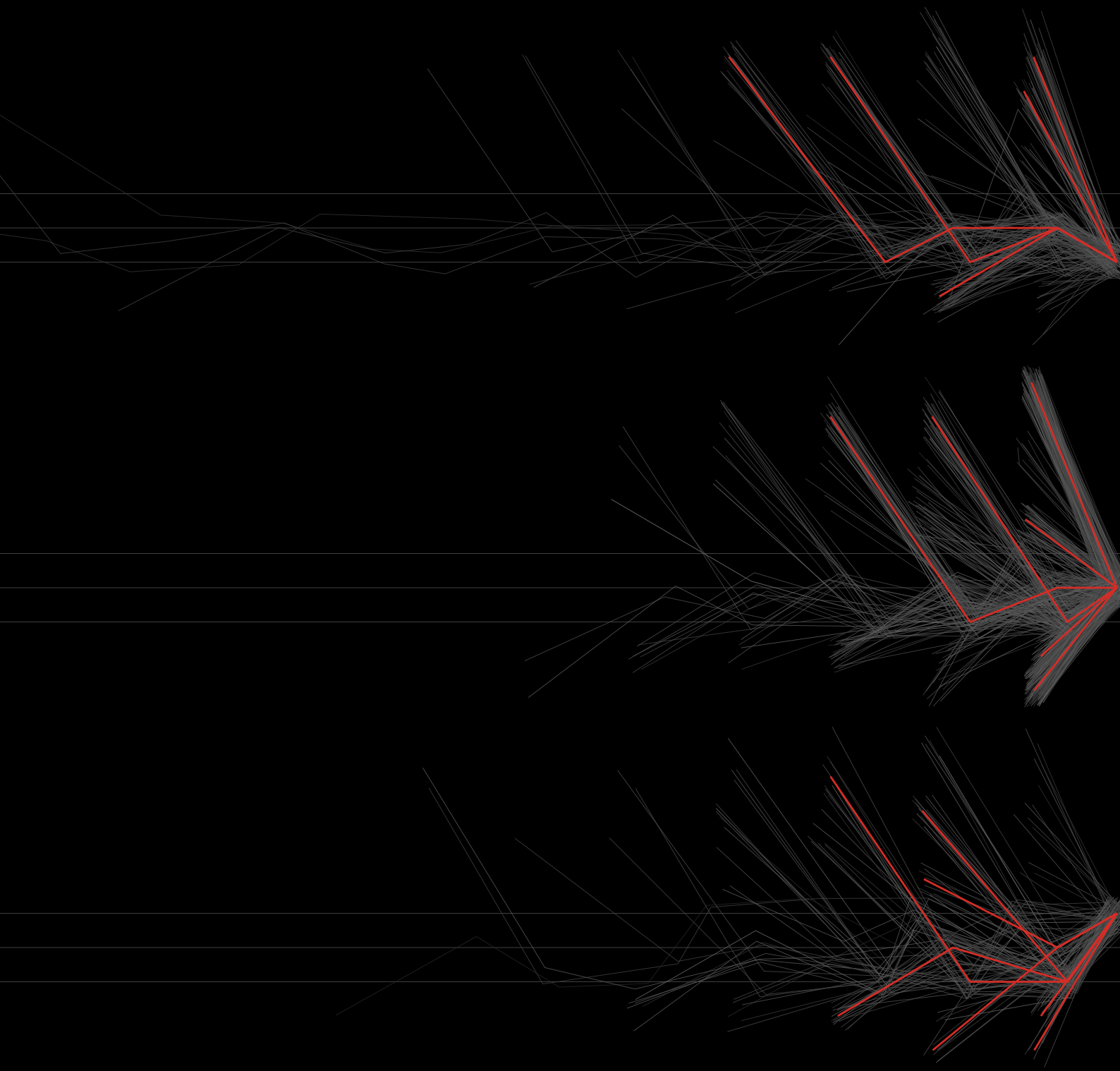
2019年度データ漏洩/侵害調査報告書



verizon

凡例と定義

2019年度データ漏洩/侵害調査報告書（DBIR）の本文をお読みいただく前に、曖昧さを回避するため、本報告書全体で使用されている用語、区分表示、図表についてご説明します。

VERISリソース

「攻撃（threat action）」「攻撃者（threat actor）」「種類（variety）」「経路（vector）」という言葉が何度も登場します。これらは、一貫性をもって正確にセキュリティインシデントの詳細情報を収集するためのフレームワーク「情報セキュリティ事象記録とインシデント共有のための言語（Vocabulary for Event Recording and Incident Sharing：VERIS）」で使用される用語の一部です。以下に、各用語の定義と、フレームワークおよび区分の詳細情報へのリンクを示します。

攻撃者（Threat actor）：
情報セキュリティ事象の背後にいる人物。フィッシング詐欺を仕掛けている外部の「悪者」の場合もあれば、飛行機の座席ポケットに機密文書を置き忘れた従業員の場合もあります。

攻撃（Threat action）：
資産に影響を及ぼすために使用された手口（行為）。VERISでは、マルウェア、ハッキング、ソーシャル、不正使用/悪用、物理的攻撃、ヒューマンエラー、環境という7つの主要攻撃カテゴリーを使用します。大まかな例としては、サーバーのハッキング、マルウェアのインストール、人の行動に影響を及ぼす、などが挙げられます。

種類（Variety）：
上位カテゴリーをより具体的に分類した区分。例えば、外部の悪者を「組織犯罪グループ」に分類したり、ハッキング行為を「SQLインジェクション」や「ブルートフォース」として記録する場合に使用します。

詳細情報はこちらをご覧ください。

- github.com/vz-risk/dbir/tree/gh-pages/2019 – DBIRの図表および図表内データ。
- veriscommunity.netには、フレームワーク情報とともに、例や区分リストが掲載されています。
- github.com/vz-risk/verisには、VERISの全スキームが掲載されています。
- github.com/vz-risk/vcdbより、公開されている漏洩/侵害に関する弊社データベース「VERIS Community Database」にアクセスできます。
- http://veriscommunity.net/veris_webapp_min.htmlでは、自社のインシデントおよび漏洩/侵害を記録することができます。データはローカルで保存され、データを共有するかどうかはご自身で選択できますので、ご安心ください。

インシデント vs. 漏洩/侵害

本報告書に多く登場する「インシデント」と「漏洩/侵害」という言葉は、以下の定義で使用しています。

インシデント：
情報資産の完全性、機密性、可用性を損なうセキュリティ事象。

漏洩/侵害：
権限のない者への（データ漏洩の可能性だけでなく）データ漏洩が確認されたインシデント。

[1] https://en.wikipedia.org/wiki/Confidence_interval

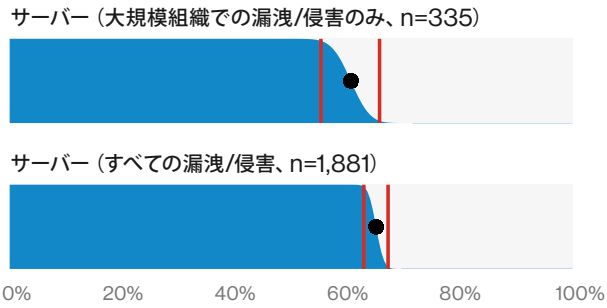
業界区分表示

弊社のコーパス（文章の集積）では、被害に遭った組織の分類に関し、北米産業分類システム（North American Industry Classification System：NAICS）の基準に沿っています。この基準では、企業および組織の分類に、2～6桁のコードを使用しています。通常、弊社では2桁レベルでの分析を行っており、業界区分にNAICSコードを併記しています。例えば、グラフに「金融業（52）」という区分表示がある場合、52という数字は、調査結果の値ではなく「金融保険業」を表すNAICSコードです。図表内では、簡潔にするため「金融業」という総称的な区分表示を使用しています。コードおよび分類システムに関する詳細情報は、以下でご確認いただけます。

https://www.census.gov/cgi-bin/sssd/naics/naicsrch?chart=2017

新グラフの説明

棒グラフの形状が、従来のような「長方形のバー」ではないことにお気づきかと思います。昨年、方法論（Methodology）のセクションで信頼性について少し触れましたが、「数値はXである」と言った場合、実際は「X ±若干数」となります。



図表1 最も漏洩/侵害件数の多い資産

今年は棒グラフにその誤差を反映させています。黒いドットは値を示し、棒グラフの先端のスロープ状の部分は、実際の値の範囲を表しています。例示したこの図表では、範囲を示す赤いラインを引いています。20の棒グラフのうち19（95%）[1]において、実際の値は、2本の赤いラインの間のどこかに存在します。ご覧のとおり、サンプル数（n）が少なくなればなるほど、スロープはなだらかに広がります。上の棒グラフの下限ラインと、下の棒グラフの上限ラインがオーバーラップする場合、これらは「統計的に類似する」とされ、「XはYよりも大きい」とは言えなくなります。

ご質問、ご意見・ご感想、アイデアのご提案はこちらへ
皆様のご意見をぜひお聞かせください。メール（dbir@verizon.com）またはLinkedInの弊社ページまでご連絡いただくか、@VZEnterpriseに、#dbirを付けてツイートしてください。データに関するご質問は、Twitter（@VZDBIR）までお問い合わせください。

目次

イントロダクション

「傷は、あなたの中に光を取り込む場所である」— ルーミー

この度は、2019年度ベライゾンデータ漏洩/侵害調査報告書（DBIR）をお手に取っていただき、ありがとうございます。本報告書の見解はデータに基づくものであり、本報告書の基盤であるインシデントコーパス（情報の集積）、または複数のセキュリティベンダーから提供された非インシデントデータセットをもとに導き出されたものです。

この報告書は、41,686件のセキュリティインシデント（内、2,013件は確認されたデータ漏洩/侵害）の分析に基づいて作成されています。ここ数年で調査結果がどのように変化したか（あるいは、していないか）を検証するとともに、脅威環境の全体像や侵害に関わる攻撃者、攻撃、資産について掘り下げていきます。また、最もよく見られる攻撃とその影響を受けた資産の組み合わせについてもご紹介します。

これらの情報により、これまでとは違う侵害分析の方法や、既に知っているインシデント分類パターンとは別の共通性を発見する新たな手段をご提供できるでしょう。

とはいえ、これまでの9つのインシデント分類パターンもまだ有効であり、弊社は引き続き、それらパターンと業界との相関性に焦点を当てていきます。9つの主要パターンに加え、弊社では、金銭を目的としたソーシャルエンジニアリング（FMSE: Financially-Motivated Social Engineering）攻撃を抽出するためのデータサブセットを作成しました。これらの攻撃の目的は、マルウェアのインストールではありません。FMSEは、認証情報の盗取や、人を騙して不正口座に送金させることを狙った犯罪です。また、業界別脅威プロファイルの比較に加え、今回も各業界を個別に取り上げたセクションを主軸に構成しています。

ますます増大するインシデント・漏洩/侵害コーパスと併せて、インシデント以外のデータセット（マルウェアブロック、フィッシング対策トレーニングの結果、脆弱性スキャニング等）を使用した、いくつかの分野の調査結果も取り入れています。多種多様な情報源（ハニーポットやインターネットスキャンリサーチなど）を活用し、時にはそれらを組み合わせることで、データドリブン型のコンテキスト情報の取得が可能になります。

弊社の役割は、各業界の組織を狙う攻撃者がよく使う手口に関する情報を提供することです。本調査報告書の目的は、情報セキュリティの「傷」に塩を塗ることではなく、その傷から「光」を取り込み、認識を高め、過去から学ぶ力を養えるようにすることです。セキュリティに対する意識、知識、予算を獲得するためのひとつのツールとして、ぜひ本書をご活用ください。本報告書が「必読文献」になっているというお話を度々伺います。そのため弊社では、皆様に眠気や疲労感といった有害な副作用をもたらすことなく、アクションにつながる情報をご提供できるよう努めています。

弊社はこれまでに続き、73のデータソース（内、66がベライゾン外部の組織）が協調して実施するデータ共有の取り組みに支えられ、これを活用しています。データ協力を行うこのコミュニティには、本年次報告書の発行を支援する、世界各国・地域の公共機関および民間の事業体が参加しています。この場をお借りして、時間やデータをご提供くださり、ご支援を賜っているコミュニティの皆様に改めて感謝申し上げます。

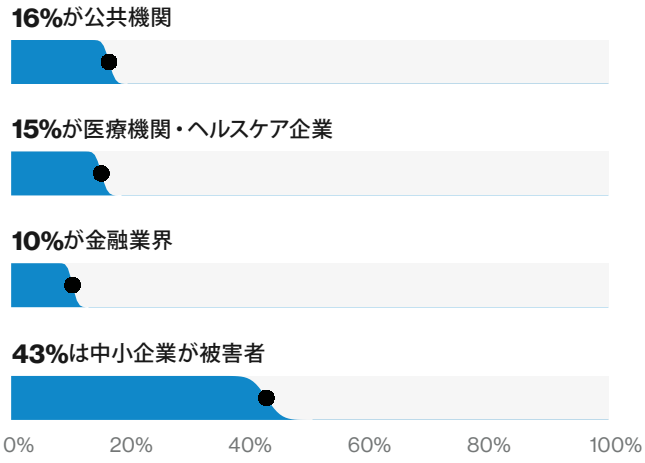
我々には皆、傷があり、すべてを知っている人などいません。

お互いに学び合いましょう。

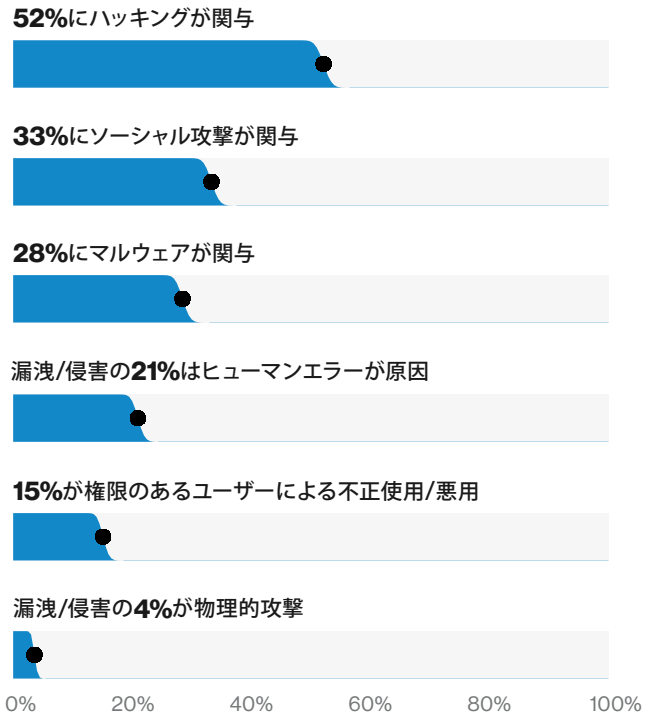
Excelsior!（さらに上を目指して！）[2]

[2] マーベルコミック編集委員スタン・リーの決まり文句がここに登場するとは思わなかった方は、本報告書を初めて読む方ですね。
「Welcome to the party pal!」（パーティにようこそ！「ダイハード」より）

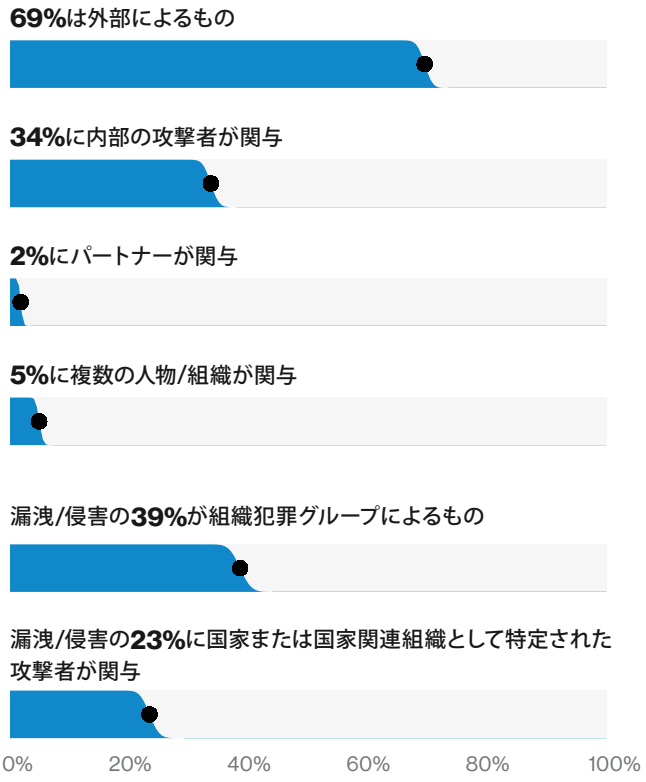
調査結果サマリー



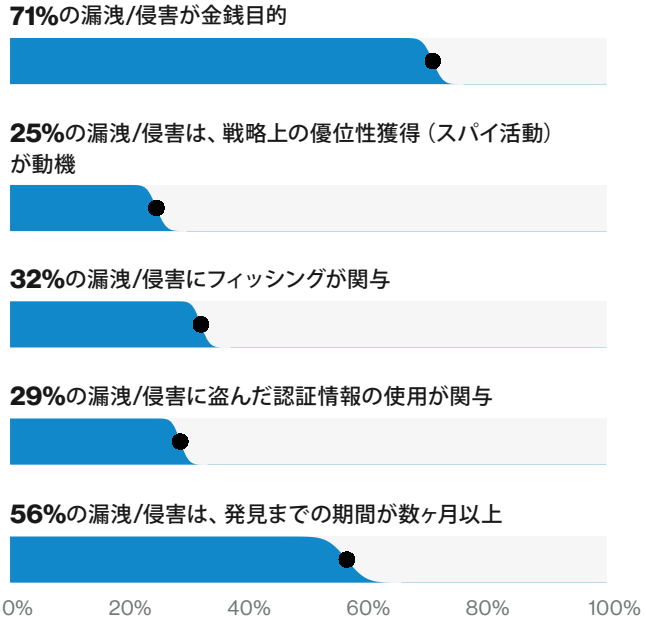
図表2 被害者は誰か？



図表3 使われた手口・原因は？



図表4 漏洩/侵害の背後にいるのは誰か？



図表5 その他の共通点は？

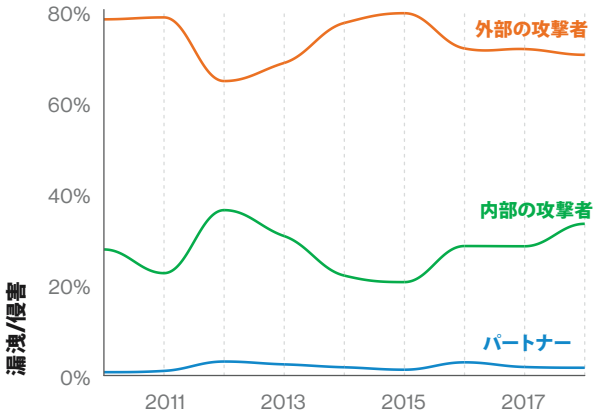
結果および分析

本セクションおよび以降のセクションに掲載する調査結果は、一般公開されているセキュリティインシデント、ベライゾンの脅威リサーチアドバイザリーセンター（Threat Research Advisory Center：VTRAC）の調査担当者、並びに外部協力者から提供されたケースなど、多様な情報源から収集したデータセットに基づいています。前年と比較しているデータセットには、新たな情報源からのインシデント・漏洩/侵害データも使用されます。これは弊社が、網羅するイベントの多様性とカバー範囲を広げるために、情報共有にご賛同いただける組織を探し、協力を仰ぐ取り組みを行っているためです。これは便宜的サンプルであり、新たな組織の参加や、今年は参加できない組織があるといった協力機関の変更は、データセットに影響を与えます。さらに、対象分野における潜在的な変化も、経時的変化を追う上で、影響を与える要素となる可能性があります。つまり、毎年全く同じ分野の同じ組織を調査・分析しているわけではない、ということです。その他、調査結果に影響を及ぼす要素として考えられるのは、データや大規模イベントの下位分類の方法の変更です。これは時に、ある年の指標に影響を及ぼすことがあります。これらすべてを考慮し、必要に応じて本文中に注記を加え、読者に適切な背景・文脈を提供しています。

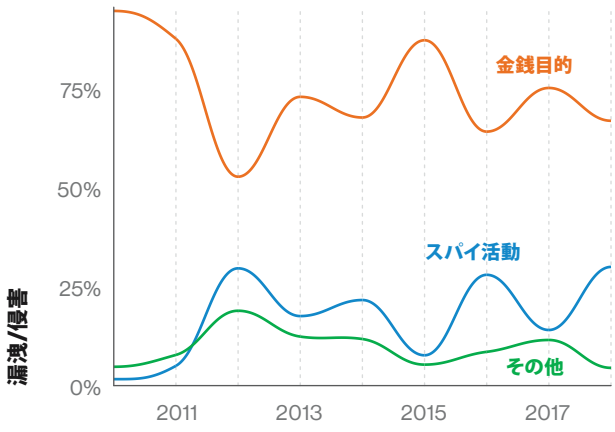
こうした前提のもと、まずは攻撃者（とその動機）[3]の経時的変化を検証し、さらに、攻撃とその影響を受けた資産の経時的変化を見ていきます。続いて、従来どおり、各攻撃カテゴリーに焦点を当てながら、今年のデータセット全体を深く掘り下げていきます。攻撃に関する調査結果には、攻撃者の手口についての認識を高める目的で、関連性のある非インシデントデータが含まれています。

脅威の定義

攻撃者（Threat actor）とは、侵害の背後にいる人物（エラーの場合、それを引き起こした人物）を表す用語です。攻撃者は「外部」「内部」「パートナー」という3つの大きなカテゴリーに分類されます。長年、確認されたデータ漏洩/侵害の犯人として最も多く見られるのは外部攻撃者であり、このトレンドは今年も続いています。総合的なコーパスから除外されているデータサブセットがいくつかあり、中でも特に顕著なのが、5万件を超えるボットネット関連の侵害です。これらは外部グループによるものと考えられ、もしこれらがコーパスに含まれれば、外部攻撃者と内部攻撃者の差はさらに大きくなるでしょう。

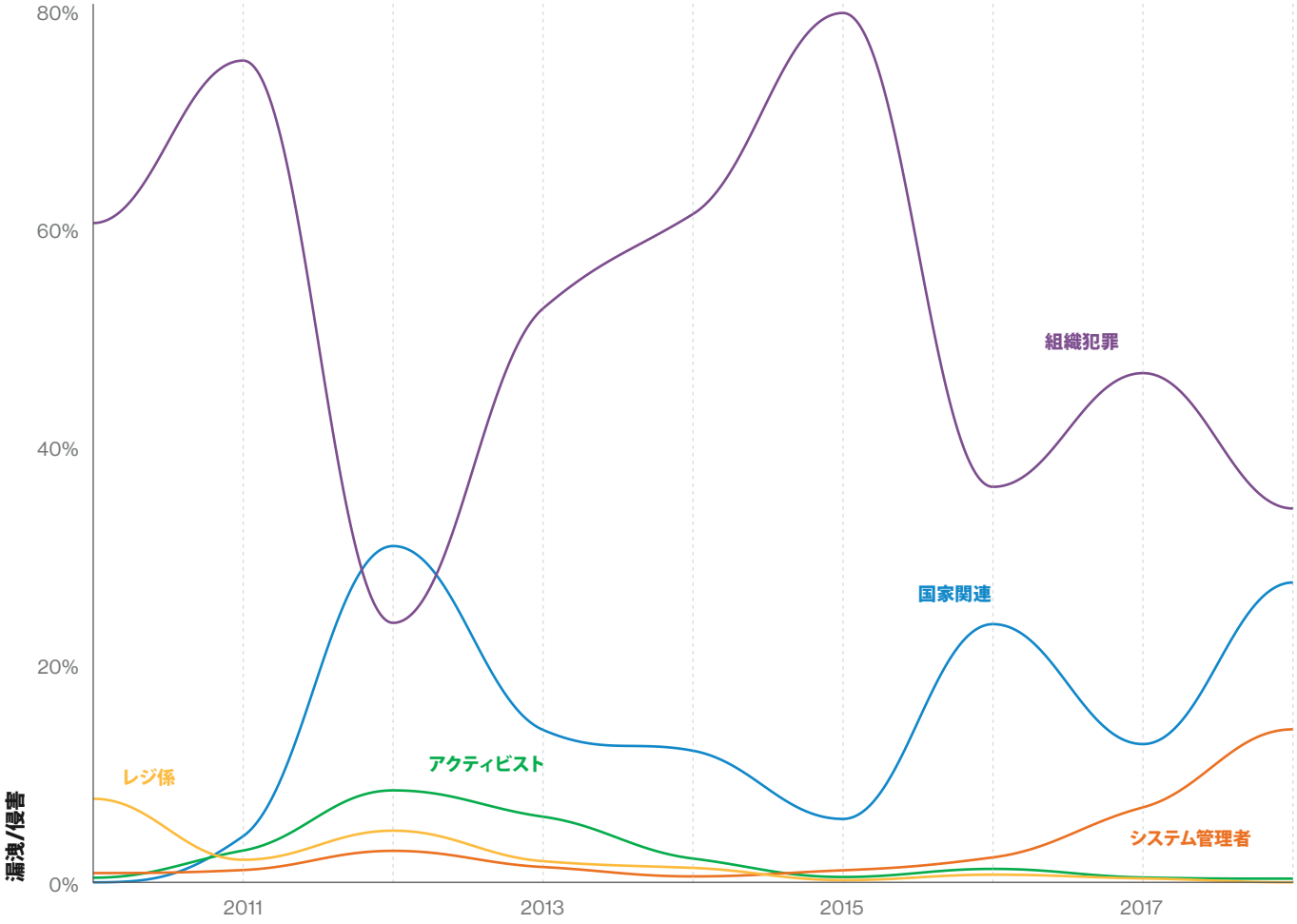


図表6 漏洩/侵害における攻撃者の経時的変化



図表7 漏洩/侵害における攻撃の動機の経時的変化

[3]統計手法について詳しくは「付録B：方法論」に記載しています。



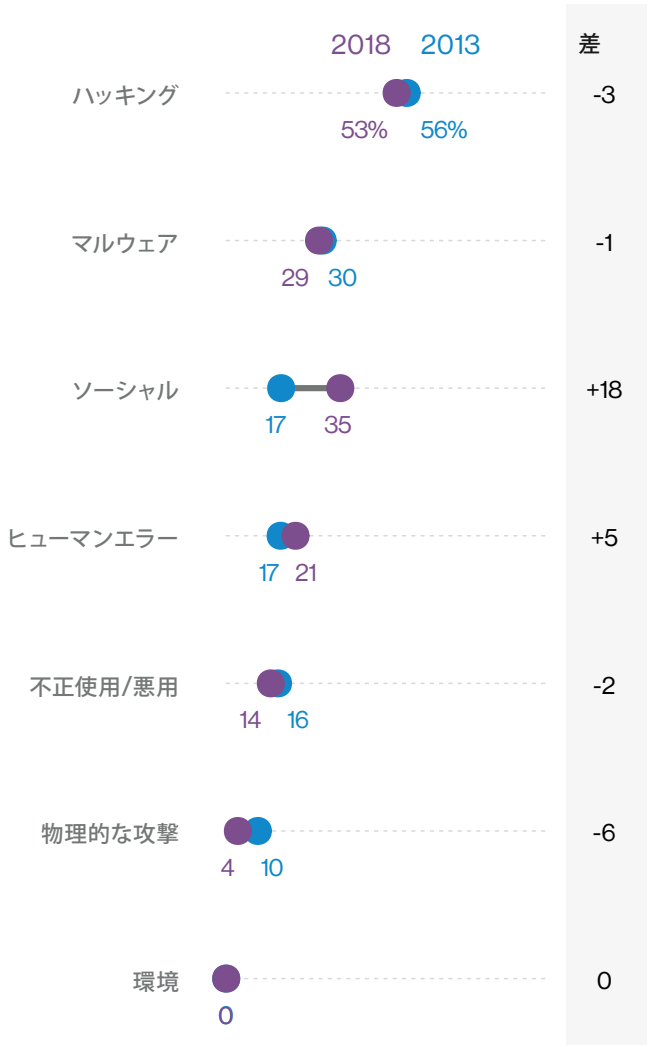
図表8 漏洩/侵害における特定の攻撃者の経時的変化

動機が判明している、または適用されるカテゴリーにおいて（ヒューマンエラーは動機が適用されないカテゴリー）、最も多いデータ漏洩/侵害の動機は、依然として、金銭的利益です。個人的または金銭的利益が引き続き上位に挙がっているのは、予想どおりと言えます。コーパスから除外されたボットネット侵害の他にも、日和見的犯罪者が、多数の被害者を攻撃することで、被害が大規模になる可能性がある侵害タイプがいくつかあります[4]。戦略上の優位性獲得を最終目的とした侵害が多く見られ、その4分の1がスパイ活動に関連する侵害となっています。金銭的動機とスパイ目的の動機を示す値の増減は、データ協力機関の変更や、複数の被害者を伴う大量被害の発生を示唆しています。

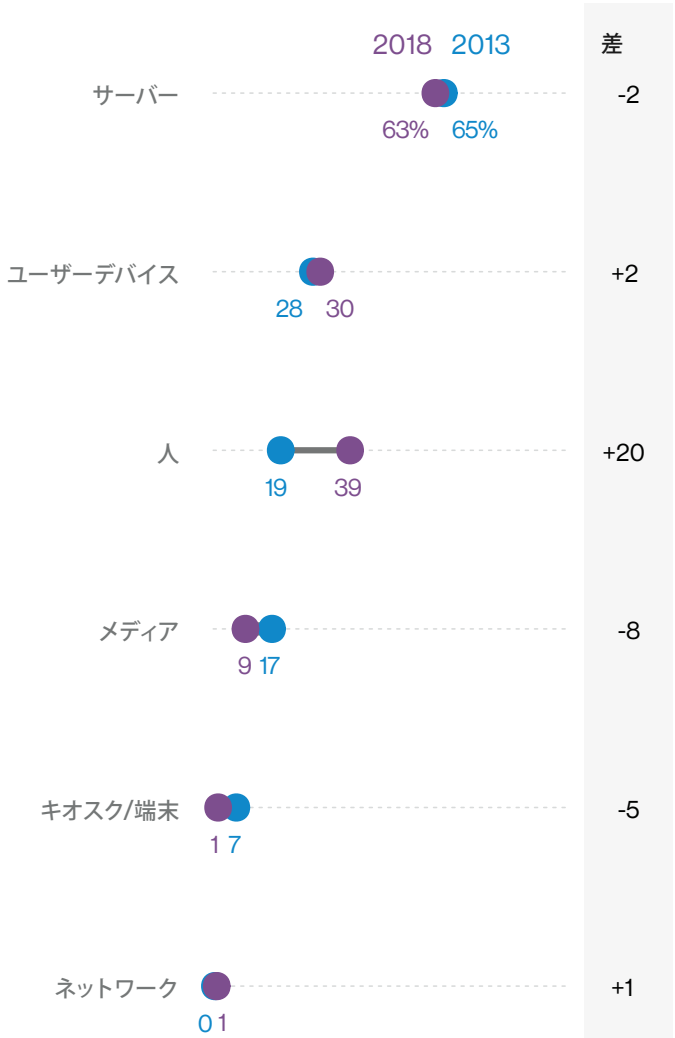
POS環境やカード読み取り操作が関与する、対面カード取引における侵害は、今年も引き続き減少しています。

上の図表8が示すとおり、組織犯罪グループおよび国家関連の侵害行為にも同様に、割合の変化が見られます。過去から現在までの変化を追う中で、もうひとつ目立つのが、アクティビストのグラフに見られる一時的な上昇です。2012年度DBIRの「確認されたデータ侵害/漏洩」において、一発屋的な増加が認められます。レジ係（飲食店スタッフや銀行窓口を含む）による侵害も、ほとんど見られなくなりました。システム管理者の割合は少しずつ上昇しています。分かりやすい要因として、ロジックボムなどの攻撃を仕掛ける悪意ある管理者も存在しますが、内部の侵害行為で最も多いのは「ヒューマンエラー」です。これは、不正アクセスをもたらすサーバーの設定ミス、あるいはアクセス制限をかけるべき情報の公開、のいずれかによるものです。臭いもの、ではなく大切なものには蓋をしましょう！

[4]「付録C：監視者の監視」において、我々はこれを、限界費用ゼロ攻撃と呼んでいます。



図表9 データ漏洩/侵害における攻撃の経時的変化 n=2,501（2013年）、n=1638（2018年）



図表10 データ漏洩/侵害における資産カテゴリーの経時的変化 n=2,294（2013年）、n=1,513（2018年）

図表9および10は、2013年から2018年までの攻撃とその影響を受けた資産の変化を示しています[5,6]。（ご覧のとおり）ここでの時間枠は7年間ではありません。これ以前の年は、デフォルト認証情報を利用したPOSデバイスへの自動攻撃を特徴とするペイメントカード侵害の影響が大きかったため、ここでは2013年を分析の開始点としています。2つの図表で明白なのは、ソーシャルエンジニアリングの台頭であり、攻撃カテゴリー「ソーシャル」と、それに関連する「人的資産」が共に増加しています。

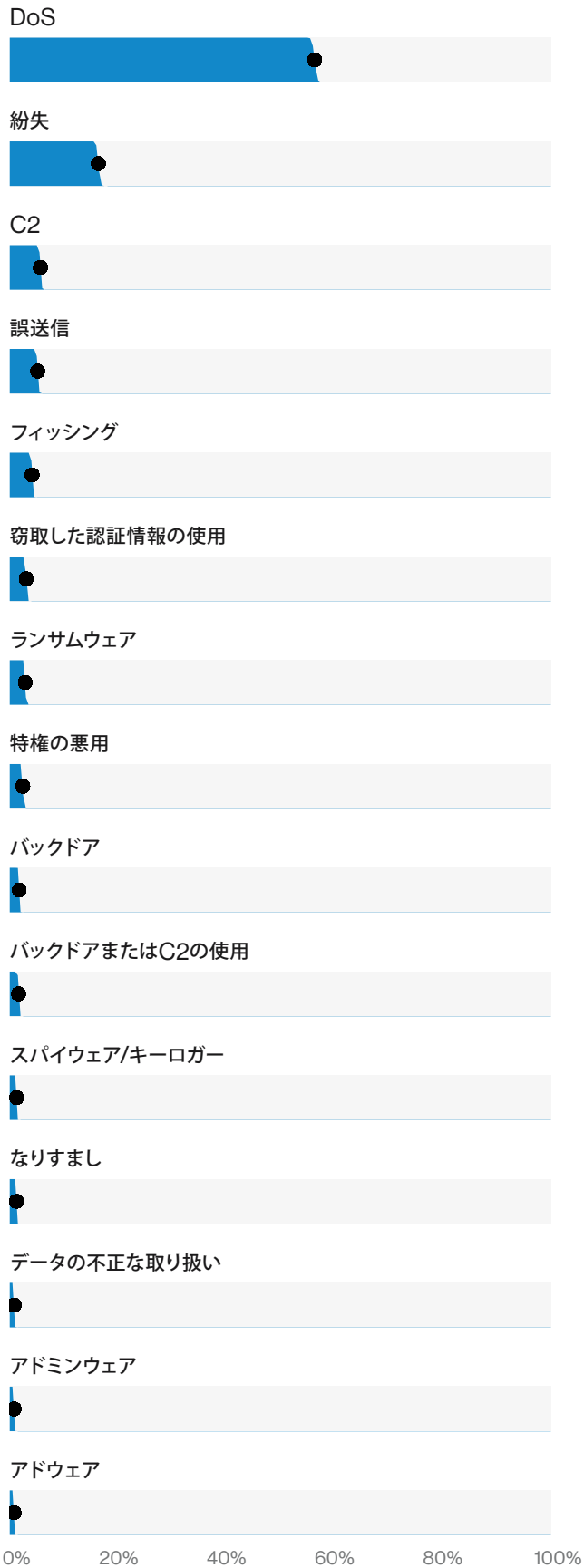
攻撃の種類

攻撃について種類別に掘り下げて検討するとき、頭に浮かぶのが「悪者たちは何をしているか」という疑問です。図表11は、DoS攻撃（サービス妨害攻撃）が、セキュリティインシデントにおける攻撃の種類の最上位であることを示していますが、確認されたデータ漏洩/侵害においては、DoS 攻撃はまだ極めて稀な存在です。同様に、紛失（資産の紛失、または置き忘れ）のインシデントは、失くした資産がラップトップや電話の場合、データへの不正アクセスの有無を確認する手段がないため、データ漏洩/侵害の区分には入りません。一方、紛失した資産が印刷された文書であった場合、それはデータ漏洩とみなされます。

次に図表12「漏洩/侵害」をご覧ください。ここでひときわ目立つのがフィッシングと、ハッキング行為の一種である窃取した認証情報の使用です。その下に続くのが次の3項目、バックドアまたはコマンド＆コントロール（C2）マルウェアのインストールとその使用です。これらは、これまで最も良く使われてきたデータ漏洩/侵害の手口であり、弊社データによれば、この手口の成功率は未だに高くなっています。

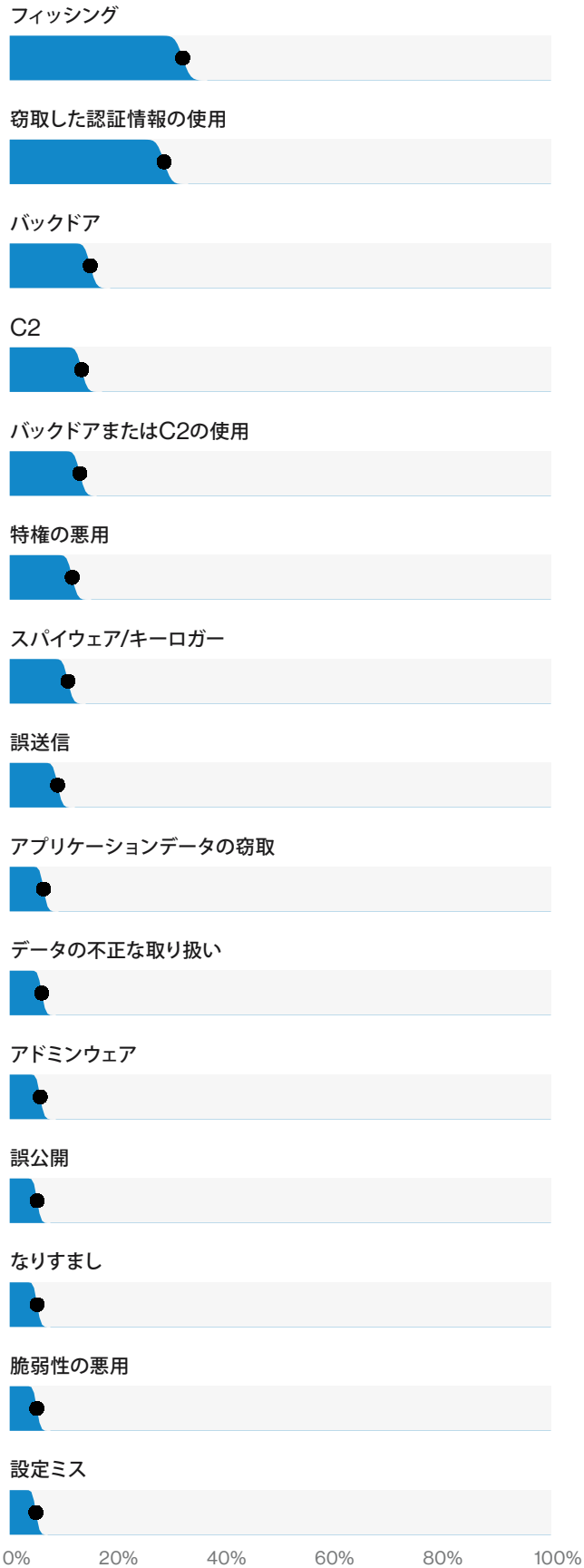
[5] 各要素の出典：このダンベルチャートは、 http://www.pewglobal.org/2016/02/22/social-networking-very-popular-among-adult-internet-users-in-emerging-and-developing-nations/のデザインおよびhttps://rud.is/b/2016/04/17/ggplot2-exercising-with-ggalt-dumbbells/のコードを基に作成されたものです。

[6] これらはインシデント発生年であり、DBIRの発行年ではありません。2018年の漏洩/侵害はすべて同じ年のデータですが、2012年の漏洩/侵害の中には2013年まで発覚しなかったものもあり、その場合、2014年のDBIRに記載されることとなります。



インシデント

図表11 インシデントによく見られる攻撃の種類 (n=17,310)

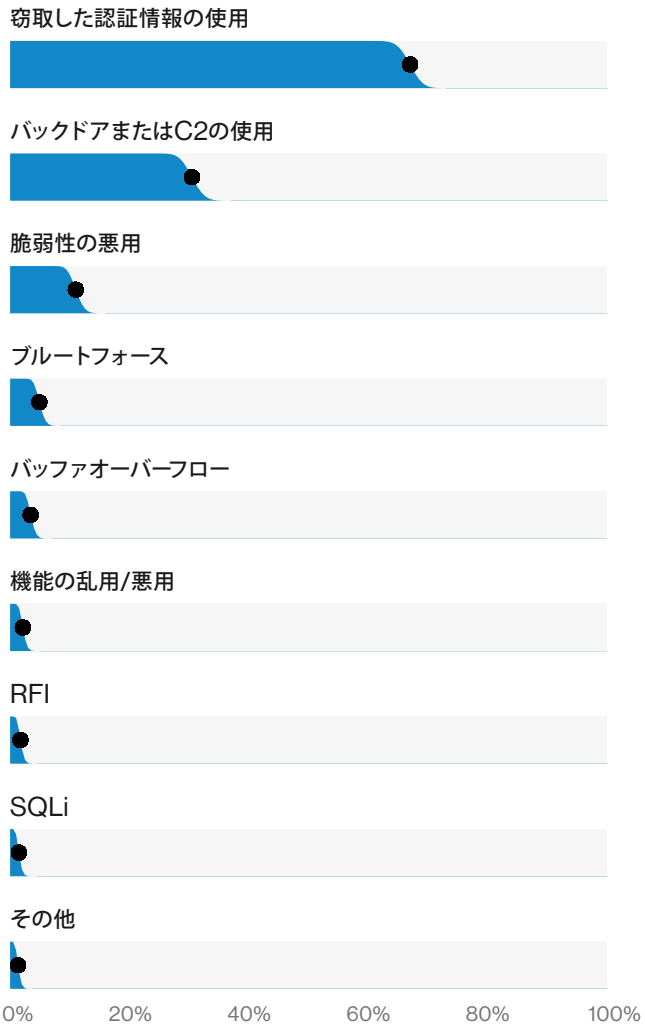


漏洩/侵害

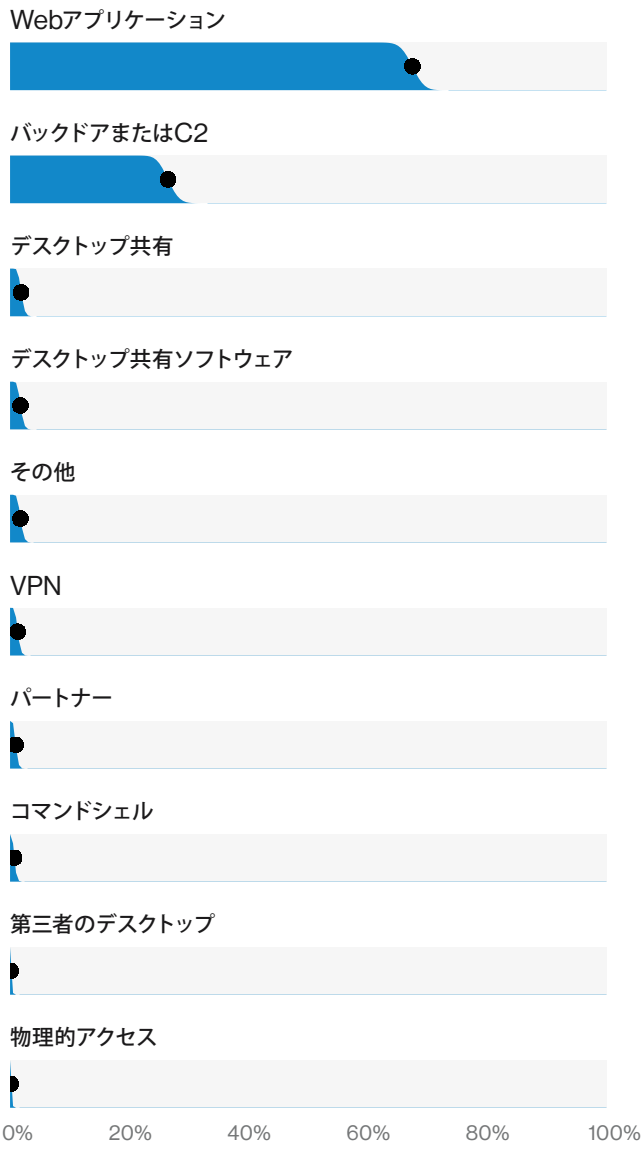
図表12 漏洩/侵害によく見られる攻撃の種類 (n=1,774)

ハッキング

以下の図表を見ると、2つの顕著なハッキングの種類と経路の組み合わせがあることが分かります。最も分かりやすいシナリオは、バックドアまたはC2チャネルを介したものです。また、そこまで明白ではありませんが、より興味深いのが、窃取した認証情報の使用です。
有効な認証情報を使ってWebアプリケーションを不正に使用するという手口には、特に新しさはありませんが、特筆すべき理由は、Webアプリケーション侵害の60%が、フロントエンドからクラウドベースのメールサーバーへの侵入という経路を取っていたという点です。



図表13 漏洩/侵害によく見られるハッキングの種類（n=755）



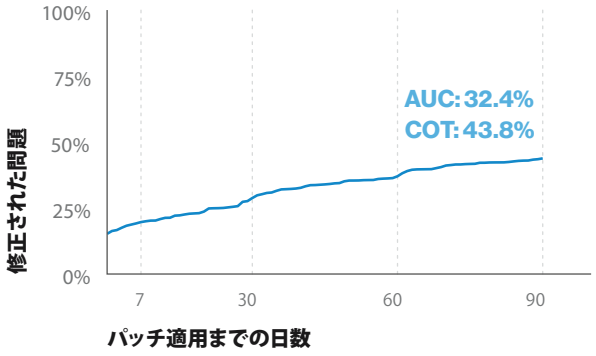
図表14 漏洩/侵害によく見られるハッキングの経路（n=862）

窃取された認証情報がパッチ適用に直接関連していなくても、やはり必要かつ的確な対策であると言えるでしょう。今年の弊社データセットにおいて、侵害の6%は脆弱性の悪用に関連するものでした。自社ネットワークをスキャンして脆弱性を診断し、結果が0件だったときのことを思い出してください。その夜は、目覚まし付きラジオから「I Got You Babe」が流れてくるまで、一晩中ぐっすり眠れたことでしょう。脆弱性スキャンでは必ず何らかの結果（良い情報も含め）が表示され、承認するか対処するかの判断は管理者に委ねられます。

図表15は、脆弱性スキャンを提供する複数の協力機関から収集した、数百の組織で行われたパッチ適用に関する情報を示しています。スキャン履歴をもとにした弊社の分析によると、組織は通常、初めて問題が発覚した時点では、その修復に大きな努力を払い、その後、問題が修復される割合は徐々に高くなり、最終的に安定します。交際中と結婚後とで、ロマンチックさや相手への気遣いに変化が生じるのと似ています。何となく伝わりましたでしょうか。

曲線下面積（AUC: area under the curve）は、積極的にパッチ適用を行っている間の保護の度合いを示しています。迅速に修復が行われると、AUCは大きくなります。期限内完了率（COT: completed-on-time）は、所定の期限内（弊社では90日間）にパッチが適用された脆弱性の数を示しています。貴社のCOT指標はこれとは異なる可能性があります。インターネットに接続しているデバイスやブラウザの脆弱性や、現在蔓延している攻撃への脆弱性に対して、異なるCOTを使用するのは当然のことです。

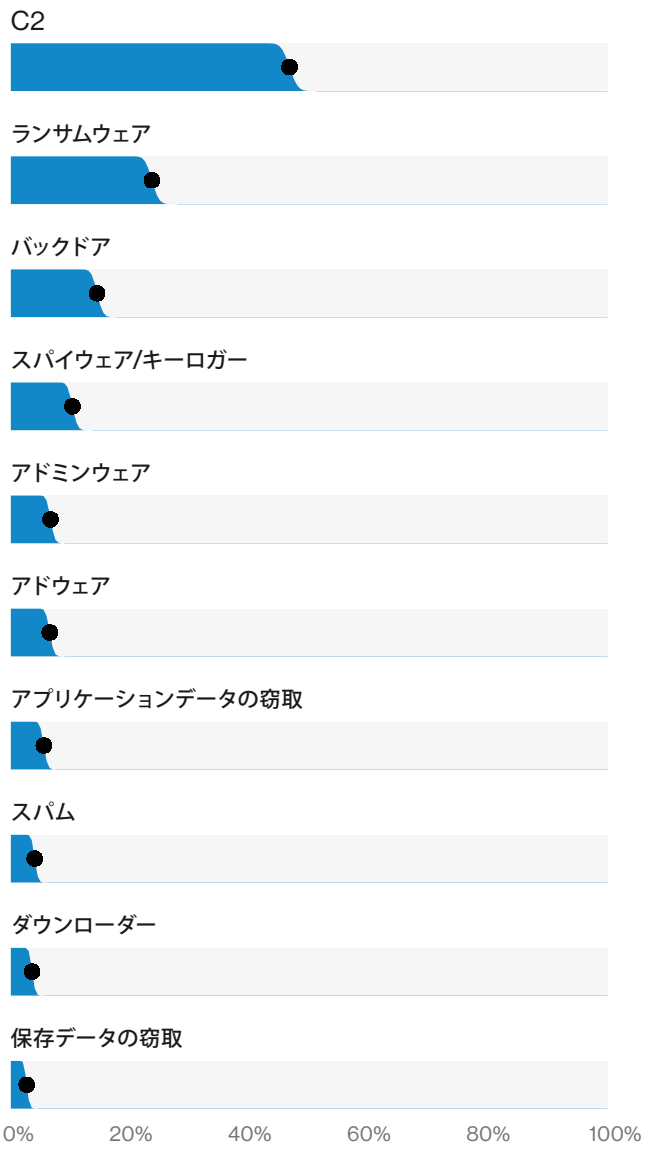
脆弱性スキャンで何らかの問題が見つかるのは当たり前であることを認識することが大切です。そこで鍵となるのは、重要な問題を優先し、それ以外の対処可能な脆弱性に対するプランを策定すること、そして、未対応の問題への防御策を講じることです。



図表15 パッチ適用までの時間

マルウェア

マルウェアは、攻撃を仕掛ける、または攻撃を進めるために、さまざまな形で活用されます。コマンド＆コントロール（C2）とバックドアは、セキュリティインシデントと漏洩/侵害の双方に見られます。ランサムウェアは、組織にとって今も大きな問題であり、データ窃取に頼らずに利益を得ることができる手口です。

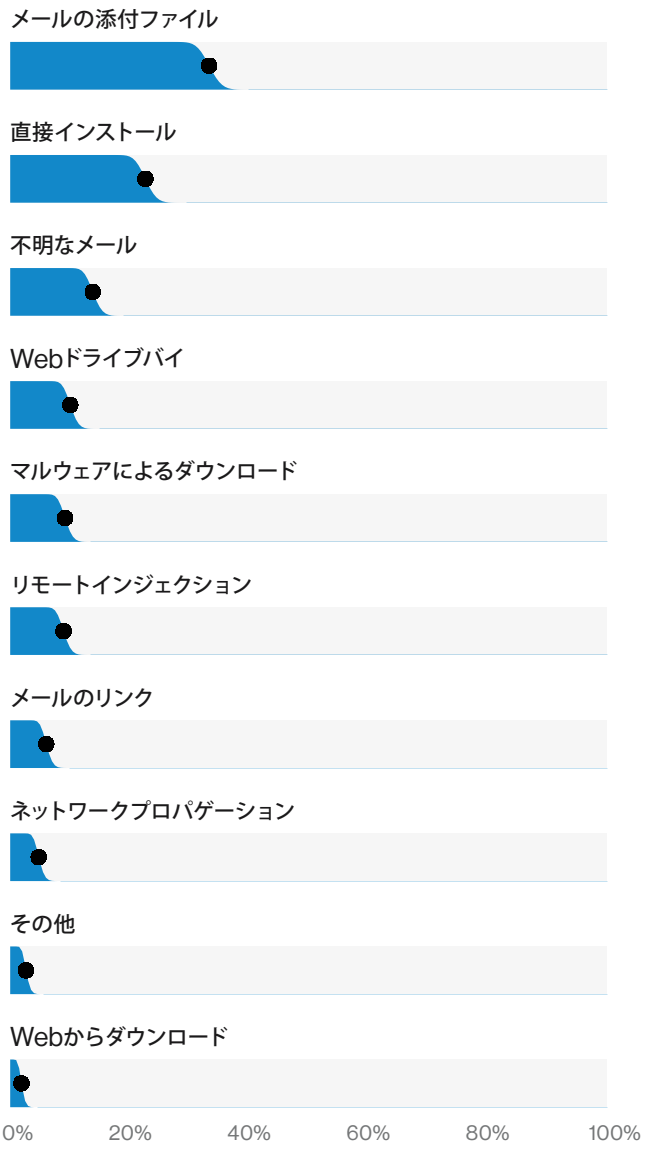


図表16 インシデントによく見られるマルウェア攻撃の種類（n=2,103）

ある日、流行に敏感な人々が集うカフェに行くと、そこのお客さんたちが「次に来るのはクリプトマイニングマルウェアだ」と話していました。しかし、今年のデータセットの数字はその噂を支持しておらず、クリプトマイニングマルウェアは、攻撃の種類トップ10にも入っていません。過去のVERISでは、クリプトマイナーはクリック詐欺の一種として扱われていましたが、今年からは固有の区分が与えられています。この新しい区分とこれまでの区分での件数を合わせると、今年は合計39件でした。ゼロではないにせよ、今年約500件発生したランサムウェアのケースに比べると、まだかなり少ないと言えます。

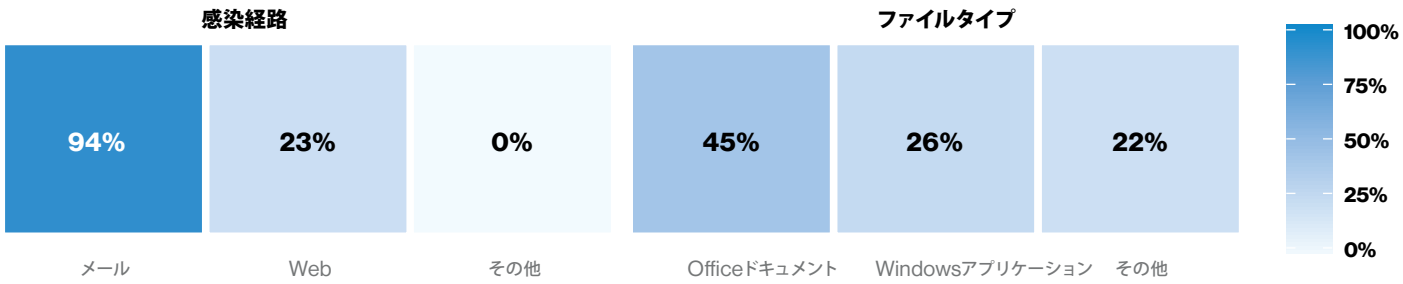
漏洩/侵害

図表17 漏洩/侵害によく見られるマルウェア攻撃の種類（n=500）



インシデント

図表18 インシデントによく見られるマルウェアの感染経路（n=795）



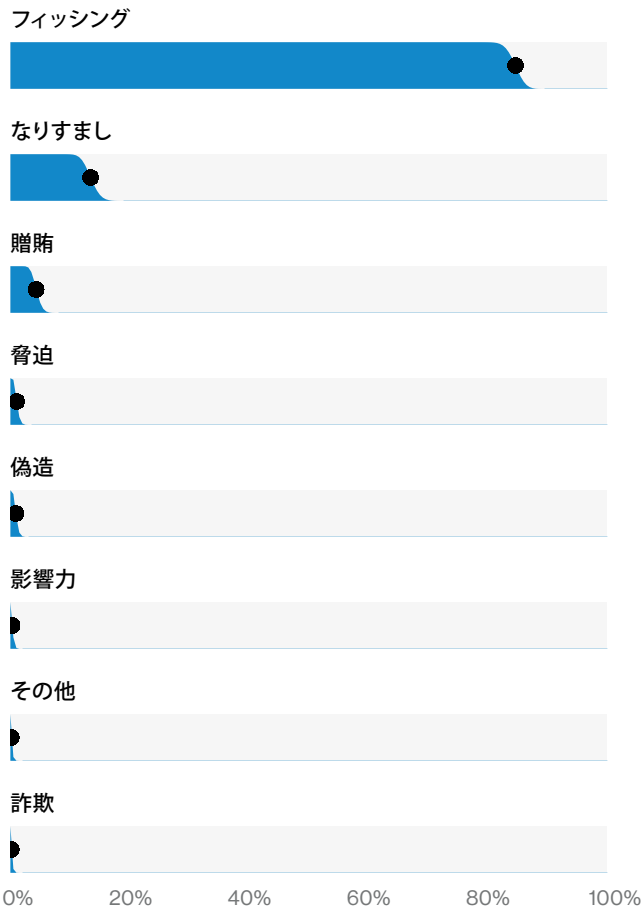
図表19 マルウェアのタイプと感染経路

図表18は、マルウェアのインストール方法が判明しているケースの中で、最も多く見られた侵入方法はメールであったことを示しています。この結果を裏付けているのが図表19です。数百万件のマルウェアデトネーション（爆発）の調査から得たデータを示すこの図表は、中央値の企業で検知されたマルウェアの90%以上が、メールで受信したものであることを表しています。直接インストールとは、既に感染しているデバイスを示唆するもので、アクセスが確立した後にマルウェアがインストールされます。マルウェアがメールを介して侵入し、足掛かりを得たところで、さらに別のマルウェアがダウンロードされ、検知を避けるようエンコードされて、直接インストールされる可能性もあります。他の多くの区分と同様、これらは互いに排反するものではありません。

ソーシャル

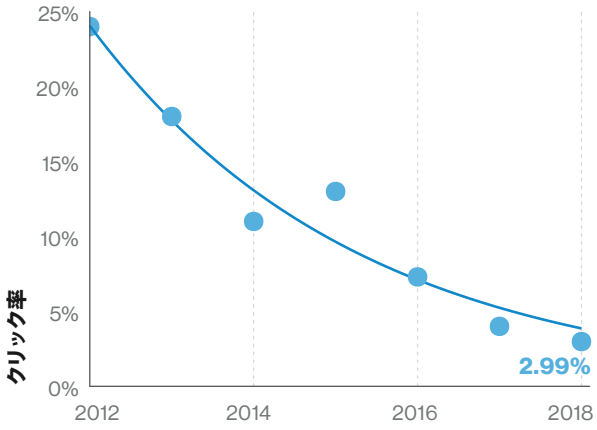
データ漏洩/侵害と聞いて、皆様が真っ先に思い浮かべるのはハッキングや悪意あるコードという言葉かと思いますが、長年にわたり横行し、現在も到るところに存在する攻撃カテゴリーは他にもあります。ソーシャルエンジニアリング、不正使用/悪用、ヒューマンエラー、物理的な攻撃は、情報通信技術がなくても実行できるものであり、間違いなく議論する価値のある問題です。ではここで、これらの犯罪について、人の行動を操る手口から見ていくことにしましょう。

フィッシングに関しては、希望の持てる結果が出ています。セキュリティ意識向上を支援する複数のベンダーの調査結果を統合したデータによると、クリック率は減少しており、図表21にあるとおり、クリック率3%となっています。



図表20 漏洩/侵害によく見られるソーシャル攻撃の種類（n=670）

これら攻撃の事象連鎖において、通信の読み込み/やり取りが行われたデバイスに、フィッシングの過程で、悪意あるコードがインストールされなかった場合は、そのデバイスは「影響を受けた資産」として記録されないことがあります。例えば、ユーザーが偽サイトに誘導され、認証情報を入力してしまった場合、その認証情報を使用してアクセスされた資産と人的資産が記録されます。ユーザーが他のことに気を取られている瞬間は、犯罪者たちにとって、モバイルデバイスに送ったSMSやメールを介してフィッシング詐欺を行う絶好のチャンスとなります。承認されたフィッシング対策トレーニングでのクリックの18%が、モバイル上で行われたものであることが、このことを裏付けています。以下の囲みは、モバイルデバイスとその利用方法が、フィッシング攻撃の成功にどれだけ寄与しているかについての考察であり、Avant Research Group, LLCの主任テクノロジストで調査員のアルン・ヴィシュワナート氏によって提供されたものです。



図表21 承認されたフィッシング対策トレーニングにおけるクリック率の経時的変化

調査によると、モバイルデバイスでソーシャル攻撃を受けると、ユーザーが被害に遭う確率が大幅に高くなることが明らかになっています。これはメール経由のスピアフィッシング（標的型詐欺）、正式なWebサイトに見せかけて誘導するなりすまし攻撃、ソーシャルメディアを介した攻撃に見られる傾向です[7, 8, 9]。

その理由は、モバイルのデザインと、ユーザーのモバイルの利用方法に起因しています。ハードウェアの観点から言うと、モバイルデバイスは比較的画面が小さいため、アクセスやきちんと表示される範囲が制限されます。また、ほとんどのスマートフォンは複数のページを横に並べて表示することができないため、ページ間・アプリケーション間を移動するには、トグルして切り替えるしかありません。これらの要素により、モバイルでは、メールやリクエストが本物かどうかをチェックするのに手間がかかります。

モバイルのOSやアプリケーションでは、メールやWebページが詐欺かどうかを確認するために必要な情報の可用性にも制限があります。例えば、多くのモバイルブラウザでは、ユーザーがWebサイトのSSL証明書のクオリティを十分に評価することはできません。同様に、多くのモバイル用メールアプリケーションでは、表示させるメールヘッダ情報が制限されていたり、メールの送信元情報にアクセスできないこともあります。また、モバイルソフトウェアでは、承認、返信、送信、いいね！など、アクションを促すGUIエレメントが強調されているため、ユーザーはリクエストに簡単に応えることができます。つまり、モバイルデバイスのハードウェアとソフトウェアは、利用できる情報の質に制限がある一方で、ユーザーの即断即決を促す環境となっているのです。

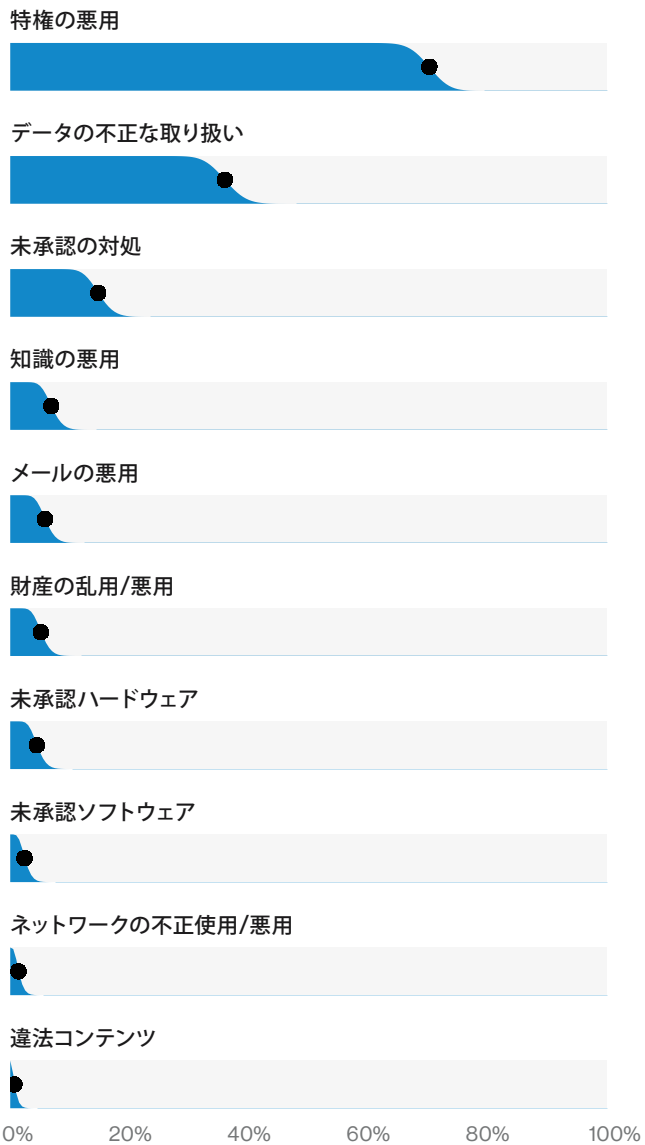
さらに、モバイルが標的にされる決定的な理由となるのが、人々のモバイルデバイスの使い方です。多くの場合、ユーザーは、歩きながら、話しながら、運転しながらなど、他の活動をしながらモバイルデバイスを使っているため、入ってくる情報への注意力が散漫になっています。ただでさえ情報が制限されている上、リクエストに応えるよう促す通知が画面に表示され、多くの場合、その送信元であるアプリケーションにわざわざ移動しなくても対応できるため、反射的にリクエストに応えてしまう可能性がさらに高まります。

つまり、モバイルのデザインとその使い方が相まって、ユーザーは十分な情報を得ないまま、簡単に即断即決することが多くなり、そのせいで、モバイルデバイスへのソーシャル攻撃に対する脆弱性が大幅に高まっているのです。

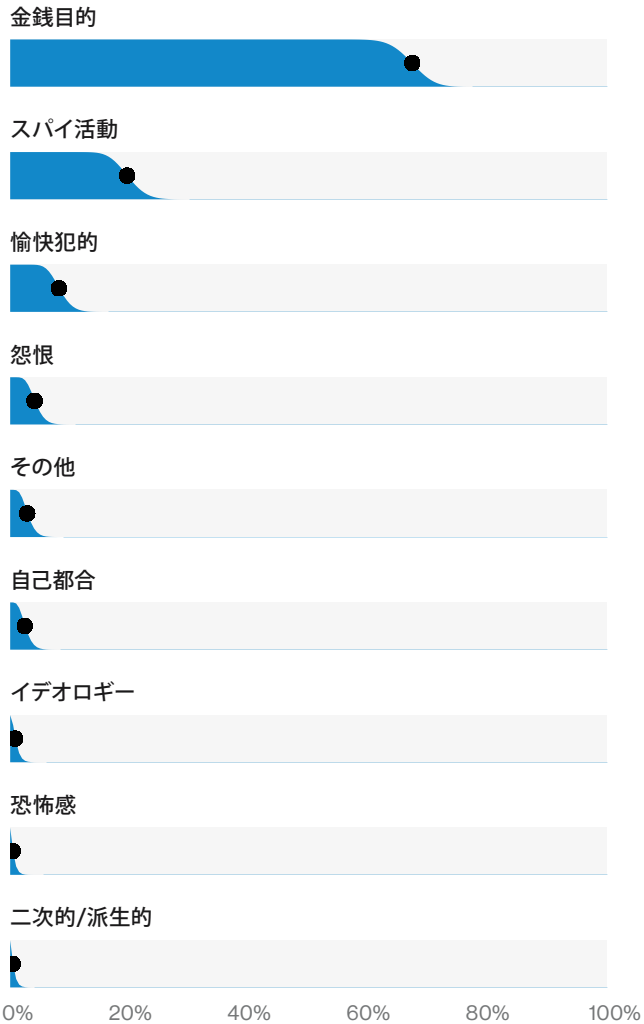
[7] Vishwanath, A.（2016年）。Mobile device affordance: Explicating how smartphones influence the outcome of phishing attacks. Computers in Human Behavior, 63, 198-207.
[8] Vishwanath, A.（2017年）。Getting phished on social media. Decision Support Systems, 103, 70-81.
[9] Vishwanath, A., Harrison, B., & Ng, Y. J.（2018年）。Suspicion, cognition, and automaticity model of phishing susceptibility. Communication Research, 45（8）, 1146-1166.

不正使用/悪用

不正使用/悪用とは、与えられている権限の悪用、または不適切な使用を指します。提供されている情報の粒度が十分でないことが多いため、本報告書ではこれ以上の定義はできません。このことは、図表22で攻撃の種類の最上位にある区分表示が「特権の悪用」という、総称的な表現になっている点にも反映されています。動機は主に金銭目的ですが、転職先で優位性を得るために、従業員が退職時に機密データを違法に盗むというケースもよく見られます。



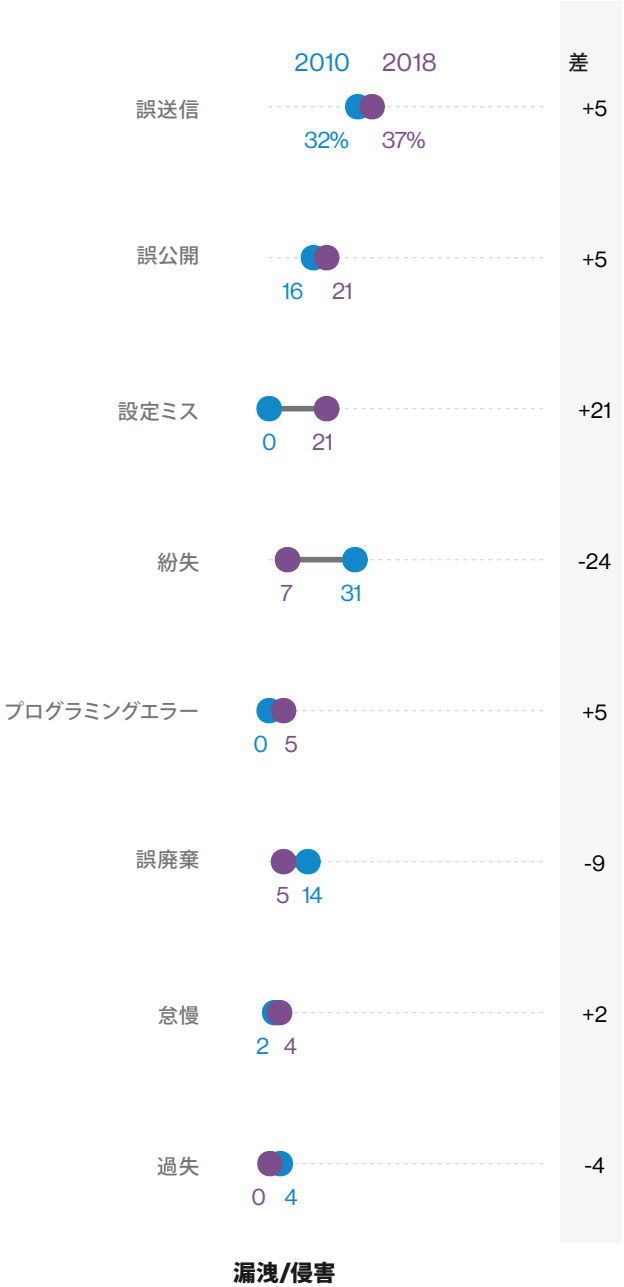
図表22 漏洩/侵害によく見られる不正使用/悪用 (n=292)



図表23 不正使用/悪用による漏洩/侵害における攻撃者の動機 (n=245)

ヒューマンエラー

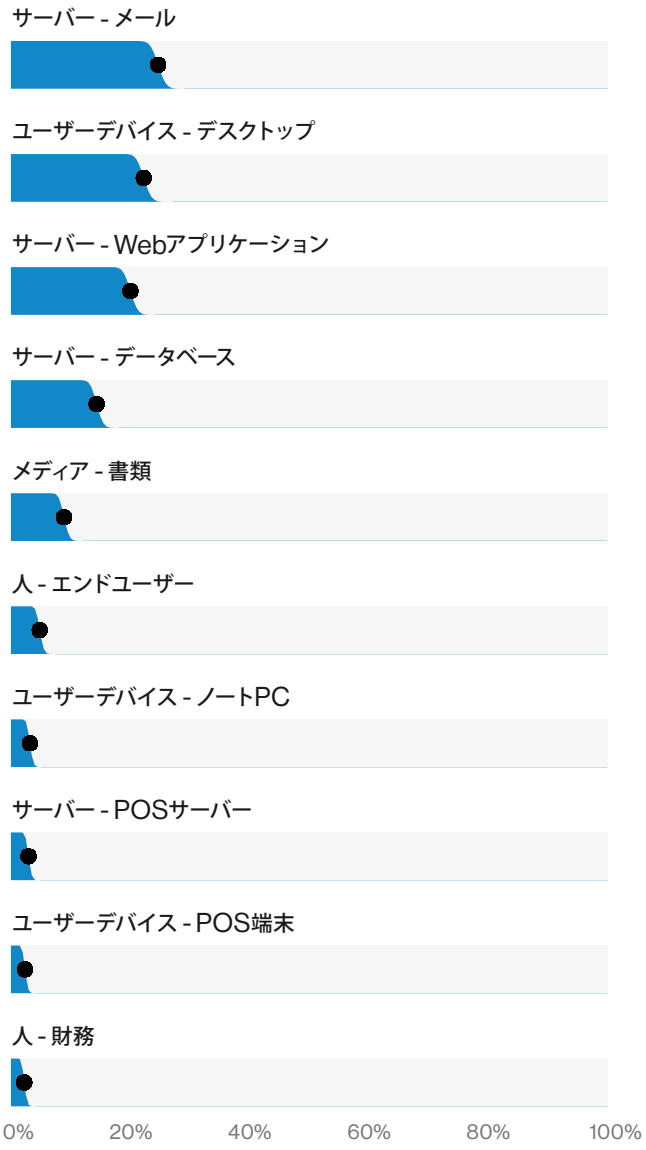
図表24が示すとおり、ヒューマンエラーの上位2項目は前回の報告書と変わっていませんが、今年は「紛失」と「誤廃棄」に代わり、「設定ミス」が増加しています。間違った相手へのデータ送付（メールまたは郵送）という問題もまだ残っています。同様に、一般公開されているWebサイトへのデータの流出（公開エラー）や、意図しないアクセス権限をゲストに付与してしまう「資産の設定ミス」も、依然としてよく見られます。



図表24 漏洩/侵害でよく見られるヒューマンエラーの経時的変化
n=100（2010年）、n=347（2018年）

影響を受けた資産

データ漏洩/侵害において影響を受けた資産の上位グループには、ワークステーション、Webアプリケーション、そして驚くべきことに、メールサーバーが入っています。漏洩/侵害の事象連鎖内での攻撃と資産との関連性については、学ぶべきことがたくさんあります。では早速、表1から見ていきましょう。表1では、2019年度のDBIRデータが提供する興味深いストーリーを読み取ることができます。



図表25 漏洩/侵害によく見られる資産（n=1,699）

攻撃	資産	件数
ハッキング - 窃取した認証情報の使用	サーバー - メール	340
ソーシャル - フィッシング	サーバー - メール	270
ソーシャル - フィッシング	ユーザーデバイス - デスクトップ	251
マルウェア - バックドア	ユーザーデバイス - デスクトップ	229
マルウェア - C2	ユーザーデバイス - デスクトップ	210
ハッキング - バックドアまたはC2の使用	ユーザーデバイス - デスクトップ	208
マルウェア - スパイウェア/キーロガー	ユーザーデバイス - デスクトップ	103
マルウェア - アドミンウェア	ユーザーデバイス - デスクトップ	91
不正使用/悪用 - 特権の悪用	サーバー - データベース	90
マルウェア - アプリケーションデータの窃取	サーバー - Webアプリケーション	83

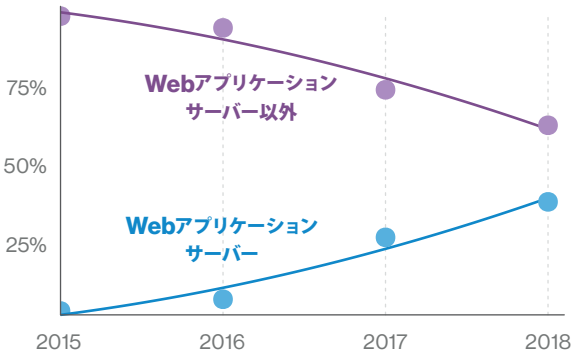
表1
漏洩/侵害によく見られる攻撃と資産の組み合わせ（n= 2,013）

上の表では、攻撃の具体的な種類が分かっていない資産は除外されています。フィッシングによる侵害の大部分で、影響を受けたユーザーの役割を明確に特定できていないため、「人 - 不明」というデータが存在します。「匿名の人物」へのフィッシングは、デスクトップへのマルウェアのインストール、またはユーザーを騙して認証情報を提供させるという攻撃につながるものと推測できます。

多くの場合、これらの窃取された認証情報は、クラウドベースのメールサーバーのものであり、ユーザーのメールアカウントを侵害するために認証情報を狙う攻撃者の増加が見られました。この新たに見つかったアクセスには、いくつかの活用方法があることが分かっています。ひとつは、そのアカウントから大規模なフィッシングキャンペーンを実行するという方法です。あるいは、アカウントの所有者がある程度の影響力を持っている人物であれば、支払い権限を持つ従業員に標的を絞って巧妙なメールを送り、偽の請求書への支払いをさせるという手口もあります。

また、組織のメールアカウントを侵害し、攻撃者が支払いに関する会話に侵入する、というケースも多く見られました。この時点で攻撃者は、転送ルールを追加できる立場にいるため、正当なアカウント所有者を会話から締め出した上で、他のメール受信者たちに「今回は○○という理由で、別の口座に送金する必要がある」と伝えるのです。

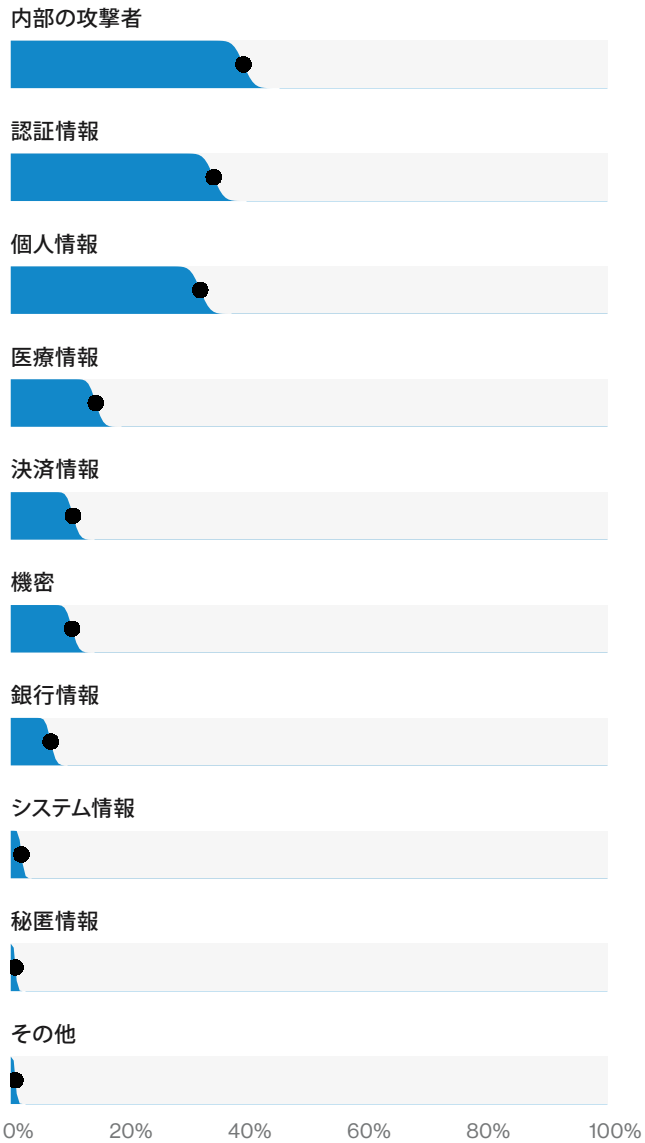
今年のデータセットに見られるもうひとつのトレンドは、ATM/ガソリンスタンドでのスキミングやPOSシステムを経由したペイメントカードへの攻撃から、Eコマースアプリケーションへと大きくシフトしたことです。Webアプリケーションに関連する漏洩/侵害が83件あったことと、攻撃に「アプリケーションデータの窃取」という項目が入っていることが、この変化を表すひとつの指標となっています。以下の図表26は、ペイメントカードの侵害が、徐々にWebサーバーに関連するものに変化してきていることを示しています。このことについて詳しくは、小売業のセクションに記載しています。



図表26 決済情報の漏洩/侵害との関連性の経時的変化（Webアプリケーションサーバー vs Webアプリケーションサーバー以外）

データ侵害

図表27は、今年発生したデータ侵害によって漏洩したデータの種類を示しています。やはり目立つのが、個人情報の漏洩です。認証情報と内部情報は、統計的に同等であり、同一の侵害で双方が認められるケースも多くなっています。非常によく見られる例は、前述した認証情報の窃取から、企業メールへの不正アクセスへと発展するケースです。

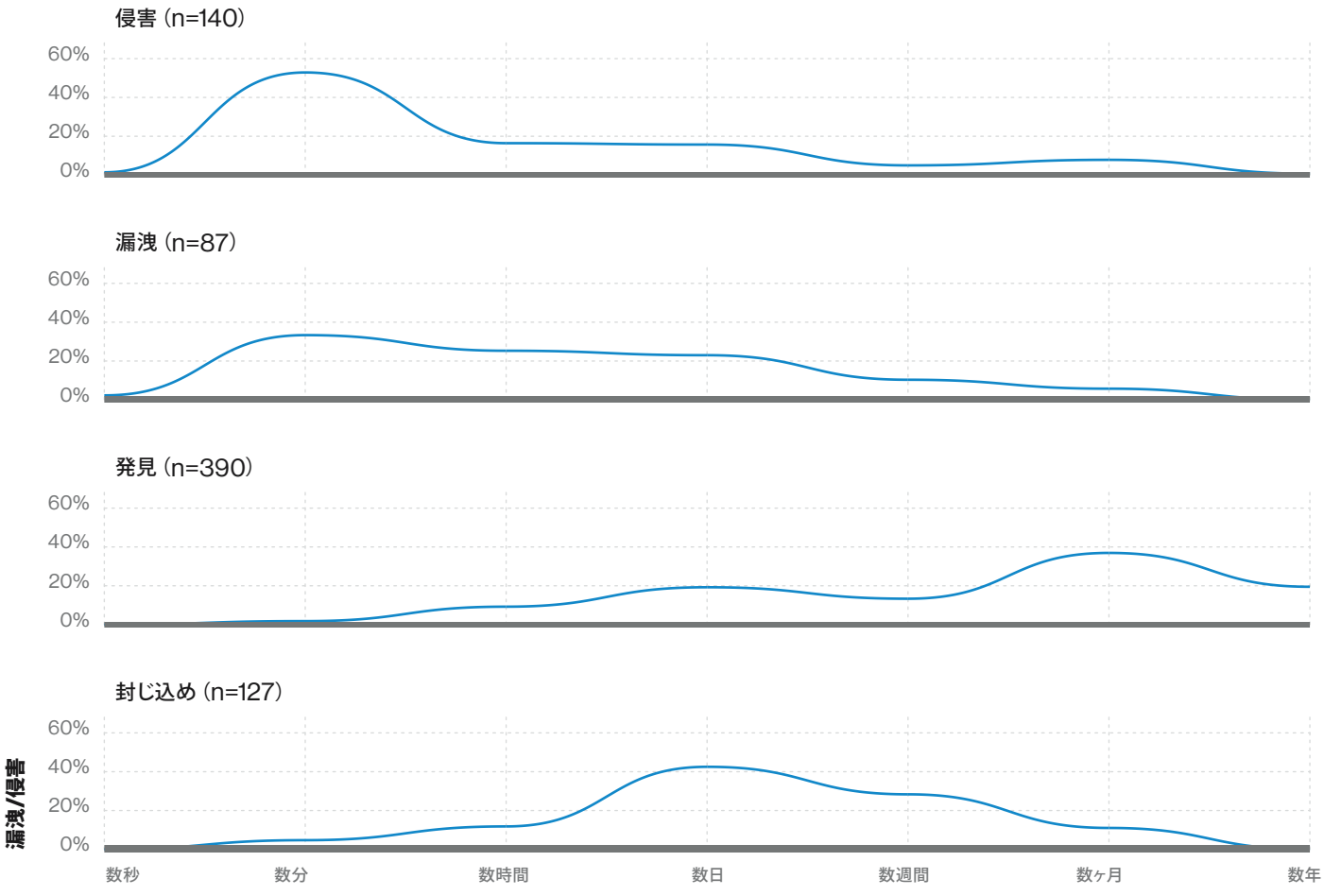


図表27 漏洩/侵害被害の多いデータの種類（n=1,285）

漏洩/侵害タイムライン

過去の報告書でも述べてきたとおり、侵入に成功した場合、情報漏洩までの時間は非常に短いのが一般的です。当然ながら、私たちには、情報収集やその他の準備に、攻撃者たちがどれだけ多くのリソースを費やしているかを知ることはできませんが[10]、1つの事象連鎖内での攻撃者の最初の行為から、資産への最初の損害までの時間は通常、わずか数分という速さです。一方、発見までの時間は、数ヶ月ということもよくあります。発見までの時間は、攻撃の種類によって大きく左右されます。例えば、ペイメントカードへの侵害は通常、窃取されたデータの不正使用によって発覚しますが（一般に、数週間または数ヶ月）、ラップトップの場合、車のガラスが割られてコンピュータが盗まれるなど、盗取されたことがすぐに分かるため、その発覚は大幅に早くなります。

言うまでもありませんが、最も理想的なシナリオは、侵害を受けないことです。そのためには、所有データの中で標的となる可能性が高いデータのタイプを把握することに注力し、（たとえデバイスが最初の侵害を受けても）簡単にデータにアクセスされたり、情報が漏洩しないよう、適切な管理・制御システムを導入することがきわめて重要です。残念ながら、弊社では情報漏洩までの時間に関するデータは数多くありませんが、貴社の組織内で、その指標と発見までの時間を改善することで、大損害をもたらすデータ漏洩/侵害を予防することが可能になります。



図表28 漏洩/侵害タイムライン

[10] 弊社でも侵害前と侵害後についての考察に取り組み始めており、「データ漏洩/侵害：広範」のセクションに掲載しています。

攻撃パス

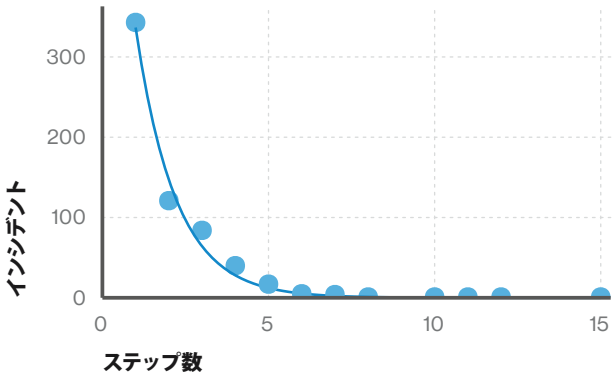
このセクションは、読者の皆様の興味と利益に叶う内容になっているとは思いますが、初めに明確にしておくべきいくつかの注意点があります。1つ目は、弊社が、事象連鎖に関するデータ収集を可能にするため、ごく最近VERISスキームのアップデートを行った、という点です。2つ目は、すべてのインシデント・漏洩/侵害の記録が、攻撃者が通ったパス（道）を突き止めるのに十分な詳細情報を提供しているわけではない、という点です。

弊社では、攻撃の各ステップで、攻撃、攻撃者、資産、属性に関する情報を収集しています。しかし、攻撃のある段階でそれが起きなかった場合、その項目の情報は「不明」となるか、完全に省略されます。弊社では、これら要素から1つのパスを作成するにあたり、そのパスの最初にある第1ステップに、まず攻撃者を配置します。次に攻撃を配置し、続いてそのステップに見られる属性を配します。以降、各ステップの攻撃から属性へ、さらに次のステップの攻撃へと進めていき、省略されている項目は飛ばす、という方法を取っています。

ヒントはゴルフにあり

昨年私たちは、ネットワークを攻撃する犯罪者は、まさに、ゴルフコースを攻め進んでいくゴルファーのようである、とお伝えました[11]。ゴルフコースの設計者は、コースの難易度を上げるため、バンカーや池といった障害物を配置します。また、ラフの芝の長さやグリーン上のピンの位置など、その他の要素を追加することで、そのホールの平均打数を上げることができます。我々の業界で言えば、これは抑止・検知・保護のための防御策や緩和策の追加に相当します。ゴルファーたちと同様、攻撃者はバッグから「攻撃」という名のアイアンを取り出し、フェアウェイの柔らかい芝の上にある標的、「属性」に到達するために、あらゆる手を尽くします。

まず知っておくべきは、最初のショットを打つためにティーグラウンドに優雅に近づくゴルファーとは違い、攻撃者に礼儀やマナーは通用しない、ということです。図表29を見ると、短い攻撃パスのほうが、長い攻撃パスよりも圧倒的に多いことが分かります。ルール無用なら（ルールを守っている攻撃者などいません）、どうしても必要でない限り、わざわざティーグラウンドから打つ必要はありません。初めからグリーンにボールを置いて、バーディー、場合によってはダブルイーグルを狙ってしまえばよいのです。良識ある普通のゴルファーは、係員に見られているかもしれないので、多かれ少なかれコースのルールを守り、1番ホールからスタートしますが、攻撃者はいつも容赦なく速攻をかけてきます。攻撃対象が機密性であろうと、完全性であろうと、可用性であろうと、狙っているホールから攻め始めるのです。

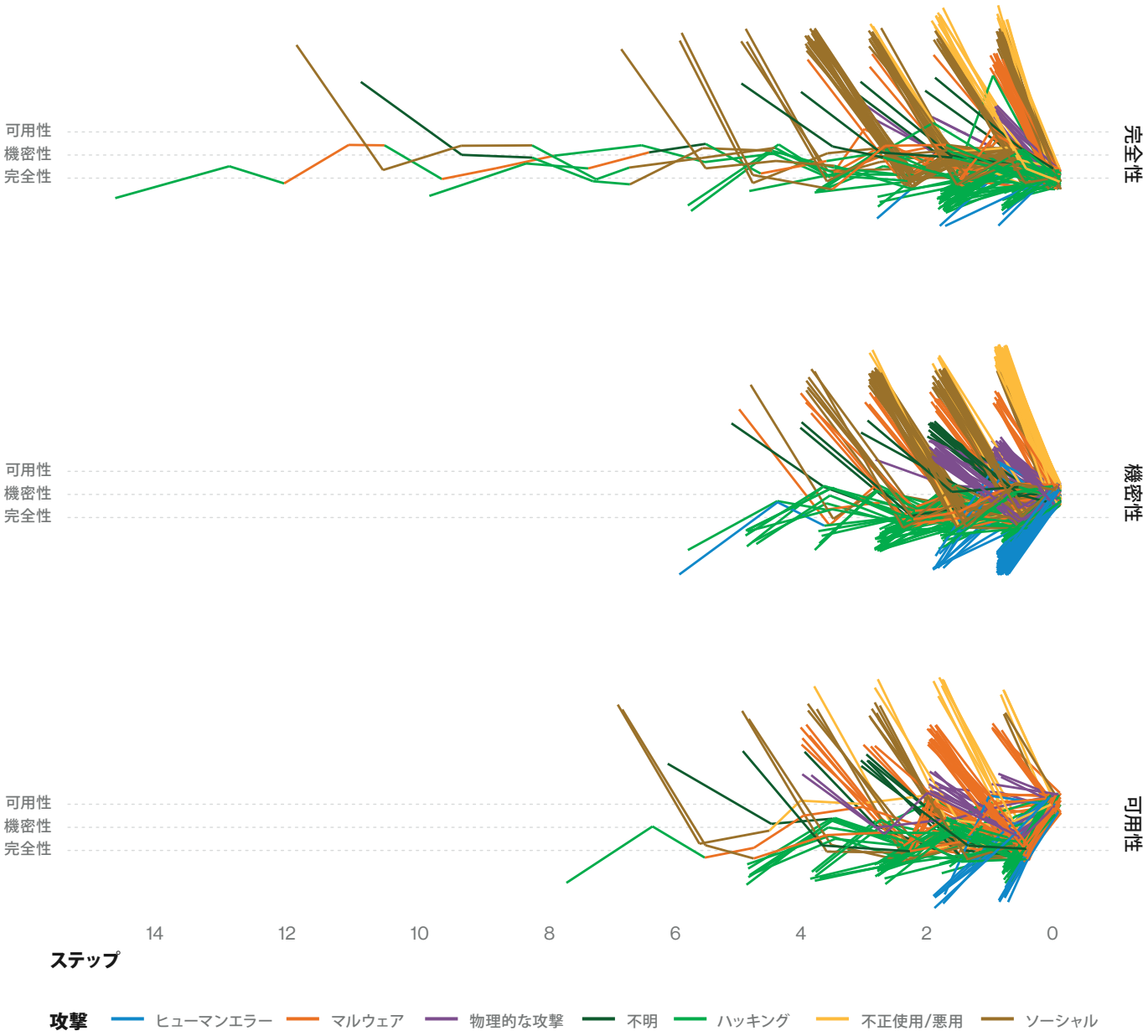


図表29 インシデント別ステップ数（n=1,285）長い攻撃パスよりも、短い攻撃パスのほうが圧倒的に多い。

「私の~~ゴルフ~~の安定感（セキュリティ）を支えているのは、心の中の静かな祈りと励ましと不安定な視覚化だ。その支えは非常に繊細で弱く、他人に見られているという大きなプレッシャーによって、その脆い骨組みは崩れ、バラバラに砕け散ってしまうのだ。」
— 詩人ジョン・アップダイク、情報セキュリティ責任者（CISO）への同情を込めて

図表30は「情報セキュリティ」ゴルフコースの3つのホールを示しています。ここには、最後に侵害された属性別に、攻撃チェーンにおける事象と攻撃の数が示されています。把握すべきことは多数ありますが、いくつかのポイントを指摘したいと思います。

[11] ハッカーたちの髪型が、90年代初頭のジョン・デーリー（ゴルファー）のような、襟足だけが長いマレットヘアだと言っているわけではありません。そのことを裏付けるデータはありません。でも実は、そうなのではないかと想像しています。イラストの中のハッカーが皆、フードをかぶっているのはそのせいではないかと。



図表30 最終的に侵害された属性別攻撃チェーン[12] (n=941)

まずは機密性のグラフから見ていきましょう。不正使用/悪用およびヒューマンエラーによる短い攻撃パスが非常に多いことご注目ください。また、比較的少ないですが、物理的攻撃から始まるパスも認められます。一方、ハッキング攻撃については、いくつかのステップごとに属性間を行き来しています。完全性のグラフには、ハッキングから始まる非常に長いチェーンがあり、途中でマルウェアに切り替わったり、再びハッキングに戻ったりしながら、標的の機密性と完全性を侵害しています。

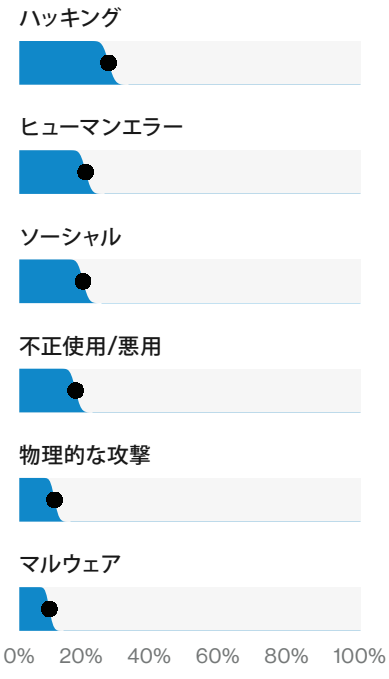
ご覧のとおり、図表30はグラフの線がかなり込み入っています。これをより分かりやすく示したのが、インシデント開始時の行為（図表31）、途中の行為（図表32）、インシデント終了時の行為（図表33）に分けたものです。

[12] かなり込み入った図表となっています。時間をかけて、じっくり研究してみてください。例えば、短時間の攻撃と長期的な攻撃の違いに着目してみましょう。

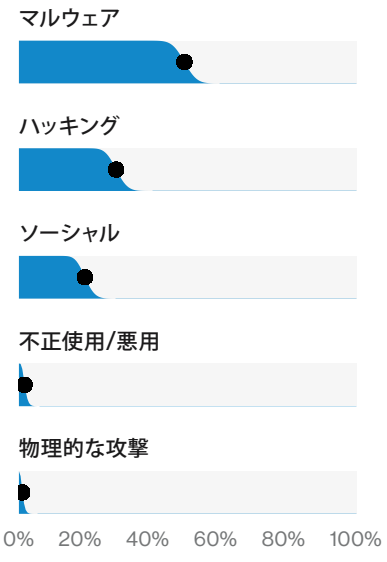
ハッキングが他よりやや多めですが、ほぼどのような行為も、インシデントの最初の行為になり得ることが分かります。最も興味深いのは、マルウェアはこのグラフの最下位であり、攻撃を行うときに攻撃者がその場にいる必要のある「物理的攻撃」よりも少ないことです。マルウェアは通常、ティーショットに使うドライバーにはなりません。侵害の多くは、ソーシャル攻撃やハッキングを通じてもたらされるということを覚えておいてください。

次に図表32を見ると、今度はマルウェアが大きく台頭しています。つまりマルウェアは、最初の一打には使用しないけれども、信頼できる7番アイアン（または3番ウッド、ご自身のゴルフの腕前によって喩えを置き換えてください）のような、途中のショットでよく使うクラブといった感じです。興味深いことに、弊社データセットにおいては、攻撃の途中の行為として「不正使用/悪用」や「物理的攻撃」はほとんど見られず、「ヒューマンエラー」は1件もありませんでした。その第一の理由は、これらは短い攻撃パスであり、途中の攻撃にリストアップされるには、攻撃チェーン内に3つ以上のイベントが必要となるからです。

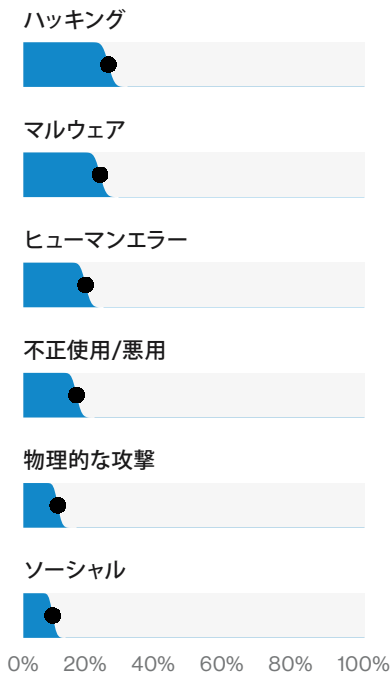
最後に、攻撃の最終段階を示す図表33をご覧ください。特筆すべきは、ここでは「ソーシャル」が最下位に位置しているという点です。図表31が示すとおり、攻撃の開始時や攻撃途中ではソーシャル攻撃の割合は大きいものの、最終段階ではめったに使用されません。



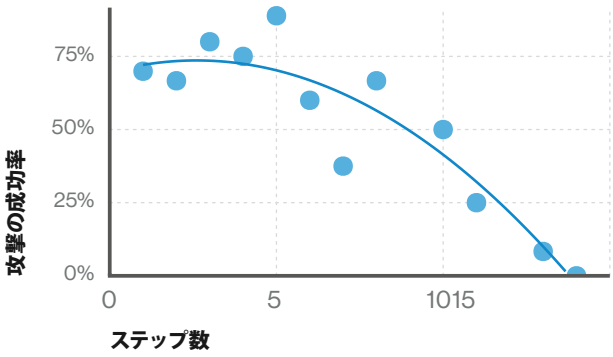
図表31 インシデントの最初のステップにおける攻撃/行為（n=909）。その他32件のインシデント（すべてのパスの3.40%）は、開始時の攻撃/行為が不明。



図表32 インシデントの途中のステップにおける攻撃/行為（n=302）



図表33 インシデントの最終ステップにおける攻撃/行為（n=942）



図表34 インシデントのシミュレーションにおける攻撃チェーンの長さと攻撃成功率（n=87）

この時点で皆様の頭に浮かぶのは「我が社のバンカーの難易度は高いのだろうか」という疑問でしょう。図表34は、漏洩/侵害シミュレーションデータから作成したものです。この図表は、テストにおいて、短い攻撃パスの阻止に失敗した回数は、長い攻撃パスに比べ、かなり多いことを示しています。自社のシステムを見渡しながら「うちは大丈夫」などと油断していたら、短時間での攻撃を被ってしまいます。

攻撃パスと緩和策

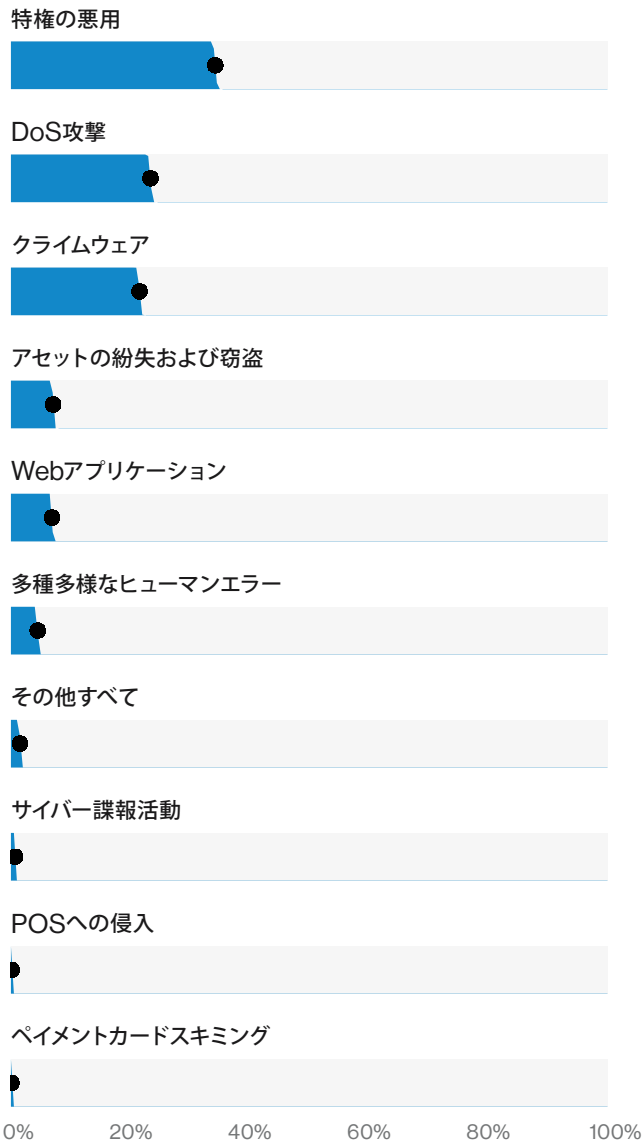
弊社の協力機関であるインターネットセキュリティセンター（Center for Internet Security）より、攻撃パスの抑止に関するアイデア提供がありました。

セキュリティの大部分は、多数の管理・制御ツール、漠然としたベンダーの約束、時間と労力を要するルール設定、組織の安全確保のための膨大な数のタスクの上に成り立っています。おびただしい数のオプションがある中、予算の正当化、人員の配置、組織のビジネスニーズへの対応も行う必要があります。攻撃パスモデルの活用は、攻撃に関する理解を形式化するための重要なステップとなるだけでなく、防御を理解するための一手段にもなります。以前は、攻撃のサマリーデータの確認時に利用できたのは、攻撃者のあるプロセスを抜き出したスナップショットであり、それをもとに、先行するイベントと後続するイベントを推測する必要がありました。そうした解釈は、認識しているか否かにかかわらず、防御策をどのように構築するかに影響を及ぼします。マルウェアが、ソーシャルエンジニアリングを介して仕込まれるのか、ドライブバイダウンロード（ユーザーの知らない内に自動にダウンロード）によって取り込まれるのか、USBデバイスを介して内部者によって持ち込まれるのかによって、マルウェアに対する防御策のアプローチは異なるからです。

加えて、終わりがないように見える潜在的攻撃のリストを前にして、スナップショットだけに範囲を限定することも、これらの攻撃の共通点を見出す能力を阻害することになります。そうした共通点は、攻撃者のプロセスにおける重要な依存先である可能性があり、我々にとっては、攻撃を妨げるチャンスになり得るものです。1つの攻撃の中で起きている一連のイベントを理解すればするほど、私たちはコミュニティとして、攻撃者たちが同じプロセスを再利用できないよう対策を立てやすくなります。

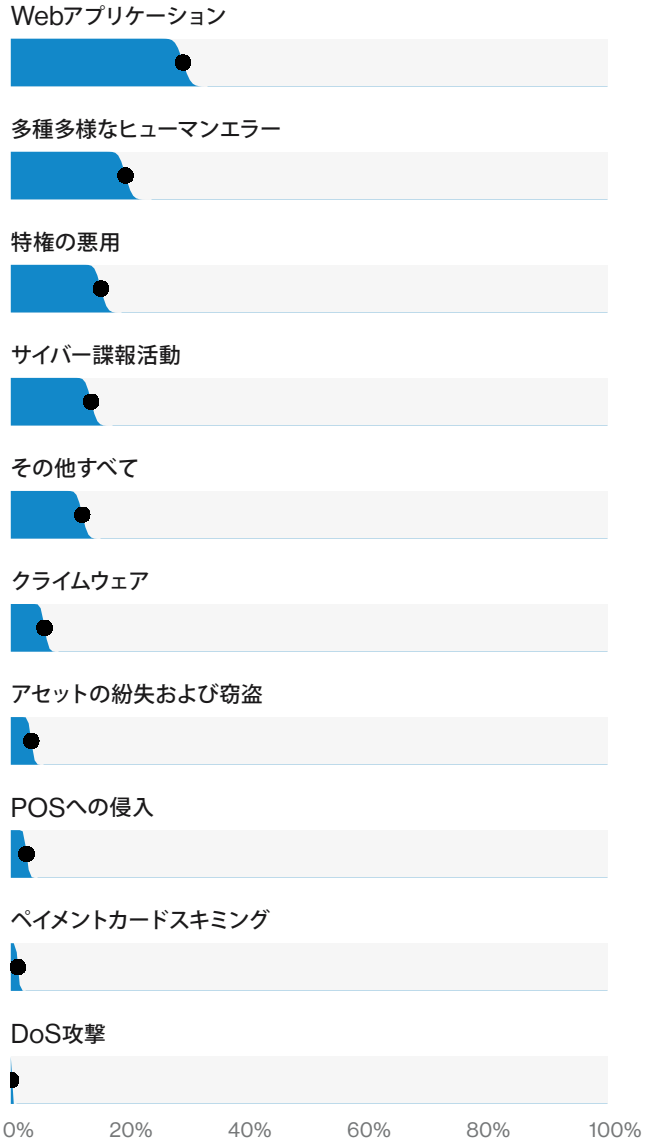
インシデントの分類パターンおよびサブセット

2014年の報告書以降、弊社では9つの基本パターンを使用して、セキュリティインシデントとデータ漏洩/侵害を、いくつかの類似する特徴ごとに分類しています。この分類は、インシデント・漏洩/侵害の大部分は、たとえそれが標的型の高度な攻撃であっても、何らかの共通点を持っているのが一般的であり、いずれかのカテゴリーに分類することができる、ということを伝えるとともに、各パターンが特定の業界のデータセットにどれだけの頻度で見られるかを研究する取り組みの一環として行われたものです。6年前、弊社が初めてパターンを特定した際、過去10年間の弊社コーパスにおけるインシデントの92%は、9つのパターンのいずれかに分類できるとの報告を行いました。そして現在、37万5,000件を超えるインシデントと1万7,000件を超えるデータ漏洩/侵害のうち、セキュリティインシデントの98.5%およびデータ漏洩/侵害の88%は、これまで同様、当初の9つのパターンのいずれかに分類することができます。人がなかなか変われないように、インシデント・漏洩/侵害も変わらないように思えます。



インシデント

図表35 インシデントにおける攻撃パターンの内訳 (n=41,686)



漏洩/侵害

図表36 漏洩/侵害における攻撃パターンの内訳 (n=2,013)

パターンについては、業界別セクションで詳しく見ていきますが、各パターンの周知・再確認のために、以下にその定義をご紹介します。

クライムウェア：
特定のパターンに当てはまらない、マルウェアが関与するすべての実例。このパターンを構成しているインシデントの大部分は、日和見犯罪的な性質のもので、その動機は金銭です。

注目すべき事項：コマンド＆コントロール（C2）は、インシデントで最もよく見られる手口（47%）であり、その次がランサムウェア（28%）となっています。

サイバースパイ：
このパターンのインシデントには、国家関連組織が関与するネットワークまたはシステムへの不正アクセス、またはスパイ活動が動機となっているもの、あるいはその双方が含まれます。

注目すべき事項：国家関連組織あるいは国家に属する攻撃者を合計すると、この漏洩/侵害の96%を占め、残りは元従業員、競合他社、組織犯罪グループとなります。フィッシングは、サイバースパイのインシデントの78%に認められ、バックドアおよび/またはC2マルウェアのインストール・使用は、インシデントの87%超に見られました。内部の攻撃者が関与する漏洩/侵害は、内部の攻撃者および特権の悪用のパターンに分類されます。

DoS攻撃：
ネットワークやシステムの可用性の侵害を目的としたあらゆる攻撃。これには、システムに過剰な負荷をかけ、パフォーマンスを低下させたり、サービスを妨害することを目的としたネットワークやアプリケーションへの攻撃が含まれます。

注目すべき事項：このパターンは、DoS攻撃における特定のハッキング行為がベースとなっています。弊社データセットにおけるDoS攻撃の被害者の99%以上は、大規模組織です。

内部の攻撃者および特権の悪用：
不正使用/悪用の攻撃カテゴリーに属するすべてのインシデント（組織リソースの無許可使用または悪用）がこのパターンに当てはまります。

注目すべき事項：これは主に、内部の人間による不正使用/悪用ですが、データセットには、元社員や、裏で共謀している社員やパートナーも見られます。

多種多様なヒューマンエラー：
意図していない行為が、ある資産のセキュリティ属性を直接侵害したインシデント。

注目すべき事項：機密情報の誤配、意図しない閲覧者へのデータ公開、サーバーアカウントの設定ミスが、このパターンの85%を占めています。

ペイメントカードスキミング：
ペイメントカードの磁気ストライプのデータ読み取りを行う装置に、スキミングデバイスが物理的に設置（改ざん、改造）された、あらゆるインシデント。

注目すべき事項：昨年に比べ、ATMやガソリンスタンドのカードリーダーの物理的改ざん件数は減少しました。これは、EMV規格（Europay,MasterCard,Visaによる共通規格）や対面決済時のカード詐欺防止策に起因するものと考えられます。

POSシステムへの侵入：
小売店において対面決済が行われる環境を対象としたリモート攻撃。攻撃対象となる資産は、POS端末およびPOSサーバーです。PIN入力デバイス（PED: PIN entry device）のパッドやスワップアウトデバイスの物理的改ざんについては、ペイメントカードスキミングのセクションで取り上げています。

注目すべき事項：ホテル業界は今なお、このパターンの被害が最も多い業界となっていますが、今年は漏洩/侵害の件数は減少しました。

物理的窃盗および紛失：
どこかに置き忘れたのか、悪意ある行為による紛失かを問わず、情報資産が失われたあらゆるインシデント。

注目すべき事項：物理的窃盗および紛失による漏洩/侵害の被害を受けた資産の上位2つは、紙の書類とラップトップです。記録されたものの中で、盗難場所として最も多かったのは、被害者の職場、または従業員所有の車両でした。

Webアプリケーション攻撃：
Webアプリケーションが攻撃経路となったインシデント。これには、アプリケーションのコードレベルの脆弱性を狙ったものや、認証メカニズムの侵害が含まれます。

注目すべき事項：このパターンの漏洩/侵害の半数以上は、クラウドベースのメールサーバーへの不正アクセスに関連するものです。

その他すべて：
前述の9つのパターンのどれにも分類されなかったインシデントまたは漏洩/侵害。

注目すべき事項：「その他すべて」のパターンに分類された241件の漏洩/侵害のうち、28%は、本セクションの後半で触れる「金銭を目的としたソーシャルエンジニアリング攻撃」というサブセットに含まれます。

パターンの中のパターン

業界別内訳を確認する上で、注目すべきインシデントのサブセットが2つあります。メールサーバー（およびメールアカウント）侵害が増加したことと、決済詐欺につながったソーシャル攻撃により多額の金銭的損失が生じたことをきっかけに、「Webアプリケーション攻撃」または「その他すべて」に該当するインシデントや漏洩/侵害を含む「金銭を目的としたソーシャルエンジニアリング（FMSE）」というサブセットが策定されました。これらのインシデントは主要コーパスにも含まれていますが、弊社では、これらについて個別の検証も行うことになりました。「ボットネット」サブセットから成るインシデントは、ボリュームが膨大であるため、主要データセットには含まれていません。これらのインシデントは、マルウェアを受け取ったという観点ではクライムウェアに分類でき、ボットネットが被害者から認証情報を盗み、その情報が他の組織のアプリケーションに使用された場合は、Webアプリケーションに分類できます。弊社データは、後者、つまり盗取されたユーザー認証情報を経由してログインされたシステムの所有者である組織から収集されたものです。

「金銭を目的としたソーシャルエンジニアリング」サブセット：
結果的にデータ漏洩/侵害または不正取引が発生した、金銭を目的としたインシデントのうち、ソーシャル攻撃の関与は認められるが、マルウェアのインストールや従業員による不正操作/悪用は認められないもの。金銭を目的とした、なりすまし攻撃やフィッシング攻撃（例：ビジネスメールの侵害、W-2フィッシング）は、このサブセットに含まれます。（W-2: アメリカでの税申告フォーマット）

注目すべき事項：370件のインシデントのうち248件は、このサブセットに該当する確認されたデータ漏洩/侵害となっています。インシデントはほぼ半々の割合で、上位パターン「その他すべて」と「Webアプリケーション」に分けられます。漏洩/侵害については「Webアプリケーション」対「その他すべて」が、3:1の割合となります。

分析によると、今年、漏洩/侵害で影響を受けた人事担当者の数は6分の1に減っていることが分かっています。この結果は、W-2詐欺との相関性があり、弊社データセットからはほとんど姿を消しています。これは、組織内での意識の向上に起因するものと考えられますが、弊社のデータからは、この減少の理由について明確な答えを導き出すことはできません。

「ボットネット」サブセット：
バンキング型トロイの木馬または認証情報を窃取するその他のマルウェアの被害者となった、5万例以上の顧客から成るサブセット。これらは詳細情報が少なく、主要分析データセットのそれ以外の部分に影響が及ばないよう、個別に分析されるのが一般的です。

注目すべき事項：被害者の84%は金融保険業（52）であり、10%が情報産業（51）、5%が専門/科学/技術サービス（54）でした。これらの侵害を受けた国と地域は180に及んでいます。ボットネットには、境界というものがなく、あまり労力をかけずに実行できる攻撃であり、銀行口座の侵害を通じて、攻撃者に直接利益をもたらすことも、攻撃の起点となるインフラを与えることもできます。

「二次攻撃」サブセット：
DDoSソースまたはマルウェアホスティングといった二次攻撃に使用された、6,527件のWebアプリケーションインシデントで構成されるサブセット。これらは正式なインシデントですが、詳細情報が少なく、主要分析データセットとは別に分析されます。

注目すべき事項：これらは具体的な情報に欠けることが多いのですが、その39%にマルウェアによる攻撃が関与しており、それらの70%がDDoS攻撃で、30%が脆弱性の利用および追加のマルウェアのダウンロードを用いた攻撃であることは分かっています。攻撃者にもインフラが必要であり、「ボットネット」サブセットと同様に、攻撃者にWebアプリケーションを乗っ取られると、組織のインフラはマルチテナントに変換されます。

データ漏洩/侵害：広範

情報セキュリティにおいては、攻撃者のほうが一枚うわてであるように思えます。認証情報を盗み、脆弱性を突き、不正にアクセスし、まんまと莫大な金銭的報酬を得るチャンスを獲得しています。一方、私たちは、OSのサポートが終了するサーバーを交換するだけでも、4年がかりのプロジェクトが必要となります。しかし、この不公平な状況に気を取られていると、大局を見失いやすくなります。攻撃に明確な狙いがある場合、通常、短時間（数時間またはそれ以下）で攻撃が行われるのは事実であり、組織への侵害が成功した場合、その発見までに数ヶ月またはそれ以上かかることが多いのもまた事実ですが、そうであるならば、そこにはまだ、楽観視する余地があります。攻撃パスのセクションでは、攻撃者がA地点からB地点に行くために通るルートについて検証しましたが、このセクションでは、攻撃の前に起きる事象、および攻撃者が利益を実際に手に入れるために攻撃終了後に行う必要のある事象に目を向けます。

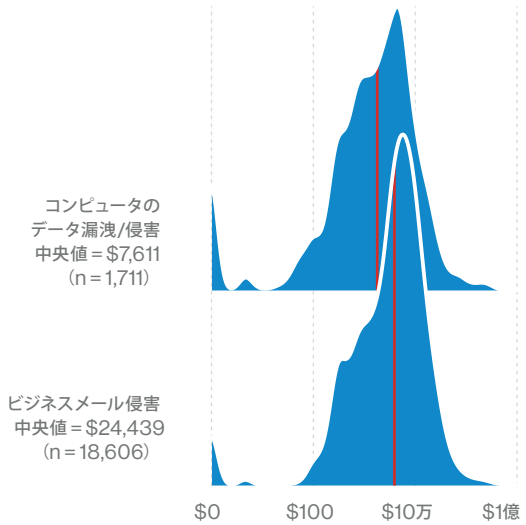
「私に支点を与えよ。そうすれば地球を動かしてみせよう。」—アルキメデス

あらゆる物語がそうであるように、攻撃者にも「取っ掛かり」が必要であり、その取っ掛かりが脆弱なサーバーのリストであろうと窃取したメールや認証情報であろうと、十分な長さの梃子があれば、そこから組織の境界を突破してきます。そのため、攻撃者にできるだけ「取っ掛かり」を与えないよう、あらゆる手を尽くして対策を講じるのが賢明です。脆弱性に対してはパッチの適用が可能であり、認証情報に関しては、多要素認証を用いて保護を強化することができます。とはいえ、最高のセキュリティ部門でさえ、できることに限界があるということも私たちは十分認識しています。ヒューマンエラー、不正使用/悪用または物理的な攻撃が関与していない侵害の62%に、窃取した認証情報の使用、ブルートフォース（総当たり攻撃）、フィッシングが認められます。そして、どんなマルウェアも自然発生しているわけではありません。当然ながら、侵害前に犯罪者側で行われている開発、準備、標的の選定、配布、その他の不正行為については、私たちにできることは多くありませんが[13]、侵害後に関しては、全く状況は違います。

ヒントはグラフに

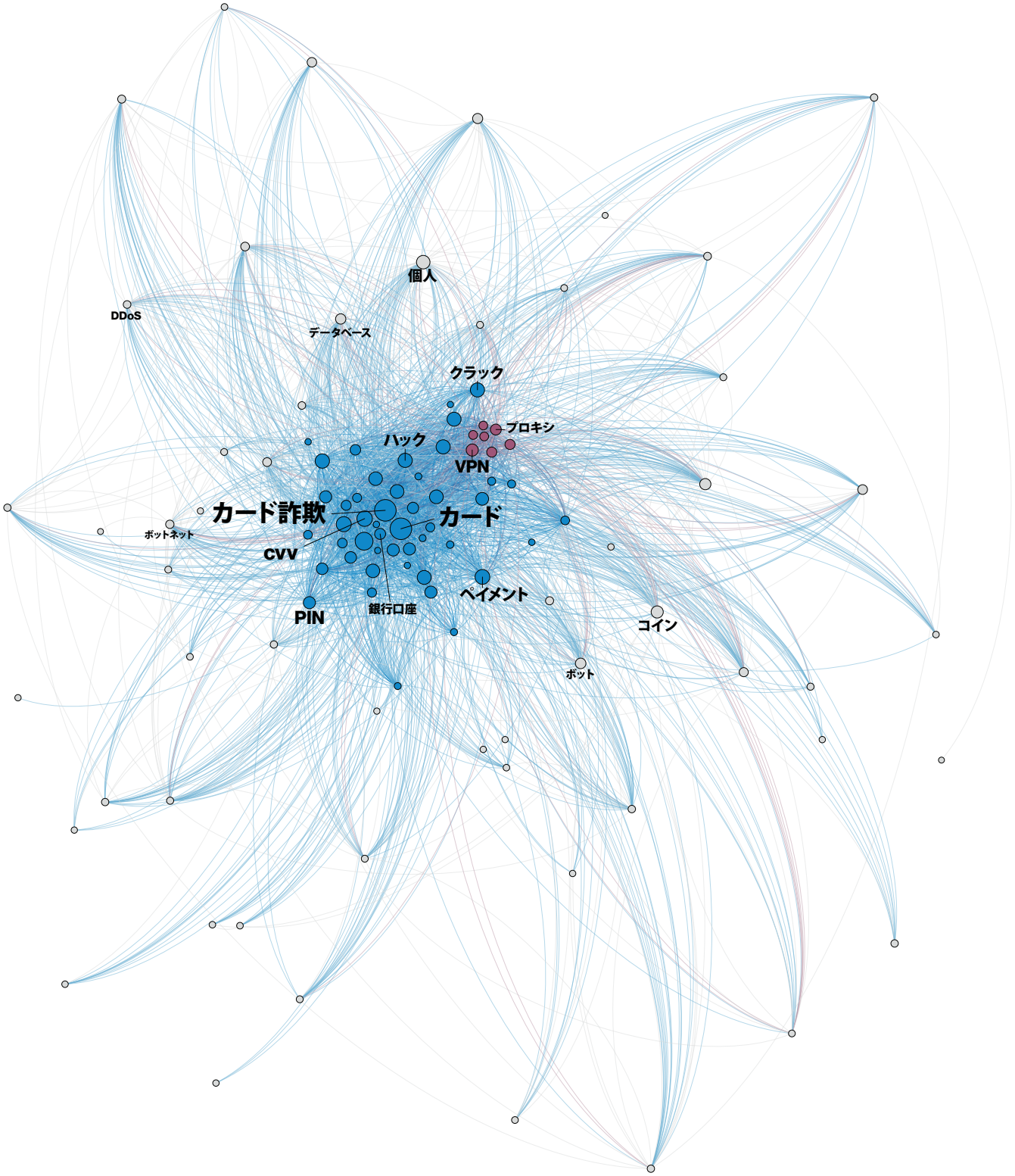
盗取されるものに着目してみましょう。図表37は「ビジネスメールの侵害」と「コンピュータのデータ漏洩/侵害」という2つのタイプの漏洩/侵害における損失額の分析を示しています。この損失額のデータは、FBIのインターネット犯罪苦情センター（FBI IC3: Internet Crime Complaint Center）の協力により提供されたものです。FBI IC3には、本セクションの最後に掲載した囲み記事において、有益なヒントをご提供いただきました。この分布図を見てまず気づくのは、ゼロの位置に見られるグラフの上昇です。つまり、すべてのインシデント・漏洩/侵害で損失が発生しているわけではないのです。2つ目の良い知らせは、ビジネスメールの侵害による損失額中央値は、中古車1台の平均価格程度である、という点です。悪い知らせは、金額を示すグラフは直線的ではない、ということです。損害額がゼロから中央値までの侵害件数と、中央値から1億ドルまでの侵害件数は、ほぼ同数となっています。そうなるともはや、中古車1台分というレベルの話（超高額な旧車は別として）ではなくなってきます。

先に述べたとおり、侵害行為を、やるだけの価値のあるものにするためには、侵害の後にも多くのアクションが必要となります。例えば、ビジネスメールの侵害には通常、攻撃者が所有する銀行口座への不正送金が伴います。



図表37 漏洩/侵害タイプ別被害額

[13] 闇市場や防弾ホスティング（bullet-proof hosting、匿名のホスティングサービス）にまで追跡の手を広げた一部の巨大組織は例外です。



図表38 犯罪フォーラムや犯罪市場への投稿に見られる用語のタームクラスタ

この点については、良いお知らせが沢山あります。IC3のリカバリーアセットチーム（RAT:）がビジネスメール侵害（BEC: Business E-mail Compromise）に呼応して動き、また送金先銀行と連携した場合、米国におけるビジネスメール侵害全体の半数で、被害額の99%の回収または凍結が実現されています。回収が不可だった被害者は、全体のわずか9%でした。そう考えると、BECは、思ったほどは犯罪者の利益に繋がっていません。その理由は、攻撃者が第一段階の攻撃に成功した後でも、我々は、その損害を軽減する対策を講じることができるからです。

それでもなお、BECには手っ取り早く金銭を得られるという、犯罪者にとって好都合な面があります。他のタイプのデータ侵害の場合、窃取したデータを利用可能な財産に変換するには、攻撃者側により多くの労力が必要となります。換金のためによく使われる手口には、個人情報やメールアドレス、認証情報、クレジットカード番号、または侵害したリソースへのアクセス権など、窃取したものを転売するという方法があります。図表38は、インターネットの闇サイトで販売されているさまざまなものに関する情報を示しています（驚くべきことに、1990年代のテレビゲームのメッセージボードに似ています）。この図表の中央には、大きな青色のクラスタがあります。このクラスタは主にクレジットカード関連の投稿で構成されています。つまり、金儲け、金銭の盗取、現金化による利益獲得を目的とした、クレジットカードの売買情報です。ここには、カードそのものの窃盗に関わる攻撃に関連した、より小さなノードも含まれています。右上には、認証情報の窃取に関連する、さらに小さなクラスタが存在します。中には、銀行口座など、より収益性の高いものへの不正アクセスを提供する情報もありますが、多くはテレビゲームや動画ストリーミングなど、攻撃者が直接使用する消費者向けサービスへの不正アクセスのための情報です。

盗んだデータをダークウェブで販売するという方法以外には、盗んだデータを使ってIDを窃取し、自らが直接詐欺を行う、という方法もあります。税務・医療関連情報を窃取するメリットはここにあります。不正な納税申告や保険料の不正請求は、現金を手に入れるために行われる比較的分かりやすい手口です。ただし、納税申告や保険請求では、番号未登録の紙幣や、南米への電信送金という形で支払いを受けることはできないため、侵害後に、マネーロンダリングという、もうひとつの手順を踏む必要が出てきます。通常、マネーロンダリングは、費用とリスクを伴う作業です。例えば、金銭が最後の受取人のところに届くまでに3人の人物を経由する場合、それぞれに取り分を支払う必要があります。しかも、3番目の人物が送金を受け取っていないと言い、最初の人物が間違いなく送金したと主張した場合、攻撃者は誰を信頼するのでしょうか。まさに「盗人に仁義なし」です。

これが、暗号通貨を好む攻撃者が多い大きな理由です。暗号通貨なら、比較的安価で、ほとんどリスクを負うことなく、資金を洗浄し、送金できるというメリットもあります。しかし、明らかな欠点もあります。このタイプの通貨は、使用できる範囲がやや限定されるという点です。そのため、どこかの時点で他の通貨に換金する必要があります。こうした理由から、不正目的での暗号通貨の洗浄や換金にまつわるリスクと費用の増大に関する調査研究には、侵害の間接費を増加させ、ひいては、その手の犯罪の相対的収益を減じる手段となる大きな可能性があります。

IC3について

FBIのインターネット犯罪苦情センター（Internet Crime Complaint Center：IC3）は、一般市民がインターネットを使った犯罪の疑いに関する情報を提供できるよう、信頼性と利便性が高く利用しやすい報告メカニズムを提供しています。

IC3では、BECを「企業および個人をターゲットに、電信送金させるよう仕向ける高度な詐欺」と定義しています。

リカバリーアセットチーム（Recovery Asset Team：RAT）は、BECインシデントに関連して窃取された資金の特定および凍結をサポートする、IC3の取り組みの1つです。

損害額にかかわらず、被害者にはオンライン（www.ic3.gov）で苦情申立てを行うよう推奨しており、法執行機関から指示されるケースも多くなっています。IC3 RATが、回収の取り組みを支援できるケースもあります。

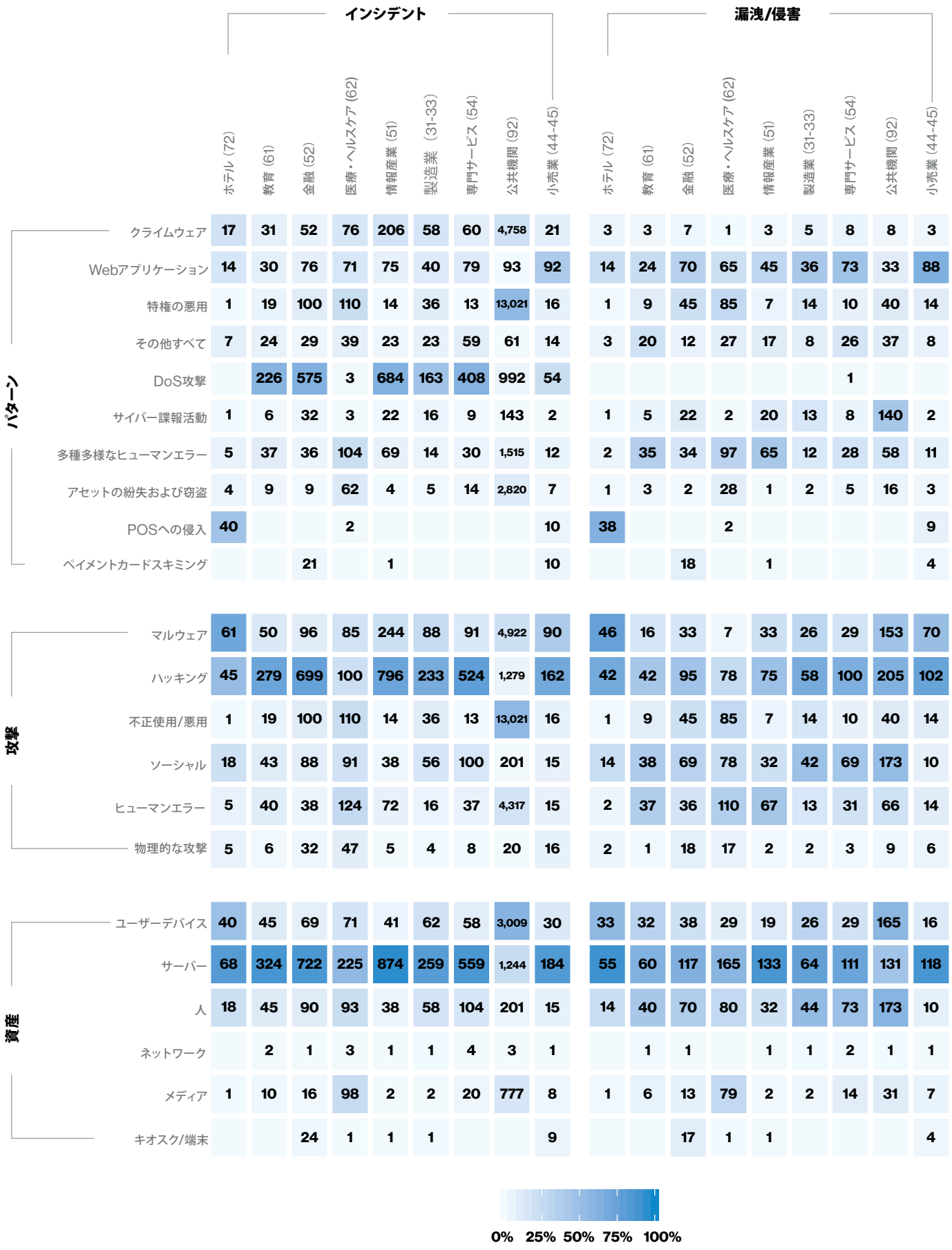
被害者についての統計および業界分析

インシデント：	合計	小規模	大規模	不明	漏洩/侵害：	合計	小規模	大規模	不明
ホテル（72）	87	38	9	40		61	34	7	20
行政（56）	90	13	23	54		17	6	6	5
農業（11）	4	2	0	2		2	2	0	0
建設業（23）	31	11	13	7		11	7	3	1
教育（61）	382	24	11	347		99	14	8	77
エンターテイメント（71）	6,299	6	6	6,287		10	2	3	5
金融（52）	927	50	64	813		207	26	19	162
医療・ヘルスケア（62）	466	45	40	381		304	29	25	250
情報産業（51）	1,094	30	37	1,027		155	20	18	117
管理（55）	4	1	3	0		2	1	1	0
製造業（31-33）	352	27	220	105		87	10	22	55
鉱業（21）	28	3	6	19		15	2	5	8
その他サービス（81）	78	14	5	59		54	6	5	43
専門（54）	670	54	17	599		157	34	10	113
公共機関（92）	23,399	30	22,930	439		330	17	83	230
不動産（53）	22	9	5	8		14	6	3	5
小売業（44-45）	234	58	31	145		139	46	19	74
卸売業（42）	34	5	16	13		16	4	8	4
運輸業（48-49）	112	6	23	83		36	3	9	24
公益事業（22）	23	3	7	13		8	2	0	6
不明	7,350	0	3,558	3,792		289	0	109	180
合計	41,686	429	27,024	14,233		2,013	271	363	1,379

表2
被害を受けた業界および組織の規模別セキュリティインシデント数

本報告書のデータセットの総数は、10万インシデント以上、具体的には、10万1168件です。前のセクションで詳述したサブセットを除外し、最小限の複雑性フィルタを適用した上で、主要分析に使用するデータセットが確定されます。表2は、被害を受けた業界および組織の規模別（既知の場合）のデータセットの内訳です。

毎年申し上げていますが、この内訳における禁忌をここでお伝えします。この内訳を使い、業界の優劣をつけないでください。建設会社のセキュリティ担当者が、この表をちらつかせながら、金融企業のセキュリティ担当者をからかう、などということは絶対にあってはなりません。



図表39 業界比較
（左：すべてのセキュリティインシデント、右：漏洩/侵害のみ）

弊社の協力機関のコミュニティ、開示要件、各業界の人口規模は、上記の数字を左右する大きな要素となります。図表39は、組織の実際の脅威状況をより詳細に示しています。この表は、各業界に最もよく見られる攻撃パターンを、攻撃カテゴリーおよび影響を受けた資産の内訳と共に示しています。この後の業界別セクションでは、「侵害」という名のジャングルを、山刀で切り込みながら、深く探求していきます。

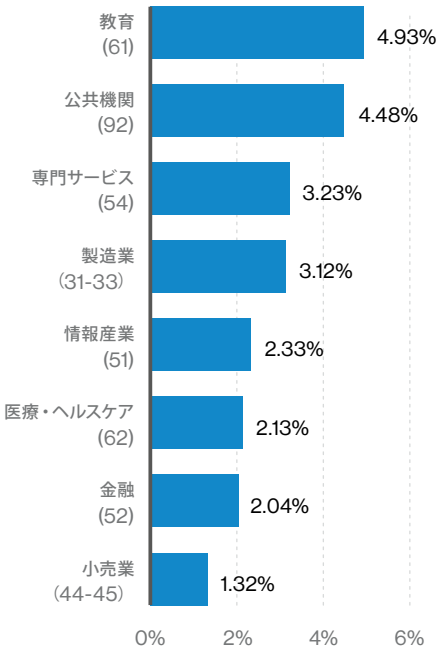
図表40 業界別FMSEインシデント (n=370)

ではここで、皆さんがそれぞれご自身の業界のセクションに移動する前にご確認いただきたい、いくつかの非インシデントデータソースをご紹介します。

各業界を分析していくと、例えば図表40では、「金銭を目的としたソーシャルエンジニアリング（FMSE）」インシデントは、専門サービス、医療・ヘルスケア業界、金融業界に偏って影響を及ぼしており、POS中心の業界は、リストの下のほうに位置していることが分かります。しかし、FMSEインシデントがあらゆる業界に影響を及ぼしているのは明らかであり、トレーニングの受講や予防のための準備は、すべての組織に必要であると言えます。

フィッシング

図表41は、セキュリティ意識向上のための承認済みトレーニング演習における、業界別クリック率のランキングとなります。このデータは、意識向上を支援するベンダー数社から提供されたデータを、分析のために統合したものです。先の表では、他の業界をからかってはいけないと少し厳しくご忠告申し上げましたが、こちらの表は、場合によっては、いい意味で刺激するのに使っていただいて構いません。ただし、度を越さないようにお願いいたします。「こちらのグラフでは、建設業は...あ、載っていないようですね」というのは程よい嫌味です（信頼してください。嫌味は得意なので）。明るい話題としては、すべての業界のクリック率は、2年前の同調査よりも全体的に低くなっています。これは大変喜ばしいことです。



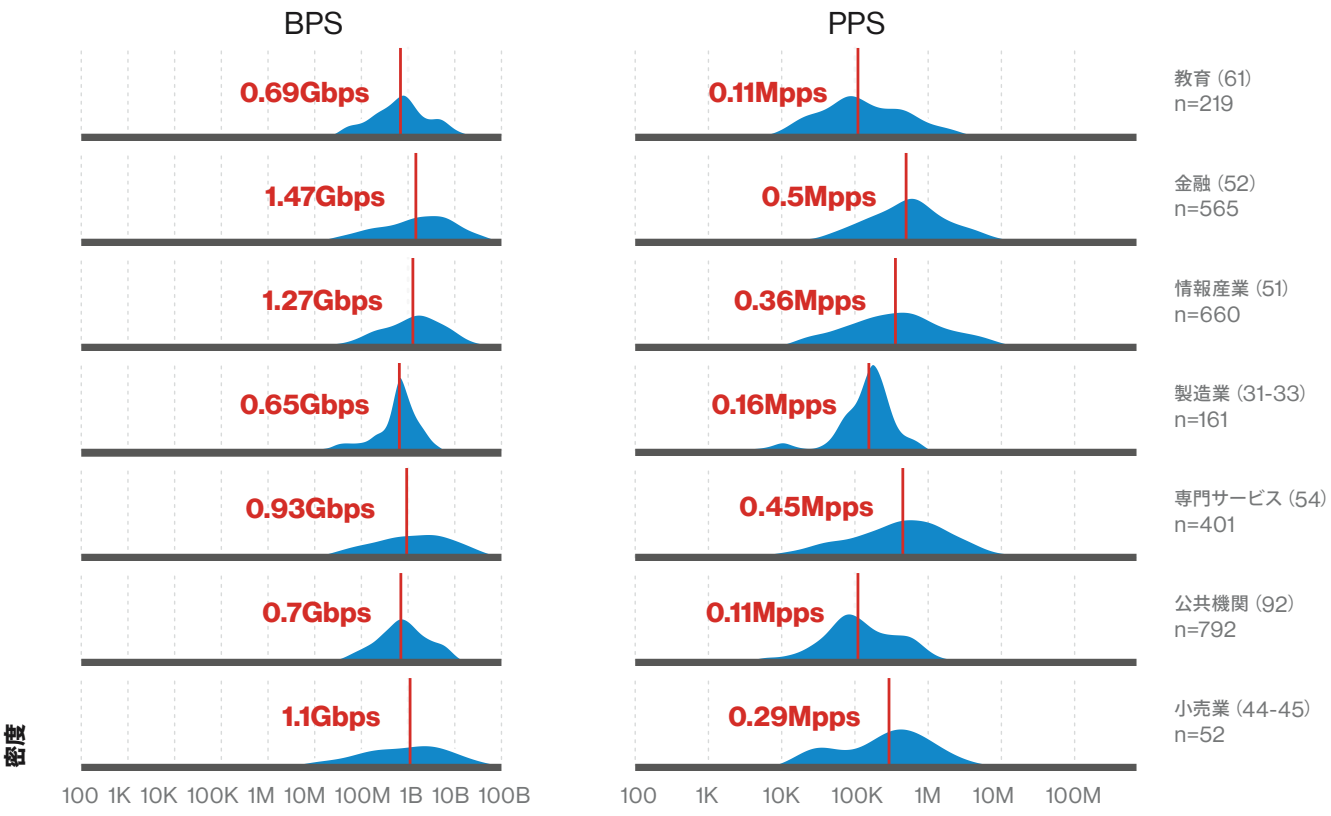
図表41 フィッシングテストにおける業界別クリック率

DoS攻撃

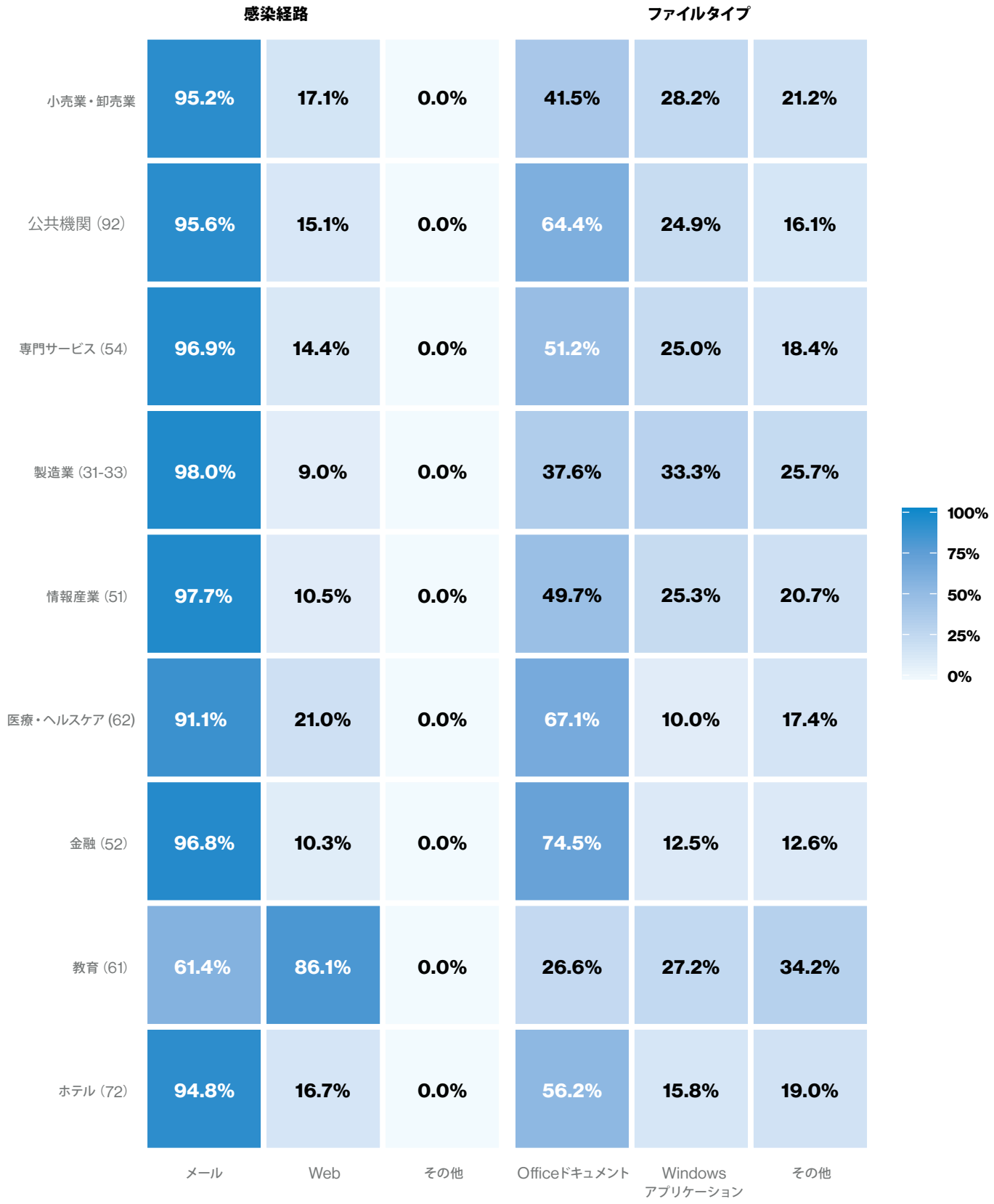
DDoS攻撃の規模は年々、（図表42の製造業のように）一部に集中するようになってきています。とはいえ、他の業界を見ると、必ずしもそうであるとは言い切れません。一部の業界、例えば情報産業では、より広い範囲にわたって攻撃されています。もう1つの重要な点は、DDoSの中央値はどの業界もあまり変わらない、ということです。業界中央値の最大と最小の差は、800Mbpsと400Kppsです。

侵入経路

図表43は、マルウェアの侵入経路およびファイルタイプの割合の中央値を業界別に示したものです。言い換えれば、組織に侵入してくるマルウェアを検知する上で、どこに着目すべきか、どのような形で侵入してくるのかを知るのに役立つ情報です。まず、最初のマルウェアの大部分は、メールで送られてきます。二次感染源は、最初のマルウェアによってダウンロードされるか、直接インストールされるため、ネットワークツールを使って見つけ出すのがより難しくなります。次に、業界ごとに多少異なりますが、マルウェアの媒体として最もよく使用されるものとして、Officeのドキュメントや Windowsアプリケーション、さらには「その他」に分類されるもの（アーカイブ、PDF、DLL、リンク、Flash/iOS/Apple/Linux/Androidアプリケーション）が挙げられます。



図表42 業界別DDoS攻撃の対象となった帯域とパケット数



図表43 業界別マルウェアのタイプと感染経路

ホテル、飲食業

弊社のデータセットにおける漏洩/侵害件数の合計は、昨年よりも減少しています。その主な原因は、パートナー認証情報の窃取により多数の企業が侵害を受けた、POSベンダーのインシデントがほとんど無かったためです。

頻度	インシデント87件、確認されたデータの暴露61件
上位3つのパターン	POSへの侵入、Webアプリケーション攻撃、クライムウェアの3つのパターンが、ホテル業界のデータ漏洩/侵害全体の93%を占める
攻撃者	外部（95%）、内部（5%）（漏洩/侵害）
攻撃者の動機	金銭目的（100%）（漏洩/侵害）
侵害されたデータ	決済情報（77%）、認証情報（25%）、内部情報（19%）（漏洩/侵害）

サービス業ならではの悩み

ホテル業界はおもてなしに誇りを持っていますが、長年の間、犯罪者まで温かくもてなし過ぎたと言えます。金銭的動機を持った攻撃者は、POS環境を侵害して顧客のペイメントカードデータを収集することにより金銭を得ています。表3に、攻撃の種類と資産の最も一般的な組み合わせを10組示します。これらの組み合わせは、同一の漏洩/侵害で認められたものですが、漏洩/侵害における同一のイベントまたは同一のステップで認められたものとは限りません。

前述の通り、これらの組み合わせの一部は、特定の行為が特定の資産に対して行われたことを示しています（例えば、RAMスクレーパーと呼ばれるマルウェアをPOS端末に感染させる、など）。その他の組み合わせは、一部の行為が、特定の資産を標的とした事象連鎖の序盤または終盤に実行されていることを示しています。つまり、ラップトップではなく、まず人を標的としてフィッシングを行い、次のステップでその人物のラップトップにマルウェアをインストールするのです。要するに、この業界の犯行手口は変わっていません。POSサーバーが侵害を受けると、ペイメントカード情報をメモリに保存するよう特別に設計されたマルウェアがインストールされ、サーバーに接続されたPOS端末に広がっていきます。こうしたPOSへの侵入は、小企業の問題である場合が多いですが、大手ホテルおよびレストランチェーンもこのデータから学ぶことができます。また、フランチャイズのビジネスモデルを採用している企業の場合は、この知識を加盟店に広めることができます。

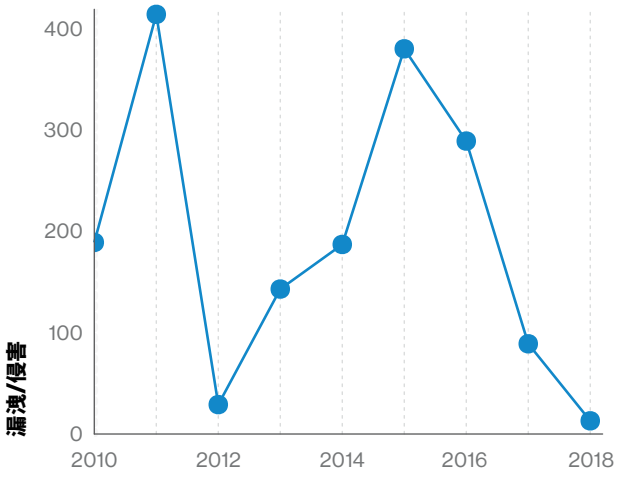
RAMスクレーパーは、この業界の名物かもしれませんが、マルウェアはシステムに自然に発生するものではありません。感染経路が分かっているものの中では、攻撃者が、窃取した認証情報または推測可能な、あるいは初期設定のままの認証情報を使ってPOS環境にアクセスし、マルウェアを直接インストールする経路が一般的です。

楽観視は禁物

POS環境に対する攻撃は、ホテルおよび飲食企業を標的としたインシデントの大部分を占める一方で、その件数は昨年度版の報告書の307件から本報告書の40件にまで減少しました。数値だけ見ると素晴らしいことのように思えますが、弊社ではデータ漏洩/侵害の件数を「改善」「悪化」の確かな指標として使用することはありません。というのも、弊社の協力機関自体に変化があるだけでなく、協力機関が重点的に対処するイベントの種類も年々変わっていくためです。これほど劇的な変化でも、前例がないわけではありません。図表44は、この種のデータ漏洩/侵害の件数の変動を示したものです。POS侵害は、組織犯罪グループが多数の標的を侵害する目的で実行する場合が多く、同一のハッキンググループが関与する数百件もの大量被害が発生しています。2011年には、400件以上もの被害が証明しているように、初期設定のままの認証情報が利用されハッキングに大成功しています。また、最近の大量被害は、侵害を受けたPOSベンダーから派生して、その顧客ベースにまで被害が及んだことが分かっています。

攻撃	資産	件数
マルウェア - RAMスクレーパー	サーバー - POSサーバー	32
マルウェア - RAMスクレーパー	ユーザーデバイス - POS端末	27
ハッキング - 窃取した認証情報の使用	サーバー - メール	8
ソーシャル - フィッシング	サーバー - メール	8
ハッキング - 窃取した認証情報の使用	サーバー - POSサーバー	7
ハッキング - 窃取した認証情報の使用	ユーザーデバイス - POS端末	7
マルウェア - バックドア	サーバー - POSサーバー	6
マルウェア - バックドア	ユーザーデバイス - POS端末	6
ハッキング - ブルートフォース	サーバー - POS サーバー	5
ハッキング - ブルートフォース	ユーザーデバイス - POS端末	3

表3
ホテル業界のデータ漏洩/侵害によく見られる攻撃と資産の組み合わせ（n= 61）



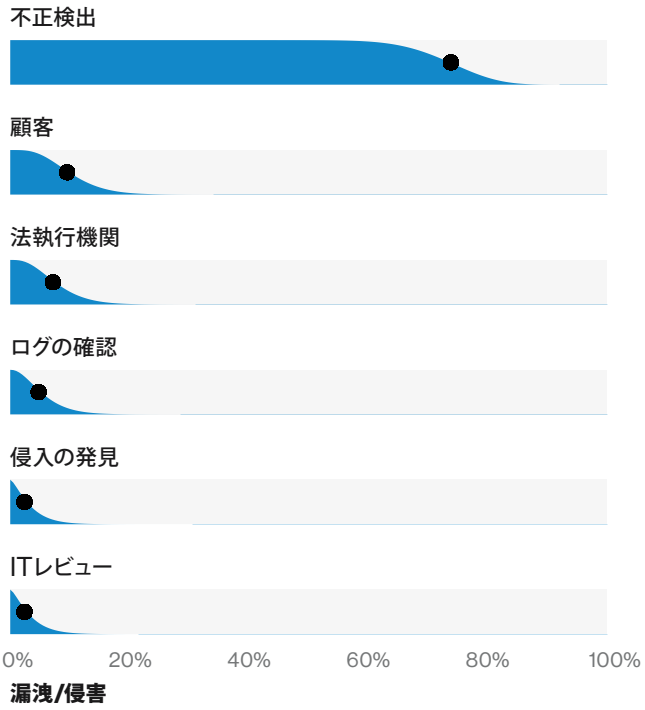
図表44 ホテル業界の漏洩/侵害におけるPOS侵入の経時的変化

昨年のデータセットに大量被害が出なかったことは、数字の低下に反映されています。しかし、（常に「しかし」が付きまとうようです）データの締め切り後、この報告書を書く間に被害に遭った複数の飲食企業に影響を与えるPOSベンダーの漏洩/侵害がすでに公表されています[14]。そこで、2020年度版のDBIRを先取りして見てみましょう。POS攻撃が実際には絶滅寸前ではないことが分かります。

悪いニュースと言えば

データ漏洩/侵害の被害に遭ったホテル企業は、図表45に示される通り、ほとんどの場合CPP: Common Point Purchase（共通の利用先）の警告を通じて被害に遭っている状況を知らされます。事実、この業界におけるPOS侵入の100%が外部の方法を介して発見されています。このことは、POS侵害に対する予防的コントロールがまだ不十分であることを示すと同時に、侵害の検出についても同様に改善の余地があることを明確に示していると言えます。これらの被害者の多くは家族経営などの小規模事業であり、現実的に考えて、これらの組織にファイルの完全性を監視する高度なソフトウェアや情報漏洩対策を求めることが実行可能なアクションプランではないことは理解できます。POSベンダーと協力し、まずは手始めに既存のリモートアクセス方法でその環境に侵入者がアクセスした際に、誰かが把握できるようにしておきましょう。パートナーによって正当な仕事がなされていることを事業主に知らせる実用的なプロセスが、確実に現在の状況を抜け出すもう一つのシンプルなステップとなるでしょう。

[14] https://ncbpdataevent.com/



図表45 ホテル業界の漏洩/侵害における発見手法 (n=42)

考慮すべきこと：

攻撃の余地を与えない
年間のデータ漏洩/侵害の合計件数は、POSスマッシュ＆グラブ（ショーウインドー破り）として本書で以前説明した被害に遭った小規模フードサービス企業により左右されます。初期設定のままの認証情報や盗まれた認証情報のどちらを利用するかにかかわらず、組織犯罪グループは多数の小規模事業を狙うことが多いですが、常にそうだとは限りません。いくつかの世界的ホテルチェーンやレストランも被害に遭っています。最初の侵入手法はインターネットをスキャンして、初期設定のパスワードを発行するほど簡単ではなかったかもしれませんが、ここから学べることはいくつかあります。静的認証が有効な認証情報を使用して回避されると、次に行われるのはRAMスクレーパー（RAM内のデータを収集するマルウェア）とPsExecやPowerShellといったアドミンウェアのインストールです。

これらをインストールすることにより、複数の地点にある複数の端末へのマルウェアの拡散が促されます。

資産を保護する
データは前年と比べてPOSサーバーおよび端末に影響をおよぼすマルウェア関連の問題があることを示しています。マルウェア対策の防御策をこれらの環境に導入して、導入の範囲とコントロールの現状を繰り返し確認しましょう。発見的コントロールにも注力しましょう。ペイメントカードの不正利用の第三者による相関分析が、貴社のPOS環境にマルウェアが侵入したことを知る唯一の手段であるべきではありません。POSサーバーへのリモートアクセスを制限し、貴社事業所間にあるPOSシステムの相互接続性に対するビジネスニーズと、最初に侵害を受けた地点からのマルウェア拡散からの防御とのバランスを取りましょう。

常に警戒を怠らない
完全に安全なシステムを構築することは不可能なため、深夜の不審なログインを監視するうえでセキュリティオペレーションが役立ちます。予算を組むことが可能であれば、セキュリティオペレーションチームの配備は必須です。社内スタッフでチームを構成することが難しい場合でも、サービスとして外部委託するか、あるいはPOS契約やIT契約の一部として義務付けることでも賄うことができ、スケールメリットを生かすことができます。

ICチップとEMV対応端末
ICチップ内蔵のカードを正しく構成されたEMV対応のPOS端末に通すと、再利用可能な磁気ストリップの静的情報（PAN）は開示または保存されません。これは防犯上有効なことであり、非接触型決済手法と同様、犯罪者による従来の情報窃盗を阻止することにつながります。EMV技術を攻撃することは、理論上は可能であっても、現実への応用にはつながっていません。サイバー犯罪者は狡猾であり、攻撃を完全に防げる手はないことは分かっていますが、弊社は今後もペイメントカードの不正利用に対する防御策の基準を高めるために新しい技術を採用し、導入してまいります。

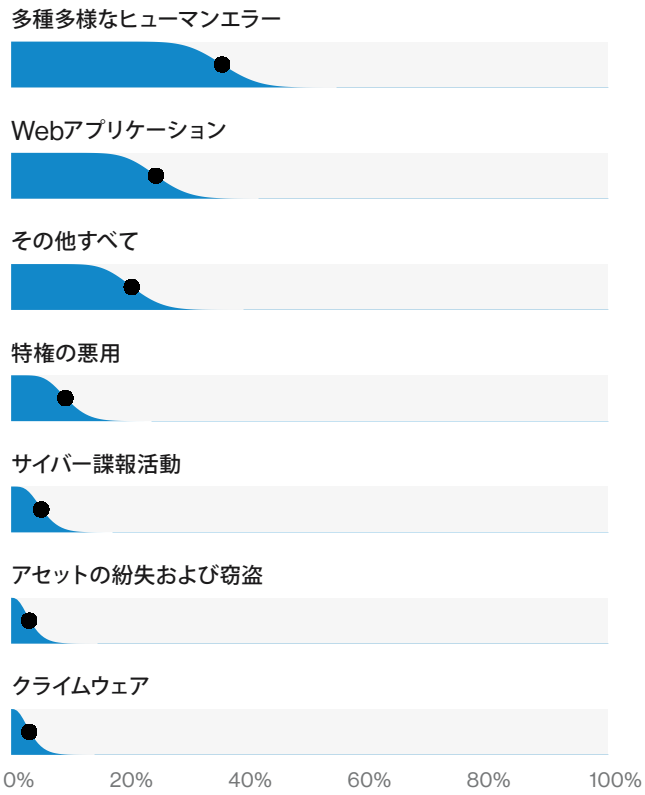
教育サービス

依然として教育サービス業界で被害が多いのは、ヒューマンエラー、ソーシャルエンジニアリング攻撃、セキュリティが不十分なメール認証情報の漏洩/侵害です。インシデントに関しては、教育サービス業界における全インシデント件数の半分以上がDoS攻撃で占められています。

頻度	インシデント382件、確認されたデータの暴露99件
上位3つのパターン	多種多様なヒューマンエラー、Webアプリケーション攻撃、その他すべてが、漏洩/侵害の80%を占めている
攻撃者	外部（57%）、内部（45%）、複数の関係者（2%）（漏洩/侵害）
攻撃者の動機	金銭目的（80%）、スパイ活動（11%）、愉快犯（4%）、怨恨（2%）、イデオロギー（2%）（漏洩/侵害）
侵害されたデータ	個人情報（55%）、認証情報（53%）、内部情報（35%）（漏洩/侵害）

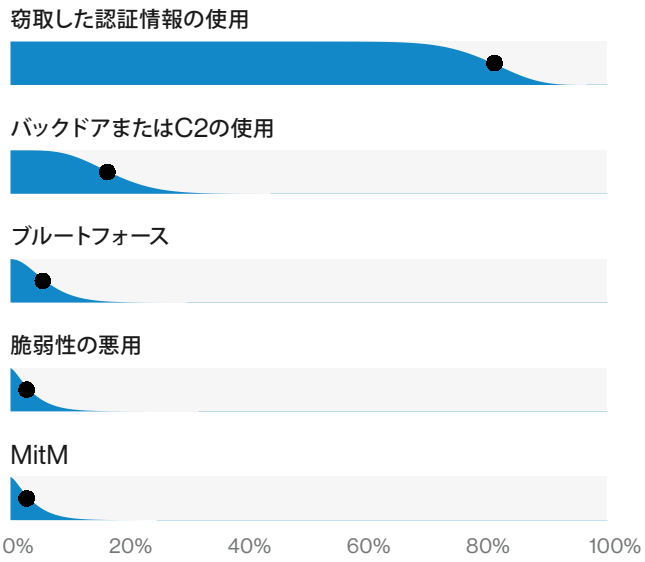
シラバスどおり

教育サービスの上位パターンを予想することは、ボールがどのカップに入っているかを当てる、手品の「スリーシェルゲーム」に少し似ています。ボールは3つのカップのいずれかに（おそらく）入っていますが、ようやくカップを指さした時、データが証明するのは、器用な手品師（統計）にまんまと騙されたという事実です。統計上は3つのパターンが激しくせめぎ合っており、オランダの3,000m女子スピードスケート選手のように、他を大きく引き離しています。多種多様なヒューマンエラー（35%）が堅調にリードを保っています。というのは、他の選手がまだ一瞬脚光を浴びた程度だからです。これらのエラーの大部分が、私たちにとってお馴染みとなってきた、誤配や誤公開など典型的な種類のエラーです。

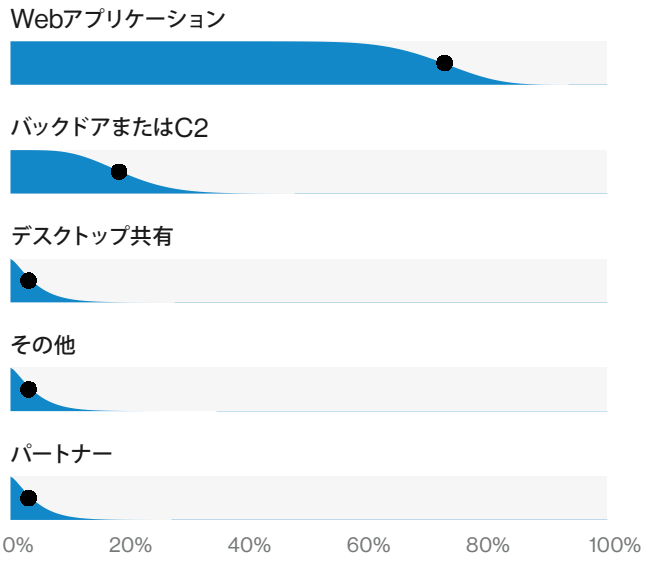


図表46 教育機関における漏洩/侵害のパターン (n=99)

Webアプリケーション攻撃は教育サービス業界のデータ漏洩/侵害のおよそ1/4を占めています。これはクラウドベースのメールサービスが偽ログインページへと転送するフィッシングリンクを介して頻繁に侵害されていることが主な原因です。そのため、こうしたサービスを日常的に使用する場合は、二要素認証を導入し、IMAPをオフにするなど、パスワードのセキュリティを強化することを検討したほうが良いでしょう。



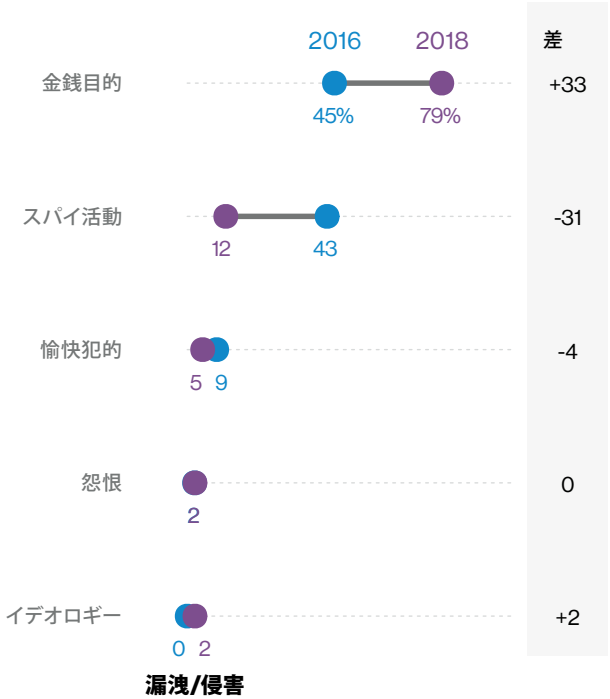
図表47 教育サービスの漏洩/侵害におけるハッキングの種類 (n=37)



図表48 教育サービスの漏洩/侵害におけるハッキング経路 (n=33)

上記以外はすべて、前述の通りほぼ「落とし物入れ」のようにごちゃまぜのパターンです。この中には頻繁に出くわす多数のインシデントタイプが含まれていますが、他のパターンに分類するのに必要な詳細情報が不足しているためにここにまとめられています。例えば、メールサーバーが侵害を受けたが、侵入起点が盗んだWeb認証情報であったかどうかが明らかになっていないパターンなどです。こうしたデータ漏洩/侵害の約半分以上がフィッシングを介したソーシャルエンジニアリング攻撃が原因であることが考えられます。

分かっている限りでは、動機は主に金銭目的で、組織犯罪グループが実行している場合がほとんどです。今年のデータセットでは、国家に関連したスパイやサイバー諜報活動の事例が2017年の報告書と比較して減少しています（図表49を参照）。この結果は、調査結果やその他のスパイ関連の目標は、この業界において攻撃が家庭科と同じ運命をたどっているのだと言っているわけではありません。むしろ、弊社のパートナーから提供されたインシデントの件数と種類に関係しているのです。



図表49 教育サービスにおけるデータ漏洩/侵害の外的動機の経時的変化
n=44（2016年）、n=42（2018年）（二次的動機は除外）

考慮すべきこと：

ロッカーをきれいに
この業界の代表的な漏洩/侵害の大半は、不十分なセキュリティハイジーン（衛生）や細部への注意不足に起因しています。可能な限りヒューマンエラーを一掃し、Webサーバーなどのインターネットに対応した資産を中心に、セキュリティのベースラインを構築してください。また、2019年にはこれらのサーバーの2FA（二要素認証）がセキュリティのベースラインとなります。

大学代表とJV（ジョイントベンチャー)
シリコンバレーの民間企業と提携している大学や、政策研究所またはリサーチセンターを運営する大学は、サイバー諜報活動の標的となる可能性が中等教育機関よりもおそらく高いでしょう。貴校がどのようなデータを持っていて、歴史的に見てどのような敵がそのデータを狙っているかを把握しましょう. 貴校は最先端のテクノロジーを研究しているわけではないかもしれませんが、少なくとも学生や教員に関するPII（個人を特定できる情報）を持っているでしょう。

セキュリティの適合性
どれだけ個別化されていると感じても、すべての人が対処しなければならない脅威があります。フィッシングと一般的なメールセキュリティ、ランサムウェア、DoSはいずれも、脅威モデリングを行い、対処すべき起こり得る問題です。これらのトピックは今さらと思われるかもしれませんが、まだ学び足りないようです。

金融保険業

依然として件数が多いのは、DoS攻撃と銀行アプリケーションの認証情報の窃取です。攻撃がフィルタリングされると、侵害を受けたメールアカウントが明らかになります。ATMスキミングは引き続き減少しています。

頻度	インシデント927件、確認されたデータの暴露207件
上位3つのパターン	Webアプリケーション攻撃、特権の悪用、多種多様なヒューマンエラーが、漏洩/侵害の72%を占めている
攻撃者	外部（72%）、内部（36%）、複数の関係者（10%）、パートナー（2%）（漏洩/侵害）
攻撃者の動機	金銭目的（88%）、スパイ活動（10%）（漏洩/侵害）
侵害されたデータ	個人情報（43%）、認証情報（38%）、内部情報（38%）（漏洩/侵害）

ソーシャルメディアの写真だけでないフィルターの使用方法

弊社では、特定の業界や攻撃者に照準を絞ってデータ解析を行い、興味深い議論のトピックを抽出するためにフィルターを使用します。また、偏りを減らし、その他のトレンドや結果を見逃さないために特定のデータサブセットを除外する際にもフィルターが有効です。これは、弊社がその存在を無視または否定しているのではなく、本報告書の別のセクションでそれらのデータサブセットを個別に分析しています。この業界では、バンキング型トロイの木馬ボットネット経由での顧客認証情報の窃取を認識し、フィルターしています。今年のデータセットにおけるその件数は、この攻撃が重要性の低い問題ではないことを示しています。

ボットネット関連のデータ漏洩/侵害件数は40,000件を超えており、これらは金融部門向けに個別に分析されています。これら両方のシナリオについては、「結果と分析」のセクションで詳しく取り上げていますが、この主題についてこれまでに語られなかった新しい事柄はあまりありません。以下は残りを示したもので、一般的な攻撃と資産のさまざまな組み合わせから見て行きましょう。

データ漏洩/侵害は多くの場合複数のイベントであり、上記の組み合わせの複数が同一のデータ漏洩/侵害において認められることもあります。

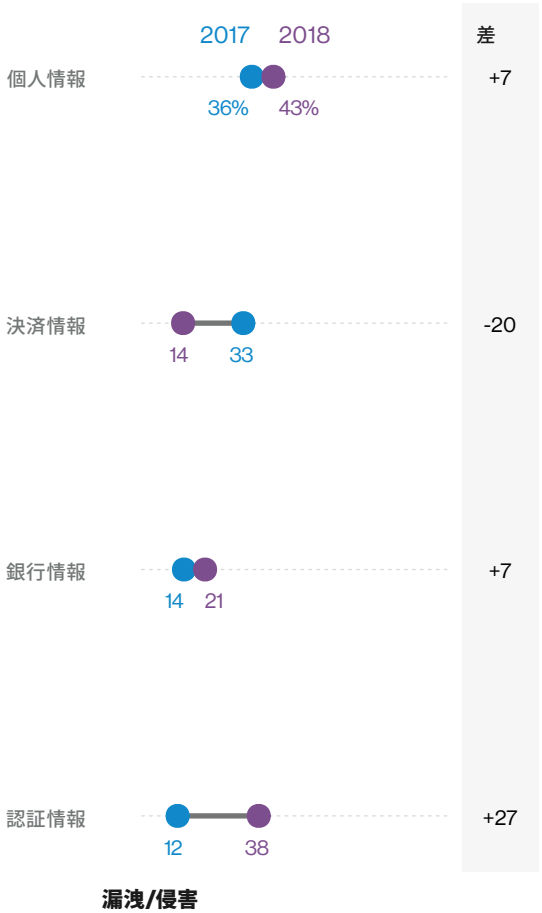
犯罪者はフィッシングを好む

表4の「影響を受けた資産」としてのメールサーバーの攻撃と資産の2つの組み合わせを見ると、犯行の手口が見えてきます。敵はソーシャルエンジニアリングの戦術を使ってユーザーを騙し、Webベースのメール認証情報を入力させているのです。そして次に、盗み取ったそれらの認証情報を使ってメールアカウントにアクセスしています。メールサーバー侵害の手口が分かっていないデータ漏洩/侵害もありますが、アカウントが利用され、フィッシングメールが同僚に送信されたことが分かっています。そのため、特定のフィッシング行為は（ソーシャル攻撃の定義がそうであるように）人に対して行われ、その前または後にメールサーバー侵害が行われています。しかも、フィッシングがメールアカウントへのアクセスの前後両方に行われないという法則もありません（フィッシング行為を規制する不正アクセス禁止法はあるのですが）また、フィッシングは悪意のあるペイロードを送信するのに便利な方法でもあります。

時代の終焉？

ATMに対する物理的な攻撃は2010年代初頭の全盛期と比べると減少傾向にあります。ATM所有者への責任の移行の影響を受けてデビットカードへのEMVチップの導入が進んだことが、この減少の理由のひとつであればと考えています。ATMジャックポットと呼ばれるハッキング手法は、ひと儲けするには面白い手口ですが、それほど広まってはいません。図表50は、昨年度の報告書と比較したペイメントカードのデータ漏洩/侵害件数の減少を示しています。

ペイメントカードのデータ漏洩/侵害件数は減少傾向である一方で、個人情報は2018年度の報告書と比較して最も大幅な増加を示しています。個人データの侵害による金融データの漏洩/侵害に注目すると、ソーシャル攻撃（「その他すべて」に分類）、データの誤送信および設定ミス（「多種多様なヒューマンエラー」に分類）、Webアプリケーション、特権の悪用が背景にあり、85%を占めています。



図表50 金融データ漏洩/侵害における一部のデータ種別の経時的変化
n=144（2017年）、n=125（2018年）

攻撃	資産	件数
ハッキング - 窃取した認証情報の使用	サーバー - メール	43
ソーシャル - フィッシング	サーバー - メール	41
ハッキング - バックドアまたはC2の使用	ユーザーデバイス - デスクトップ	17
マルウェア - C2	ユーザーデバイス - デスクトップ	16
物理的な攻撃 - スキミング	キオスク/端末 - ATM	16
不正使用/悪用 - 特権の悪用	サーバー - データベース	14
ハッキング - 窃取した認証情報の使用	サーバー - Webアプリケーション	10
ソーシャル - フィッシング	ユーザーデバイス - デスクトップ	10
エラー - 誤送信	ユーザーデバイス - デスクトップ	9
マルウェア - バックドア	ユーザーデバイス - デスクトップ	9

表4
ホテル業界のデータ漏洩/侵害によく見られる攻撃と資産の組み合わせ（n= 61）

考慮すべきこと：

取り組みに参加し、
全てに2FAを。顧客向けアプリケーションやリモートアクセス、クラウドベースのメールのすべてに強力な認証を導入しましょう。反対意見の人は、すぐさま侵害を受けた二要素認証の例を挙げて指摘するかもしれませんが、導入していない理由の釈明にはなりません。

フィッシングを撲滅する
顧客が最新のマルウェア対策を講じていることを保証するため、または顧客のフィッシング対策を万全にするために金融機関ができることは限られていますが、セキュリティに対するちょっとした認識を広めることは損にはなりません。セキュリティに対する認識は、従業員がメールでやりとりする際に用心するよう促すためにも活用しましょう。

内部犯行
特権の悪用に関連するデータ漏洩/侵害が45件確認されています。これに関する詳細は不足していますが、実証済みのコントロールは依然として実質的価値があります。機密の金融データへのアクセスを監視および記録し（すでに行っているとは思いますが）、監視や記録が行われており、貴行が不正な取引を認識できることをスタッフに分かるようにします。言い換えるならば、「悪用は割に合わない」ということを感じさせるのです。

医療・ヘルスケア

医療・ヘルスケア業界は、大部分の漏洩/侵害に内部者が関わっているという点で、他業種とは状況が異なります。DoS攻撃の頻度は低いものの、ランサムウェアの形で可用性の問題が生じています。

頻度	インシデント466件、確認されたデータの暴露304件
上位3つのパターン	多種多様なヒューマンエラー、特権の悪用、Webアプリケーション攻撃が、医療・ヘルスケア業界のインシデントの81%を占めている
攻撃者	内部（59%）、外部（42%）、パートナー（4%）、複数の関係者（3%）（漏洩/侵害）
攻撃者の動機	医療情報（72%）、個人情報（34%）、認証情報（25%）（漏洩/侵害
侵害されたデータ	個人情報（43%）、認証情報（38%）、内部情報（38%）（漏洩/侵害）

医師にも診断できない問題

病院が好きな人は少ないですが、通院が避けられなくなると、私たちのケアをしてくれる親切な人々が完璧であると強く信じるしかありません。しかし残念ながら、彼らは完璧ではありません。医療・ヘルスケア業界はペースが速くストレスの多い業界ですが、非常に規制の厳しい業界でもあります。この業界で働く人々は仕事を正確かつ迅速にこなしつつ、HIPAA法およびHITECH法（米国）などの法律を遵守しなければなりません。それだけでも十分に無理難題ですが、この業界の最も一般的な攻撃者は組織内部にいるという事実と相まって、さらに課題は困難になります。

内部攻撃者の場合、最も大きな問題は、彼らが業務をこなすために既にシステムへのアクセスを許可されているということです。表5の医療・ヘルスケア業界における攻撃と資産の組み合わせ上位のひとつが、データベースに対する（内部攻撃者による）特権の悪用です。効果的な監視を行い、業務上または患者のケアをするうえで不要なデータへの異常または不適切なアクセスを検出して警告をすることは、この業界において実際的に重要な関心事です。すべての業界で内部攻撃者によるデータ漏洩/侵害は比較的検出が難しく、外部攻撃者が関与しているデータ漏洩/侵害の検出よりも何年もかかることが多いといえます。

メールからの侵入

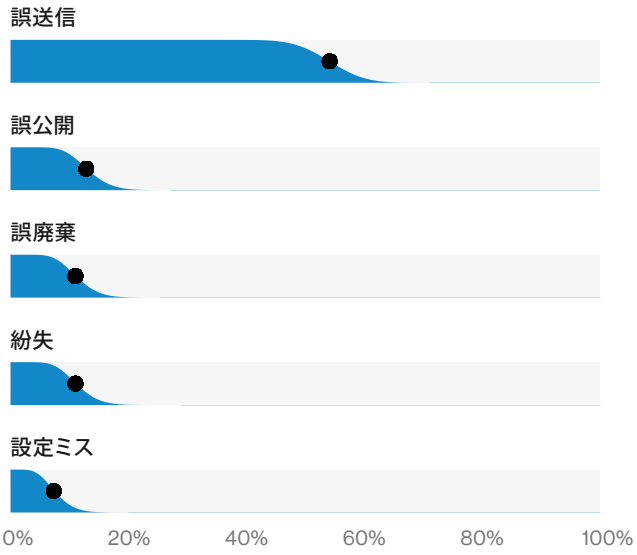
医療・ヘルスケア業界は電子媒体と紙媒体の両方を使用しているため、メールに関して多角的な問題を抱えています。この業界も他の業界で見られるような、騙されやすいユーザーにフィッシングメールが送られ、ユーザーが偽サイトへのリンクをクリックして自身のメール認証情報を入力するという非常に一般的なシナリオをはじめ、同様の攻撃の影響を受けないわけではありません。こうして新たに盗まれたログイン情報は次にユーザーのクラウドベースのメールアカウントへのアクセスに使用され、受信トレイや送信トレイ、その他のフォルダに保存されている患者データが侵害され、次に開示されます。

データを誤った受信者に送る誤送信は、医療・ヘルスケア業界を悩ませているもうひとつの一般的な脅威です。図表51に示されるように、これはデータ漏洩/侵害につながるさまざまな種類のエラーの中で最も一般的なエラーです。次のページの表5に示すように、よく侵害を受ける資産は文書です。患者さんの自宅住所に書類を郵送する際や退院書類の発行時またはその他の医療記録を誤った患者に送った際に起きたエラーが原因かもしれません。

ランサムウェアの「漏洩/侵害」

ランサムウェアのインシデントの大部分は、データ損失が確認されていないため本研究においてデータ漏洩/侵害とは定義されていません。残念ながら、医療・ヘルスケア機関は開示義務により、米国の規制要件に従って、ランサムウェア攻撃を確認されたデータ漏洩/侵害として報告する必要があるのです。

この義務は、医療・ヘルスケア部門に関連するランサムウェアのインシデント件数に影響を与えます。こうしたバイアスを認めたうえで、ランサムウェアのインシデント件数は、2年連続でこの業界におけるマルウェアの全発生件数の70%を超えています。



図表51 医療・ヘルスケア業界におけるデータ漏洩/侵害によく見られるエラーの種類（

考慮すべきこと：

アクセスを制限する
主要なデータのストレージがどこにあるかを把握し、必要なアクセスを制限し、すべてのアクセス試行を追跡しましょう。業務上必要でないと思われるアクセスの回数が多いユーザーから監視を始め、不要な検索を検出することを目標にしましょう。

内部告発を促す
フィッシング報告の方法を改善し、性急なクリックに迅速に対応して、以後のクリックを防止できるようにしましょう。また、可能であれば報奨金をかけることを検討しましょう。甘い蜜でより多くのハエを捕まえることができます。そして、捕まえたハエはさらに魚を釣るのに利用できます。フライ「フィッシング」の原理です。

不完全であることを知る
個人情報や医療情報の送信・公開・破棄に使用されているプロセスを把握し、そこにチェック機能が含まれていることを確認して、1つのミスがデータ漏洩/侵害に直結しないようにしましょう。

攻撃	資産	件数
ハッキング - 窃取した認証情報の使用	サーバー - メール	51
不正使用/悪用 - 特権の悪用	サーバー - データベース	51
ソーシャル - フィッシング	サーバー - メール	48
エラー - 誤送信	メディア - 書類	30
物理的な攻撃 - 窃盗	メディア - 書類	14
エラー - 誤公開	サーバー - Webアプリケーション	13
エラー - 誤廃棄	メディア - 書類	12
エラー - 紛失	メディア - 書類	12
エラー - 誤送信	ユーザーデバイス - デスクトップ	12
ハッキング - 窃取した認証情報の使用	人 - エンドユーザー	7

表5
攻撃と資産の種類の上位組み合わせ（n= 304）

情報産業

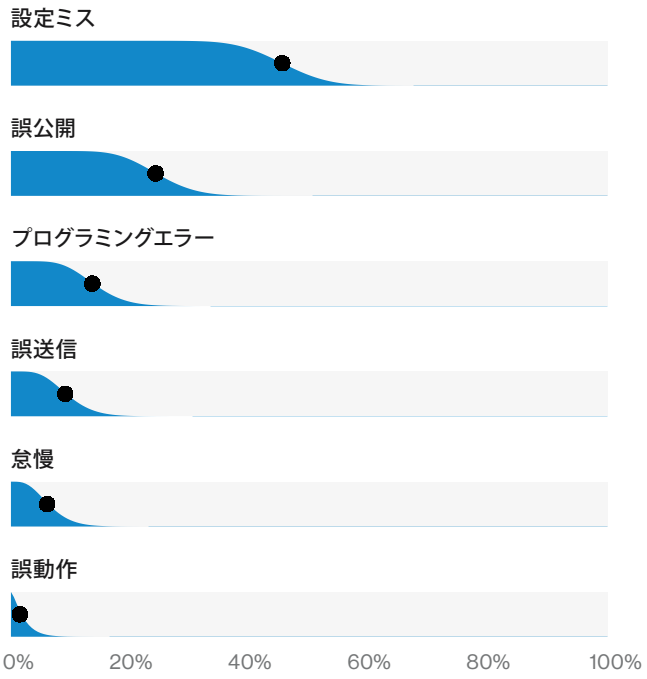
Webアプリケーションが、可用性攻撃のターゲットになっていると同時に、クラウドベースの組織内メールアカウントへのアクセスを目的としても悪用されています。

頻度	インシデント1,094件、確認されたデータの暴露155件
上位3つのパターン	多種多様なヒューマンエラー、Webアプリケーション攻撃、サイバー諜報活動が、情報産業における漏洩/侵害の83%を占めている
攻撃者	外部（56%）、内部（44%）、パートナー（2%）（漏洩/侵害））
攻撃者の動機	金銭目的（67%）、スパイ活動（29%）（漏洩/侵害）
侵害されたデータ	個人情報（47%）、認証情報（34%）、機密情報（22%）（漏洩/侵害）

情報社会

情報産業は、情報の作成、送信および保存に関係する組織を満載したトラックのようなものです。被害者の幅広さを考えると、攻撃はあらゆる場所で行われているのではないかと思われるかもしれませんが、実際にこのカテゴリについて2019年度の報告書から見て取れることは、昨年度の結果と全く同じということです。2018年度と同様、この業界におけるインシデントのほとんどがDoS攻撃（63%）です。事実、この業界はテレビと映画の両方をカバーしていると言えます。というのも、インシデントの観点から見ると、いろいろな意味で昨年のプログラミングの再放送のようなものだからです。

確認されたデータ開示に関して言うと、上位3パターンのうち2つが（順番こそ異なりますが）昨年度と同じで、もうひとつは新たに発生したパターンです。頻度の高い順に、パターンは各種エラー（42%）、Webアプリケーション攻撃（29%）そしてサイバー諜報活動（13%）です。最も一般的なエラーを以下の表に示します。



図表52 情報産業における漏洩/侵害のエラーの種類（n=66）

攻撃	資産	件数
エラー - 設定ミス	サーバー - データベース	24
ソーシャル - フィッシング	人 - 不明	22
ハッキング - 不明	サーバー - Webアプリケーション	19
マルウェア - C2	ユーザーデバイス - デスクトップ	16
ソーシャル - フィッシング	ユーザーデバイス - デスクトップ	16
マルウェア - バックドア	人 - 不明	15
マルウェア - バックドア	ユーザーデバイス - デスクトップ	15
マルウェア - C2	人 - 不明	15
エラー - 誤公開	サーバー - Webアプリケーション	14
ハッキング - 窃取した認証情報の使用	人 - 不明	14

表6
よく見られる攻撃と資産の種類の組み合わせ（n= 155）

笑えないミス

完璧な人などいませんが、システム管理者ほどそれを露呈する場を与えられる人はいないでしょう。図表52はヒューマンエラーがどのようにして検出されるかを説明しています。弊社のデータが示しているように、設定ミス（45%）および誤公開（24%）はデータ開示の発生を許してしまった一般的なヒューマンエラーです。表6の攻撃と資産の関係を見ると、エラー関連のデータ漏洩/侵害の36%（67件中24件）にデータベース、多くの場合クラウドストレージの設定ミスが関与しています。これは良い傾向ではありません。明らかにこれらのデータベースには大量の情報が保存されており、そこに穴が開いていると、貴社が気付くまでにすべて漏れてしまっている可能性があります。これらのサーバーは多くの場合、非公開データが保存されたままの状態で、一般に公開するために急いでオンラインに移行され、設定されています。Webアプリケーション上での誤公開は、意図したよりもはるかに広範な閲覧者に対して同様のデータ曝露をもたらしています。ちなみに、プログラミングエラーはWebサーバー上および複数のデータベース上で犯されたものだということを申し添えておきましょう。

Webアプリで読めるのは文学だけではない

貴社のIT部門が前述したような重大なエラーを犯さなかったとしても、安心はできません。データが盗まれるリスクは他にもたくさんあります。犯罪者は好んで出来立ての新しいWebアプリケーションを攻撃する傾向があります。盗んだ認証情報の違法利用（および再利用）は、業界を問わずよく見られるWebアプリケーションに対するハッキング行為のひとつです。マルウェア攻撃で盗まれるさまざまなアプリケーションデータは、一般的に電子小売業者が持っているデータですが、盗まれるアプリケーションデータはユーザーが入力した決済情報です。あまり一般的ではないですが、実際の物理的商品ではなく、コンテンツを販売するインターネットポータルや会員専用サイトは情報部門に分類されます。コンテンツの購入に使用されたペイメントカードは、オンラインで靴を買うのに使われたカードと同じ価値があるということです。

サイバー諜報活動によるフィッシング

情報産業の3つ目のデータ漏洩/侵害パターンは、サイバー諜報活動です。驚くべきことに、外部攻撃者のうち36%がさまざまな国家に関連したスパイであり、これは統計的に組織的犯罪と等しい数字です。これまでに何度も指摘してきた通り、ほとんどのサイバー諜報活動による攻撃はフィッシングキャンペーンの成功から始まりますが、情報産業におけるソーシャル攻撃の84%をフィッシングメールが占めている理由がこれでいくらか説明できます。

イングランドの哲学者フランシス・ベーコンの有名な言葉に「知識は力なり」というものがあります。これを2019年に応用するならば、「情報を得てコントロールすることは力なり」となるでしょうか。情報を所有し配布する組織がそのような攻撃の標的になっていることは当然と言えるでしょう。

考慮すべきこと：

資産のアシスタント
故意のWeb攻撃かヒューマンエラーによるものかにかかわらず、データベースとWebアプリケーションサーバーはいずれも、特にこの業界において侵害を受けることの多い資産です。「チェックリスト」を使ったセキュリティについて不満を言う人が多い一方で、クラウドサーバーへの移行と機密データのWebサイトへの公開に関する標準的な手順（導入および遵守されている場合）は、ヒューマンエラーやケアレスミスの緩和に大いに役立つでしょう。

パケットをそぎ落とす
本セクションではデータ漏洩/侵害に注目しましたが、DoS攻撃のインシデント発生率を鑑みると、DDoS攻撃に対する防御対策は情報機関にとって欠かすことのできないコントロールです。トラフィックの急増に備えた継続的な監視とキャパシティプランニングで、悪意のない中断から組織を守りましょう。

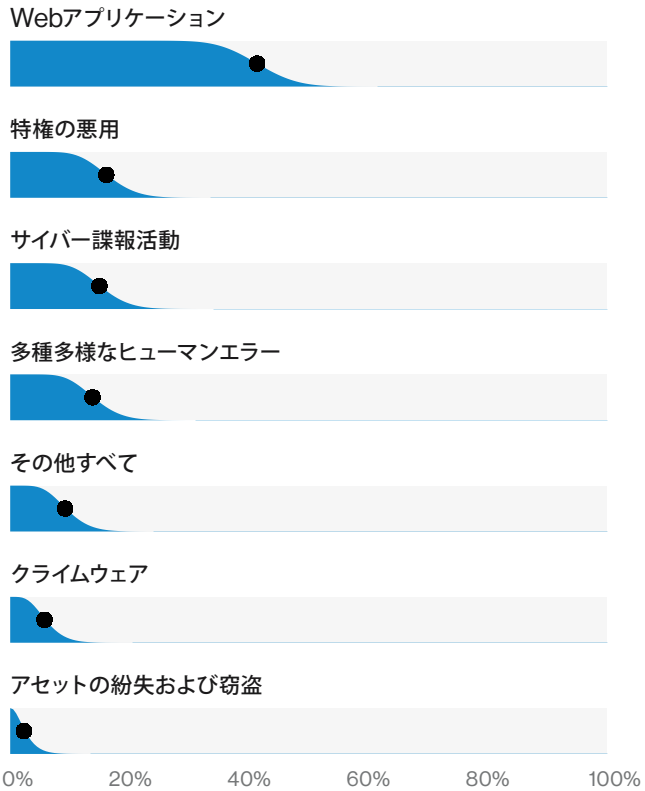
何度も強調しますが…
「知識は力なり」。国家関連組織による攻撃の増加は、弊社が注目し続けるデータポイントです。これは単なる急増であってトレンドを示したものではない可能性は大いにありますが、情報機関が持っているデータは攻撃者にとって魅力的であり、動機も1年で消滅しそうにはありません。これらの攻撃は多くの場合、「不審な」性質を持っており、ワークステーションの侵害に始まり、そこからどんどんエスカレートしていきます。

製造業

製造業においては、金銭目的の漏洩/侵害が過去2年間で増加していますが、スパイ活動も依然として強力な動機となっています。大部分の漏洩/侵害に、フィッシングや窃取された認証情報の使用が関与しています。

頻度	インシデント352件、確認されたデータの暴露87件
上位3つのパターン	Webアプリケーション攻撃、特権の悪用、サイバー諜報活動が、漏洩/侵害の71%を占めている
攻撃者	外部（75%）、内部（30%）、複数の関係者（6%）、パートナー（1%）（漏洩/侵害）
攻撃者の動機	金銭目的（68%）、スパイ活動（27%）、怨恨（3%）、愉快犯（2%）（漏洩/侵害）
侵害されたデータ	認証情報（49%）、内部情報（41%）、機密情報（36%）（漏洩/侵害）

より可能性の高い説明は、通常、サイバー諜報活動に関するデータを提供する弊社のパートナーの一部が、今年度は参加できなかったか、単にその他の種類の調査に取り掛かっていたせいでしょう。そのために、これらの結果にバイアスが生じた可能性があります。つまり、実際のサイバー諜報活動の割合はもっと高かったということです。1つのケースの相対的割合が下がると、結果的にその他のケースの割合が上がったように見えるのです。



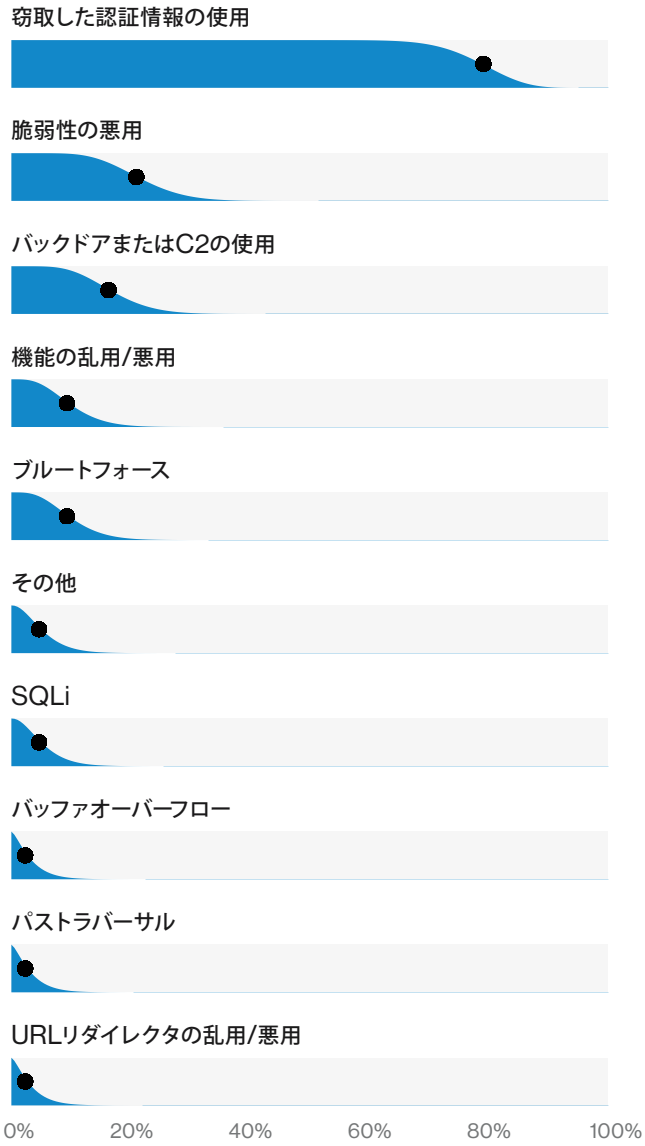
図表53 製造業における漏洩/侵害のパターン (n=87)

金銭的動機

製造業におけるデータ漏洩/侵害の主な理由として、金銭的動機による攻撃の割合が2年連続でサイバー諜報活動の割合を上回っています。そして今年は、その差がより顕著（40%差）になっています。金銭は圧倒的多数の攻撃の理由であるため、これが他のほとんどの業界についても言えることであれば、ここで取り上げるまでもないのですが、製造業は過去数年間にわたって他の業界よりもスパイ関連のデータ漏洩/侵害を多く経験してきました。この結果から、私たちは有名な2人のスパイ、ジェームス・ボンドとイーサン・ハント[15]が遂にそれぞれの敵を完全に打ち負かしたと結論付けるべきでしょうか。そして有名なコカ・コーラのコマーシャルのように世界中の人たちと喜びを分かち合うべきでしょうか？答えはおそらくNoです。

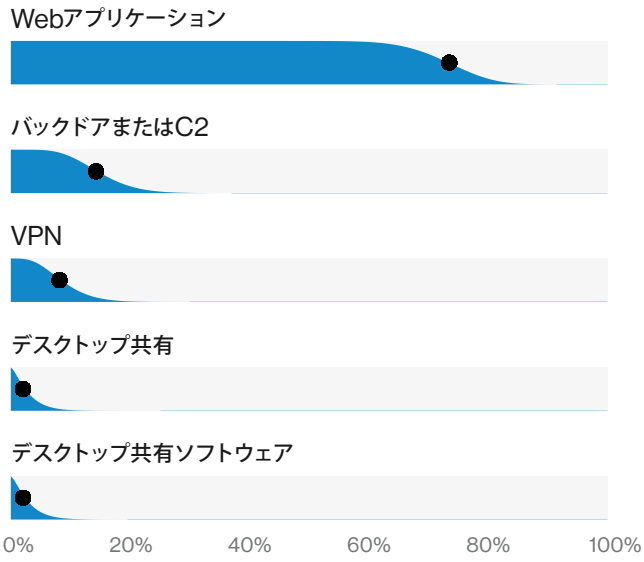
[15] 年配読者の皆様は、ご希望に応じてポップカルチャーからの引用をスパイ大作戦のローリン・ハンドに置き換えてください。

Webアプリケーション攻撃について言うと、この業界も他の業界と同じくWebメールの認証情報の窃取に対処する負担を抱えています。Webアプリケーションを介したデータ漏洩/侵害の大部分においても、メールサーバーが影響を受けた資産として挙がっています。



図表54 製造業の漏洩/侵害におけるハッキングの種類 (n=43)

データ漏洩/侵害全体から見ても、盗まれた認証情報とWebアプリケーションの利用は、最も一般的なハッキングの行為および経路でした（図表54および55を参照）。



図表55 製造業の漏洩/侵害におけるハッキング経路 (n=49)

秘密と真実

サイバー諜報活動のパターンは、過去のの報告書ほどは顕著ではないものの、依然として製造業が防御すべきと弊社が推奨する攻撃タイプです。ユーザーにリモートアクセスツールをインストールするよう説得し、被害者から競合に関する重要情報を窃取するための足掛かりをつくり、それを実行に移すというフィッシング攻撃の典型的な利用方法は変わっていません。

前述の金銭的動機による攻撃の増加と足並みをそろえるように、加害者が明らかになっている場合、たいていが組織犯行グループによる犯行です。データの種類に関しては、この業界で顕著に見られる4種類のデータタイプがあります。Webメール攻撃で盗まれた認証情報（49%）と内部情報（41%）– 具体的なデータタイプが不明の場合、侵害を受けた組織のメールの分類には「内部情報」が使用されています。機密情報（36%）- スパイ目的の動機が減少したことに比例して、上位だった前回よりも順位が下がりました。4番目は個人情報（25%）- 従業員の源泉徴収票（W2）の情報やなりすまし詐欺に利用され得るその他の情報を含むデータタイプです。

考慮すべきこと：

単要素よりも多要素認証のほうが安全
対応しているすべてのシステムに多要素認証を導入することをお勧めします。また、パスワードの再利用をやめるよう促しましょう。これらの措置は、組織全体で認証情報窃取の影響を緩和するのに間違いなく役立ちます。

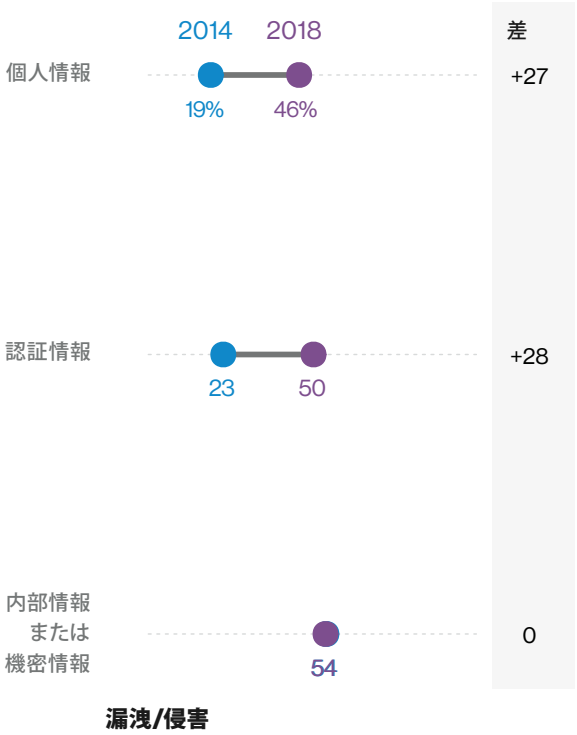
セキュリティにもリサイクルを
動機の種類に関わらず、この業界におけるデータ漏洩/侵害の多くはフィッシングまたはなりすましによる攻撃から始まっています。従業員にセキュリティに関する研修の機会を頻繁に与えることで、こうした攻撃の罠にかかる可能性を減らすことができます。

常に安全装置の着用を義務付ける
不都合でない限り、工事現場の作業員のように常に安全対策を心がけましょう。スパイ目的でのデータ漏洩/侵害において、マルウェアの使用が広がっているため、そうした脅威の検出と阻止に役立つ最新のソリューションを配備し維持することが推奨されます。

専門、技術、科学サービス

クラウドベースのメールアカウントに関連するフィッシングや認証情報の窃取が増加しており、顕著な攻撃タイプになっています。

頻度	インシデント670件、確認されたデータの暴露157件
上位3つのパターン	専門サービス業界内では、Webアプリケーション攻撃、その他すべて、多種多様なヒューマンエラーが、漏洩/侵害の81%を占めている
攻撃者	外部（77%）、内部（21%）、パートナー（5%）、複数の関係者（3%）（漏洩/侵害）
攻撃者の動機	金銭目的（88%）、スパイ活動（14%）、自己都合（2%）（漏洩/侵害）
侵害されたデータ	認証情報（50%）、内部情報（50%）、個人情報（46%）（漏洩/侵害）

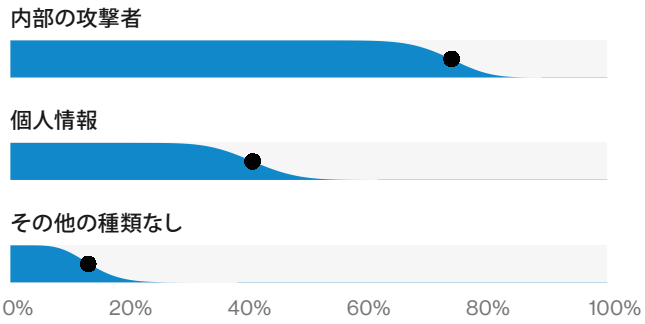


図表56 専門サービスの漏洩/侵害によく見られるデータの種類の経時的変化 n=105（2014年）、n=137（2018年）

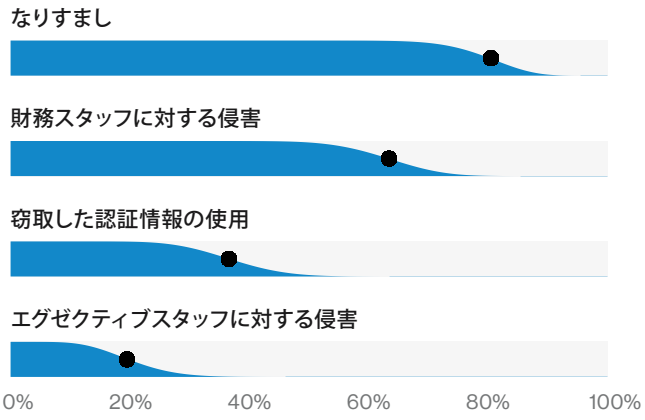
幅広いサービス、標的を絞った脅威

専門サービスは幅広いカテゴリであり、NAICS（North American Industry Classification System：北米産業分類システム）基準でも法律事務所や広告代理店、エンジニアリング会社、設計会社など多岐にわたる職業が含まれています。まずは157種の専門サービスにおけるデータ漏洩/侵害で喪失したデータをまとめた図表56を見てみましょう。これらのケースで最も被害に遭っているデータタイプのイメージが浮かび上がります。

個人情報および認証情報の漏洩/侵害の全体的な増加が認められています。今日では、その多くが複数のデータタイプを同時に侵害するデータ漏洩/侵害から生じています。多くの場合、認証情報はその他の行為への扉を開く鍵となっています。図表57は、ほとんどの場合、内部情報や個人情報の侵害へ向かっていることを示しています。このことから、盗んだ認証情報を使ってWebメールにログインすることにより、ユーザーの受信トレイにアクセスしていることが分かります。



図表57 専門サービスの認証情報の漏洩/侵害におけるその他のデータの種類 (n=69)



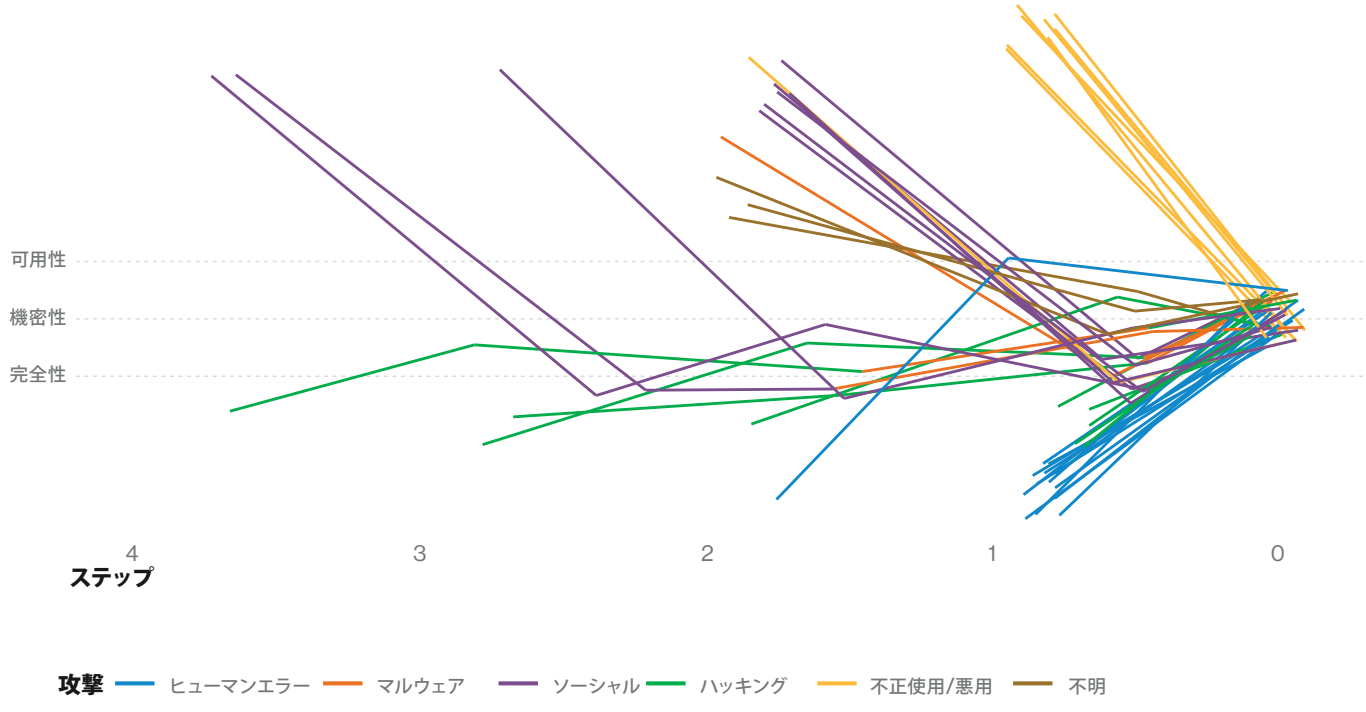
図表58 不正取引インシデントにおける特定の区分 (n=41)

言葉巧みな上司の指示に注意

窃取した認証情報を使ってメールを侵害し、上司などになりすまして企業から金銭をだまし取るビジネスメール詐欺（BEC: Business Email Compromise）が増加しています。図表58は、BECが専門サービス業界にとって問題であることを示す十分な証拠を示しています。不正取引に関わるインデントにおいては、財務スタッフが侵害に遭うケースが多いですが、エグゼクティブもインシデント全体の20%の割合で侵害に遭っており、専門サービスのデータ漏洩/侵害において侵害を受けた資産としては、平均的な業界と比較して6倍の確率になっています。この手口を考えた攻撃者にはお見事というほかありません。ある時、誰かが「回りくどいハッキングなど飛ばして、直接金を要求してみよう」と思いついたに違いありません。

不正への道のり

後に、図表59は攻撃の種類とそれに要したステップを示したもので、不正使用/悪用とヒューマンエラーによるデータ漏洩/侵害はワンステップである一方で、ソーシャルおよびハッキングによる漏洩/侵害にはわずかに時間が長くかかることもここから見て取れます。この結果はどの企業にとっても身近で優れた教訓となるでしょう。



図表59 専門サービスにおけるインシデントの機密性の攻撃チェーン (n=90) 不正使用/悪用やヒューマンエラーは短い攻撃パスである一方で、ソーシャルおよびハッキングは長期間かかる傾向があります。

考慮すべきこと：

1ほど寂しい数字はない
うるさく繰り返すつもりはありませんが、静的認証は非常に重要です。パスワードマネージャーと二要素認証は、錠前のピンのようなものです。ドアがある場所はすべて忘れずに監査しましょう。ほとんどの入口に金庫のようなダイヤル錠をかけていても、裏口が網戸一枚では何の役にも立ちません。

知人を装ったメールに注意
認証情報を盗み出す一番の方法をご存知ですか？ソーシャル攻撃です。少なくとも私たちはその出所を知っています。リンクや実行ファイル（Officeのマクロ有効文書など）を含んだメールには注意しましょう。部門内で、フィッシングやなりすましの疑いがあるものについて、報告方法を周知してください。

過ちは人の常
スタッフを加害者にさせないために、個人情報にアクセスするプロセスを監視し、多重のコントロールを追加して、1つのミスがデータ漏洩/侵害に直結しないようにしましょう。

公共機関

公共部門では、サイバー諜報活動が蔓延しており、外部攻撃者による漏洩/侵害の79%は、国家関連組織が関与したものです。特権の悪用と内部者によるエラーが漏洩/侵害全体の30%を占めています。

頻度	インシデント23,399件、確認されたデータの暴露330件
上位3つのパターン	サイバー諜報活動、多種多様なヒューマンエラー、特権の悪用が、漏洩/侵害の72%を占めている
攻撃者	外部（75%）、内部（30%）、パートナー（1%）、複数の関係者（6%）（漏洩/侵害）
攻撃者の動機	スパイ活動（66%）、金銭目的（29%）、その他（2%）（漏洩/侵害）
侵害されたデータ	内部情報（68%）、個人情報（22%）、認証情報（12%）（漏洩/侵害）

この部門の膨大なインシデント件数を見れば、政府機関のインシデント対応担当者はマントとタイツ姿のスーパーヒーローか、ストレスに犯され辛うじて崖っぷちにぶら下がっているかのどちらかに違いないと思われるでしょう。実際、そうかもしれませんが、この業界は非常に視認性が高い業界です。その理由の一部には、（少なくとも米国内の）メンバーに弊社のデータシェアリングパートナーであるUS-CERTにインシデントの報告を義務付ける規制要件が挙げられます。それよりも興味深いことは、漏洩/侵害件数は昨年度の報告書と同様であるにも関わらず、漏洩/侵害の割合に変化が見られたことです。

サイバースパイの急増

昨年度の報告書では、この業界におけるサイバー諜報活動のパターンは最も目立っていたものの、サイバー諜報活動のパターンにおける漏洩/侵害件数は昨年度の件数の168%に上っています。図表60は昨年度からの割合の推移を示しています。表7に示す、よく見られる攻撃と資産の組み合わせは、「穴を見つけて悪意のある添付文書を送り、足掛かりを得る」という簡単なステップであることを物語っています。人的資源[16]とワークステーションが影響を受けた資産であるデータ漏洩/侵害には、5つの攻撃パターンがあります。馴染みのある手口であるフィッシングが最も多く、次にバックドアまたはC2、そして新たに取得したチャネルを使ったネットワークへの侵入が続きます。確かに、詐欺やデバイスの初回侵害の裏で何が起きているかについてはあまりデータがありません。マルウェアの一種であるキーロガーの侵入は、さらなる認証情報の窃取か再利用が次に行われる可能性が高いという指標です。

図表60 公共部門におけるデータ漏洩/侵害の経時的パターン
n=305（2017年）、n=330（2018年）

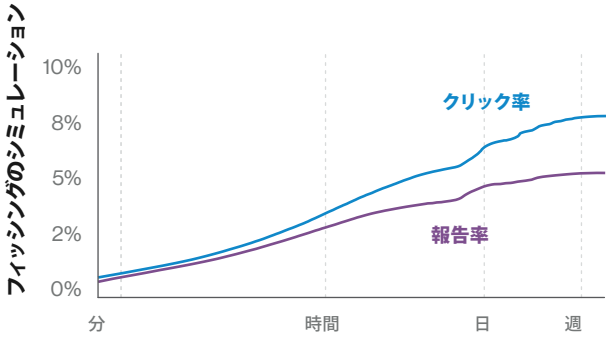
[16] 人 – 不明は、標的に関連する組織内の役割が知られていないフィッシングの件数が多かったため除外していません。

攻撃	資産	件数
ソーシャル - フィッシング	人 - 不明	155
ソーシャル - フィッシング	ユーザーデバイス - デスクトップ	139
マルウェア - バックドア	人 - 不明	130
マルウェア - バックドア	ユーザーデバイス - デスクトップ	129
ハッキング - バックドアまたはC2の使用	人 - 不明	119
ハッキング - バックドアまたはC2の使用	ユーザーデバイス - デスクトップ	119
マルウェア - C2	ユーザーデバイス - デスクトップ	100
マルウェア - C2	人 - 不明	99
マルウェア - スパイウェア/キーロガー	ユーザーデバイス - デスクトップ	82
マルウェア - スパイウェア/キーロガー	人 - 不明	81

表7
公共部門におけるデータ漏洩/侵害によく見られる攻撃と資産の組み合わせ（n=330）

我クリックする、故に我あり

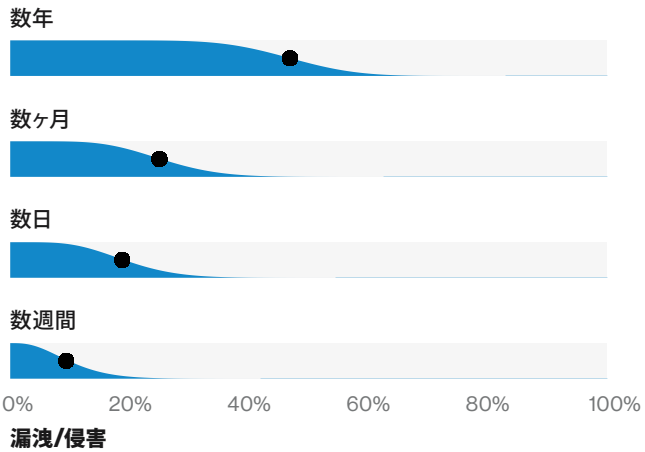
悪意のあるメールの問題を少し明確にしてきたので、ここで今年弊社が入手したセキュリティ認識度に関するトレーニングのデータを詳しく見ていきたいと思います。図表61はこの部門の従業員がフィッシングメールをクリックまたは報告するまでの時間を示しています。トレーニングの前半ではユーザーによるクリックと報告の割合は同様ですが、最初の1時間を過ぎた頃から報告の割合が下がり、クリックのほうが多くなります。ベストな結果ではありませんが、これは認可を受けた実際には悪意のないメールだったため、最初の報告を受けた後、報告者を讃える以外には何事も起きませんでした。実際の攻撃に備えて、文書化された了解済みおよび検証済みのインシデント対応プランを用意しておくことで、最初の1時間の間に封じ込めのプロセスを開始し、攻撃をすばやく特定してその有効性と影響を制限することができます。これにより、受信トレイを整理していないユーザーが、数日後に悪意のあるメッセージを開くといった可能性も制限されるでしょう。



図表61 公共部門のフィッシングのシミュレーションにおけるクリック率と報告率の経時的変化

政治機構の発見は遅れがち

データ漏洩/侵害のタイムラインの指標を導き出すのに十分な情報がある場合、公共部門における漏洩/侵害は発見まで数ヶ月から数年を要していることをデータが示しています。公共部門のデータ漏洩/侵害は何年も発見されない可能性が2.5倍以上高いのです。諜報活動関連のデータ漏洩/侵害は通常、外部の不正検出に頼らない分、発見までに時間を要しますが、この種の漏洩/侵害のタイムラインデータは入手できていません。特権の悪用は、データ漏洩/侵害の中でも、数ヶ月以上にわたり発見されなかった最も一般的なパターンです。



図表62 公共部門における漏洩/侵害の発見までの時間 (n=32)

考慮すべきこと：

人的要因を理解する
フィッシングの標的としての観点からだけではなく、人的要因を理解しましょう。データの誤送信や誤公開といった形のエラーが再び増加しています。内部攻撃者による悪用も引き続き懸念されるため、定期的にユーザーの特権を評価する取り組みを行うようにしましょう。 既存の特権で不正にまたは悪意を持って行動する従業員が及ぼす損害の額を制限しましょう。

裏口（バックドア）を見張る
バックドアまたはC2マルウェアがインストールされた徴候と考えられる、外部へ出て行く怪しいトラフィックを監視するコントロールが配備されていることを確認しましょう。

マルウェアの難題
無数のエンドポイントからなる巨大なコミュニティを抱える大規模な政府機関は、広範をカバーする最新のマルウェア対策を確実に実装するという難しい課題に直面しています。一方で、小規模な組織は、デスクトップ用ウイルス対策以外に追加のマルウェア対策を装備するための予算が不足している可能性があります。デスクトップ用セキュリティソフトについてよく理解し、具体的にどのような課題があるかを知りましょう。

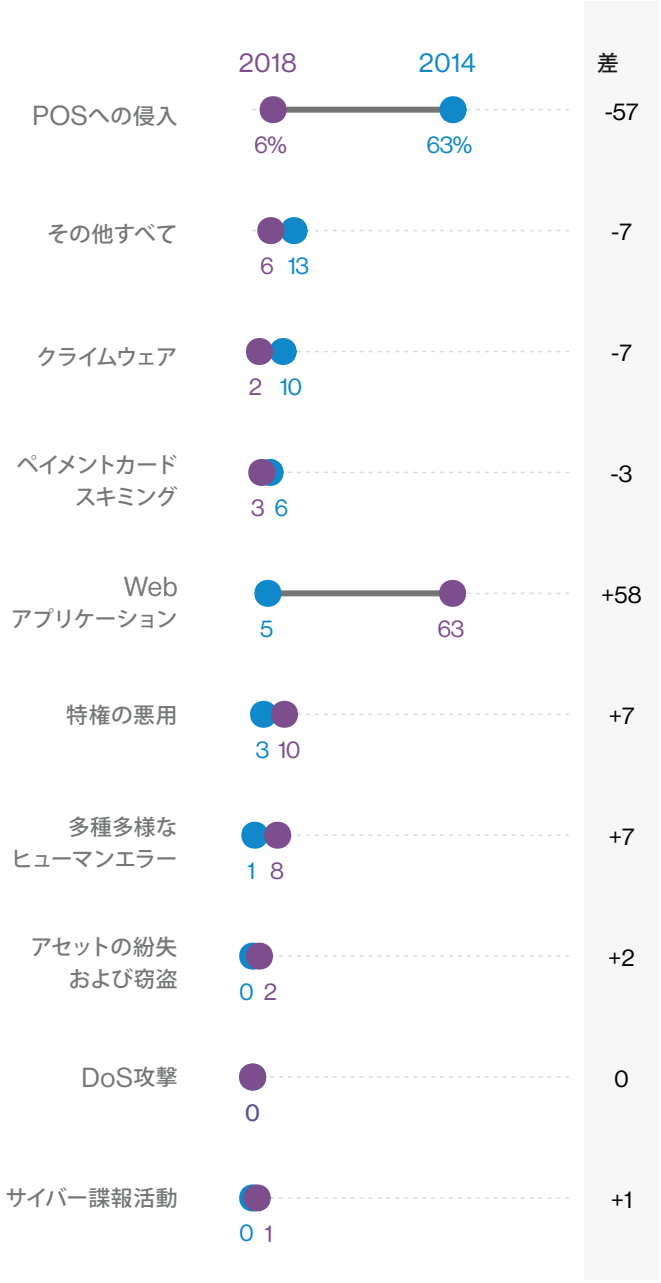
小売業

POSの侵害やガソリンスタンドのスキマーに伴うカードの漏洩/侵害は、引き続き減少しています。Eコマースの決済アプリケーションに対する攻撃は、この業界をターゲットにしている攻撃者の金銭的動機を満たしています。

頻度	インシデント234件、確認されたデータの暴露139件
上位3つのパターン	Webアプリケーション攻撃、特権の悪用、多種多様なヒューマンエラーが、漏洩/侵害の81%を占めている
攻撃者	外部（81%）、内部（19%）（漏洩/侵害）
攻撃者の動機	金銭目的（97%）、愉快犯（2%）、スパイ活動（2%）（漏洩/侵害）
侵害されたデータ	決済情報（64%）、認証情報（20%）、個人情報（16%）（漏洩/侵害）

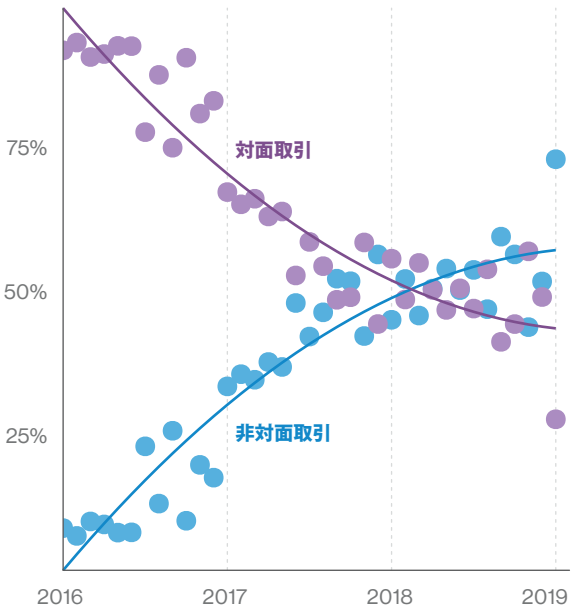
脆弱なPOSは過去の話

DBIRのタイムマシンに乗って、4年前に遡ってみましょう。小売業界のインシデント分類パターンと上位パターンがPOSへの侵入であることを特集した2年目のことでした。また、POS環境のリモート侵害と、それに伴うあらゆるマルウェアとペイメントカード情報の引き出しについても取り上げました。今年のデータセット（図表63）に戻ると、時代は変わっていることが分かります。



図表63 小売業界におけるデータ漏洩/侵害パターンの経時的変化
n=145（2014年）、n=139（2018年）

基本的に、Webアプリケーション攻撃はPOSへの侵入の義務を終えて、タイムカードを押して退社したと考えて良いでしょう。このことは小売業界だけに見られる現象ではありません – 図表64は弊社のパートナーである米国サイバー鑑識・訓練協定（NCFTA）が作成した図表ですが、被害者の業界に関係なく、同組織が追跡した対面取引と非対面取引の不正を比較したものです。



図表64 対面取引と非対面取引の不正の比較

上記の表の推移は確かに、POS侵害の減少と、比較的程度は少ないですが、ペイメントカードのスキミングの減少を裏付けています。ガソリンスタンドの給油ポンプ端末での支払いも、小売業界に分類されます。弊社では、EMV対応端末が私たちの間に潜んでいるサイバー犯罪者にとっての対面不正取引の価値を低下させたものと、慎重ながら楽観しています。それでも残念なことに、犯罪者たちが金銭の搾取をやめて自立したコミュニティに引越し、質素な暮らしをするようにはならないでしょう。

1つの扉が閉まっても、別の扉をこじ開ける

EコマースWebアプリケーションに対する攻撃は再び増加しています。これは左の図表64と、ページを遡って「結果と分析」のセクションの図表26にも表れています。決済アプリケーションに対する攻撃にどのような戦術が使われたかについてもっと詳しく調べるために、攻撃と影響を受けた資産の組み合わせに話を戻しましょう。

一般的な手口は、下の表8から読み取ることができます。攻撃者はWebアプリケーションを侵害して、決済アプリケーションにコードをインストールし、顧客が買い物を終えて決済を行う際に、コードを介して顧客のペイメントカード情報を窃取します。データ漏洩/侵害の中には、スパイウェア/キーロガーに分類されるform-grabberと呼ばれるマルウェアが見つかっていますが、これはユーザーの入力情報を窃取する別の手口です。

攻撃	資産	件数
マルウェア - アプリケーションデータの窃取	サーバー - Webアプリケーション	49
マルウェア - スパイウェア/キーロガー	サーバー - Webアプリケーション	39
ハッキング - 脆弱性の悪用	サーバー - Webアプリケーション	15
ハッキング - RFI	サーバー - Webアプリケーション	11
マルウェア - RAMスクレーパー	サーバー - POSサーバー	8
マルウェア - RAMスクレーパー	ユーザーデバイス - POS端末	7
ハッキング - 窃取した認証情報の使用	サーバー - データベース	6
ハッキング - 窃取した認証情報の使用	サーバー - メール	6
ハッキング - 窃取した認証情報の使用	サーバー - Webアプリケーション	6
不正使用/悪用 - 特権の悪用	サーバー - データベース	5

表8
小売業界における漏洩/侵害によく見られる攻撃と資産の組み合わせ（n= 139）

それ以外は「ペイメントカードデータを収集した悪意のあるコード」のようなステートメントを除いて、得られたのは限られた情報のみでした。それらのインスタンスでは、より一般的な機能のキャプチャアプリのデータが使用されていました。実際には、これら2つの組み合わせに違いはほとんどまたは全くないものと考えられます。Webアプリケーションがどのようにして侵害されたかについても情報がやや不足しています。RFI（Remote File Include:外部にある悪意のあるコードを読み込ませる手法）のような具体的な手法が検出された場合は、その情報を収集しています。多くの場合、Webの脆弱性が悪用されたのであれば、（VERISの最新版に新たに登場した）「脆弱性の悪用」の一種とするのが一般的な表記だと思われます。これまでに分かっている事実を考慮に入れて、論理的に導き出すと、この一般的な事象連鎖は次のようになるでしょう：Webアプリケーションの脆弱性を探す > それを悪用して侵入する > マルウェアを投下する > ペイメントカードデータを収集する > 利益を得る。以前のデータ漏洩/侵害時の初回ハッキングからマルウェア感染までの間に、バックドアの一種であるWebShellが設置されているケースが認められています。そうした行為は今回のデータセットにおいて目立った件数は記録されていませんが、検出作業を行う際に注意するべき新たなブレッドクラム（パンくず）のひとつです。要するに、脆弱性の高いインターネット経由のEコマースアプリケーションは、効果的かつ広範囲に広がり得る自動攻撃への経路を与えてしまいます。そして、この種の攻撃に特化して、容易に利益を得ている犯行グループが存在するのです。

考慮すべきこと：

完全性が完全を生む
Webアプリケーションの侵害はもはや保存データに対する攻撃にとどまりません。コードを挿入するインジェクション攻撃では、顧客がWebフォームに入力すると同時に顧客データが収集されます。ファイル完全性ソフトウェアを広範囲に実装することは、現実的な対策ではないかもしれませんが、マルウェア対策に加えて決済サイトにこれを導入することは検討すべきです。これはもちろん、OSにパッチを適用し、決済アプリケーションの暗号化を行ったうえで追加しましょう。

実店舗に鉄壁の防御を
犯罪者に貴社のPOS端末を破滅へと追い込ませないように、これからも新たなテクノロジーを導入して保護を強化しましょう。EMVやモバイルウォレットなど、クレジットカード番号（PAN）ではなく1回限りの取引コードを使用する手法を推奨します。

標的はペイメントカード業界だけではない
犯罪者コミュニティにとって有益なデータタイプは、ペイメントカードだけではありません。特典プログラムも、「ポイント」交換や顧客基盤の個人情報窃取に利用できるため標的になり得ます。

最後に

本年次報告書第12版のご報告内容は以上となります。DBIRをお酒に例えるならば、1本100米ドルほどの上質なスコッチウイスキーだと自負しておりますが、本書は無料でお届けしています。上質なウイスキーの後味同様に、本書を読み終えた後に皆様が行う意思決定の内容も大きく違ってくるでしょう[17]。本書をお読みになる皆様には、楽しみながら情報を得ていただければ幸いです。

本書の作成にあたったチームに代わりまして、読者の皆様にご支援と励ましを賜りましたことを心より感謝申し上げます。

本書は情報セキュリティ担当者の皆様をはじめ、業界全体にとって有益であるものと信じております。今回も皆様に本書をお届けする機会をいただけたことをありがたく思います。本書の作成にご協力をいただき、お時間や労力、知見、そして何より、貴重なデータをご提供いただきました皆様に、深く感謝を申し上げます。本書の作成は決して簡単な作業ではなく、皆様の寛大なご支援がなければ成し得なかったことです。来年も次号をお届けできることを楽しみにしております。それまでの間、皆様方には本号をお役立ていただき、万全のセキュリティで無事に過ごされますことをお祈りいたします。それでは、巻末の付録に入る前に、2018年にVTRACが公表したセキュリティ関連の注目の出来事を振り返りながら、本書を締めくくりたいと思います。

[17] 弊社にはそれを裏付ける十分なデータがないため、お客様の判断が大きく異なるとは断言できません。確かに、私たちの推測ですが、内部の研究は継続中です。

年間総括

1月

今年に入って2日目に、ベライゾンの脅威リサーチアドバイザリーセンター（Threat Research Advisory Center：VTRAC）は、最新のマイクロプロセッサに「メルトダウン」と「スペクター」という新たな情報開示脆弱性が見つかったことを知りました。これらの脆弱性は、基盤となるCPUの設計に起因するものでした。パッチの配布は2018年を通して繰り返されました。2018年に発生したメルトダウンとスペクターの攻撃の成功例については報告を受けていません。1月第1週には、韓国の平昌で開催された2018年冬季オリンピックを狙ったマルウェア攻撃について初の報告を受けました。調査ジャーナリストは、インドの国民識別番号のデータベース「Aadhaar」がデータ侵害に遭い、12億人以上ものインド国民が影響を受けたことを伝えました。中南米の銀行を狙った攻撃に関する報告が届き始めました。攻撃者はワイパー型マルウェアを使用して、彼らの行為の証拠を隠滅し、銀行の損失の範囲を小さく見せていたと考えられます。1月26日にランサムウェアGandCrabに関する最初の報告を受けました。

2月

2月には、朝鮮のサイバー攻撃グループAPT37が、Excelスプレッドシートにエクスプロイトを埋め込み、Adobe Flash Playerのゼロデイ攻撃が始まりました。インドのパンジャブ・ナショナル銀行（PNB）は1,160億ルピー（17億7,000万米ドル）の不正送金を報告しました。ロシア中央銀行は「承認されていない業務」が3億3,900万ルーブル（480万ユーロ）の損害をもたらしたことを報告しました。「オリンピックデストロイヤー」と呼ばれるマルウェアが平昌オリンピックの開会式を妨害しましたが、式の中止には至りませんでした。GitHubが適切に設定されていないmemcachedサーバー（分散型メモリキャッシュサーバー）を利用した新種のDoSリフレクション攻撃を受けました。GitHubおよびその他の組織は、迷惑メールによる1.35Tb/sのトラフィックストームに耐えました。

3月

平昌オリンピックの攻撃に関する情報収集は、2月25日の閉会式が終わった後も継続されました。Gold Dragon、HaoBaoおよびHoneybeeのキャンペーンが早くも2017年7月に始動しました。3月にはAPT28、menuPass（別名：APT10）、Patchwork、MuddyWater、OilRig、LazarusおよびCobaltなど、APT攻撃（持続的標的型攻撃）全般に関する情報を収集しました。US-CERTは、米国の重要インフラを攻撃したロシアの攻撃者に関する情報をまとめた15通の文書を公開しました。マレーシア中央銀行は、偽造したSWIFT送金依頼書を利用した攻撃を阻止しました。Drupalプロジェクトは、「Drupalgeddon」と呼称される2014年の脆弱性を彷彿とさせる、リモートより任意のコードを実行可能な脆弱性のパッチをリリースしました。

4月

ロシアの攻撃者によるCisco IOS搭載スイッチの「Smart Install」対応ソフトウェアを標的とした攻撃は、おそらく4月に発生した情報セキュリティ業界における最も注目すべきリスクだったでしょう。VTRACでは、ロシアの攻撃者「Energetic Bear」に関する最新情報を収集しました。Latitude Technologies社に対するサプライチェーン攻撃により、天然ガスパイプライン運営企業4社が顧客とのコンピュータ通信を一時的に停止することを余儀なくされました。Latitudeはエネルギーおよび石油業界に電子データ交換（Electronic Data Interchange：EDI）サービスを供給する企業です。3月に発覚したDrupalの脆弱性は、サイバー犯罪者を確実に惹きつけました。IoT機器を狙うボットネットMiraiの一種がDrupalサーバーの脆弱性を探し、サーバーを侵害してクリプトマイニングソフトウェアをインストールするという攻撃を開始しましたが、この脆弱性は以後「Drupalgeddon2」として知られるようになりました。暗号通貨イーサリアムを保管できるウォレット「MyEtherWallet」から15万米ドル相当のイーサリアムが盗まれたサイバー強盗が発生しましたが、その手口に使われた、インターネットのインフラを狙ったBGPハイジャックのほうがむしろ深刻な問題でした。

5月

Internet Explorerに見つかったゼロデイ攻撃脆弱性「Double Kill」に関する情報が4月末に収集されました。5月には、悪意のあるPDF文書にゼロデイ攻撃脆弱性が新たに2つ（Adobe PDF ReaderとWindowsにそれぞれ1つずつ）見つかり、VTRACはその情報を集めました。MicrosoftとAdobeは5月の「パッチチューズデイ」（月例パッチリリース）に、3つすべての脆弱性に対するパッチをリリースしました。ランサムウェアGandCrab感染の急増は、5月に実施された数回の情報収集の焦点となりました。新たな情報収集によりハッカー集団Cobaltによるフィッシングキャンペーンが、金融部門を標的にしていることが明らかになりました。複数の情報源から、ルーターやネットワークHDD（NAS）機器がマルウェア「VPNFilter」に感染したという情報が寄せられました。ルーターを制御して、ルーターを経由するトラフィックを制御しましょう。

6月

複数の情報源から、北朝鮮の攻撃者がサイバー紛争およびサイバー犯罪の活動に関与したという最新情報が発表されました。AdobeがFlashの新しいゼロデイ攻撃脆弱性パッチをリリースしました。2月のFlashゼロデイ攻撃と同様に、悪意のあるExcelファイルに使用されていましたが、今回の標的は中東でした。CIBC（カナダ帝国商業銀行）の2つの子会社であるBMO（モントリオール銀行）とSimplii Financialで、約9万件の顧客情報が漏洩しました。両行は、攻撃者が顧客情報と引き換えに75万米ドルを要求してきたことで、データ漏洩/侵害があったことを知りました。Lazarusを標的とした攻撃者により、およそ₩350万ウォン（約3,100万米ドル）相当の暗号通貨が、韓国を拠点とする暗号通貨取引所Bithumb（ビッサム）から盗まれました。オーストラリア・コモンウェルス銀行を狙った新たなバンキング型トロイの木馬「DanaBot」が発見されました。

7月

サイバー犯罪集団Magecartが2018年に最初に行った大規模な攻撃は、Ticketmasterの英国支店に対するものでした。ハッカーは同社に機能を提供している外部サプライヤーのInbenta社を侵害。Inbenta社経由でTicketmasterの複数のWebサイトにデジタルスキマーを設置しました。Ticketmasterへの攻撃は、カードデータの大規模な侵害を目的として第三者プロバイダーを狙ったキャンペーンの一環でした。7月のMagecartに関する情報収集には、800以上のWebサイトを侵害した脅威の痕跡情報（Indicator of Compromise：IOC）が含まれていました。悪意のあるモバイルデバイス管理プラットフォームが、13のiPhoneプラットフォームと一部のAndroidおよびWindowsプラットフォームに極度に標的を絞った攻撃に利用されました。 ハッカーグループMoneyTakerが、ロシアのPIR Bankの支店に設置されていた、サポートの切れた古いCiscoルーターを侵害し、同行のネットワークに侵入。PIR Bankは5,800万ルーブル（92万米ドル）の損失を被りました。

8月

暗号通貨を狙った2018年2度目となるBGP（Boundary Gateway Protocol）のハイジャックが発生し、Amazon DNSサーバーから合法的なトラフィックがリダイレクトされました。悪意のあるDNSサーバーによりMyEtherWalletのユーザーがなりすましサイトにリダイレクトされ、認証情報が収集されました。サービスのユーザーは約15万2,000米ドル相当のイーサリアムを失いました。インドのプネーを拠点とするCosmos Bankが、SWIFTおよびATMからの虚偽の送金により1,340万米ドルの被害に遭いました。米司法省がハッカーグループFIN7（別名：Anunak、Carbanak、Carbon Spider）のマネージャー3人を逮捕したと発表しました。情報が示すところによると、2017年3月に発覚したApache Strutsのマルチパーサー「Jakarta」の脆弱性（CVE-2017-9805）に次ぐ新たな脆弱性（CVE-2018-11776）の存在が浮上しました。2017年の脆弱性はEquifax社のデータ漏洩につながりました。北朝鮮と関連のあるマルウェアのコード再利用攻撃に関する詳細な調査により、ほとんどのマルウェア攻撃にLazarus Groupが関与していることが明らかになりました。APT37はそのほんの一部に関与していましたが、より高度で国家戦略的目的を持ったグループであると判断されました。

9月

新たな情報により、MenuPass（別名：APT10）が日本企業を標的としていることが明らかになりました。9月6日、ブリティッシュ・エアウェイズがデータ侵害を受け、顧客データの窃盗に遭ったことを発表しました。その1週間以内に、我々はブリティッシュ・エアウェイズがMagecartによる別の攻撃の被害に遭ったという情報を得ました。情報が示すところによると、過去6ヶ月間に、米国のオンラインショップNeweggを含む7,339のEコマースサイトに、Magecartのペイメントカードスキミングスクリプトが注入されていました。リモートアクセス型トロイの木馬「FlawedAmmyy RAT」のペイロードを送り込むために検出を回避しようとしている、兵器化されたIQY（Excel Web クエリ）添付ファイルが見つかりました。FBIおよびDHSはリモート デスクトップ プロトコル（RDP）に関する警告を発表しました。告の中でRDP接続を悪用するいくつかの脅威が挙げられていました。例えば、ランサムウェアファミリーに分類されるCrysis（Dharma）、CryptonおよびSamSamです。DanaBotがその標的をイタリア、ドイツ、オーストリアに拡大しました。

10月

VTRACは中国の攻撃者がテクノロジーサプライチェーンを侵害したという主張を検証し、有益な情報ではないという判断を下しました。関連するレポートには十分な技術的詳細や確証がなく、正規ではない未確認の情報源に基づいていたためです。US-CERTは、攻撃グループmenuPass（別名：APT10）によるマネージドセキュリティサービス（MSS）プロバイダーに対する攻撃に関する最新の警告を発表しました。複数の情報源から、北朝鮮の攻撃グループが制裁を受けている北朝鮮政府に収入をもたらすことを意図したサイバー犯罪に関与したとの報告がありました。GreyEnergyは、Sandworm、BlackEnergy、Quedagh、Telebotsなどの名で知られるサイバースパイグループの後身であるグループの現在の呼称です。GreyEnergyは、エネルギー部門およびウクライナとポーランドにおけるその他の戦略的標的に対する過去3年間の攻撃に関与したとされています。DanaBotは米国内の金融サービス機関を標的に攻撃を始めました。Magecartは、7,000以上のEコマースサイトで使用されている顧客によるスコアリングプラグインShopper Approvedに対するサプライチェーン攻撃を実行しました。8月と10月に発行された詳しい報告書が示すところによると、Cobaltが熟練および見習いのメンバーからなるグループと、より高度なキャンペーンを手掛ける熟練メンバーのみの第2グループに再編成されました。

11月

Magecartのマルウェアに関する調査に基づく情報が示すところによると、Magecartによる攻撃の実行犯は少なくとも6人いるとされています。2016年後半に成功裏に実行された最初のMagecartによる攻撃と、今年6月に注目を集めたTicketmaster英国支店/Inbenta社を発端とする攻撃は、バンドワゴン効果を生みました。その他の攻撃者が模倣し、Magecartの初期の攻撃者によるTTP（戦術、技術、手順）に改良を加えました。ランサムウェアSamSamによる攻撃は、2人のイラン人ハッカーが600万米ドルの強奪で起訴された後、休止しました。CiscoはCisco セキュリティアプライアンスソフトウェアであるASA（Adaptive Security Appliance Software）およびCisco Firepower Threat Defenseソフトウェアの脆弱性に対する「活発な悪用」を受けて勧告を発表しました。これらの脆弱性は、不正なリモート攻撃者にサービス妨害を引き起こすことを許す恐れのあるものでした。US-CERTは、攻撃者が「環境寄生」戦術に利用している5つのツールに関するアクティビティアラート、AA18-284A「Publicly Available Tools Seen in Cyber Incidents Worldwide（世界のサイバーインシデントにおいて見られる公開ツール）」を発表しました。マリオットは2014～2018年のデータ漏洩/侵害により、同社系列のスターウッドホテルの予約システムから最大で5億人分の個人情報が流出したと発表しました。

12月

VTRACの12月の情報収集は、“Operation Poison Needles” についての情報から始まりました。正体不明の攻撃者がAdobe Flashの3つ目のゼロデイ攻撃脆弱性を悪用し、ロシアの大統領政権下の総合病院を攻撃しました。“Operation Sharpshooter” は原子力、防衛、エネルギーおよび金融企業を標的とした世界的なキャンペーンでした。石油ガス請負業者のSaipem社が、新種のワイパー型マルウェア（データを破壊するマルウェア）Shamoonを使った攻撃を受けました。12月のパッチチューズデイには、FruityArmorのAPT攻撃に悪用されていた最新のWindowsゼロデイ攻撃脆弱性「CVE-2018-8611」を修復するパッチが配布されました。ビットコイン77%急落の影響を一部受けて、サイバー犯罪者はクリプトマイニングを完全に中止はしませんでしたが、代わりにランサムウェアSamSamおよびGandCrabを使って企業や政府機関、大学その他の大規模組織を攻撃しました。犯罪者は、何日にもわたるビジネスの喪失やバックアップからの生産性回復、再イメージングその他のBCP/DR（事業継続/ディザスタリカバリ）対策と引き換えに身代金を支払う可能性の高い、資金の豊富な組織を標的にしました。そして、2018年末にはVTRACはF1レースカーのごとく全速力で敵を追い越し、追いかけながら、常に技術の向上に取り組みました。

付録A：国際的ハッカーに関する調査報告

標的の選び方と戦術、技術、手順に関する知見

— 米国シークレットサービスDeputy Assistant Director、
マイケル・ダンブロージオ氏

過去15年間にわたり、米国シークレットサービスは、重要度の高いサイバー犯罪者を多数特定し、彼らの居所を突き止め、逮捕することに成功しました。これらの人物は、広く報道された最も重要度の高い、公共および民間の業界ネットワークのデータ漏洩/侵害の一部に関与していました。この期間、シークレットサービスのサイバー部門は、世界中の法執行機関と互恵的な提携関係を築いてきましたが、このことはシークレットサービスの調査活動の範囲を従来の限界を大きく超えて拡大することにつながりました。この協力的提携ネットワークのおかげで、シークレットサービスは国外に逃亡した容疑者の引き渡しを受け、米国で起訴することができるようになりました。シークレットサービスは、サイバー犯罪者の居所を問わず、その追跡と逮捕という我々の使命を推進するため、引き続き新たな国際提携関係を構築してまいります。

金銭的動機を持ったサイバー犯罪と闘うという任務の一環として、シークレットサービスは調査活動と併せて教育アウトリーチ（公共福祉）プログラムを行っています。これらの取り組みは、公共および民間部門の組織がさまざまなサイバー犯罪から自衛する能力を強化することを目的としています。シークレットサービスは、犯罪実行中のサイバー犯罪者の活動や、彼らが使用するツールおよび方法論を詳しく分析し、サイバー犯罪者が金融機関その他の標的となり得る機関に与える、進化し続ける脅威をより的確に評価できるよう努めています。シークレットサービスは次にそのレビュー結果を、アウトリーチプログラムを通じて公共および民間パートナーのネットワークと共有しています。

シークレットサービスのサイバー部門は、サイバー犯罪の傾向を最も的確に予知する情報は、サイバー犯罪者自身から得られることが多いことを学びました。そこでシークレットサービスは、逮捕したサイバー犯罪者から詳細な取り調べを行い、彼らから直接得た知識を、侵入および搾取の標的となる特定の対象を選定する際に彼らが使用したさまざまな要素をより詳しく理解するために活用します。シークレットサービスは最近、歴史上最も重大なネットワーク侵入の一部に関与したとされる、高度な技術を持った一握りのサイバー犯罪者に対するそのような取り調べを完了し、これらの人物が標的を選んで犯罪を実行する方法には共通の特徴があることに気づきました。

サイバー犯罪者は、世界中のコンピュータネットワークに存在するヒューマンエラーやITセキュリティへの無頓着さ、技術的不備に付け込んでいます。下記に取り上げるこれらの戦術、技術、手順（TTP）はいずれも、常に最初から成功するとは限らず、簡単に軽減できそうに思えますが、複数のTTPを連携させて使用した場合、サイバー犯罪者はその動機に関わらず、コンピュータネットワークに侵入してアクセスを維持することができるのです。ネットワーク内部に侵入すると、その次の手順は毎回ほぼ同じです。すなわち、継続的にアクセスを確立し、権限を昇格または管理者権限を取得し、忍び足で徘徊してネットワーク全体をマッピングし、開放されているポートを探し、「宝石」の場所を特定して、可能な限り長期間にわたりデータを密かに抽出します。

標的の選定は継続的なプロセスです。サイバー犯罪者も研究しています。これらの取り調べの中で、必ずと言って良いほどハッカーは、同じサイバーセキュリティ関連のブログやオンラインIT出版物、ネットワーク管理者が注視しているであろう脆弱性レポートの名前を挙げ、有益な情報をそこから収集していると供述しました。彼らは脆弱性が明らかになると、わずかな間だけならば、標的となる組織に対してその脆弱性の悪用を試みる時間があるということを知っています。脆弱性が開示されるか、システムアップデートやパッチがリリースされるたびに、ハッカーはそこに機会を見出します。彼らは脆弱性を悪用することが可能か、可能な場合はどこかを学ぶために開示やアップデートの内容を研究し、脆弱性を収益化する最大の機会を探っているのです。ハッカーはまた、脆弱性に関する情報と悪用の技術をハッキングフォーラムで連絡し合っています。標的が定まると、ハッカーは標的となる組織とそのネットワークについて綿密な調査を行います。その際によく使われるのが、無料および市販のインターネットスキャニングツールです。彼らはこれを使って、標的となる会社のネットワークに関するきわめて有用な情報を収集します。

WebサーバーやWebページのハッキングは非常に有効な主要攻撃経路です。というのも、さまざまな悪用の経路があるからです。その中には当該機関のメインWebサイトまたは比較的セキュリティの甘いリンク先Webサイトが含まれ、そこから今度はメインのネットワークに侵入することができます。悪意のあるコードをSQLデータベースに挿入して追加で使用する侵入手法は、Webサイトのどのアクセスポイントにも活用できるため、非常に効果的な攻撃経路です。Webサーバー攻撃経路には他にも、開発やベータテストの実施、あるいは同一または共通のドメインを使用している外部のWebサーバーやデータサーバーがあるために、見落とされたか忘れられたIPアドレスなどがあります。いまだにUnicodeを使用している管理されていないサーバーも、特定の文字を使ってURLをエンコードし、アプケーションフィルタを回避すれば悪用することができます。

その他、従来の効果的な攻撃経路も見逃してはなりません。これらの経路には、ログイン認証情報をピンポイントで狙うスピアフィッシングや、セキュリティの甘いルーターやWebゲートウェイを経由してマルウェアを送り込み、通信する2者間で一方になりすまし、盗聴や改ざんを行う「中間者（Man in the Middle：MITM）」攻撃などがあります。ボットネットは比較的安価なツールで、パラレル戦術に関連してネットワークにデグレードまたはブルートフォースアタック（総当たり攻撃）を仕掛けるのに利用されています。熟練のハッカーはシークレットサービスに対し、海外銀行のネットワークに侵入を試みるその他のハッキングがすべて失敗に終わったとき、共謀した従業員（インサイダー脅威）に金銭を支払うことになったことを認めました。

ネットワークに侵入すると、サイバー犯罪者は調査と偵察を続けます。ハッカーは多くの場合、Webサーバーのデフォルトエラーページを精査します。これらのページには標的となるネットワークシステムに関する情報が詰まっているからです。サイバー犯罪者は収集できる限りのネットワーク情報を集め、仮想マシン（VM）を使って標的となる企業のネットワークを模倣した模擬システムを構築します。これは悪用の手法を試すため、ならびにそのシステム内にどのようなネットワーク防御策が施されているかをよりよく理解するために行われます。

標的とするネットワーク内でサイバー犯罪者が使用するエクスプロイトは、インストールされているネットワーク防御策によって異なります。間違いなくハッカーは、システムに確実にアクセスできるようにするためにWebshellのインストールを試みます。別の維持手法としては、クロスサイトスクリプティング（XSS）を使用して、悪意のあるコードをユーザーのJavaScript、ActiveX、Flashその他のコードバンクに挿入し、有効なユーザーのセッションをハイジャック（Cookieを窃取）するという方法があります。スピアフィッシングを通じて有効なユーザーにマルウェアを送信することが、このプロセスの重要な要素です。

さらに、ハッカーはWebサーバーに対してディレクトリトラバーサル攻撃（別名：ディレクトリクライミング、バックトラッキングなど）を使って、SSL（Secure Socket Layer）プライベートキーやパスワードファイルなど、アクセス制限されたディレクトリへのアクセスを試みます。ハッカーはさらに、上記のようなディレクトリにアクセスすることにより、サーバー上でコマンドを実行することもできます。管理者権限を取得した後は、一般的にリモートアクセスプロトコル経由でトンネルを使って極めて重要なデータを密かに抽出します。サイバー犯罪者はまた、開放されているポートを探し、さまざまな悪用を目的として非標準ポートに任意のソフトウェアをインストールしようと試みます。標的とするネットワークから有益なデータを継続的に入手できそうな場合、勤勉なハッカーは悪用したネットワーク内の自分の「痕跡」を継続的に消去し、自身の存在を永久に隠し続けます。別の有名なハッカーが説明するには、複数の「バックドア（Webshell）」を使って企業のネットワークに10年間持続的にアクセスし続け、自身の「仕事」が検出されないように継続的に消去を行っていたと言います。現実には、我々が取り調べを行ったハッカーの多くが、標的とするネットワークに他のハッカーの痕跡が見えることがよくあり、そのせいで彼らのハッキングエクスプロイトを隠すことが困難になることがあったと言います。

これらはシークレットサービスが観察した、被害者のネットワークを悪用するために犯行グループにより使用されていた戦術、技術、手順の一部に過ぎません。脅威は現実に目の前にあり、多種多様な動機に駆られて敵は常に進化しています。犯行の成功は多くの場合、脆弱性が明らかになると同時に、ネットワーク管理者が防御策をどれだけうまくその脆弱性に適応させることができるかにかかっています。

シークレットサービスは引き続き、サイバー犯罪者がどこにいようとも彼らを追跡、逮捕および起訴してまいります。また、我々は今後も、当機関のパートナーである法執行機関や教育機関、公共および民間部門などのサイバーセキュリティ対策をさらに強化するために、調査から得た攻撃手法の貴重な分析結果を提供してまいります。

付録B：方法論

読者の皆様が本報告書について最も重視される内容のひとつが、我々がデータを収集、分析および提示する際に適用している厳格さと完全性の水準の高さです。読者がそのことを重視し、本書の情報を鋭い目で読み解いてくださっているからこそ、我々は誠実でいられるのです。我々の手法を詳細に説明することが、その誠実さの重要な部分です。

我々の全般的な手法はここ数年ほとんど変わっていません。本報告書で取り上げたすべてのインシデントは、個別にレビューし、匿名かつ共通の集計データセットを作成するために必要に応じてVERISフレームワークに転換しました。VERISフレームワークをご存知ない方のために説明すると、VERISとはVocabulary for Event Recording and Incident Sharing（イベント記録とインシデント共有のための言語）を略したもので、無料で利用できます。VERISのリソースへのリンクは本書の冒頭に記載されています。

収集方法およびデータ転換に使われた技術は、協力機関により異なります。一般的に以下に説明する3つの方法が使用されました。

1 有償で外部委託した法医学調査およびVerizonがVERIS Webappを介して実施した関連諜報活動を直接記録。

2 パートナーがVERISを使って直接記録。

3 パートナーの既存のスキーマをVERISに転換。

すべての協力機関には、関連する組織や個人を特定し得る一切の情報を除外するよう指示が送られました。

レビュー済みのスプレッドシートおよびVERIS Webapp JavaScript Object Notation（JSON）は、自動化されたワークフローにより取り込まれ、そこに含まれるインシデントやデータ漏洩/侵害を、必要に応じてVERIS JSON形式に変換し、欠けている場合は区分を追加し、次に記録をビジネスロジックおよびVERISのスキーマと照合して検証します。自動化されたワークフローにより、データのサブセットが作成され、結果が分析されます。この探索的分析の結果やワークフローにより生成された検証ログ、ならびにデータを提供してくださったパートナーとの話し合いに基づき、データをクリーニングおよび再分析します。このプロセスはおよそ3ヶ月間、毎晩実行され、データが収集および分析されます。

インシデントの適格性

エントリがインシデントまたはデータ漏洩/侵害データベースに登録されるためには、いくつかの要件を満たしている必要があります。エントリは、機密性、完全性、または可用性の喪失と定義された確認済みのセキュリティインシデントでなければなりません。「セキュリティインシデント」の基準となる定義を満たしているかどうかに加え、エントリのデータ品質が評価されます。また、弊社のクオリティフィルタを通過したインシデントのサブセット（サブセットについては後述）を作成します。

「クオリティ」インシデントとは、以下のようなものを言います。

- インシデントには34の分野に少なくとも7つの区分（例：攻撃者の種類、攻撃の種類、完全性喪失の種類など）があるか、DDoS攻撃である必要があります。確認されたデータ漏洩/侵害については、区分が7個未満でも例外となります。

- インシデントには既知のVERISの攻撃カテゴリ（ハッキング、マルウェアなど）が1つ以上ある必要があります。

クオリティフィルタを通過するのに十分なだけの詳細に加え、インシデントは分析期間内（本報告書の場合は、2018年11月1日から2018年10月31日まで）である必要があります。本報告書では2018年の事例に主に的を絞って分析を行いましたが、本報告書を通じては全期間のデータが参照されており、特に傾向のグラフにはこれが反映されています。また、組織属性の損失に結び付けることのできない個人に影響を及ぼすインシデントおよびデータ漏洩/侵害については、これを除外しました。例えば、ご友人の私用ノートPCがCryptoLockerの攻撃を受けた場合は、本報告書には含まれません。

最後に、DBIRに含まれるための条件として、我々が認識しているイベントである必要があります。それは、サンプリングバイアスに関わってくるためです。

サンプリングバイアスに関する確認事項

繰り返しますが、弊社は本報告書の調査結果が、すべての組織におけるすべてのデータ漏洩/侵害を常に表すものであることを主張するものではありません。すべての協力機関からご提供いただいた記録を集計した記録のほうが、単独の記録よりも現実をより忠実に反映していますが、それでもサンプルはサンプルでしかありません。弊社では本報告書の調査結果の多くが、一般化にふさわしいものと信じていますが、（また、このことに関する我々の自信は、より多くのデータを集めて他のデータと比較するにつれて、ますます大きくなります）バイアスは確かに存在します。残念なことに、我々は実際どの程度のバイアスが存在するのか、正確な誤差をご提示するためにそれを測定することはできません。弊社では、すべてのデータ漏洩/侵害の何割がここに含まれているかを知るための方法を持ち合わせていません。というのも、すべての組織における2018年のデータ漏洩/侵害の合計件数を知る術がないからです。多くのデータ漏洩/侵害が報告されずにいます（弊社のサンプルにはこれら未報告のデータが多く含まれています）。また、被害者にもまだ知られておらず、そのため弊社でも把握していない漏洩/侵害も数多くあります。

本報告書でご提示している調査結果の多くが適切なものであると信じていますが、一般化、バイアス、および方法論的欠陥は間違いなく存在します。しかし、今年度は73の協力機関にお力添えいただき、パートナーの皆様の異なるデータ収集手法、優先順位、および目標に沿ってデータを集計しました。この集計結果が各サンプルの個々の欠陥による影響を最小限に抑え、本調査全体として大いに皆様のお役に立ちますと幸いです。

統計解析

弊社ではDBIRの統計の正確性を確保するよう努めています。今年のデータサンプルでは、信頼区間は少なくともデータ漏洩/侵害では±2%、インシデントでは±0.5%[18]でした。サンプルサイズの小さいデータ（諜報活動パターンのデータ漏洩/侵害など）の場合は、サイズが小さい分、この範囲が広くなります。弊社では、DBIR内のすべての文言を探索的分析に基づく仮説[19]として扱うよう努め、すべての文言が所定の信頼区間（通常95%）において正しいことを確認しました。また、目次の前の「凡例と定義」のセクションで説明した、条件付き確率の棒グラフでこの信頼区間を表すよう努めました。

[18] ベイズ法、95%信頼区間。

[19] 弊社がなぜこれらを調査結果としてではなく仮説として扱うか疑問に思われた方のために説明を加えると、仮説を確認または否定するためには、事前に調査していない固有の2つ目のデータセットが必要になります。

弊社のデータは非独占的多項データであり、「攻撃」などの1つの特徴に複数の値（「ソーシャル」「マルウェア」および「ハッキング」など）が存在する場合があります。これはつまり、パーセンテージの合計が必ずしも100%にならないことを意味します。例えば、ボットネットによるデータ漏洩/侵害が5件あった場合、サンプルサイズは5です。しかし、それぞれのボットネットがフィッシングを利用し、キーロガーをインストールし、盗んだ認証情報を利用したとすると、ソーシャル攻撃が5件、ハッキング攻撃が5件、マルウェア攻撃が5件となり、合計は300%となります。これは正常かつ想定されることであり、弊社の分析およびツール設定で正しく処理されます。

もう1つの重要なポイントとしては、調査結果を見る際に「不明」は「未測定」と同義と捉えてください。つまり、記録（または記録の集合）が「不明」とマークされた要素（インシデントに関係する記録の件数といった基本的なものから、マルウェアが含んでいた特定の機能といった複雑なものまで）を含んでいる場合、その特定の要素について現状の記録のままではコメントすることができないことを意味します。情報が少なすぎる場合には測定が不可能なためです。これらの記録は「未測定」なので、サンプルサイズにも含まれていません。数値が「その他」の場合は、数値は不明だがVERISの一部ではないことを示しているため、サンプルサイズに含まれています。最後に、「該当なし」（通常「NA」と表記）は、仮説によって含まれたり含まれなかったりします。

データサブセット

弊社のクオリティ要件を満たしたインシデントのサブセットについては先ほど触れましたが、分析の一環として弊社がデータのサブセットを定義しているその他のインスタンスがあります。これらのサブセットは正当なインシデントではあるものの、そのまま放置するとかすかなトレンドを覆い隠してしまうインシデントで構成されています。これらは除外して個別に分析しています（関連するセクションに詳述のとおり）。今年度の報告書では、データセット全体の一部として、正当なインシデントで構成される2つのサブセットを設定しています。

1 二次ターゲット（Webサイトを乗っ取り、マルウェアを拡散させる、など）として特定されたWebサーバーのサブセットを個別に分析しました。

2 ボットネット関連のインシデントを個別に分析しました。

これら2つのサブセットは昨年も個別に分析されました。

最後に、分析をさらに進めるためにいくつかのサブセットを作成しました。特に、別途記載のない限り、単一のサブセットをDBIR内のすべての分析に使用しました。これには上で説明したクオリティインシデントと前述の2つのサブセットのみが含まれます。

インシデント以外のデータ

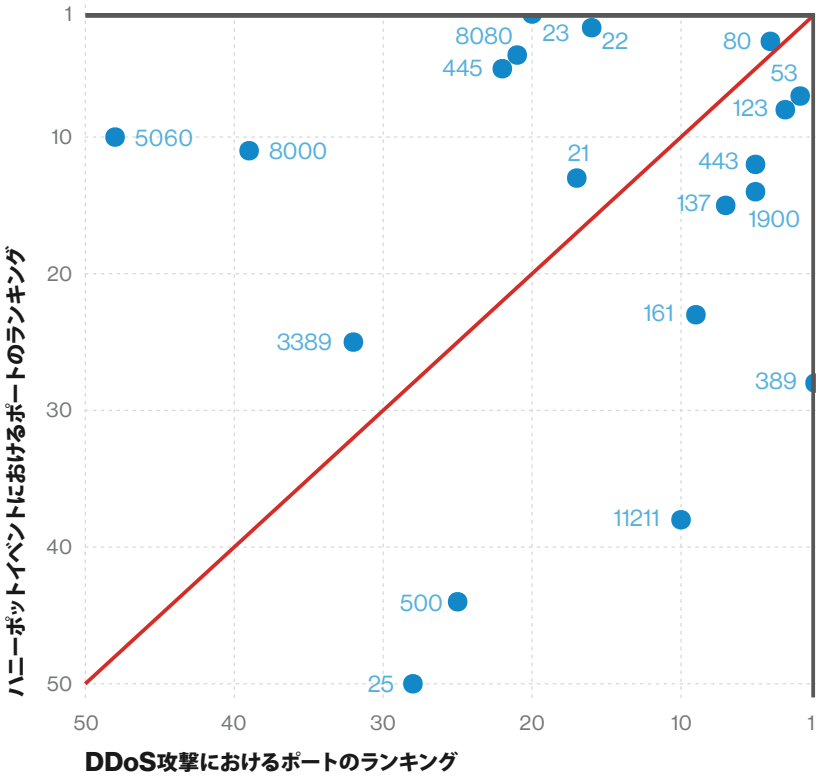
2015年以来、DBIRには「インシデント」または「データ漏洩/侵害」という弊社の通常のカテゴリに当てはまらなかった分析を必要とするデータが含まれています。インシデント以外のデータの例としては、マルウェア、パッチ、フィッシング、DDoS、その他の種類のデータが挙げられます。インシデント以外のデータのサンプルサイズは、インシデントデータよりもはるかに多い傾向がありますが、データのソースは限られています。弊社ではデータを正規化するために、あらゆる努力を行っています（例えば、すべてのデータの平均ではなく、平均的な企業について報告する、など）。また、同様のデータを持つ複数の協力機関を組み合わせて、可能な限り一緒に分析しています。分析が完了すると、関連する協力機関と調査結果について話し合い、またはデータについての彼らの知識に照らして検証するよう努めています。

付録C：監視者の監視

昨年度版の付録「Feeling vulnerable?」では、spray and pray型のインターネットスキャニングにおいて攻撃者たちが探しているサービスや弱点について触れ、それらが標的型攻撃において攻撃者たちが探しているものとは必ずしも同じではないということをお伝えしました。本セクションでは、インターネットに公開されているサービスと、それらのサービスに対する攻撃について改めて詳しく見ていきます。当然のことながら、攻撃者が探しているものが分かれば、彼らにとって価値のあるものについて多くのことが分かります。

ポートの限界費用と価値

少なくとも一定の価値を提供し、同時に攻撃者にとって投資が少額で済む（TCP/UDP）ポートは、多くの注目を集めます。経済学者は攻撃者が1回の攻撃に投資した金額を限界費用と呼ぶかもしれません。犯罪者の視点から見た最高の攻撃とは、標的1件あたりの費用が一切かからない攻撃でしょう。これを本書では「限界費用ゼロ攻撃」と呼びます。

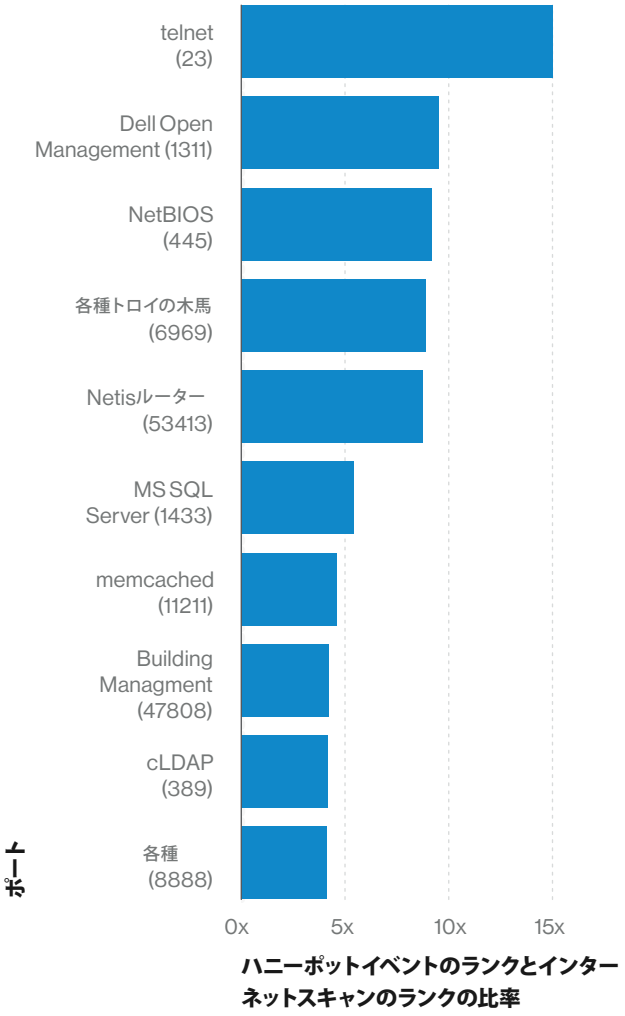


図表65 DDoS攻撃およびハニーポット攻撃におけるポートの比較

図表65は、ハニーポットとDDoS攻撃の両方によく見られる50のポートを図に表したものです（右上の「1」が最もよく見られるもので、そこから頻度が下がります）。特定のポートを攻撃者が探す頻度を、攻撃者にとってのそれらのポートの価値を示す指標として捉えることができます。赤線より下に位置するポート、すなわちcLDAP（389）、DNS（53）、およびNTP（123）が、攻撃者にとってDDoSアンプ攻撃への利用価値が高いと考えられます。一方、赤線より上に位置するポート、すなわちSSH（22）、telnet（23）、HTTP（8080）、NetBIOS（445）などは、攻撃者にとって非DDoS攻撃への利用価値が高いと考えられます。

攻撃者にとって価値のあるポートとは

限界費用ゼロ攻撃における特定のポートの攻撃者にとっての価値を判断する最も効果的な方法は、おそらく、ハニーポットスキャンによる犯罪者のランキングとインターネット上の攻撃者の母集団のランキングを比較検討することでしょう。定期的にインターネットスキャンを実行している組織は無数に存在しますが、DBIRにデータを提供していただける組織はほんのわずかです。そうした親切な組織にご提供いただいたデータをもとに分析した結果を図表66に示します。



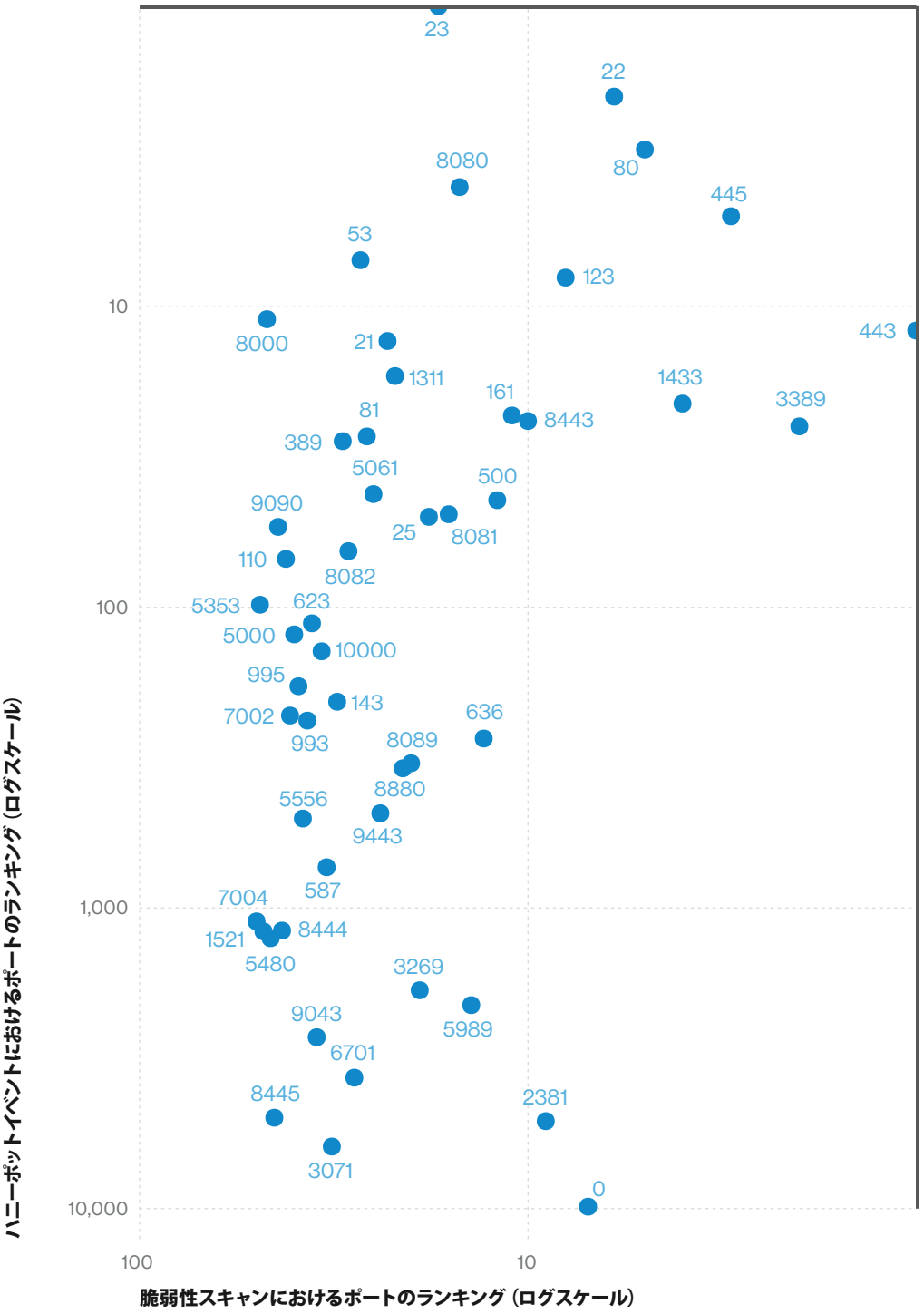
図表66 実在する台数と比較したポートのスキャン回数の倍率

図表66は、ハニーポットが記録したアクティビティとインターネット上のアクティビティを比較した倍率上位10位のポートを一覧にしたものです[20]。これらの一部、例えばTelnet、NetBIOS、およびSQLサーバー（かなり昔から既知の弱点があるレガシーサービス）は、もはや一般的に使用されていないかもしれませんが、まだ存在しており、攻撃者に見つかるとピンク・フロイドの「マネー」のイントロが聞こえてくるぐらい確実に標的となります。これらいずれかのサービスをインターネットにつないでいる組織は、今すぐ対処したほうが良いでしょう。本報告書を読み進める前に、ここで時間をとって今すぐ対処してください。本報告書の更新は年に一度ですが、これらのポートは毎日攻撃に遭っています。

攻撃者にとって、ありふれていて価値のないポートとは

前のセクションからひとつの疑問が生まれます。「攻撃者が頻繁に探しているものがポートで、それがめったに見つからないなら、開放されたポートの中でも多数あるのに攻撃者がめったに探さないのは、どんなポートでしょうか？」ご質問ありがとうございます。ほとんどの場合、それは割り当てられていないエフェメラル（短命な）ポートです。もっと興味深いのは、脆弱性スキャンでは検出されるが、ハニーポットでは検出されないポートです。図表67から、そうした領域のポートについての知見を得ることができます。ここでの主なメッセージは、ハニーポットの視点で見ると図の底辺にたくさんのポートが集まっています（図の左下のほうに大きな塊があります）が、これらが脆弱性スキャンでよく報告されるものだということです。これらの脆弱性は攻撃に有用かもしれませんが、標的が小規模すぎるか、内部者のピボッティング（足場を作る）か、または攻撃者にとって全く興味がないかのいずれかです。

[20] 例えば、ハニーポットスキャンで上位に挙がるポートがインターネット上でよく見られる15位のポートだった場合、倍率は15倍となります。



図表67 脆弱性スキャンとハニーポットイベントにおけるポートの比較

対策を講じましょう

地球上にある海はたったの7つですが、ポートの数は65,535個もあります。上の図表にはすべては載っていませんが、これよりはるかに多く存在するのです。では、次に何をすれば良いのでしょうか。まずは貴社が「限界費用ゼロ攻撃」に脆弱かどうかを調べることをお勧めします（ハニーポットスキャンとインターネットスキャンの比率で簡単に調べることができます）。もし脆弱な場合は、重要なセキュリティ基準を満たしていないことを意味しますので、基準を満たすよう対策を講じてください。貴社はハニーポットを設置していますか？そうでない場合は、ポートを開放している理由は何でしょう。最後に、「攻撃パス」のセクションからヒントを得て、その他に緩和できるリスクについて学んでください。これらのサービスを悪用するために攻撃者が利用しそうなパスを把握しましょう。

付録D：協力機関

SOCIAL-ENGINEER

edgescan

bit-x-bit SM

Gillware

CISA CYBER+INFRASTRUCTURE

Qualys. Continuous Security

RAPID7

BeyondTrust

Center for Internet Security

Carnegie Mellon University Software Engineering Institute

MOSSADAMS

LARES

DELL

3E

NetDiligence

CISCO

swisscom

CROWDSTRIKE

Akamai

CYLANCE

CIRCL Computer Incident Response Center Luxembourg

zscaler

digital shadows_

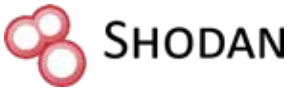
Check Point SOFTWARE TECHNOLOGIES LTD

EMERGENCE

apura


ATTACKIQ


V
C
D
B


SHODAN


GRA QUANTUM


FORTINET


KASPERSKY


MALICIOUS STREAMS


DRAGOS


NCFTA


wandera


PALADION
HIGH SPEED CYBER DEFENSE


KnowBe4
Human error. Conquered.


CyberSecurity
MALAYSIA
An agency under MOSTI


BITSIGHT
The Standard in SECURITY RATINGS


Digital Edge


WINSTON
&STRAWN
LLP


LIFARS
your digital world, secured


MWR
an F-Secure company


AVANT
RESEARCH GROUP


IRISS
Irish Reporting and
Information Security Service


NETSCOUT


Recorded
Future


VESTIGE
Digital Investigations


INTERSET


DFDR
CONSULTING


McAfee


CERT-EU


paloalto
NETWORKS


Mishcon de Reya


tripwire


proofpoint
Security Awareness Training


JPCERT CC


CHUBB


HSC
HYDERABAD SECURITY CLUSTER


S21
SEC

A

Akamai Technologies
Apura Cyber Intelligence
AttackIQ
Avant Research Group, LLC

B

BeyondTrust
BinaryEdge
BitSight
Bit-x-bit

C

CERT Insider Threat Center
Chubb
Cisco Security Services
CrowdStrike
Cylance

D

Dell
DFDR Forensics
Digital Edge
Digital Shadows
Dragos, Inc

E

Edgescan
Emergence Insurance
EUコンピュータ緊急対応チーム

F

Fortinet

G

Gillware Digital Forensics
GRA Quantum
GreyNoise Intelligence

I

Interset

J

JPCERT/CC

K

KnowBe4

L

Lares Consulting
LIFARS

M

Malicious Streams
Mishcon de Reya
Moss Adams（旧ASTECH consulting）
MWR InfoSecurity

N

NetDiligence
NETSCOUT

P

Paladion
Proofpoint

Q

Qualys

R

Rapid7
Recorded Future

S

S21sec
Shodan
Social-Engineer, Inc.
SwissCom

T

Tripwire

V

VERIS Community Database
Verizon Digital Media Services
Verizon DOS Defense
Verizon Network Operations and Engineering
Verizon脅威リサーチアドバイザリーセンター
Verizonサイバーリスクプログラム
Verizonプロフェッショナルサービス
Verizonマネージドセキュリティサービス
Vestige Ltd

W

Wandera
West Monroe Partners
Winston & Strawn LLP

Z

Zscaler

あ

アイルランドレポートおよびインフォメーションセキュリティサービス（IRISS-CERT）

い

インターネットセキュリティセンター

さ

サイバーセキュリティ マレーシア、マレーシア科学技術革新省（MOSTI）管轄下の機関

す

スペイン治安警察サイバー犯罪中央作戦部隊（スペイン）

ち

チェック・ポイント・ソフトウェア・テクノロジーズ

て

テランガナ州情報技術及び電子通信部門（ITE&C）事務局

は

パロアルトネットワークス

へ

米国コンピュータ緊急事態対策チーム（US-CERT）
米国サイバー鑑識・訓練協定（NCFTA）
米国シークレットサービス
米国連邦捜査局インターネット犯罪苦情センター（FBI IC3）

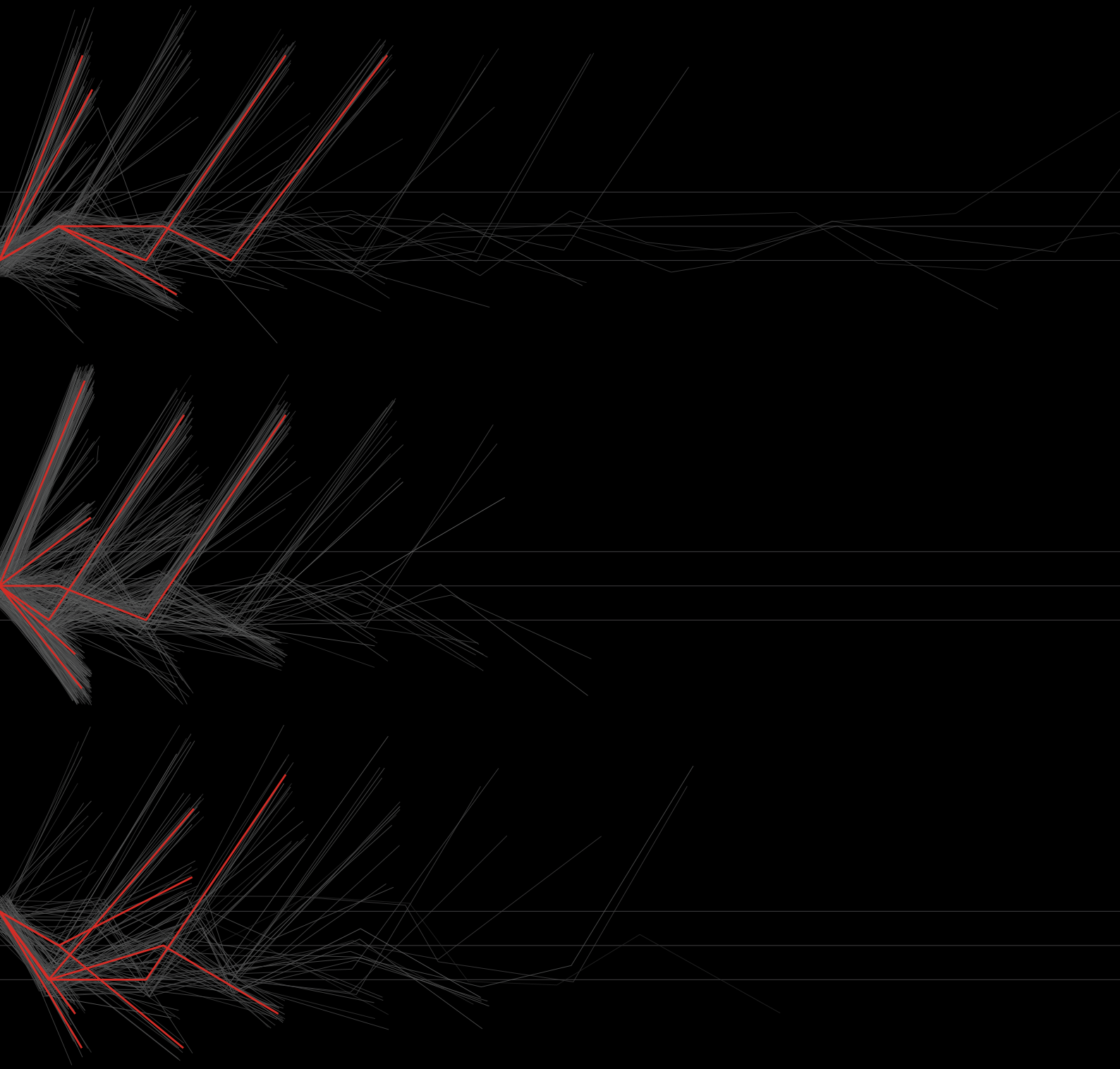
ま

マカフィー

る

ルクセンブルク コンピュータインシデント対応センター（CIRCL）

2019年度データ漏洩/侵害調査報告書



verizon