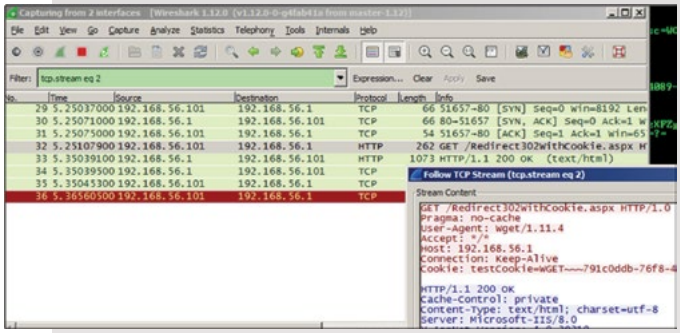


図21：WGETツールがJavaScriptチャレンジに失敗

第4世代のHTTPチャレンジ：ヘッドレスブラウザーの登場

第3世代のHTTPチャレンジを迂回したい攻撃側は、ブラウザーの動作を可能な限り模倣する方法を探し始めました。これにより、DDoS攻撃で「ヘッドレスブラウザー」が使用されるようになりました。ヘッドレスブラウザー（PhantomJS、HTMLUnitなど）は、ブラウザーとして機能するツールですが、GUIを備えていません。ヘッドレスブラウザーの最も一般的な使用法は、テストの自動化です。これは、ブラウザーのように動的コンテンツ（JavaScriptなど）を自動的に解析して実行できるためです。

このような洗練された攻撃を緩和するため、DDoS対策ソリューションでは「マウス移動」チャレンジを採用しました。DDoSツールは、書き込み時にこの機能をサポートできません。簡易スクリプトの場合、PhantomJSはすべてのチャレンジを簡単に迂回しますが、「マウス移動」チャレンジで停止します。

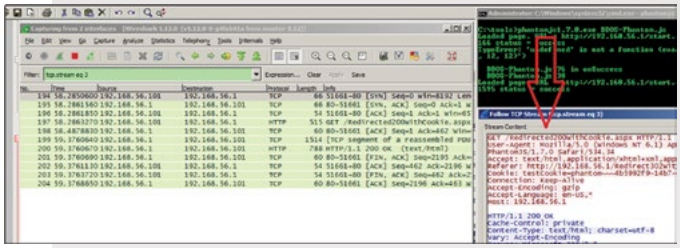


図22：ヘッドレスブラウザー - PhantomJS「マウス移動」チャレンジに失敗

次世代のHTTPチャレンジ

ヘッドレスブラウザーは急速に進化しています。コミュニティーから支援を受けたオープンソースの拡張機能（CasperJSなど）は、「マウス移動」チャレンジを含め、前述のすべてのHTTPチャレンジを通過できるようになりました。その結果、DDoS対策ソリューションのレーダーを迂回し、正当なトラフィックになりすますことができます。

このような洗練された攻撃は一般的ではありません。そのため、次世代のチャレンジは、このような自動侵入者を特定して合成しなければなりません。

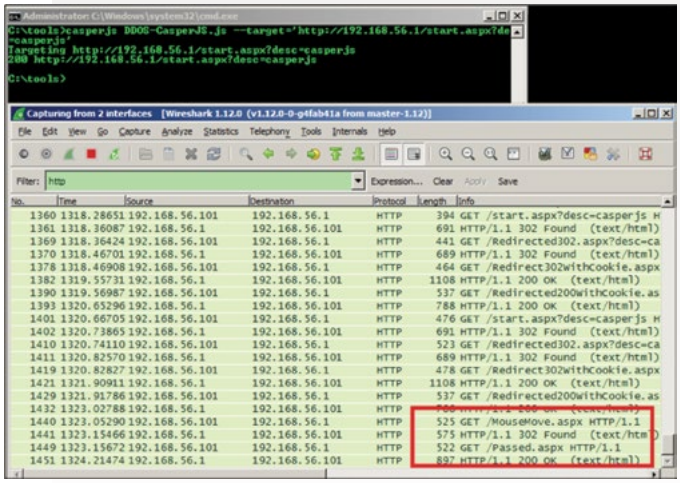


図23：ヘッドレスブラウザー - CasperJS「マウス移動」チャレンジを迂回

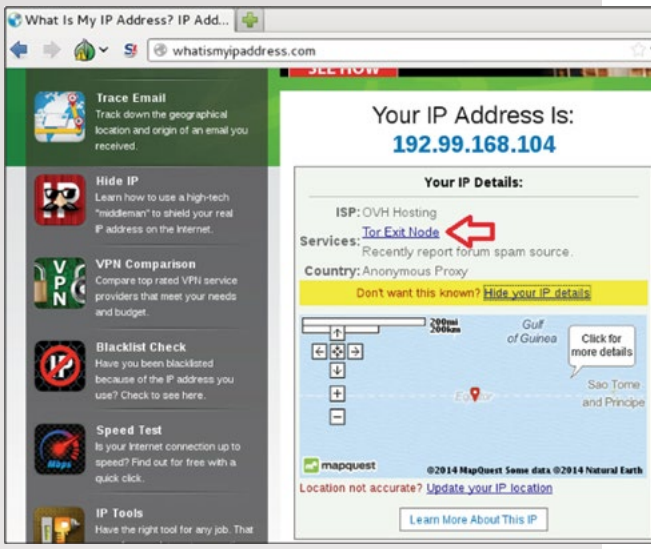


図24：Tor匿名プロキシ

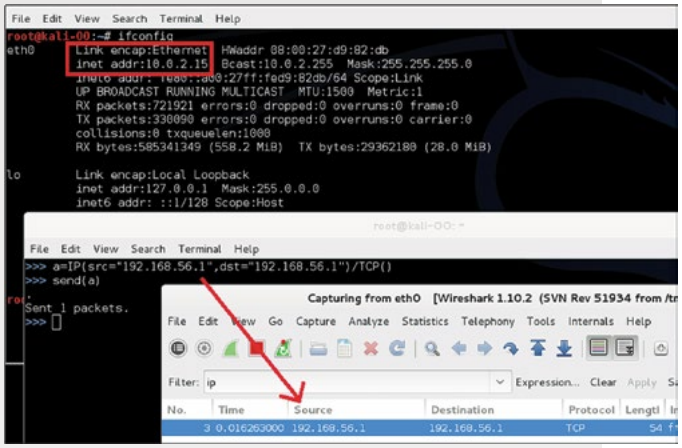


図25：IPソースポートのなりすまし

```
POST /xmlrpc.php HTTP/1.1
Host: pingbackSupportWP
Proxy-Connection: keep-alive
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/37.0.2062.103 Safari/537.36
Accept-Language: en-US,en;q=0.8
Content-Type: text/xml
Content-Length: 232

<methodCall>
  <methodName>pingback.ping</methodName>
  <params> <param><value><string>http://victim</string></value></param>
<param><value><string>http://SomeWordPressSite/p=1</string></value></param>
  </params>
</methodCall>
```

図26：User-Agent HTTPヘッダーの値のなりすまし

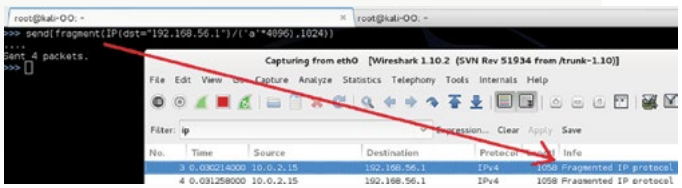


図27：パケットの断片化

混合型攻撃の台頭

組織がサイバー防御のために複数のメカニズムを導入しているため、攻撃側もそれに適応しています。攻撃側は、1回の攻撃に複数の技術を組み合わせることで防御ラインを通過し、サーバー側の脆弱性を悪用して、サーバー側のリソースに負荷をかけることができます。本項では、個々の技術の一部についてレビューし、組織のサイバー防御を妨害するためにそれらをどのように組み合わせることができるかについて説明します。

匿名化となりすまし

攻撃をミティゲートするための簡単なソリューションは、悪意のあるIPや許可されていないクライアントからのトラフィックをブロックすることです。このため、攻撃側は自分のIPアドレスを匿名のプロキシやサービス（Torなど）の背後に隠します。

Torネットワークから送信されたトラフィックを見分けることはできますが、すべての組織がこのトラフィックのブロックを望んでいるとは限りません。

IPアドレスを隠すもう1つのテクニックは、IPソースアドレスやUser-Agent HTTPヘッダーの値など、通信内のフィールドを変更することです。

2014年第1四半期、攻撃側はWordPressのPingback機能を悪用し、約160,000のWordPress Webサイトに対し、HTTP GETリクエストを犠牲となるサイトに送信するよう指示しました。

攻撃側が身元を隠すための、もう1つの一般的な方法は、リモートの侵害されたホストから（多くの場合、集められたボットネット経由で）攻撃を開始することです。

断片化

パケット検査のメカニズムは、与えられたパケット内でパターンを探します。攻撃側は、パケットをいくつかの小さいパケットに断片化することで、この検知を迂回できます。断片化では、検知チャレンジの合成に加えて、この検知回避を処理するためにトラフィックの断片化解除を実行する必要があるセキュリティーシステムに負荷がかかります。したがって、高レートの断片化トラフィックによって、セキュリティーインフラストラクチャー自体が危険に晒されます。

暗号化

SSL（Secure Sockets Layer）経由でアクセス可能なリソースを標的とする攻撃が増えています。その結果、トラフィックが暗号化され、多くの場合、防御メカニズムはそのトラフィックを検査できません。このような場合、防御メカニズムは、実際の検査を行わずに、伝送制御プロトコル（TCP）のペイロードをプロキシに送ります。

防御メカニズムが実際にSSL復号化を行った場合、復号化と暗号化の処理が大量に実行され、リスクが生じます。この処理は、SSLサーバー側のコンピューティングリソースとメモリーリソースに大きな負荷をかけます。このため、多くの攻撃者は、実際に検知をすり抜けるためではなく、負荷を大きくするために暗号化を追加します。

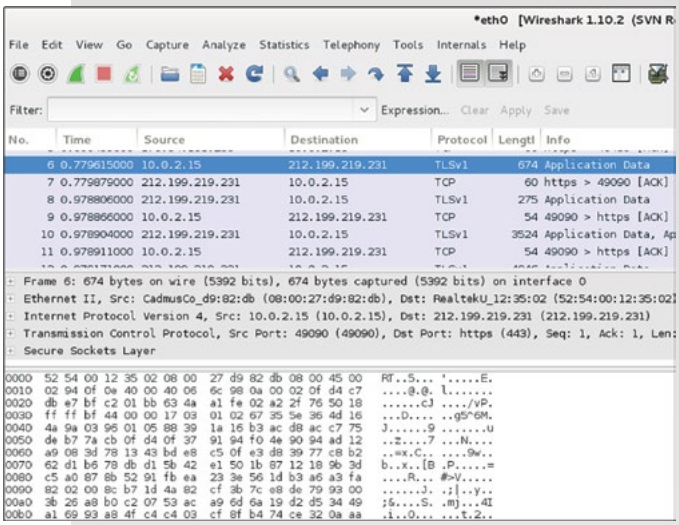


図28：SSL経由でアクセス可能なリソースを標的とした攻撃

動的パラメーター

もう1つの攻撃技術は、同じ攻撃を様々なパラメーターで繰り返し送信することです。動的パラメーターは、パケットの完全な静的シグネチャとコンテンツデリバリーネットワーク（CDN）の効果を排除します。各伝送が「新規」とみなされるためです。CDNは動的コンテンツを元のサーバーに自動的に転送するため、CDNを完全に迂回することができます。

図29：動的パラメーター攻撃

検知回避およびエンコード

根本的に、検知回避技術は問題を避けることです。一例としてペイロードのエンコードがあります。

攻撃側は、HTMLエンコード、URLエンコード、ダブルエンコードなど、ペイロードを様々な方法でエンコードすることで検知を回避します。例えば、攻撃側は、javascript:alert(/xss/)を送信する代わりに、ペイロードのURLエンコードを2回行います。防御メカニズムは、ペイロードのデコードを1回行って、悪意のあるパターンがないかを検索し、ペイロードをバックエンドサーバーに送信します。バックエンドサーバーはペイロードを受信し、再度デコードして悪意のあるペイロードを実行します。

このようなメカニズムを検知するには、HTTPトラフィックを完全に正規化する必要があります。これは、多くのセキュリティーシステムでは実行されない、リソース消費型の別の操作です。

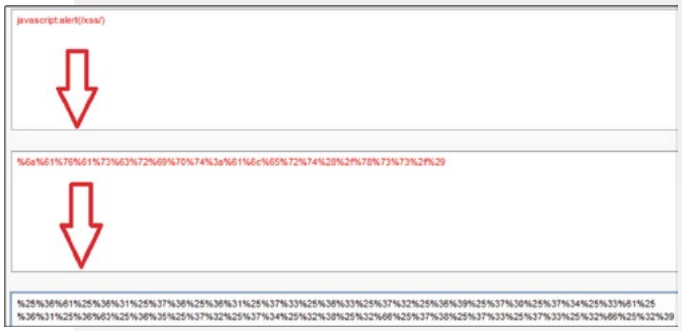


図30：検知回避技術 - ペイロードのエンコード

パラメーター汚染

場合によっては、防御メカニズムのアルゴリズムが特定の場所の値を検査する一方で、バックエンドサーバーは別の場所の値を読み取ることがあります。この場合、攻撃側は、バックエンドデータベースで実行されるSQLインジェクションのペイロードを送信できます。

広範な機能の悪用

攻撃のエンドポイントは、攻撃の成功を左右する重要な要因です。攻撃側は、実行時にサーバー側の大量のリソースが必要な機能を探しています。機能を特定すると、そのリソースに大量のリクエストを送りつけるフラッド攻撃を仕掛け、サーバーに限界まで、または限界を超えた負荷をかけます。

例えば、同じWebアプリケーションの様々なページに対してHTTP GETフラッド攻撃が実行された場合、様々な結果が生じます。最初のフラッドは、デフォルトの静的ホームページを襲います。同時に、2番目のフラッドがWebサイトの検索機能を標的とします。静的ホームページへの攻撃では、サーバーはレスポンスを素早く送信できます。最小限のリソースで静的レスポンスを生成できるためです。一方、SSL経由での検索を要求するリクエストを受信した同じWebアプリケーションは、検索操作を実行し暗号化された伝送を処理するため、サーバー側の追加のリソースを必要とします。

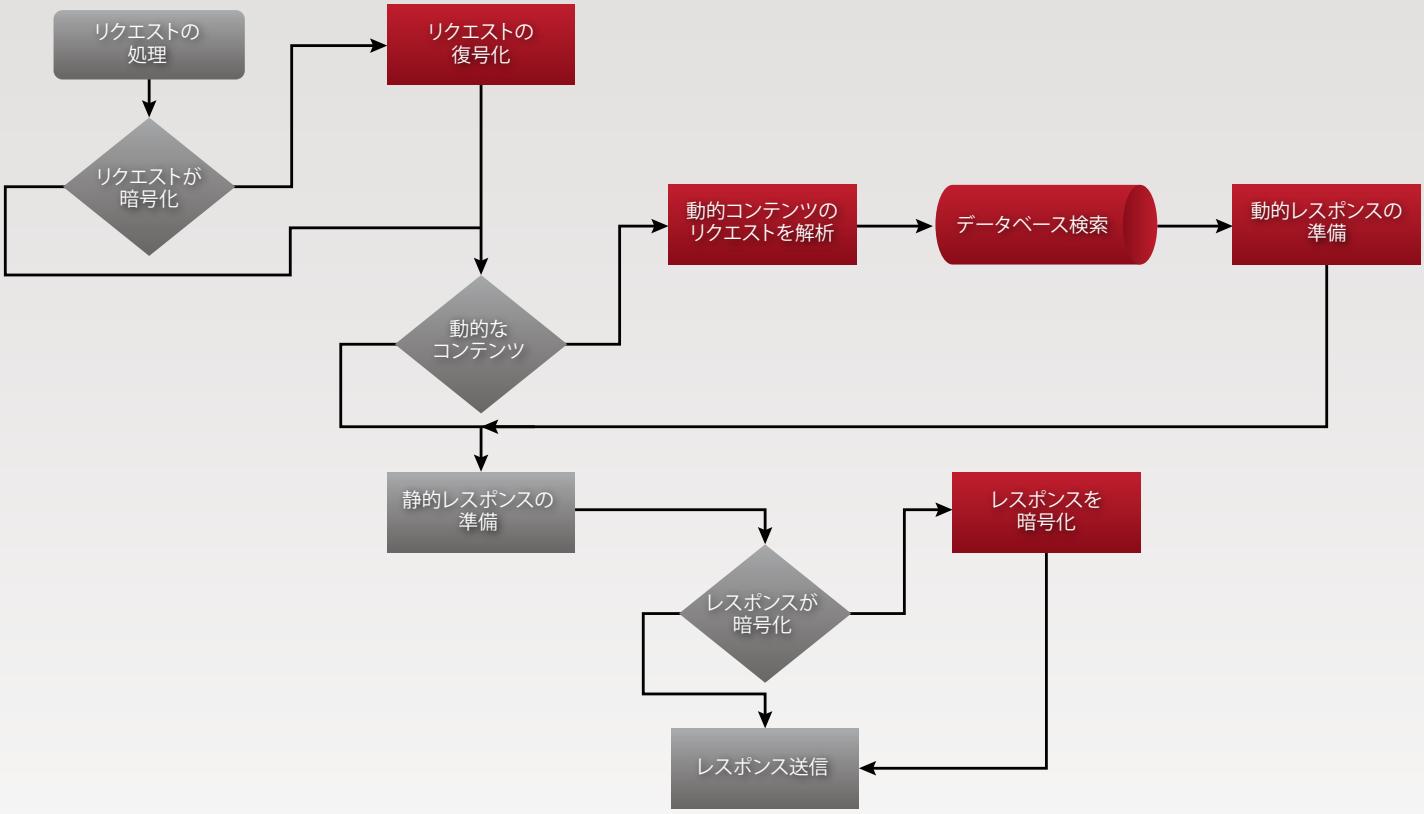


図31：暗号化された動的レスポンスの生成には追加の操作（赤の部分）が必要

混合攻撃のデモ：全体は部分の総和を上回る

複数の攻撃技術のレビューから明らかになったことは、別々に到達した攻撃はそれぞれ害を及ぼしますが、同じ技術が結合された場合、損害は悪化するということです。

このシミュレーションでは、非常に脆弱なWebアプリケーション（Damn Vulnerable Web Application）に対して混合型DDoS攻撃が実行された場合、この攻撃がどのように組織の防御ラインを通過し、バックエンドサーバーへリクエストあたり99.9%のCPU負荷をかけるかを分析します。

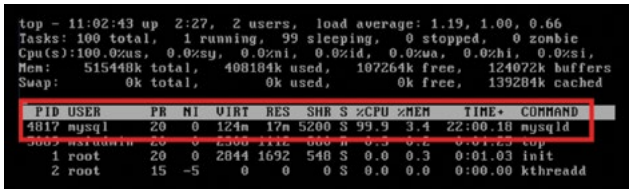


図32：DVWA（Damn Vulnerable Web Application：非常に脆弱なWebアプリケーション）に対する混合技術によるDDoS攻撃

最初に、疑わしいトラフィックのキャプチャーを分析します。

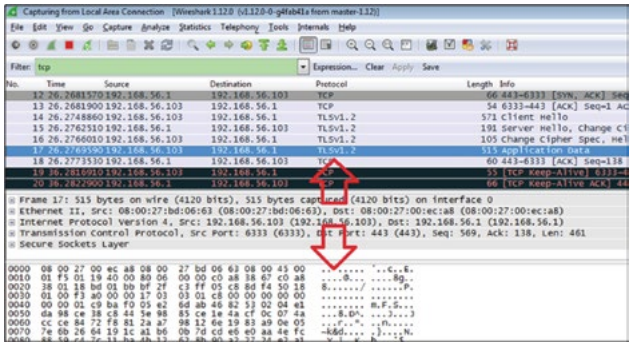


図33：疑わしいトラフィックの分析

このキャプチャーから、トラフィックが暗号化されていることがわかります。トラフィックを分析して悪意のあるパターンを検知することができない防御デバイスがあり、トラフィックの復号化と検査には追加のリソースが必要です。

復号化されたトラフィックを分析すると、悪意のあるリクエストがサーバーに送信されたことがわかります。

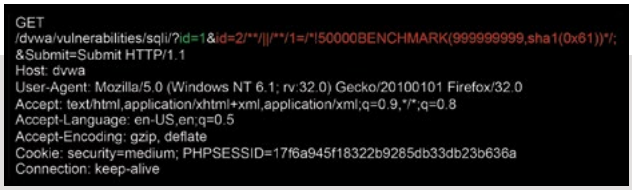


図34：復号化されたトラフィックの分析から、悪意のあるリクエストがサーバーに送信されたことが明らかになった

ペイロードは、攻撃が、クライアントからの入力を受け取るWebページへのSQLインジェクションであることを示しています。組織のWebアプリケーションファイアウォール（WAF）は、なぜこの攻撃をミティゲートしなかったのでしょうか。

ペイロードは次の技術を使用してミティゲーションを回避しました。

1. 攻撃は動的ページを標的としているため、サーバー側の追加のコンピューティングリソース（CPU、データベース操作など）が必要になります。
2. 緑と赤の部分は、IDパラメーターが重複していることを示しています。赤のテキスト内のペイロードは、2番目のIDパラメーターにSQLインジェクションのペイロードが含まれていることを示しています。緑のIDの値には、正当な値が入っています。
3. IDパラメーターは1つの値を受け付けるように構成されているため、スペースを含めることはできません。攻撃側は、完全なSQLステートメントを挿入する必要があるため、スペースに相当する/**/のコメントマーカーを使用しました。このコメントマーカーを使用すると、攻撃側は、1つの完全なSQLステートメントに複数のディレクティブを挿入することができます。これは依然としてIDパラメーター内の1つの値として解釈されるのです。
4. 攻撃側は、SQL ORディレクティブの代わりに || の組み合わせを使用します。これをパターンマッチングで選択することができます。
5. sha1(0x61)は、0x61のsha1ハッシュを計算するようサーバーに指示します。0x61は16進数でエンコードされます。これを検知回避技術として使用し、コンマ区切り文字無しでテキストを送信します。これは、文字「a」を表します。
6. /*!5000payload*/は、BENCHMARKキーワードの正規表現検索から逃れることを目的とした、もう1つのパターン検知回避技術です。
7. BENCHMARK関数は、アクションを特定の回数実行するようデータベースに指示します。

以上をまとめると、攻撃ペイロードはデータベースに対し、**1つのリクエストを受信するたびに「a」文字のsha1ハッシュを999,999,999回計算するよう指示します。**この攻撃により、大量のデータベース操作が繰り返されたため、サーバーはサービス拒否に陥りました。

障害点

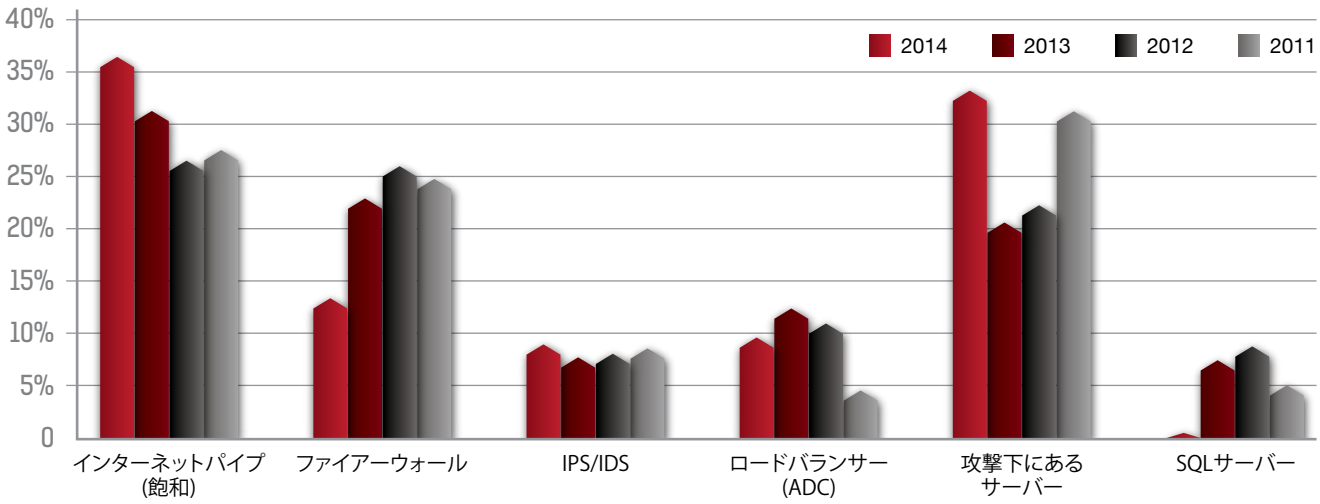


図35：DoS攻撃でボトルネックになる（またはなっていた）サービスまたはネットワークは何ですか

2011年、ラドウェアは、DDoS攻撃の障害点に関して、セキュリティーリーダーへの調査を開始しました。毎年、結果は概ね一貫しており、障害点は主に3つのエンティティに分けられます。当然ながら、最も明白なエンティティは直接攻撃を受けるサーバーです。ただし、インターネットパイプが溢れた場合はインターネットパイプ自体が障害点となります。また、ファイアウォール（ステートフルデバイス）も、サーバーよりも早く障害が発生することがあります。

2014年のラドウェアの調査では、障害点としてインターネットパイプが増えていることがわかりました。実際に、障害点の第1位というありがたくない名誉に輝いたのはインターネットパイプです。その原因として可能性が高いのは、ユーザーデータグラムプロトコル（UDP）増幅リフレクター攻撃の増加です。

増幅されたフラッド リフレクター攻撃が重要課題

10～20年前は、DoS攻撃のほとんどがSYN、TCP、UDP、およびICMPフラッドを通じてネットワークを標的とするものでした。2010～2012年にかけて、より洗練されたアプリケーション攻撃が増加し、一部の専門家はネットワーク攻撃の終焉を告げました（ちなみに、ラドウェアは常に両者は均衡すると断言しています）。

最近になって、特定の種類のDoS攻撃（増幅リフレクター フラッド攻撃）がネットワーク攻撃を復活させただけでなく、このDoS攻撃によるネットワーク攻撃が、アプリケーションを標的とするもう一方の攻撃よりも優位に立っています。

DNSやNTP、CHARGENなどを使用した攻撃を含めたリフレクター攻撃が過熱し始めたのは2013年ですが、その脅威は2014年も続きました。増幅リフレクター攻撃は一見単純に見えます。この攻撃を効果的にしているものは、攻撃の生成方法の容易さと、ネットワークに与える影響です。

「当社のネットワークで最もよく見られた攻撃は、NTPとDNS増幅攻撃でした。サービスの低下が見られたため、結果的に新しい防御策を講じました。」

ダニー・コームズ
(Dannie Combs)
CISMシニアマネージャー
ネットワークセキュリティー
US Cellular

タイプ	増幅定数	増幅方法
DNSリフレクター攻撃	x5-x100	ドメインネームサービス（DNS）の増幅定数は、その性質上5倍になります。「ANY」または別の技巧型増幅を使用すると、100倍まで増幅できます。
NTPリフレクター攻撃	X300	ネットワークタイムプロトコル（NTP）は時間同期のための重要なプロトコルです。そのMONLISTコマンドは、リクエストの300倍のレスポンスを生成できます。
CHARGENリフレクター攻撃	x50	一般に伝送制御プロトコル（TCP）と共に使用されるCHARGENは、テスト目的で1バイトストリームを受信します。ただし、ユーザーデータグラムプロトコル（UDP）もサポートするため、50倍大きいレスポンスを生成します。
UPnP SSDP	x30	ユニバーサルプラグアンドプレイ（UPnP）、特にSSDP（Simple Service Discover Protocol）。これにより、ネットワークデバイスを「知る」ことができます。

ハッカーは、あらゆるプロトコルを通り抜けて、次の大規模リフレクター攻撃に向けてインターネットパイプをどのように使用するかを判断しているように思われます。

攻撃対象へ苦痛を増大するために、2014年は帯域幅消費型攻撃が流行しました。真に大容量の攻撃（10Gbpsを超える攻撃）は、前年までは一般的ではありませんでした。しかし、2014年はこの状況が変わり、多くの組織が10Gbpsを超える攻撃の脅威に晒されました。実際に、20Gbps～50Gbpsの攻撃は珍しいものではなくなり、帯域幅消費型攻撃は、組織が理解して備えるべき重要な脅威の1つになりました。

興味深いことは、大容量攻撃は小規模組織よりも大規模組織に影響を及ぼすことです。小規模組織のラインが100Mbpsの場合、帯域幅消費型攻撃のサイズは意味がなくなります。攻撃サイズが100Mbps、1Gbps、さらには10Gbpsであっても、組織は外部のセキュリティーサービスを使用して防御する必要があります。しかし、大規模組織では状況が大きく異なります。大規模組織は、100Mbps攻撃の脅威をほとんど受けていません。攻撃が1Gを超えた場合に問題になりました。

大容量攻撃に特に悩まされるのは通信事業者です。通信事業者の場合、50Gbpsの攻撃を1人の最終顧客が受けても見過ごされることはありません。このような大容量の攻撃を頻繁に受けた場合（場合によっては週単位であっても）、通信事業者は、個々の対象だけでなくネットワーク全体を防御する必要がありました。

「増幅リフレクター攻撃（DNS、NTPなど）を受けた結果、新しい防御策を講じる必要が生じました。」

Fortune 1000に選ばれた米国を拠点とする金融サービス企業の情報セキュリティー戦略＆開発担当副社長

07 非常に破壊的かつ不変な、情報セキュリティーの3つのマクロトレンド

今日のビジネス環境には、マクロのビジネストレンドがどこからともなく現れ、企業や、場合によっては業界全体を時代遅れなものにしてしまう可能性があることを思い起こさせる数多くの事例があります。ソニーが携帯音楽を支配していたことを覚えていますか。古くはスミス・コロナのタイプライターや、その後の携帯情報端末のパームや携帯電話のBlackBerryなどの「革新的」な生産性ツールはどうでしょうか。破壊的技術に直面して、これらや他の多くの製品は旧式のものとなっています。切迫するマクロトレンドを認識していなかったか、単に時代に適応できなかったためです。

ラドウェアは情報セキュリティーのプロフェッショナルとして、技術の劇的な変化の影響とは無縁ではありません。本項では、情報セキュリティーに影響を与えている、非常に破壊的かつ不変な3つのマクロトレンドについて詳しく見ていきます。これらのトレンドを無視したり、これらのトレンドに抵抗したりして、時代遅れにならないようにしてください。

過去

様々な業界の様々な企業が、スピード、効率、競争力の名目で、自動化されたシステムやプロセスを導入していました。過去20年間、情報セキュリティーの専門家や技術は、こういった投資を標的とした脅威の環境を阻止することに努めてきました。ほとんどの場合、これらの自動化システムやその保護を目的としたセキュリティーツールには、企業と顧客との関わり方に対する長年にわたる前提が反映されていました。しかしこの36か月間、その前提に対する異議が勢いを増しています。代わりに表れた新しいモデルは、クラウドコンピューティングへの転換、「Internet of Things（モノのインターネット）」の成長、そしてSDN（Software-Defined Network）の台頭を特徴としています。

現在

クラウド移行への大きな流れの継続と企業ITの解体

今日の最後の「未開拓領域」は物理的な存在ではなくなり、論理的な存在になりました。巨大なクラウド企業がこの未開拓領域を構築し、これまで情報技術機能の範囲であったいくつかの側面を最適化しています。クラウドプロバイダーは、サービスモデルを使用して企業のインフラストラクチャー、アプリケーション、さらには特定の機能（ドメイン名の解決、セキュリティなど）の購入方法や使用方法に革命をもたらしています。

最近は、IT機能の一部の側面を「クラウドソース」していない企業を見つけることはほぼ不可能です。実際、多くの企業が、クラウド経由で提供されるITサービスのみに依存しています。Uber、Netflix、Pinterestなどのハイテク企業のトレンドは、内部のIT機能の構築にわざわざ悩まされないようにすることです。代わりに、クラウドサービスプロバイダー経由で競争します。かつて、製造プラントは使用する電気を発電していました（以前はこれが不可欠でした）が、適切なレベルのサービス品質と継続性を満たすことができる発電網への接続にシフトしましたが、クラウドへの移行はこれに似ています。現在の企業は、クラウドのコストや速度のメリットを無視できないことを理解しています。

では、情報セキュリティーの専門家にとってこれは何を意味するのでしょうか。これは、古いモデルである集中制御、内部ポリシー、従業員の意識、内部プロセスの認証（ISO 27001など）が、これまでと大きく異なるもの（現代の工場のカンバン方式に似た方法）に取って代わられようとしていることを意味します。結局のところ、マシン全体の1つの歯車だけが安全であっても、誰がそれを気にするでしょうか。すべての歯車が安全で、他のすべての歯車と連携して動いていなければならないのです。

結論：CISO（最高情報セキュリティー責任者）は、将来、自社インフラストラクチャーを持たず、内部開発された相関レポートもなく、また、従業員を教育する必要もないかもしれません。しかし、このシナリオは現在の実務者の育成方法と大きくずれています。

「サイバーセキュリティーの環境を複雑にしている「モノのインターネット」をどのように考えるべきでしょうか。「モノのインターネット」は、攻撃面を広げ、攻撃自体の洗練度を高め、ミティゲーションの要件を複雑にしています。」

ドメニコ・マルティーニ
(Domenico Martini)
ネットワークマネージャー
SEAT Pagine Gialle

モノのインターネット（IoT）による、制御されたエンドポイントの終結と、驚くほどの新しい脅威の登場

健康管理用のウェアラブルな接続デバイスであるFitBitの流行は、もう1つのマクロトレンドで、ほぼユビキタスなつながりに向けた動きを示しています。テレビ、洗濯機、冷蔵庫はすでにオンライン化されています。このトレンドが進み、自動車や広告版、レストランのテーブル、自宅が次第に「自己認識」するようになり、新しく広範な形で人間とつながるでしょう。

ほぼどんなモノからでもどこにでもつなげることができるということは、仕事や生活の効率を劇的に高めるでしょう。ただし、この「モノのインターネット」は新しい重大なリスクや脅威ももたらします。例えば、車が自動運転を始めると、車がハッキングの標的となり、誰が「ハンドルを握っている」かに関して非常に物理的な脅威が生まれます。サイバー攻撃の世界では、未来の軍隊は人ではなく、デバイスで表される「ボット」になります。現在、セキュリティー専門家の大半はBYOD（Bring Your Own Device：個人所有機器の持ち込み）の問題を心配しています。制御されていない新しいデバイスが「セキュアな」ネットワーク環境に入ってきてしまうからです。実際には、現在のBYODの電話やタブレットに関する問題は、固定型の消費者用デバイスと組み込み型の産業用デバイスの両方からの接続性に関するより複雑な問題にすぐに取って代わられるでしょう。

時が経つにつれ、セキュリティー専門家の大半は、従業員のエンドポイントデバイスをセキュリティハードウェアやソフトウェアを使用して制御することがもはや経済的、技術的、政治的に不可能であることに気づくでしょう。このため、エンドポイントのセキュリティーは、「入口」のセキュリティーに徐々に取って代わられることになります。つまり、セキュリティー調査を、ネットワーク自体ではなく企業にとって意味のあるアプリケーションとの間のすべてのリクエストに対して実行するのです。エンドポイントから入口へのシフトにより、セキュリティーの方法に劇的な変化が生じるため、熟練した実務家は転換を図る必要があります。これに抵抗する実務家（過去のビジネスモデルに固執する人）は、コストや文化、市場投入のスピードの点で、企業に致命的な打撃を加えることになるでしょう。

サイバー攻撃の環境を複雑にしているIoTをどのように考えていますか？

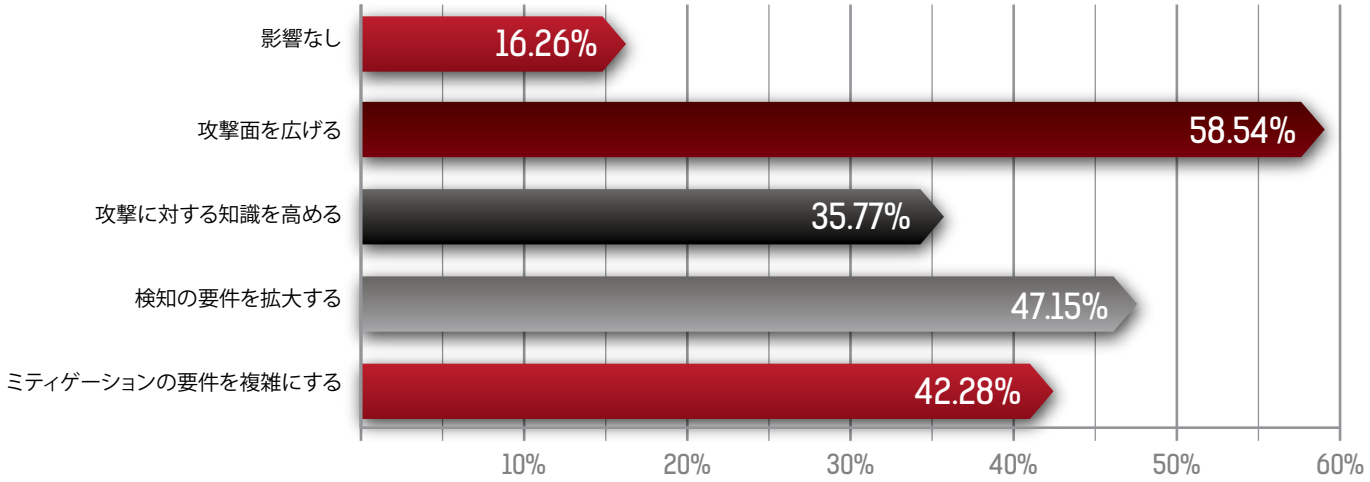


図36：サイバー攻撃環境におけるモノのインターネット（IoT）

SDN（Software-Defined Network）によるゲームのルールの変更

映画トランスフォーマーを観たことがある方は、Software-Defined Network(SDN)の考え方をすぐに理解できるでしょう。1つのもの、例えばコーヒーメーカーや自動車として設計されたデバイスが、一瞬のうちにプログラムされ乗っ取られて、他のことを実行したり、他のものになったりすることができるのです。トランスフォーマーの世界では、物理的な側面と論理的な側面を組み合わせて魔法のような変形を生み出します。現実世界ではこのような変化は現実的ではないかもしれませんが、論理変換の考え方は極めて現実的であり、すでに使用されています。

SDNをどのように活用していますか?

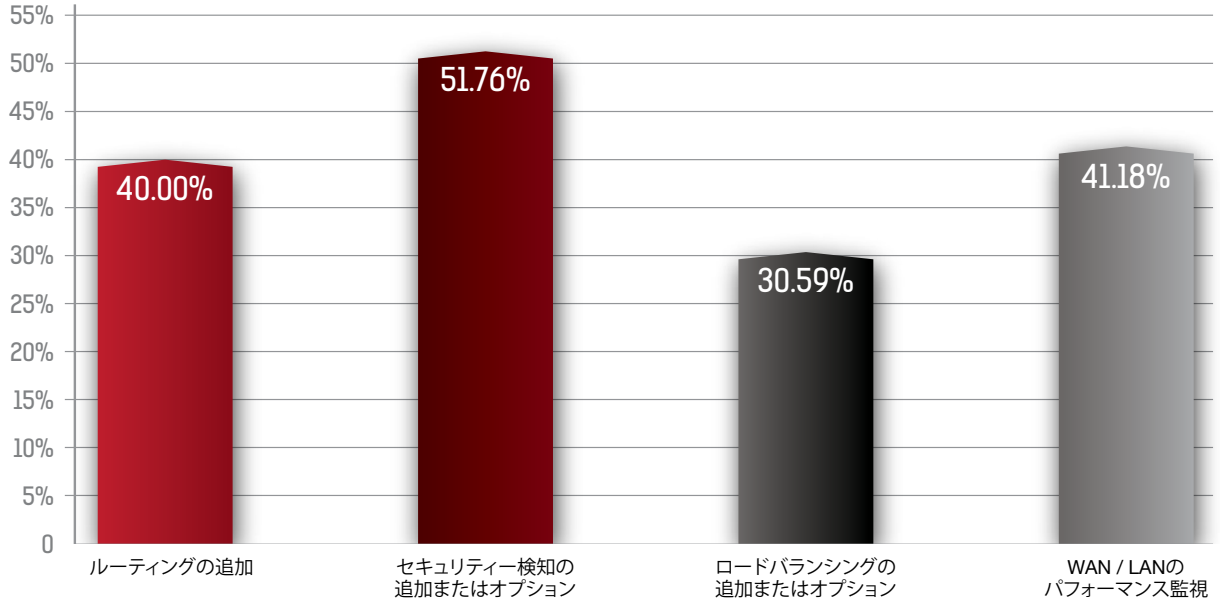


図37：組織によるSDNのr利用

SDNを使用すると、ネットワーク管理者は、下位レベルの機能を抜き出してネットワークサービスを管理できます。つまり、トラフィックの送信先を決定するシステムを、選択された宛先にトラフィックを実際に転送する基盤となるシステムから切り離すのです。私たちの世代においてほぼ間違いなく最も有望かつ破壊的なイノベーションであるSDNは、技術の活用方法を一変させる態勢にあります。

SDNの様々な「キラーアプリ」の導入および発展段階でなぜ数十億ドルもの利益や損失が生まれるかについては、2つの基本的要因で説明できます。まず、SDNは基本的に、オープンソースの概念であるOpenFlowを中心として構築されていることが挙げられます。これにより、SDNは特定のベンダーに偏よらず、概念上は制約がありません。2番目は、SDNの機能に非常に魅力があることです。この機能により、大規模ネットワークの運用を容易に管理できるほか、ネットワーク装置を効果的に使用してハードウェア実装を最大限生かしたり、過度なプロビジョニングを最小限に抑えたりすることができます。こういった機能は、仮想化やクラウドデリバリーの各モデルのアイデアよりも前に考え出された従来のネットワーク設計に関連する非常に根強いいくつかの問題を克服します。

SDNに対する1番のセキュリティー脅威は何だと思われますか?

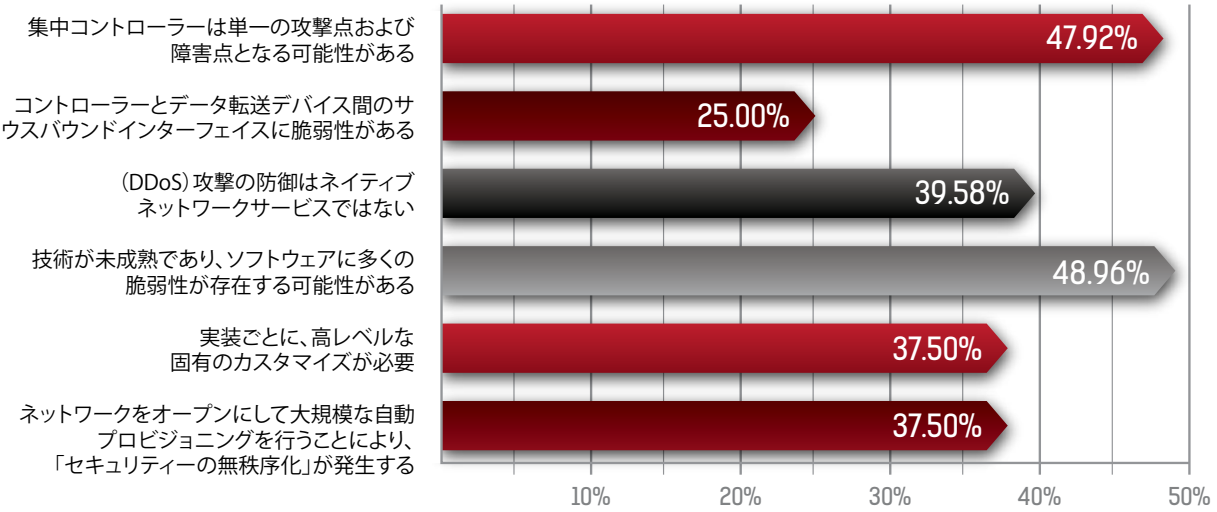


図38：SDNのセキュリティー脅威

「現在、SDNのDDoS機能は不十分なため、お客様は複雑な攻撃を効果的にミティゲートすることができません。当社独自のカスタマイズから得た詳細なデータとメトリックスにより、攻撃ベクトルに関する重要な洞察が得られ、SDNサービスプロバイダーよりも迅速かつ効率的な修復が推進されます。」

ジュリアン・ソリアーノ（Julien Soriano）
ネットワークセキュリティーマネージャー
eBay

非常に破壊的かつ不変なマクロトレンドとしてのSDNについて疑問を抱いている場合は、Googleがネットワーク全体をSDN上で構築したと宣伝していることを考えてみてください。Googleは、どのベンダーからもネットワーク装置を購入していません。コストに限った場合、Googleとの競争を望む通信事業者やクラウド企業は、SDNの運用を検討しないわけにはいきません。

SDNの機構を理解していないセキュリティー専門家は、身動きが取れなくなるでしょう。検査されたトラフィックは一定の方法で流れなければならないという原則を一掃したSDNは、現代のセキュリティデバイスの立場を奪う可能性があります。その結果、セキュリティー専門家は、固有の動的なトラフィックルート全体で情報を防御する必要性に直面します。また、今日のセキュリティー検査のアーキテクチャーには、SDNの制御機能に対する保護がありません。これは極めて重大な脆弱性です。結局、SDN機能が何らかの方法で侵害された場合、この「母艦」は環境全体に大損害をもたらす可能性があるのです。

乗り遅れないために

信じるかどうか、見たかどうか、理解したかどうかに関係なく、これらのトレンドはどれも、情報セキュリティーの環境を計り知れないほど変化させる能力を持っています。また、この3つすべてのトレンドが実現した場合、もたらされた変化によって、現在のCISOの役割は古風な時代遅れのものに変わることでしょう。

陳腐化を防ぐために次のアクションを起こしましょう：

- エンドポイント防御への投資の停止プロセスを開始する。「フィンガープリンティング」に関する革新的な考え方や技術を考慮して、新しい「入口」セキュリティーへの投資に移行します。
- アプリケーションセキュリティーを常に考慮する。モノのインターネットを経由した異種デバイスや異種テクノロジーからのアクセスがある場合、可用性が問題になります。
- 大容量攻撃に備える。サイバー攻撃では、攻撃において消費者用デバイス（電話に限らず）だけでなく、産業用デバイスも「徴兵」されます。
- SDNはもうここにあります。攻撃はそう遠くありません。SDNセキュリティーに関して厳しい質問をしてください。準備はできていますか。できていない場合、個人およびビジネス上のプロジェクトをどのように開始してギャップを埋めますか。その間、セキュリティーベンダーを賢く選択してください。SDN戦略のないベンダーは避けてください。

ボストン小児病院について

- 約25,000人/年の入院患者と、200を超える専門の臨床プログラムにより557,000人/年の外来を受け入れている、米国の上位10に入る小児専門病院

- アノニマスから複数回にわたって大量のDDoS攻撃を受け、ハクティビストグループが医療機関を標的とした最初の攻撃として記録される

- 同じISPを共有する他の7つの医療機関も同様に影響を受けた

誰もが標的に：ボストン小児病院へのDoS攻撃のケース分析

サイバー攻撃が破壊的かつ高価なだけでなく、潜在的な殺人的手段となりえる時代になったのでしょうか。2014年、ボストン小児病院（BCH）は、医療機関として初めてハクティビストグループの標的になりました。BCHは他の7つの地域医療機関と同じインターネットサービスプロバイダー（ISP）を利用しているため、この組織的な攻撃は、ボストンの重要な医療インフラストラクチャーのいくつかを停止に追い込む可能性がありました。

BCHおよびその他の機関は攻撃を乗り切りましたが、セキュリティーに関してまだ真剣に取り組んでいない医療機関にとって、この経験は「カンフル剤」となるものです。医学界は事の重大さを認識したように思えます。実際に、通常は臨床研究に焦点を当てている出版物「The New England Journal of Medicine」で、BCHのCIOであるダニエル・ニグリン（Daniel Nigrin）博士が執筆した攻撃に関する記事が特集されました。[1]

BCHへの攻撃は、情報セキュリティーがもはやIT部門のみの範囲でなくなったことを示しています。現在、医療は電子記録やネットワーク接続に大きく依存しており、システムにアクセスできない場合、臨床的およびビジネス的影響が広範囲に及ぶ可能性があります。金銭的損失が発生し、患者やスタッフの安全が脅かされ、さらに生命が失われる可能性もあります。

以下に、インシデントを最前線で経験したラドウェアの緊急対策チーム（ERT）によるレビューと、このインシデントが重要である理由を示します。

BCHへの攻撃：タイムライン

噂によると、ハクティビストグループ「アノニマス」の犯行（BCHに対するサイバー攻撃）は、3回の大きな攻撃によって行なわれました。:

ドクシング（Doxing）[2]

2014年3月20日、BCHのリーダーがアノニマスによる脅迫的なTwitterメッセージを受信しました。メッセージは、注目を集めている、子どもの監護権訴訟に関する情報を伝えるものであり、複合的な診断を受けた15歳の少女がマサチューセッツの児童保護サービスに保護されたことが書かれていました。メッセージは、病院が特定の臨床医に対して懲戒処分を行い子供を親元に返さない場合、報復すると脅すものでした。攻撃側は、この問題に関連する一部の人間の自宅と勤務先の住所、メールアドレス、電話番号などの個人情報を開示しました。この行為は「ドクシング（doxing）」として知られています。ボストン小児病院のWebサイトに関する技術的な情報が掲載されていることから、攻撃側は、病院の外部サイトも標的とすることを暗に示しているように思われました。

DDoS攻撃#1 - 比較的低レートの攻撃

4月初旬に攻撃側が開始した脅威は、病院の外部Webサイトを標的とするDDoS攻撃でした。この時点で、攻撃は比較的低レートでしたが、BCHのIT担当者はこの攻撃に気づいていました。

DDoS攻撃#2 - 攻撃の増加とミティゲーションの展開

1週間の間に攻撃は増加し、正当なインバウンドトラフィックとアウトバウンドトラフィックが遅延するようになりました。2回目の一連の攻撃はDDoS攻撃、スキャン、および侵入の試みで構成され、TCPフラグメントフラッド攻撃、out-of-stateフラッド攻撃、DNSリフレクターフラッド攻撃（UDPフラグメントフラッド攻撃を含む）などがありました。また、UDPスキャン、XSS、SQLインジェクション、ディレクトリトラバーサルなどの非DDoS攻撃も含まれていました。この時点で攻撃緩和策が導入され、標的となったサーバーへの攻撃は阻止されました。

DDoS攻撃#3 - 攻撃のピーク、一連の高レートのDDoS攻撃

3回目の攻撃で攻撃はピークを迎え、そのサイズは、2回目の攻撃の4倍である28Gbpsに達しました。また、このとき、攻撃側は、公開されたポートおよびサービスへの直接攻撃によって病院のネットワークへの侵入を何度も試みました。さらに、攻撃側は、「スピアーフィッシング」のメールも使用しました。このメールにより、埋め込みリンクをクリックしたり添付ファイルを開いたりするよう受信者を誘導し、これにより、病院のファイアウォールで守られているネットワークの一部へのアクセスが許可されたのです。

1 When 'Hacktivists' Target Your Hospital", ダニエル J. ニグリン, M.D., The New England Journal of Medicine 2014; 371:393-395
2 ドキュメントトレース（「ドクシング」）とは、インターネットを使用して、主題に関する、個人を特定できる情報を調査し、公開する行為です。

トラフィック量の不可解な急増によってアプリケーションが大幅に遅くなったことがありますか?

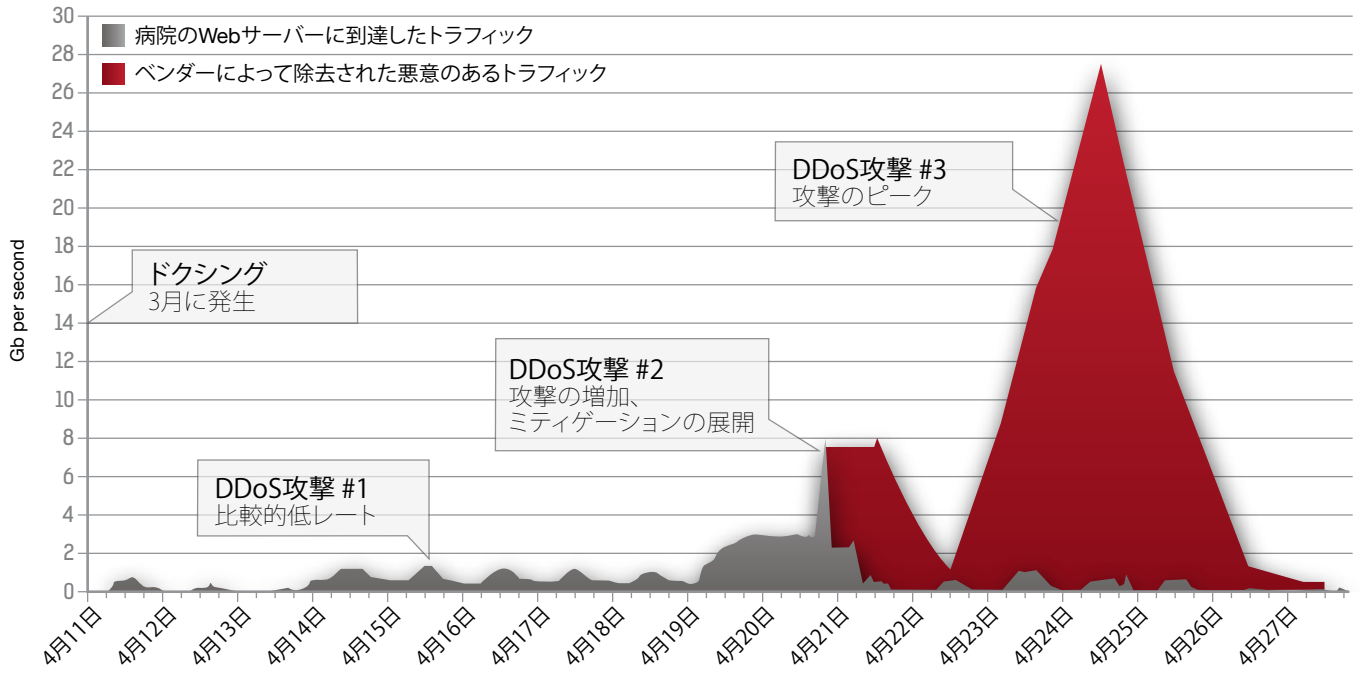


図39:DDoS攻撃中のインターネットトラフィック - The New England Journal of Medicine

対応

ボストン小児病院は、最初の脅威に気づいた後、複数の専門分野からなるインシデント対応チームを直ちに活動させました。このチームは、重大な問題に対して、ビジネス、臨床、技術の各側面から意思決定を行いました。

チームは、ビジネスと臨床の側面から、病院がインターネット接続を失った場合に、どのサービスが危険に晒されたり失われたりするかを迅速に評価する必要がありました。意義深いことには、病院は攻撃以前にこのような評価を実施したことがありませんでしたが、チームは、可能性のある3つの臨床的影響を短期間で特定しました。

- 処方箋を薬局に電子的に送ることができなくなる
- 電子メールによって重要なプロセスが支えられている部門で電子メールが停止する
- リモートに保存している電子カルテ (EHR) にアクセスできなくなる

技術的側面からは、大量のDDoS攻撃を何度も受けたため、BCHチームはラドウェアのERTおよびラドウェアのスクラビングセンターを依頼しました。BCHはISPを他の複数の病院と共有しているため、その7つの医療機関のネットワークや運用にも影響が及ぶ可能性がありました。これらの医療機関は、マサチューセッツ総合病院 (Massachusetts General Hospital)、ベス・イスラエル・ディーコネス・メディカル・センター (Beth Israel Deaconess Medical Center)、ダナ・ファーバー癌研究所 (Dana-Farber Cancer Institute)、ジョスリン糖尿病センター (Joslin Diabetes)、ハーバード大学医学大学院 (Harvard Medical School)、 ハーバード公衆衛生大学院 (Harvard School of Public Health) です。

「臨床の場では、サイバー攻撃が患者の治療に明らかに悪影響を及ぼす可能性があります。医療機関は、ITセキュリティーシステムや運用上のベストプラクティスに時間とリソースをつぎ込むことを積極的に検討し、このような新しい脅威が発生した場合にしっかりと防御できるよう準備する必要があります。」

ダニエル J. ニグリン, MD
"When 'Hacktivists' Target Your Hospital", ダニエル J. ニグリン, M.D., The New England Journal of Medicine 2014; 371:393-395
The New England Journal of Medicine

学んだ教訓

ボストン小児病院への攻撃は、その技術的な洗練度が低かったため大きな問題にはなりませんでしたが、医療機関を含むあらゆるものがサイバー攻撃の標的になりえることが示されたことに、この攻撃の重要な意味がありました。

その後、ニグリン博士はThe New England Journal of Medicineに次のように書いています。「臨床の場では、このような攻撃が患者の治療に明らかに悪影響を及ぼす可能性があります。医療機関は、ITセキュリティーシステムや運用上のベストプラクティスに時間とリソースをつぎ込むことを積極的に検討し、このような新しい脅威が発生した場合にしっかりと防御できるよう準備する必要があります。」

BCHへの攻撃は、「正しい」技術的措置をすべて講じている組織でさえ犠牲者になりえることを思い起こさせてくれました。また、医療機関が常に頑固な感染症に対して一歩先を進む必要があるように、すべての組織は情報セキュリティーに関して継続的に警戒する必要があります。計画を策定するだけでは不十分です。計画を十分に伝えると共に、脅威やリスクの進化に応じて常に更新する必要があります。

ボストンの重要なインフラストラクチャー全体に巨大な「ドミノ効果」が生じる可能性があるため、このような種類の警戒はいっそう重要です。DDoS攻撃が成功していた場合、DDoS攻撃はBCHだけでなく他の7つの病院にも影響を及ぼした可能性があります。つまり、医療の提供や患者の生命が危機的状況に陥った可能性があるのです。

すべてを負担しますか：IT基盤ソリューションプロバイダーによるネットワーク攻撃を受けた顧客の支援

私たちは、マネージドサービスの世界で生きています。つまり、あらゆる業界のあらゆる組織が運用のかなりの部分をサードパーティの専門家に外注しています。マネージドサービスのビジネスケースは魅力的なものとなりえます。しかし、サイバーセキュリティーの脅威が増大するにつれ、マネージドサービスプロバイダーのリスクも高まっています。このような企業は、自社のネットワークやデータを保護するだけでなく、顧客やさらにその顧客に代わって有効な守護者となる必要があります。

ServerCentral社は、ITインフラストラクチャーソリューションプロバイダーとして、自社および顧客のセキュリティーを確保するこの二重の役割を果たしています。シカゴに拠点を置くServerCentralは、ネットワーク攻撃およびDDoS攻撃を定期的に確認しています。こういった攻撃は数日おきに頻繁に発生しており、小規模のプロトコルフラッド攻撃から本格的なDDoSキャンペーンにまで渡り、攻撃停止の見返りとして金銭をゆすり取ることを目的としています。実際、今年の前半に、この企業の顧客の1社が脅しを含む組織的な犯罪行為の標的となりました。

プロジェクト管理用のWebベースツールを提供している、このServerCentralの顧客は、同じ犯罪グループの多くの犠牲者のうちの1社でした。このグループの手口は単純です。組織が支払要求に応じない場合ネットワークを攻撃すると脅迫するのです。

ServerCentral社について

- コロケーション、IaaS（Infrastructure as a Service）、プライベートクラウド、ネットワークサービス、ネットワーク保護などのカスタムインフラストラクチャーソリューションの設計、開発、および管理を専門とするITインフラストラクチャーソリューションプロバイダー
- ServerCentralの顧客が、過去に脅しに基づくDDoS攻撃を受けた
- 攻撃が複数の顧客やさらにその全顧客に影響を及ぼす可能性があるため、マネージドサービスプロバイダーは、自社のネットワークの保護に関して警戒を続ける必要がある

ServerCentralの顧客は、犯罪者との交渉を拒否した後、20GBのDDoS攻撃を受けました。顧客のネットワークセキュリティーの中でServerCentralが重要な役割を担っていることが、このインシデントによって明白になりました。ネットワークエンジニアリングディレクターのロン・ウィンワード（Ron Winward）氏は次のように説明しています。「ServerCentralは、ミッションクリティカルなアプリケーションやビジネス機能をサポートするインフラストラクチャーを提供できる当社の能力と同様に、サービスの実行や提供ができるお客様の能力にも誇りを持っています。当社は、お客様の顧客およびエンドユーザーに100%の稼働時間を提供することにも同等の重点を置いています。」

脅しに基づく攻撃の検知

ウィンワード氏の説明によると、ServerCentralは攻撃を様々な方法で検知しますが、脅しに基づく攻撃の場合は、顧客がその脅威をServerCentralに通知します。

ウィンワード氏は次のように述べています。「顧客が当社に連絡してきて何かがおかしいと伝えてくることがあります。顧客はそれを攻撃と認識している場合もあれば、何か異常だと確認しただけの場合もあります。攻撃は、当社のネットワーク監視ツールを使って検知することもできます。このツールは、異常を特定し、当社のネットワークオペレーションセンター（NOC）にインシデントを警告できます。」

ServerCentralの技術スタッフは、ネットワークのレポートデータの定期的なレビューも行っており、必要な場合は履歴データによるフロー分析を使用して調査分析を実行することができます。顧客がラドウェアのDefenseProおよびDefenseSSLを使用している場合、検出されたイベントがServerCentralのNOCと技術スタッフにリアルタイムに通知されます。

ServerCentralは回復力のある高パフォーマンスのネットワークを長年にわたって運用しており、脅しに基づくDDoS攻撃から顧客を保護する用意はできているとウィンワード氏は述べます。実際に、ServerCentralは、攻撃発生時に顧客のインターフェイスに適用可能なセキュリティーモデルを確立しています。

「結果的に、ほとんどの顧客は、ServerCentralの監視システムが攻撃を検知するまで、攻撃されていることさえ認識していません。」とウィンワード氏は述べています。

「あらゆる種類の攻撃が増加の一途をたどっています。すべての顧客が可能な限りの警戒心を持てるよう、この情報をお客様と共有することが当社の責任です。攻撃側はその「仕事」に100%の時間をかけて集中しています。常時「オン」の状態を維持し、攻撃のパターン、目的、および実行方法の変化に遅れずについていく必要があります。」

ロン・ウィンワード
（Ron Winward）
ネットワークエンジニアリングディレクター
ServerCentral

将来に向けた計画

多くの攻撃（特に脅しを組み込んだ攻撃）に関与しているグループには、攻撃をランダムに終了したり開始したりする習性があります。つまり、攻撃は、極めて高い確率でいつか再開されます。ウィンワード氏は、ServerCentralの核となるネットワークアーキテクチャーや、通信事業者クラスのルーターの展開、および調査分析ツールセットによって、最も予測不可能な攻撃にも確実に対応できると断言します。

「当社は、既知のまたは識別可能なフィンガープリントを使用した攻撃の存在を素早く簡単に管理できます」と、ウィンワード氏は述べています。「各顧客にDefenseProをリアルタイムオプションとして提供することで、特にアプリケーション層の攻撃とSSL攻撃における当社のポジションはさらに強力なものとなっています。」

ウィンワード氏の説明によると、ServerCentralは迅速な展開のために必要に応じてスタンバイ装置を現場に配置しますが、DefenseProのリアルタイムの応答性は、あらゆる反応技術を（それがどれだけ高速であっても）簡単に上回るものです。

攻撃の洗練度が増し、攻撃の実行が容易になったと思われる中、ウィンワード氏は、ServerCentralは次の12か月で攻撃が倍になると予測していると言います。これを考慮すると、攻撃管理に関する企業戦略を策定する上で、顧客の教育はますます重要になってきます。ServerCentralは、リスクに関する情報と、リスクを事前に予防するための手順を顧客に積極的に伝えています。

「あらゆる種類の攻撃が増加の一途をたどっています。すべての顧客が可能な限りの警戒心を持てるよう、この情報をお客様と共有することが当社の責任です。」と、ウィンワード氏は言います。「攻撃側はその「仕事」に100%の時間をかけて集中しています。ServerCentralも常時「オン」の状態を維持し、攻撃のパターン、目的、および実行方法の変化に遅れずについていく必要があります。」

09 エグゼクティブの洞察 - 役員室より

2014年、ラドウェアは、進行中の定量的調査を補足する初の定性的調査に着手し、世界中の情報セキュリティー担当エグゼクティブや技術担当エグゼクティブが直面している最も差し迫った問題や長く続いている問題について詳細な調査を行いました。

多種多様な業界のCIO、CISO、および副社長レベルのエグゼクティブを対象としたこの調査から、かつてIT部門の範囲であった情報セキュリティーは、今や経営幹部レベルおよび役員レベルが気にかけるものになっていることが判明しました。本章では、エグゼクティブが取り組んでいるセキュリティーの課題や問題、およびエグゼクティブが見出した今後の機会についても光を当てます。具体的には次のような質問を調査しました。

- 貴社の業界に関して、貴社をリスクに陥れる何か特別なものはありますか。
- 過去12か月に攻撃された回数を認識していますか。
- サイバーセキュリティー脅威への対処方法は過去5年でどのように変わりましたか。
- 最新のセキュリティー脅威に対処するために過去12か月に実施した最適な方策とその理由を挙げてください。
- 現在の最大のITトレンドであるBYOD（Bring Your Own Device）、クラウド、モノのインターネット（IoT）、およびSDN（Software-Defined Network）のうち、組織にとって最も重大なリスクであるとエグゼクティブが考えているものはどれですか。
- セキュリティー担当エグゼクティブの懸念事項とその理由を挙げてください。

- 現在、セキュリティーの脅威は貴社のCEOまたは役員レベルの懸念事項になっていますか。
- 次の12か月でサイバー脅威の環境はどのように変化すると予想していますか。
- 業界共通のエグゼクティブが今後1～3年での実施を計画している対策はどのようなものですか。

この調査は、金融サービス、政府、医療、高等教育、製造、電気通信、輸送を含む複数の業界にわたって世界中の10億ドル企業の役員室から回答を集めました。以下に、最も注目される調査結果および洞察をいくつか示します。

業界固有のリスク

業界（金融サービス、政府、医療、高等教育、製造、電気通信、輸送）に影響を及ぼすセキュリティーの脅威と問題について尋ねました。多くのエグゼクティブが実際、業界の性質上、いくつかの固有のリスクに直面していることを示しました。

ラドウェアの定量的調査では、金融サービス業界についてはサイバー攻撃の可能性がこの1年で実際に低下したことが示唆されています。とはいえ、当社の調査で、金融サービスのエグゼクティブは、業界の性質上、金融サービス業界のリスクは依然として高いと考えています。エグゼクティブは、金融サービス組織を防御するには総合的なエンドポイント管理が必要であると明確に述べています。

「[電気通信]業界を標的としたDDoS攻撃が急激に増加しただけでなく、われわれの主要な提供サービスであるモバイルデバイスを狙ったマルウェアも増加しました。ボットネットを構築して私たちのインフラストラクチャーや他の組織のインフラストラクチャーを標的とするため、多数のモバイルデバイスに侵入しようとする多くの試みが確認されました。」

ダニー・コームズ
（Dannie Combs）
CISMシニアマネージャー、
ネットワークセキュリティー
U.S. Cellular

別のエグゼクティブも、業界固有の情報の防御に関する課題に同意しています。高等教育のエグゼクティブは、コミュニティーカレッジの中核的使命である「非常に開かれたパブリックアクセス」を引用し、この機関の中心的な問題をとらえました。教育施設や情報、および他のリソースへのアクセスをより多くの人々に認めた場合、データのプライバシー、特に学生の記録に関して脆弱性が生じたり、脆弱性が合成されたりする可能性があります。同様に、連邦政府の大規模請負業者のCIO、および大規模医療システムの情報セキュリティーおよびプライバシー担当最高責任者は、管理しなければならない機密情報（それぞれ政府および医療のデータ）を挙げました。どちらの場合も、エグゼクティブは、政府および患者の機密情報のプライバシーとセキュリティーの確保を目的として策定された複雑な規則に直面しています。また、管理下にあるデータを組織が保護できなかった場合は、困難な法的影響、金銭的影響、および評判への影響にも直面します。

過去を振り返る

過去12か月に組織が受けた攻撃の数についてエグゼクティブに尋ねてみました。医療と製造のエグゼクティブは、組織が何回標的にされたかについて知らないと認めました。対照的に、教育、金融サービス、政府、電気通信、および輸送業界のエグゼクティブは、受けた攻撃を定量化できていると答えました。これらのエグゼクティブは、多くのツール（侵入検知/防止システム、ログファイル、メトリクス、分析など）を信用しており、これにより、各組織は攻撃を検知して定量化することができます。

多くのエグゼクティブにとって、この5年間は、セキュリティーの脅威に対する組織の対処方法が大きく変わった時期でした。セキュリティーは「パートタイムジョブ」ではなくなり、回答者の大半は現在セキュリティー専門チームを備えていると示しました。何人かの回答者は、攻撃の「量と複雑さに関する急激な増加」に伴って上級幹部の関心が高まっていることを指摘しました。電気通信のエグゼクティブは、投資を5倍に増加し、スタッフを増員し、セキュリティーチームがサイバーセキュリティーのリスクの特定、攻撃のミティゲーション、調査分析、およびコンプライアンス義務の管理を積極的に行うことができるように適切に位置付けるため、組織の再編成を行ったと述べました。

エグゼクティブに最近の変化、つまり過去12か月に実施した最適な対策についても尋ねてみました。一部の回答は、コミュニケーションとトレーニングの変化を反映したものでした。毎日のレビュー会議の導入、ユーザーの意識を高めるトレーニングの実施などです。また、高度な解析、侵入/脅威の検知および監視、セキュアなメール、ユーザーアクセス制御、Webブラウザーのコンテンツフィルタリング、デスクトップのサンドボックスセキュリティーなどといった新しい技術的機能を指摘した回答もありました。

U.S. Cellularのダニー・コームズ氏によると、同社はスタッフを増員し、重要なセキュリティーインフラストラクチャーの冗長性を高めました。また、可視性を高め、より詳細な調査分析が可能な新しいセキュリティーツールを追加しました。このような対策を行った主な理由は、「攻撃の量、複雑さ、頻度が年を追うごとに増加している現実があること」と言います。一方、政府にサービスを提供するグローバル企業のエグゼクティブは、内部システムをBYODデバイスから切り離すことで、脅威ベクトルの進入ポイントを制限したと報告しています。製造のエグゼクティブは、ShareFileを導入してデータの制御方法を強化したと示しました。

トレンドを追う - リスクは?

情報セキュリティーの環境を形成している最も強力な4つのマクロトレンドであるBYOD（Bring Your Own Device）、クラウドコンピューティング、モノのインターネット（IoT）、SDN（Software-Defined Networking）についても尋ねてみました。

スマートフォンやタブレットなど、モバイルデバイスの使用が急増していますが、それに伴って企業でのBYODの使用も広まってきました。BYODは組織に多くのメリットをもたらす可能性がありますが、新しい複雑なリスクをもたらす可能性もあります。同時に、あらゆる業界のあらゆる企業がクラウドへの大規模な移行を続けています。これは、従来の企業ITの終焉がそれほど先のことではないかもしれないことを示唆しています。

さらに、2つの革新的なトレンドであるモノのインターネットとSDNも登場しました。モノのインターネットは、接続デバイスの普及が進むにつれて登場しました。この接続デバイスには、コンピューターやスマートフォンだけでなく、消費者用デバイス（大型家電、自動車など）や埋め込み型の産業用デバイスも含まれます。接続性が高まると、エンドポイントセキュリティーが終わりを告げ入口セキュリティーが発達し始める可能性があります。SDNは、トラフィックの送信先を決定するシステムを、選択された宛先にトラフィックを実際に転送する基盤となるシステムから切り離すものですが、ネットワークの管理や安全確保の方法を一変させようとしています。ラドウェアの調査では、エグゼクティブの3分の1以上が、クラウドとBYOD－この2つのより確立されたトレンドー、を組織のセキュリティーリスクを高めるものとして挙げました。モノのインターネットは、エグゼクティブの4分の1以上が挙げました。SDNを挙げたのは5分の1以下です。

経営幹部レベルの懸念事項

- 金融サービス - 「担当範囲のことしかわからない。」
- 教育 - 「個人を特定できる情報や個人の記録の侵害」
- 医療 - 「攻撃検知。[私たちは]攻撃検知ができない。」
- 電気通信 - 攻撃量と頻度の増大。「30〜40Gbpsまたはそれ以上の攻撃は、当社のビジネスに即座に影響を及ぼします。」
- 製造 - 「内部的な脅威を回避できない。ユーザーは依然として、ウイルス/マルウェアのメールに疑いを持たない」
- 政府の請負業者 - 「個人情報の侵害 - 企業の評判に対するコストと影響」

眠れぬ夜：エグゼクティブの心配事は？

各業界共通のエグゼクティブの夜も眠れぬ心配事の原因についても調べてみました。エグゼクティブは、最も懸念されるリスク、脅威、およびトレンドは何であると考えているのでしょうか。同一業界であっても回答は様々でしたが、攻撃検知能力がないことに関して多くのエグゼクティブが懸念の声を挙げていました。大手金融機関の副社長は、「担当範囲のことしかわからない」と述べています。大規模病院の情報セキュリティーおよびプライバシー担当最高責任者は、攻撃検知について挙げ、病院はまったく攻撃検知ができないことを認めました。悪意または無知に関係なく、内部的な脅威は、世界的メーカーの技術、情報担当最高責任者にとって最大の懸念事項です。

大学でITを担当する副総長にとっては、個人を特定できる情報や個人の記録の侵害が一番の懸念事項でした。副総長は、容易なアクセスの促進を目的とする環境でデータのセキュリティーを確保することの難しさについて繰り返し述べています。電気通信のエグゼクティブは、攻撃の量と頻度の増加に関して不安を抱いていると明確に述べました。「30〜40Gbpsまたはそれ以上の攻撃は、当社のビジネスに即座に影響を及ぼします。」また、政府の請負業者のCIOは、最大の懸念事項として、個人情報の侵害と、その結果として企業に及ぶコストと評判面での影響を挙げています。

今後の見通し

エグゼクティブの4分の3近くが、現在、セキュリティー脅威がCEOまたは役員会レベルの懸念事項になっていると答えています。一部のエグゼクティブは、脅威への注目が高まっている要因として、マスコミのネガティブな報道を挙げています。また一部のエグゼクティブは、ビジネスへの潜在的な影響だけでなく、必要資金が増加することや、サイバー攻撃やその他の脅威に関連して法的責任が増すことを指摘しています。病院の経営幹部レベルのエグゼクティブは、情報セキュリティーについて役員やCEOが知っておくべきことに関する、米国病院協会の資料に注目しています。

このようにセキュリティーがますます重視されていることを考慮して、エグゼクティブが来年の具体的な計画を含め今後に関してどのように考えているかも聞いてみました。攻撃の量が増加または減少するか、あるいは同程度かに関して回答者の予想を尋ねたところ、一致した回答「攻撃の増加が予想される」が得られました。

今後の計画については、解析とビッグデータがテーマとして挙げられました。これは、セキュリティーインテリジェンスの向上の重要性が増していることを強調するものです。医療のエグゼクティブは、FairWarning®を実装する計画があると述べました。一方、金融サービス業界のエグゼクティブは、組織の今後の計画の中からアプリケーションのホワイトリスト化を挙げました。これは既知のプログラムのみを実行する機能です。

10 サイバー攻撃の防御に対するベストプラクティス

本項では、2014年のビジネスおよび攻撃のトレンドについて説明するほか、2015年のサイバー攻撃に対する計画を策定する上で考慮すべき一連のベストプラクティスを示します。

要点：C.H.E.W. - 動機、能力、目的

ベストプラクティスを考慮するにあたって、4つの種類のセキュリティー脅威（C.H.E.W）を思い出してください。：

サイバー犯罪（Cybercrime） - 犯罪攻撃は通常、金銭が動機になっています。数は多く、実質的に世界中のあらゆる国で発生しています。このグループのスキルレベルの範囲は、基本的なものから高度なものまで多岐にわたります。

ハクティビズム（Hacktivism） - ハクティビストの主な動機は金銭ではなく、組織などに対抗または復讐したいという欲望です。犯罪の場合と同様に、多くのハクティビストグループがあります。ただし、これらのほとんどのグループは基本スキルしか持っていません。「傑出」した数人が高度なスキルを持っており、多数の追随者を動かします。

ネットスパイ（Espionage） - この攻撃は、機密情報を取得して、国家の安全を守ったり経済的利益を得たりすることを目的としています。サイバー攻撃を使用してネットスパイを行う能力を備えた国が増えてきました。また、そのような活動を「支持」または「許容」されるグループも増えています。

サイバー戦争（War） - この4番目の攻撃タイプがおそらく最もたちが悪いです。破壊、機能低下、または拒否への欲望がその動機です。このような「他の手段による政治」形式を使用する能力を備えた国が増えてきました。また、非国家的な攻撃者が戦争形態のサイバー攻撃を引き受ける準備ができているように思われます。

サイバー攻撃の防御 = 攻撃の検知 + 攻撃のミティゲーション（緩和）

根本的に、サイバー攻撃の防御には、検知とミティゲーションの2つの要素があります。図40に示すとおり、防御の成功は、検知とミティゲーションの品質と時間に依存します。

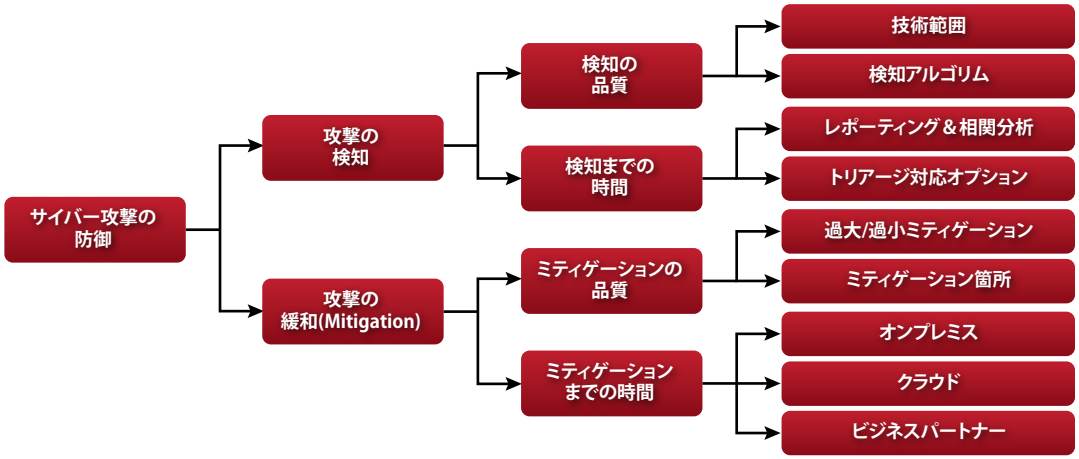


図40：サイバー攻撃の防御 = 攻撃の検知 + 攻撃のミティゲーション（緩和）

DDoSおよびサイバー攻撃のミティゲーションに関するベンダーの評価方法

DDoSおよびサイバー攻撃のミティゲーションに関してベンダーを評価する場合、核となる2つのコンピテンシー、検知およびミティゲーションについての能力と強みを調べます。各ベンダーをこれらの基準で評価し、各分野での能力を最大化することを目指します。

検知に関するベンダーの強みは何ですか？

品質 - ここでは、ベンダーが高品質の検知を提供できるかどうかを評価します：

利用可能な検知のタイプ（複数選択可）

- Netflow
- Openflow
- パケットL3/4
- 必須のパケットL7ヘッダー
- パケットL7ヘッダーレス
- OWASP脆弱性の検知
- 他のミティゲーションツールからの入力/信号

展開モデルオプション

- インライン
- クラウドのスクラビングセンター - 非同期
- OOP – 同期
- ハイブリッドクラウドオプション
- 内部のスクラビングセンター – 非同期
- SDN（Software Defined Networking）
- 仮想展開オプション
- パートナーからのフィード/他のベンダーの信号と連携

時間 - ここでは、最新の攻撃検知で必要とされるカテゴリを評価します。

- リアルタイムオプション
- シグナリング/自動オプション（高度なアプリケーション攻撃用）
- シグナリング/自動オプション（クラウド迂回用）

レポートおよび対応 - ここでは、最新の攻撃検知の制御およびレポートで必要とされるカテゴリを評価します。

- リアルタイム
- 履歴
- 調査分析
- インテリジェンスレポート
  （つまり、攻撃前の検出が可能）
- 検知サポートの対応 - リアルタイム
- 検知サポートの対応 - オンサイトオプション
- クラウドポータルでの統合レポート
- 正当なトラフィックと不正なトラフィックを
  リアルタイムで見分ける機能

ミティゲーションに関するベンダーの強みは何ですか?

品質 - ベンダーは脅威に対してミティゲーションを過大に行いますか、それともミティゲーションを過小に行いますか? また、どれだけの数の技術を役立てていますか?

- レートのみ
- ルーティング技術
- レート動作のみ
- レート動作以外
- ヒューリスティックな動作
- 統計的な動作
- シグネチャ – 静的 (更新サービスあり)
- シグネチャ - リアルタイムシグネチャ
- HTTPサーバーベースの防御
- HTTP OWASPベースの防御
- Hybridシグナリング/クラウドのスクラビングセンターの協調
- SSL防御
- HTTPリダイレクト
- JavaScriptのチャレンジ/レスポンス
- クラウドのチャンレンジ/レスポンス

時間 - ベンダーがミティゲーションを開始するまでにかかる時間はどれくらいですか。

- リアルタイムオプション
- 自動オプション

レポートおよび対応 - レポートの詳細レベルはどれくらいですか。また、ユーザーは、ミティゲーション技術が正当なトラフィックを妨げていないかどうかを確認できますか。

- リアルタイム表示
- 履歴データによるミティゲーション効果の測定
- 調査分析および詳細レポート
- 緊急対応オプション
- 正当および不正なトラフィックを表示
- すべての攻撃ベクトルを詳細に表示
- ミティゲーション対応の反撃オプション
- ミティゲーションサポートの対応 - リアルタイム
- ミティゲーションサポートの対応 - オンサイトオプション
- クラウドポータルでの統合レポート

ベストプラクティスのまとめ

サイバー攻撃に対する防御を計画する場合は、C.H.E.W.の脅威に気を配り、ベンダーへの要求事項を高く設定するとともに、次の点を常に考慮します。:

タイミングがすべて
組織は、ミティゲーションまでの時間を成功への重要な要素と考える必要があります。これを念頭に置き、展開するソリューションでミティゲーションまでの時間を最短にします。

穴を埋める
DDoSミティゲーションソリューションは、広範囲にわたって攻撃に対応し、1つの攻撃ベクトルだけでなく、インフラストラクチャーの様々なレイヤーを攻撃する複数ベクトルの攻撃も検知できる必要があります。

複数のレイヤーを使用する
単一点ソリューションの問題を解決するために、帯域幅消費型攻撃をブロックするクラウドベースの防御と、他のすべての非帯域幅消費型攻撃をブロックするオンプレミスソリューションを使用しましょう。

SSL攻撃をミティゲートする
2015年もSSL攻撃は重大な脅威です。導入しても正当なトラフィックパフォーマンスに影響を及ぼさないSSLベースのDoS/DDosミティゲーションソリューションを探しましょう。

単一のコンタクト先を探す
攻撃が発生した場合に備えて、インターネットトラフィックの迂回と、ミティゲーションソリューションの展開を支援できる単一のコンタクト先を用意しておくことが極めて重要です。

セキュリティー - 心配すべき5つのこと

11

心配すべき5つのこと

セキュリティーの専門家として、我々は、情報セキュリティーの攻撃ベクトル、サイバーインシデント、トレンドについて講演する機会が多いです。また、当社は、自らが考える最も恐ろしいリスクと、企業、政府、および個人がそのリスクをどのようにミティゲートできるかについて、意見をよく求められます。2014年を振り返り、2015年を見越した上で、ラドウェアは以下の5つの重要な懸念事項に注目します。

1 人命に関わる攻撃

何年もの間、当社は、いかなる種類の攻撃（ペースメーカー、列車、自動車、航空機システムなど）も、その攻撃がいつか人命の損失につながる可能性があることを見てきました。今日、サイバー攻撃が殺人的なものになりえて、そしてそうなるであろうことは疑問の余地がありません。「もしも」の問題ではなくなり、「いつ」の問題になったのです。

2 切迫感の低下

報道される回数や社会の意識はこれまでになく高まっているにもかかわらず、セキュリティーの意思決定者には特定の無関心や疲労感が蓄積されているように思われます。多くの意思決定者は、いつまでも繰り返される攻撃側を目の前にして、切羽詰まって正

しいことをやっても結局は無駄になると感じ、熱意をなくし、無感覚になっているのかもしれません。ラドウェアが恐れていることは、企業のエグゼクティブが、エンドポイントのセキュリティーを確保し他のポイントのセキュリティーをより効果的にする方法を次第に徹底的に調査しなくなっていることです。このようなエグゼクティブは、犠牲者になる（まだ犠牲者になっていない場合）ことは目に見えているという考えに屈服しているのではないでしょうか。

3 重要度の高いインフラストラクチャーの停止

広範囲なサイバー攻撃による混乱が広がり国の重要なインフラストラクチャーサービスが無力になる可能性があることは容易に想像できます。例えば、発電、水道、電話、テレビ配信サービス、さらには警察や救急・消防などの緊急応答ネットワークなどのサービスです。世界で最も進んだ国でさえ、これを免れません。

4 サイバー人質事件の台頭

サイバーによる恐喝行為には長い歴史がありますが、2014年は犯罪攻撃において新しいレベルの脅威が見られました。極悪なグループが、デジタル資産やサービスを人質に取り始めたのです。これらのリソースは、特定の要求（金銭的なものである場合もそうでない場合もある）が満たされるまで乗っ取られます。あるケース（少なくとも1つのケース）では、この人質事件によって企業が倒産しました。

5 国家主義的な規則を含めた、サイバー攻撃に関する大量の法律の採択

意気消沈しフラストレーションを抱えた有権者がますます増加し、国家の支援を受けたネットスパイに関する脅威も増大しているという状況に直面する中で、立法者はサイバー攻撃に関する法律の制定プロセスを開始するものとラドウェアは考えます。このような法律は恐らく、ネットワークトラフィックの流れや、重要なインフラストラクチャー企業のセキュリティーレベル、また、データ処理を行う場所の条件を指定することを目的としたものになると思われます。また、インターネットの動作に関して許容可能な構成要素を示すガイドラインが策定される可能性もあります。

12 調査回答者のプロフィール

ラドウェアは2014年9月と10月にセキュリティーコミュニティーへの調査を実施し、330の回答を得ました。この調査は、サイバー攻撃に対する計画策定時およびサイバー攻撃への対抗時に組織が直面した問題に関して、特定のベンダーに偏らない客観的な情報を収集することを目的として作成され、世界中の様々な組織に送られました。すべての調査回答者のプロフィール情報を以下に示します。すべての問題に答えていない回答者がいるため、合計が100%にならない回答もあります。

回答者の業務上の役割

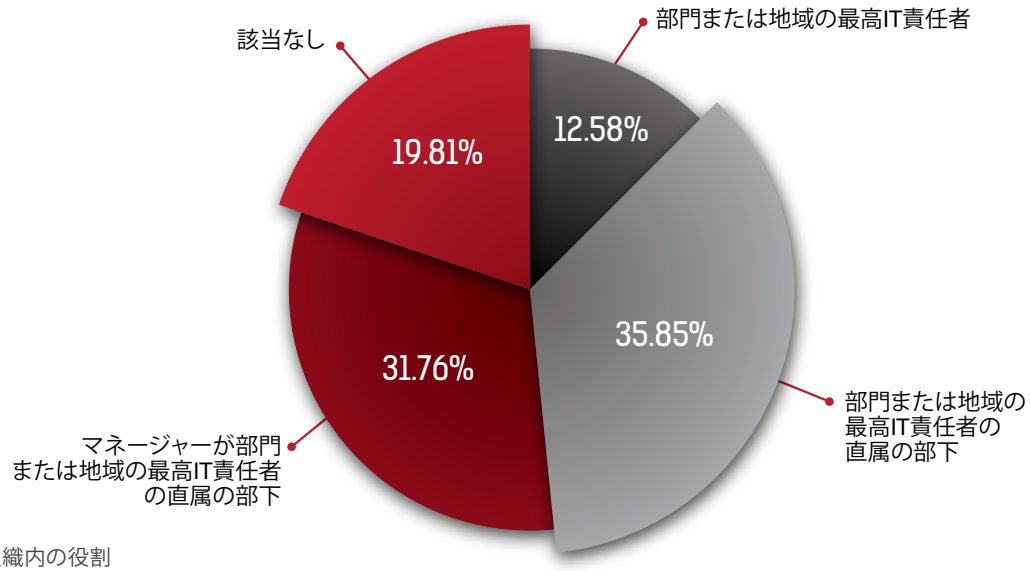


図41：組織内の役割

回答者の役職

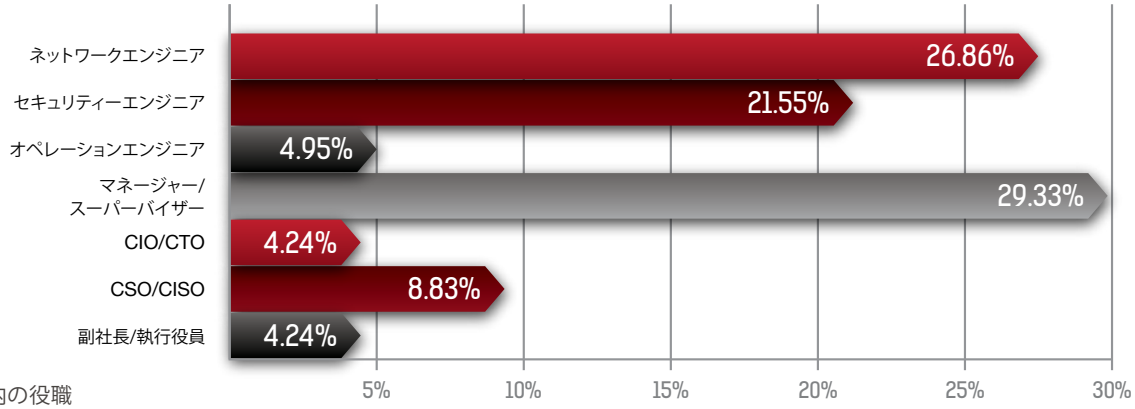


図42：組織内の役職

組織の直近年度の世界総収入

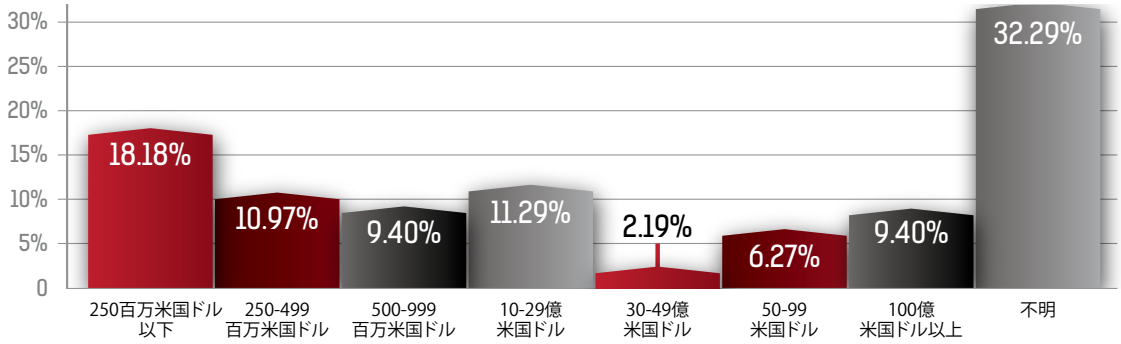


図43：年間収入

組織の現在の従業員数

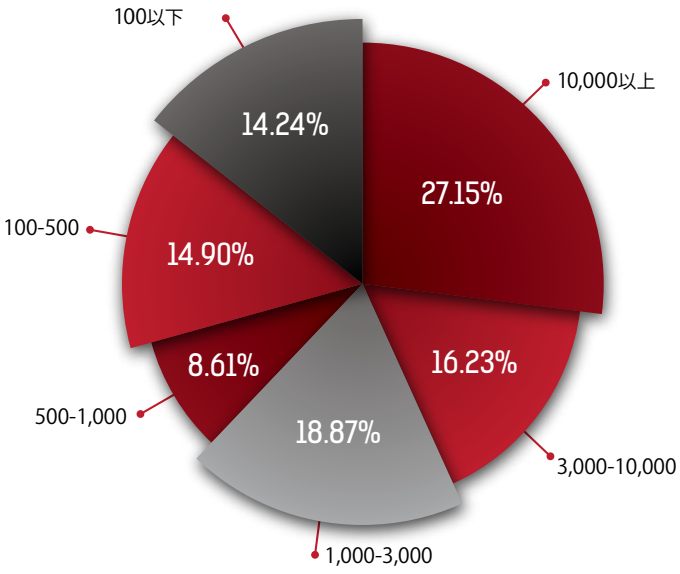


図44：組織の従業員数

組織のビジネス対象地域

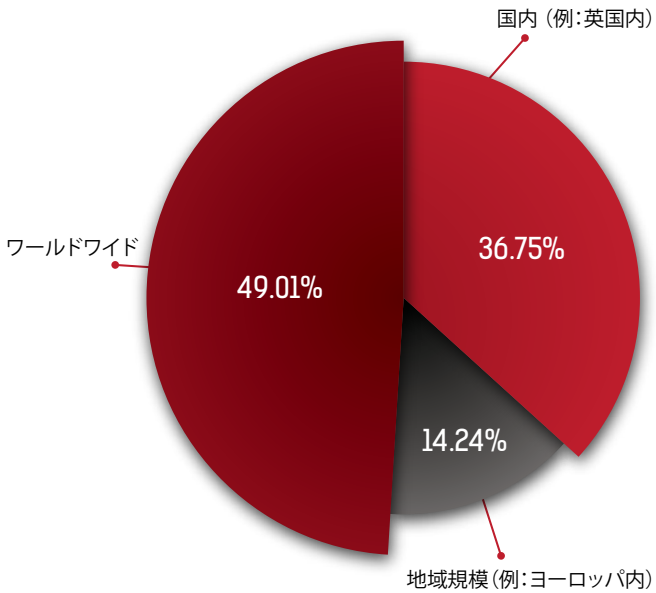


図45：組織のビジネス対象地域

回答者の企業の業界または業種

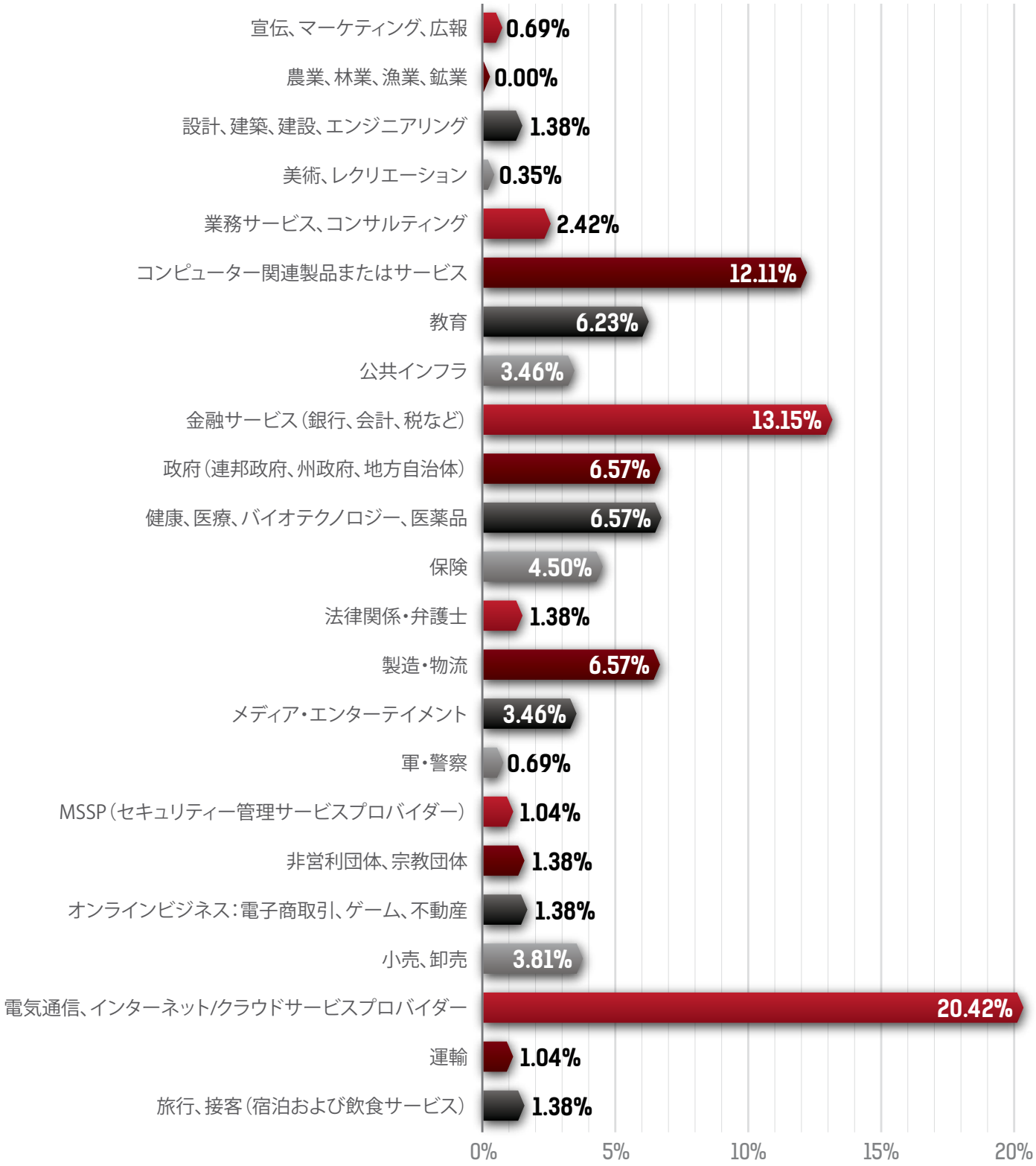


図46：業界

著者

Carl Herberger
VP Security Solutions
Radware

Ziv Gadot
ERT Consultant
Radware

Yotam Ben-Ezra
Director of Security Product Management
Radware

Oren Ofer
Senior Security Researcher
Radware

アドバイザリーボード

Werner Thalmeier
Director of Security Solutions
Radware

Alon Lelcuk
VP Security
Radware

Dudi Lavi
Director of Security ERT
Radware

Shira Sagiv
Security Product Marketing Director
Radware

協力

Carolyn Muzyka
Director, Marketing Communications
Radware

ラドウェアについて

ラドウェア（NASDAQ：RDWR）は、仮想環境とクラウドデータセンターにおける、アプリケーションデリバリーおよびアプリケーションとネットワークのセキュリティーソリューションを提供するグローバルリーダーです。数々の受賞歴のあるソリューションポートフォリオは、ビジネスクリティカルなアプリケーションを完全に回復し、最大限のIT効率を実現し、ビジネスの俊敏性を全面的に確保します。ラドウェアのソリューションは、全世界の10,000社を超える企業とサービスプロバイダーに採用されており、コスト削減と共に、企業のマーケットの課題への迅速な対応、ビジネス継続、生産性の最大化に貢献しています。詳しくはwww.radware.com または www.radware.co.jp をご覧ください。

ラドウェア緊急対策チーム（ERT）について

ラドウェアのERTは、24時間対応の専門のセキュリティーコンサルタントグループです。ラドウェアのERTメンバーは、文字どおり、サイバー攻撃への「第一応答者」として、業界でも特に顕著なハッキングエピソードに適切に対処した広範な経験を積んでおり、社内のセキュリティーチームでは対応したことがないような攻撃をミティゲートするための情報や専門知識を提供しています。

詳細情報は

その他の専門的な情報については、www.radware.com または www.radware.co.jpをご覧ください。また、DDoS攻撃ツール、トレンド、および脅威の包括的な分析については、ラドウェアのセキュリティーセンター（DDoSWarriors.com）をご覧ください。

Radware encourages you to join our community and follow us on: Facebook, Google+, LinkedIn, Radware Blog, SlideShare, Twitter, YouTube, Radware Connect app for iPhone®

www.radware.com

www.radware.co.jp