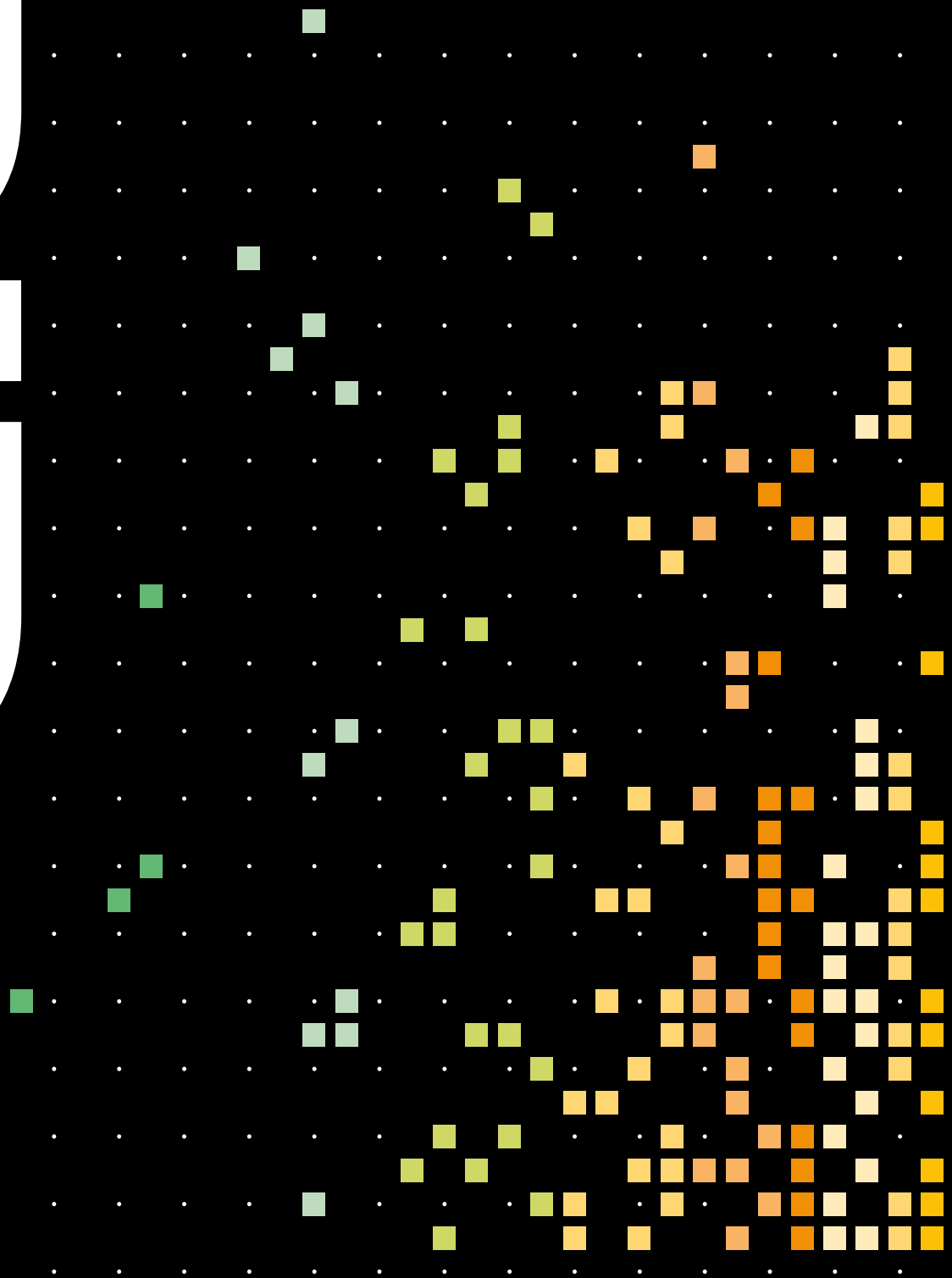
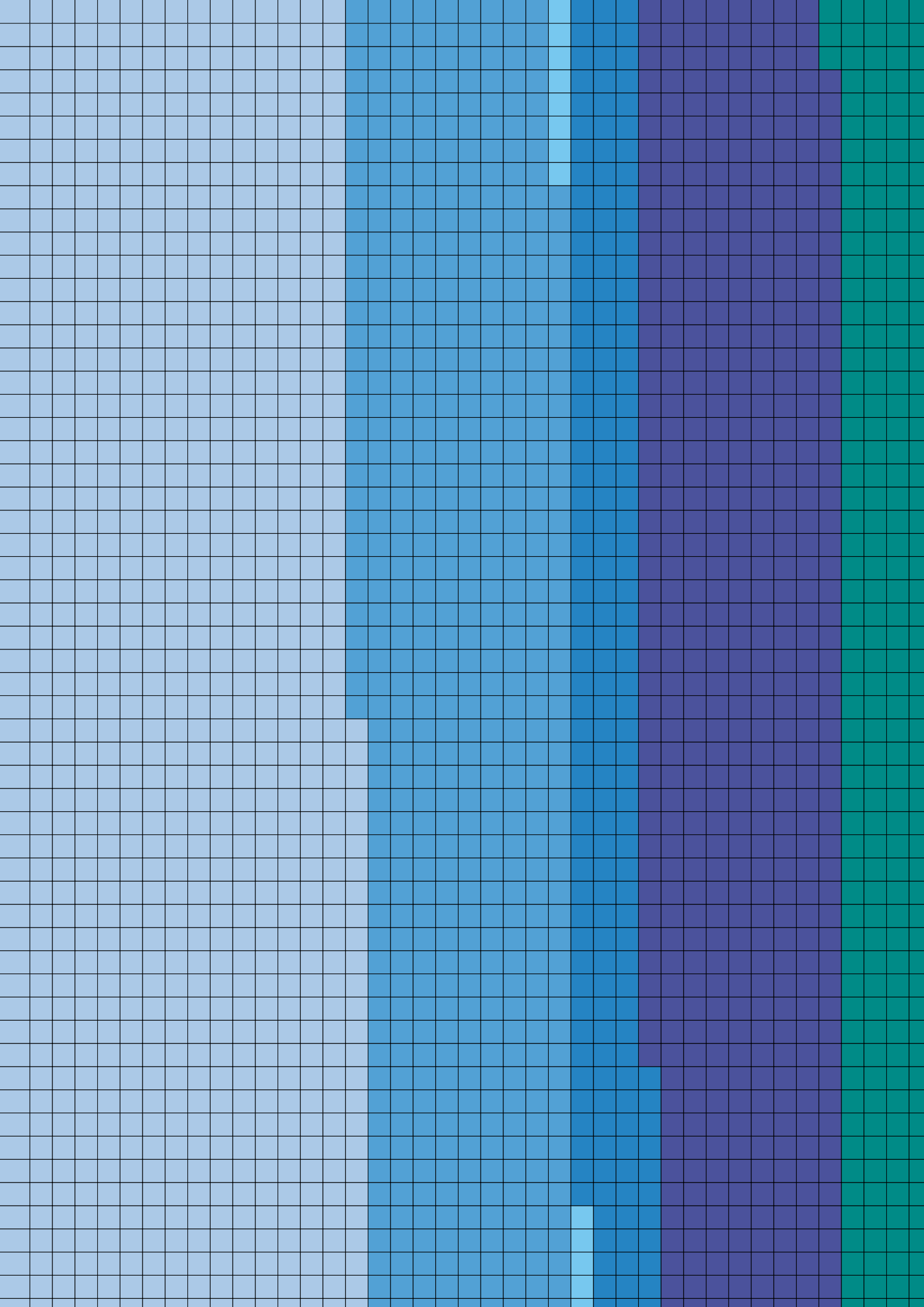
DBIR

2020 データ漏洩/侵害調査報告書



verizon



3,950件の漏洩/侵害

色分けされたこれらの小さな四角いブロックは、今年のレポートで取り上げた16の業界と世界の4つの地域を表現したものです。各ブロックはおよそ1件の漏洩/侵害を表し（正確には1.04件）、業種と地域の両方を併せて、合計4,675個のブロックで表しています

また、今年度の調査では過去最高の合計157,525件のインシデントを分析しましたが、そのうち32,002件が当社の品質基準を満たしていました。この報告書でのデータの網羅性は非常に高く、単色の表紙とは対照的に、データ駆動型のリソースであるDBIRの使命がここに強調されています。ページをめくって調査結果をご覧ください。

目次

凡例と定義

2020年度データ漏洩/侵害調査報告書（DBIR）へようこそ。本報告書完成には時間をかけて取り組んできました。命名規則、用語、定義については慎重に検討し、さらに報告書全体においてこれらを統一させるために多くの時間をかけています。分かりにくい個所もあるかと思いますが、本セクションの定義によって理解を深めていただければ幸いです。

VERISリソース

「攻撃（threat action）」、「攻撃者（threat actor）」、「種類（variety）」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「Vocabulary for EventRecording 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、ソーシャルエンジニアリング、不正使用/悪用、物理的攻撃、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、ソーシャルエンジニアリング攻撃によって人の行動に影響を及ぼすこと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」として記録しています。

詳細情報はこちらをご覧ください。

- **github.com/vz-risk/dbir/tree/gh-pages/2020 –** DBIRの結果、図および図内データ。
- **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の全スキーマ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。

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「金融および保険業」を表すNAICSコードです。図内では、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=2012

グラフのドットプロットと信頼度

昨年度は、サンプリングのバイアスによる不確実性を示すために、今ではお馴染みとなった斜めの棒グラフを導入しました[1]。 今年度に追加した改善の1つは、「トップ（何であれ）」チャートに入れられない全ての項目を「その他」の集計として提示することでした。これによって、除外されたデータについて理解を深めることができます。

今年度も負けず劣らず、弊社の素晴らしいデータサイエンティストチームは、値の分布をより良く示す方法としてドットプロット[2]の導入を試みました。

1 斜めの棒グラフの形状の意味をお忘れになった方は、2019年DBIRの内表紙に記載された「凡例と定義」の「新グラフの説明」をご確認ください。
2 ドットプロットの詳細については、マシュー・ケイの論文をご覧ください（http://www.mjskay.com/papers/chi2018-uncertain-bus-decisions.pdf）。

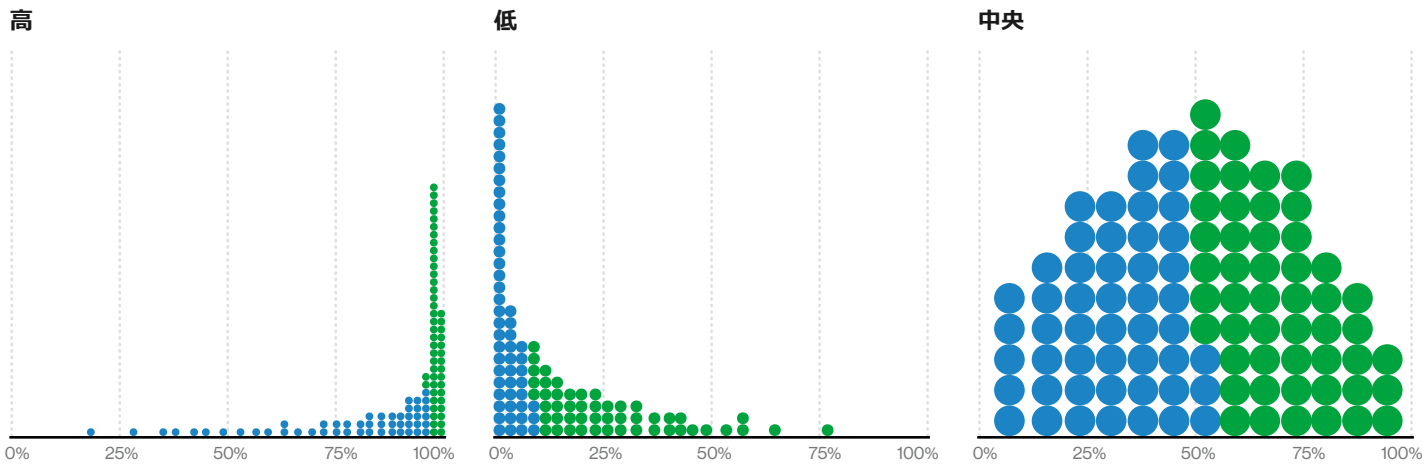


図1. ドットプロットの例

このグラフを理解するコツは、各ドットが組織を表しているということを頭に入れておくことです。つまり、（図1の各グラフのように）ドットが100個あれば、1ドットは組織全体の1%を表しているということです。図1には3つのグラフがあり、それぞれが本報告書でよく見られるデータの分布を表しています。便宜上、中央値を見つけやすくするために、前半と後半とで色を変えています。

最初のグラフ「高」では、多くの企業の数値が非常に高いことが分かります。反対に2番目のグラフ「低」では、多くの企業がゼロか低い値です。3つ目のグラフ「中央」では、途中で行き詰まってしまい、ほとんどの企業の値が中間であるとしか言いようがありません。「中央」のグラフを使えば、恐らく平均値か中央値を報告することができます。「高」と「低」のグラフの場合、平均値は統計的に明確にできません。中央値では誤解を招くことになるでしょう。そのようなことは避けたいものです。

何かご不明な点がありますか？ ご意見やご感想がございますか？VERISの「ハッキング」という用語がまだ気になりますか？

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。

3 これらのグラフは分かりやすく説明するために作ったものですので、ここでの値は気にしないでください。これ以降のグラフには実際の値を使います。

イントロダクション

「経験とは、誰もが自分の過ちにつける名前のことだ。」
ー オスカー・ワイルド
『ドリアングレイの肖像』

また弊社の新しいデータ漏洩/侵害調査報告書（DBIR）をお届けする時がやってきました。この小さな報告書の発行も今年で13回目を迎え、弊社にとっても感慨深いものがあります。つまり、私たちがティーンエイジャーのその年齢になった時と同じように、本報告書も今、大きな変化を遂げようとしているのです。13という数字と、それが災難や不運、不幸を連想させると言われていることについて、強い懸念を抱かれる方もいらっしゃるかもしれません。弊社のチームは、セキュリティにまつわる暗い迷信の隅々までデータサイエンスの光を当て、根拠のない信念を払拭するために最善を尽くし続けています。

このことを念頭に置いて、この13年目の調査報告書をお読みいただくようお願いしたします。よくご覧いただくと、あちこちにいくつかの業界が芽生え、世界の他の地域でも関心が高まり始めていることに気づくかもしれません。今年度は過去最高の15万7,525件のインシデントを分析しました。そのうち、弊社の品質基準を満たしたものが32,002件、確認されたデータ漏洩/侵害が3,950件でした。本報告書には、それらの分析結果が掲載されています。

今年度は、業界別の分析を大幅に増やし、これまでで最も多い16の業界について、業界ごとに最も多発した攻撃、攻撃者、アクションを検証しています。また、統計処理やプロトコルの改善に加え、何よりも新たな外部協力者からのデータ提供のおかげで、これまでになく地域的な視点からサイバー犯罪を調査できるようになったことも誇りに思います。本報告書は、世界のデータ漏洩/侵害に関する最も包括的な分析であると言っても過言ではありません。

さらに、インシデントと漏洩/侵害の分類と分析には引き続きVERISのフレームワークを使用していますが、このプロセスをさらに強化し、VERISと他の既存の標準との連携、Center for Internet Security（CIS）[4]のCritical Security Controls（CSC）やMITRE社のATT&CK®[5]のフレームワークとの連携を図り、本報告書で収集可能なデータの種類を改良し、適切なコントロールに対応させました。

今年度の報告書に初めて参加してくださった方々、そして長年にわたりこの調査にご協力いただいている方々を含む、81カ国を代表する81名の外部協力者の皆様には多大なる感謝の意を表したいと思います。本報告書およびここに記載されたデータと分析は皆様のご協力なしには成り得なかったものであり、皆様には心から感謝いたします。そして、このトピックを追求する一方で、内容をさらに充実させ、改善を続けていくためには、皆様のような質の高い組織に、未知のものや不確実なものとの戦いにご参加いただくしかありません。以上のことから、どうかデータ提供者になることをご検討いただき、暗い場所に光を当て続けるための手助けをしていただけるようお願いいたします。

最後になりましたが、読者の皆様には、長年にわたり愛読していただき感謝しております。また、皆様の専門知識、アドバイス、励まし、ご提案を受けることで、毎年本報告書の改善を図ることができていることにあらためて感謝いたします。

謹んで御礼申し上げます。
ベライゾンDBIRチーム

（アルファベット順）

Gabriel Bassett
C. David Hylender
Philippe Langlois
Alexandre Pinto
Suzanne Widup

4 https://www.cisecurity.org/
5 https://attack.mitre.org/

分析の要約

図2. どのような手法がとられているか?

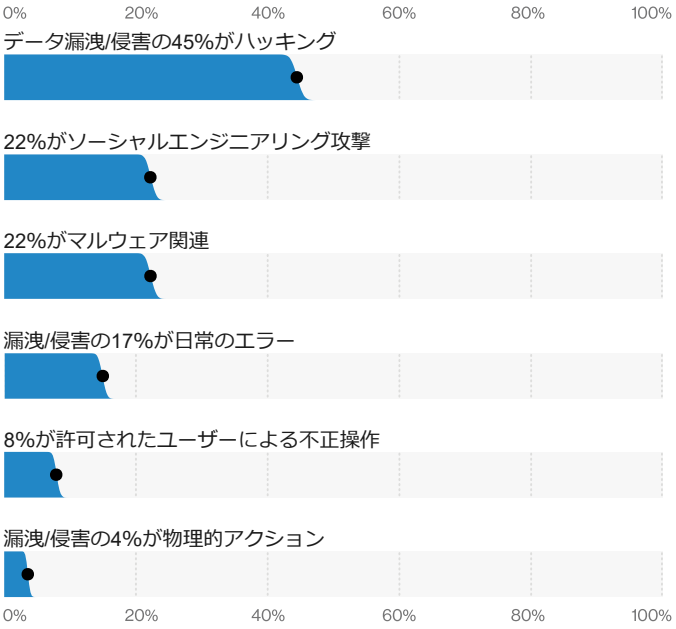


図3. 攻撃の背後にいるのは誰か?

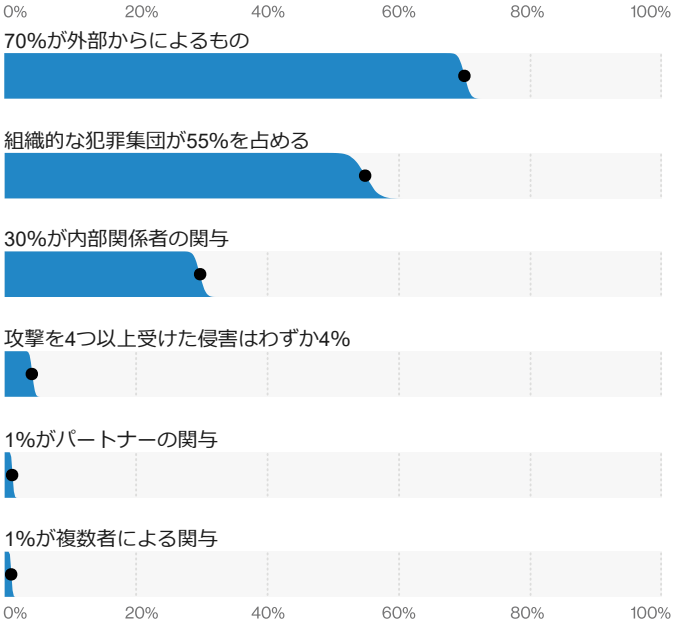


図4. 情報漏洩の被害者は誰か?

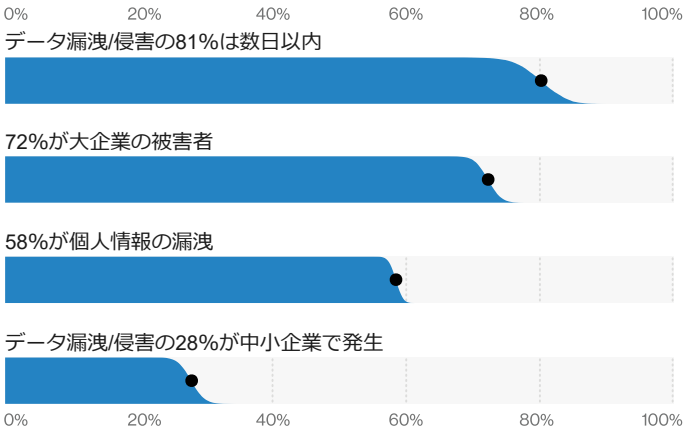
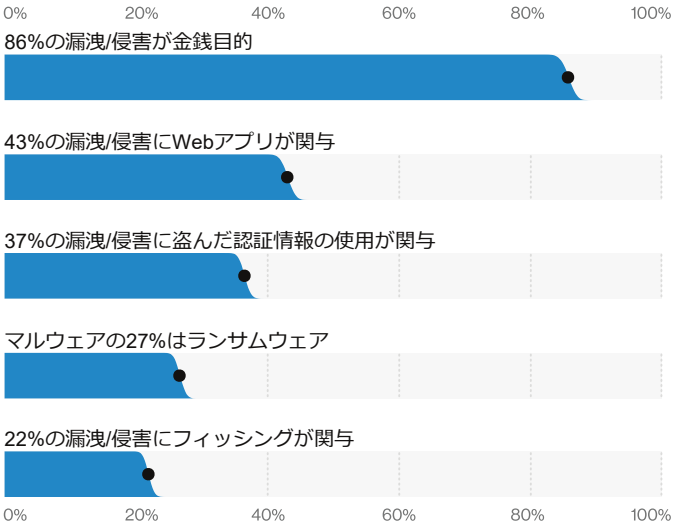
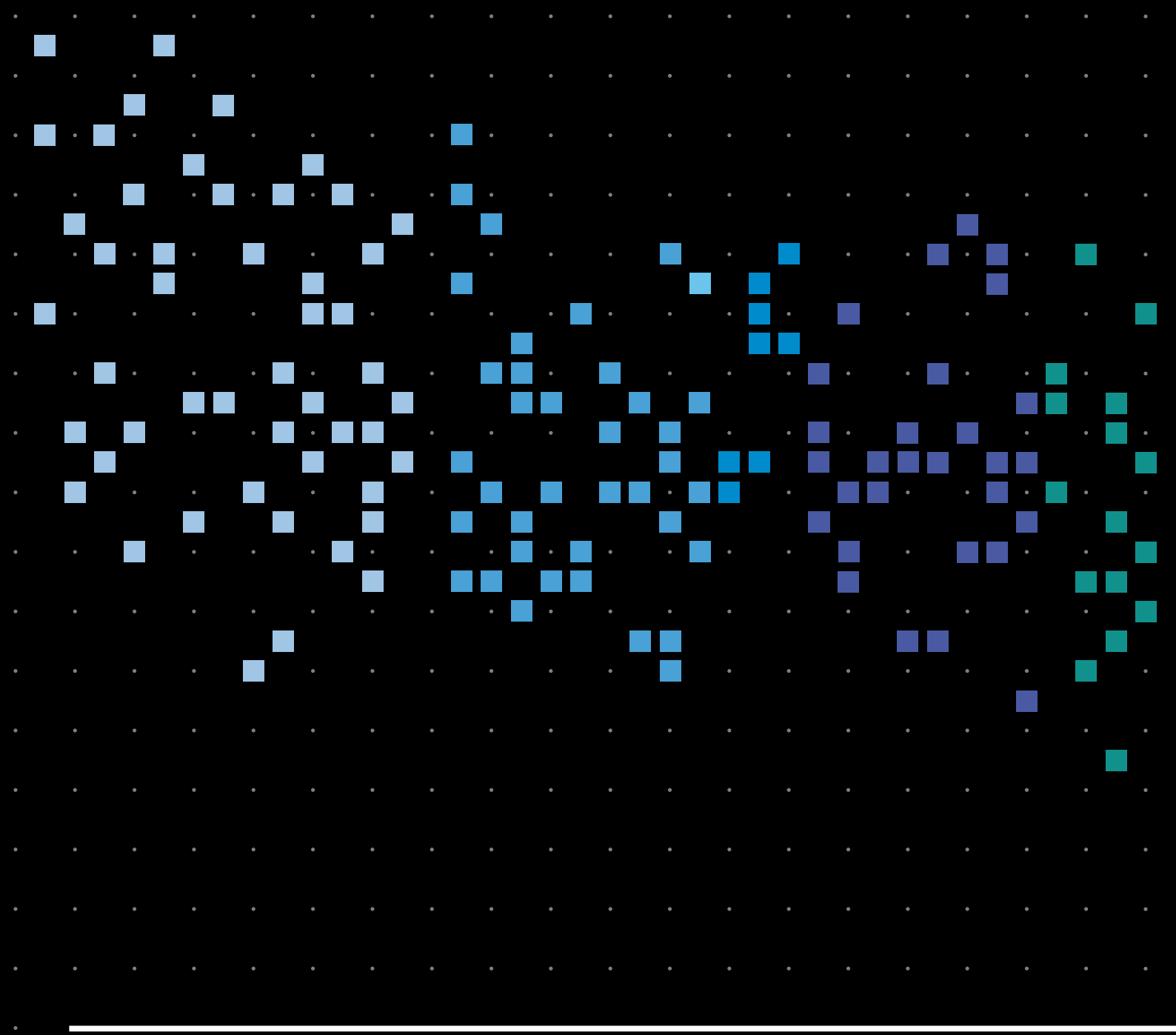
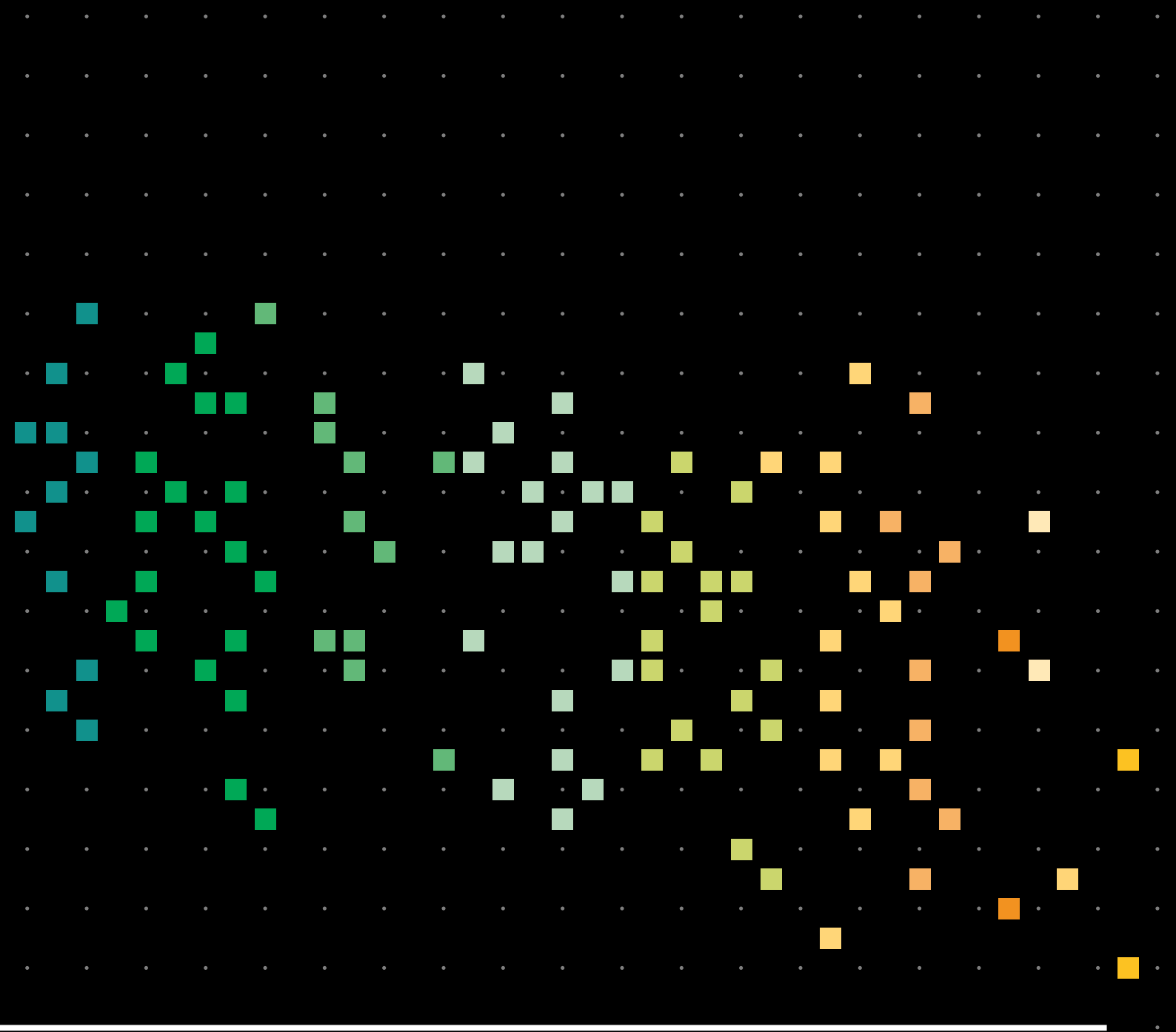


図5. その他の共通点は？





02



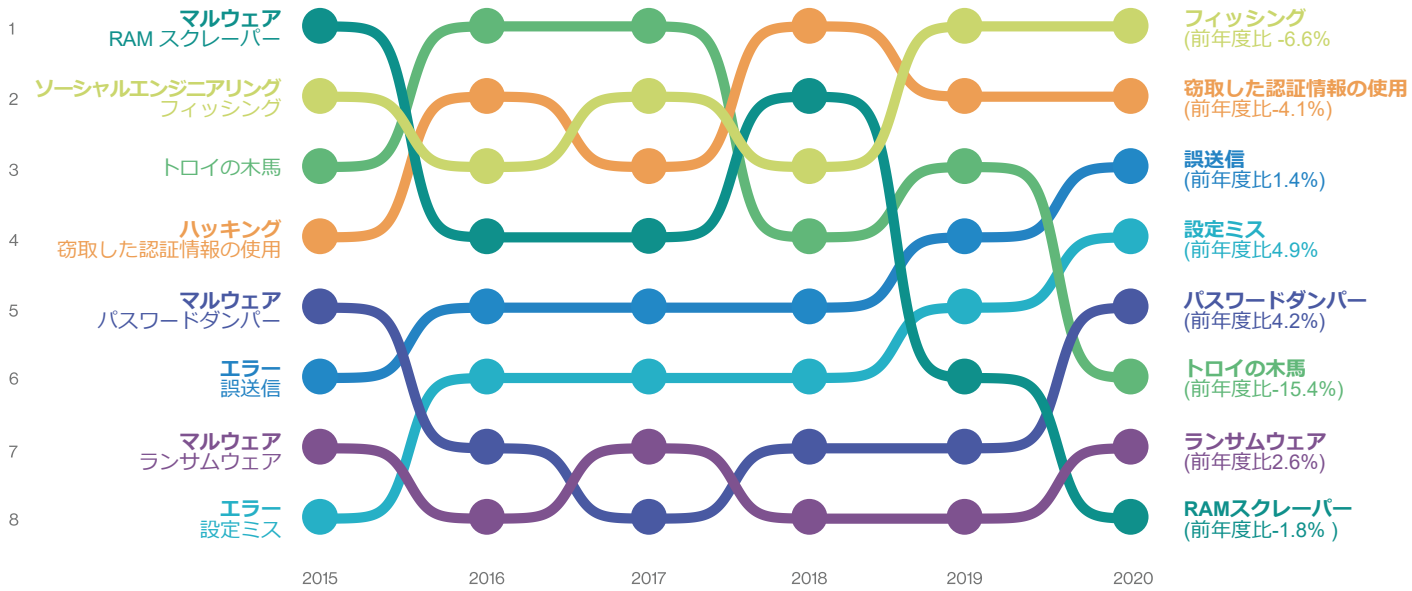
結果および分析

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VTRAC（Threat Research Advisory Center）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[6]であり、新たな組織が参加したり、参加していた組織が今年は参加できなかったりという変化はデータセットに影響を与えることになります。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。また、調査結果に影響を及ぼすその他の要素となる可能性があります。また、その他に調査結果に影響を及ぼす要素として考えられるのは、データのフィルタリングや下位分類の方法の変更です。つまり、毎年まった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。これら全てを考慮し、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。とはいえ、毎年のデータに一貫性が明らかに見られることから、細部は変化しても、主要な傾向は堅調であるという確信を得ることができます。

以上の注意事項を踏まえた上で、まず本報告書全体に見られる主な傾向のいくつかを見ていきます。図6でトロイの木馬[7]の線に注目してみましょう。ハッキング攻撃がどのように展開されるかを考えるとき、多くの人は、攻撃者がシステムにトロイの木馬を落とし、ネットワーク内でそれを足がかりにして現在の攻撃範囲を拡大したり、新たな攻撃を開始したりすることを思い浮かべるかもしれません。DBIRのデータによれば、トロイの木馬型マルウェアは2016年にはデータ漏洩/侵害全体の50%弱を占めるまでになりましたが、これをピークに以後、減少に転じ、昨年では、その割合は、わずか6.5%に留まっています。同様に、昨年初めて検出したRAMスクレーパーマルウェアの減少傾向も続いています。これについては、「小売業」のセクションで詳しく説明します。このタイプのマルウェアが減少する一方で、他のタイプの脅威が増加しています。時代が進むにつれて、攻撃者はますます効率的になり、フィッシングや認証情報の窃取などの攻撃に力を注ぐようになっています。これらについては、「ソーシャルエンジニアリング」と「ハッキング」のサブセクションで詳しく説明します。設定ミスや誤送信といった今年度に大きく伸びたデータ漏洩/侵害については、「エラー」のサブセクションで検討します。

図6. 攻撃の種類の経時的変化



6 コンビニエンスサンプリングは非ランダムサンプリングの一種であり、母集団の中の身近にある、あるいは利用可能な部分からサンプルを抽出します。詳細は、「方法論」のセクションをご覧ください。

7 今年度はマルウェアにトロイの木馬のカテゴリーを追加しました。これは、マルウェアRAT、マルウェアC2とバックドア、ハッキングでのバックドアやC2の使用、マルウェアスパイウェア/キーロガーを組み合わせたものです。

攻撃者

まずは誤解を避けるため、広く信じられているが（弊社のデータによれば）誤った信念を正したいと思います。既にご存知の方もいると思いますが、図7に示すように、弊社のデータでは、外部攻撃者の方が内部攻撃者よりもかなり一般的であり、これまでもずっとそうでした。これは、組織の人数とは関係なく、常に外部の人間の方が多いことから、実際には直感的に分かることです。内部の人間が組織のセキュリティにとって最大の脅威であるという意見が現在も広く知られていますが、この認識は間違っています。確かに、ここ数年のデータセットでは内部攻撃者が明らかに増加していますが、これは実際の悪意の証拠というよりも、従業員の過失によるエラーの報告が増えたことによるものである可能性が高いと考えられます。さらに、図8を見ると、金銭的な動機によるデータ漏洩/侵害の方がスパイ活動よりも圧倒的に多いことが分かりますが、金銭的動機自体は他の全ての動機（映画に登場するハッカーの伝統的な「お馴染みの」動機である「愉快犯」、「イデオロギー」、「怨恨」など）よりも一般的です。サイバースパイ活動といったものは、本で読んだりテレビで見たりする方が面白いことは間違いありません。しかし、弊社のデータセットによると、実際にサイバー犯罪に関与しているのは5分の1以下です。だからと言ってスパイ映画がなくなるのは困りますが。

インシデントに関しては、図9に示すように、金銭目的が依然として第一の動機になってはいますが、二次的動機もある程度高いことを認識する必要があります。再確認のために（あるいは新しい読者のために）述べますが、二次的動機のインシデントにおいて侵害されたインフラストラクチャは、主要なターゲットではなく、別の攻撃の一部として目的を達成するための手段です。実際のところ、もし二次的動機のWebアプリケーション侵害を含めていたとしたら（「インシデントの分類パターンおよびサブセット」のセクション」で述べているように、このサブセットは削除されています）、二次的動機のほうが、金銭目的よりも確実に高くなっていたでしょう。

ハッキングフォーラムや闇市場のデータを見ると、5%は「サービス」に言及しています。そのサービスには、ハッキング、ランサムウェア、分散型サービス拒否（DDoS）、スパム、プロキシ、クレジットカード犯罪関連、その他の不正行為など、ありとあらゆるものが含まれると考えられます。さらに悪いことに、その「サービス」はハードウェア上でホストされている可能性があります。つまり、資産をインターネットに晒して、自動化できてしまうほど安全でない状態の場合、攻撃者はインフラストラクチャをマルチテナント環境に変えることができるのです。

図7. 漏洩/侵害における攻撃者の経時的変化

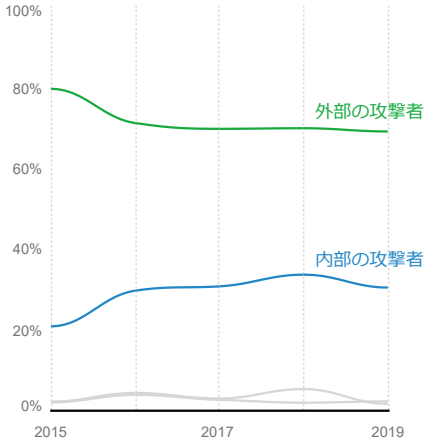


図8. 漏洩/侵害における攻撃の動機の経時的変化

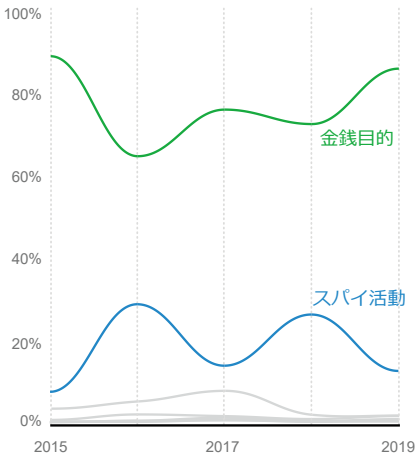
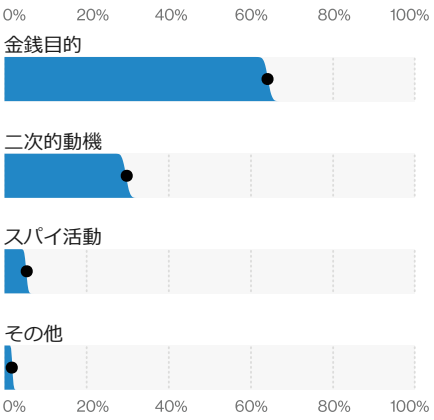


図9. インシデントによく見られる攻撃の動機（n = 3,828）



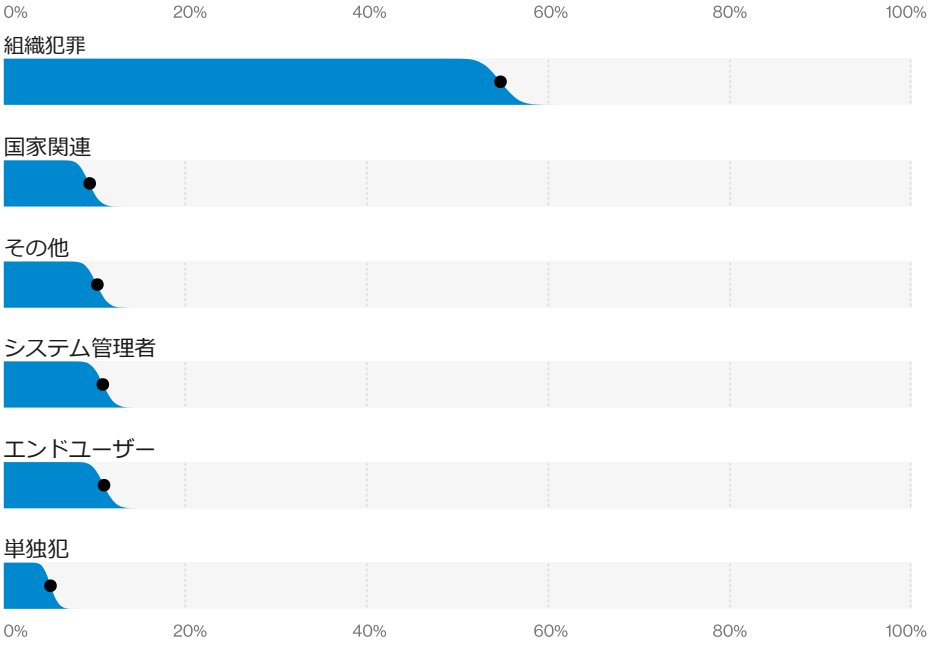


図10. 漏洩/侵害によく見られる攻撃者の種類（n = 977）

この結果を見て出てくる疑問は、「このような招かれざる侵入者はどこからやって来るのか」でしょうか。図10は、DBIRの攻撃者の種類のトップは組織犯罪[8]であることを示しています。その後に続くのはいつもの容疑者たちですが、悪事を企む国家関連の攻撃者、内部エンドユーザー、仕事感覚でエラーを発生させるシステム管理者、そして最後が単独犯です。まるでヤングアダルト向けのシリーズ本のタイトルのように聞こえるかもしれませんが、本当に興味が尽きない集団です。未知の領域から来た彼らの動機を明らかにすることは、必ずしも容易ではありません。これらの攻撃者の出自は、上記で参照したハッキングフォーラムや闇市場のデータを見ることで明らかになるかもしれません。データ漏洩/侵害やインシデントのサイバー犯罪[9]に関連するフォーラムのスレッドの約3%は、攻撃手法のトレーニングや伝授に関わるものでした[10]。

他に適切な表現が見つかりませんが、言わばこれらはまだ見習い期間を終えていないハッカー志望者たちです。実際、イギリスの国家犯罪対策庁（NCA）が指摘しているように、「攻撃者たちは、まずゲームのチートサイトや改造フォーラムに参加し始め、やがて後先を考えずに犯罪的なハッキングフォーラムへと場を移してしていくのです」[11]。言い換えれば、これは一定のスキルを持っているが、明確な方向性を持っていない個人の集まりなのです。彼らにきちんとした説明や報酬を与えられれば、彼らをダークサイドから遠ざけ、セキュリティ業界の人材プールに加えることができるでしょう。彼らに実刑判決ではなく、キャリアと将来を与えることは、長い目で見れば、全ての関係者に良い結果をもたらします。ゲームのいかさま手口を知っておくことは今も昔も役には立ちますが。

もう1つ気になるのは、攻撃者はどこからやって来るのかということです。FBIのインターネット犯罪苦情センター（IC3）に寄せられたコンピュータデータの侵害やビジネスメール詐欺の苦情のデータによると、被害者と攻撃者の85%は同じ国に、56%は同じ州に、さらに35%は同じ市内に存在しました。これは、カリフォルニア州ロサンゼルスやニューヨーク州ニューヨーク市のような人口の多い地域からの苦情が多いことが一因となっています。まさに「敵は身内にあり」ということなのかもしれません。

8 「組織犯罪」という用語は、「マフィア」ではなく「プロセスを持った犯罪者」という意味で使われます。

9 サイバー、サイバー。

10 タイトルまたは本文でガイド、チュートリアル、ラーニング、トレーニングの検索をマッチングしました。

11 Pathways into Cyber Crime, NCA, 2017（https://www.nationalcrimeagency.gov.uk/who-we-are/publications/6-pathways-into-cyber-crime-1/file）.

攻撃

図11の攻撃の概要を分析したところ、図6と同じ様相を示していることが分かりました。年々一貫して頻度が増加している唯一の攻撃タイプは「エラー」です。これは、あまり気持ちの良いものではありません。とはいえ、人は頻繁に間違いを犯すものであり、その多くは自分に向けてやっているという事実から逃れることはできません。

物理的なデータ漏洩/侵害は比較的横ばいで頻度は低いままですが、不正使用、ハッキング、マルウェア、ソーシャルエンジニアリングはすべて昨年の報告書より減少しています。ハッキングとソーシャルエンジニアリングは割合では減少していますが、過去数年間見てきたレベルに近い状態を維持しています。一方、マルウェアは過去5年間、データ漏洩/侵害に占める割合として一貫して着実に減少しています。これはなぜでしょうか？マルウェアは、ふわっとさせる髪型や礼儀のように時代遅れになってしまったのでしょうか？いいえ、ハッキングやソーシャルエンジニアリングなどの他の攻撃タイプが窃取した認証情報の恩恵を受けているため、マルウェアを追加して常駐させる必要がなくなったと考えられます。つまり、マルウェアが8トラック・テープのようになったと断言することはできませんが、マルウェアはシンプルな攻撃シナリオでは出る幕はなく、攻撃者のツールボックスの中で出番を待っている状態なのです。

注意すべき点は、上記の指摘はデータ漏洩/侵害に関するものであり、インシデントに関するものではないということです。インシデントでは、また少し違った話になります。ランサムウェアについて弊社のデータセットでは、認証情報の使用と組み合わせない限りデータ漏洩/侵害の発生はほとんど確認されませんが[12]、ランサムウェアは増加傾向にあります。しかし、マルウェアツールの進化や改善が進むにつれ、マルウェアの普及率はやや低下している感があり、データを提供してくれた弊社の外部協力者の場合「インシデント」状態になるケースが少なくなっています。このことは、マルウェアが最新型攻撃とシンプルな（とはいえ効果的な）スマッシュ＆グラブス（ショーウインドー破り）に二極化されたことが、マルウェアのデータセットに影響しているように見えます。

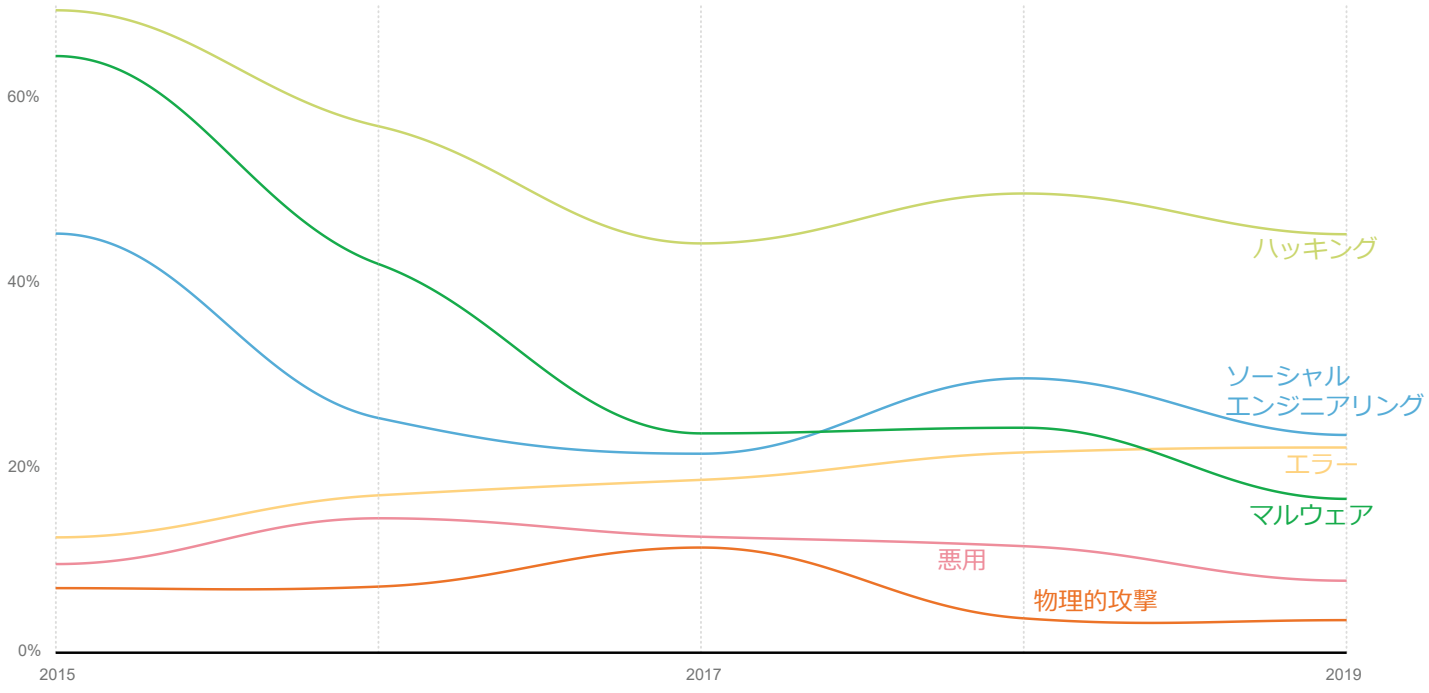


図11. 漏洩/侵害における攻撃の経時的変化

12 弊社で認識している報告の中に、身代金が支払われない場合にはデータを公開すると脅迫できるように、暗号化する前にデータをキャプチャするようになったランサムウェアファミリーがあります。しかし、ログに記録された事例は、この問題で扱うデータ範囲の終了日である2019年10月31日以降に文書化されたものです。

攻撃の種類

攻撃の種類を見てみると、攻撃者のツールボックスをもう少し深く掘り下げることができます。図12は、攻撃の種類がインシデント数を増加させているかを示すもので、驚くべきことにDoS攻撃が大きな役割を果たしています。フィッシングも多く見られますが、データの開示を確認できなかったため、インシデントにとどまり、データ漏洩/侵害にまでは至りませんでした（しかし、あと少しでデータ漏洩/侵害になるでしょう）。全体の6位には、お金を要求する貧しい親戚のようなランサムウェアが急上昇しており、しかもそのほとんどのケースで要求した金をせしめています。

次に図13のデータ漏洩/侵害に関する攻撃の種類の上位を見てみると、昔からの敵であるフィッシング、盗まれた認証情報の使用、そして設定ミスが上位5位に入っています。今年度は誤送信（主に、宛先の間違った文書やメール）が大きく目立っています。その理由を証明するデータがあるわけではありませんが、これは、特にエラーに関してデータ漏洩/侵害の情報開示がより普通になってきている（世界中の個人情報保護法でますます要求されるようになってきている）ことによるものと考えられます。

最後に、「その他」のカテゴリーを挙げてあります。本報告書の冒頭の「凡例と定義」のセクションで述べたように、「その他」とは図中のカテゴリーのいずれにも該当していないものを意味します。上位の種類のいずれにも該当しないデータ漏洩/侵害が多数（具体的には675件）あることが分かりました。データ漏洩/侵害（人や問題など）にはさまざまな形や大きさのものがあり、目の前のドアからそれほど遠くないところにあります。

図12. インシデントによく見られる攻撃の種類（n = 23,619）

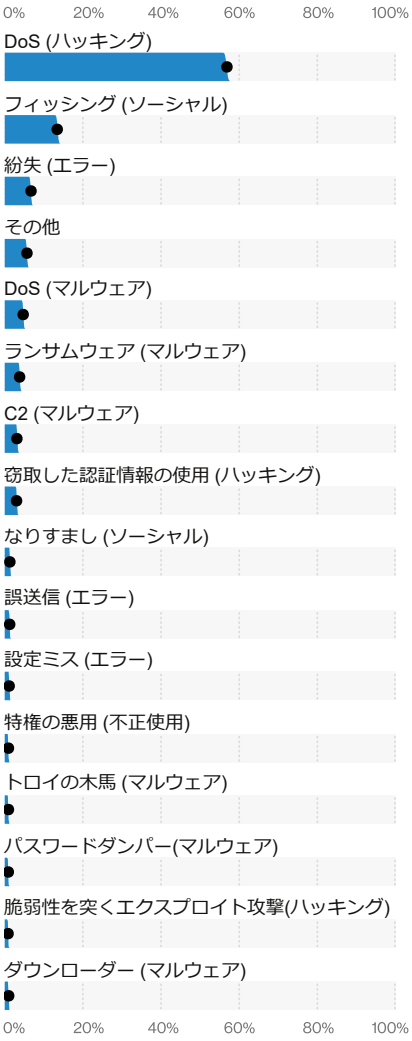
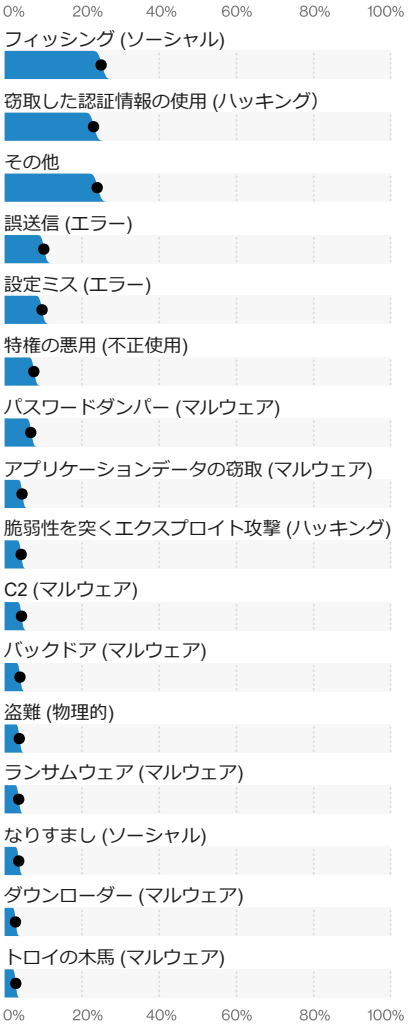


図13. 漏洩/侵害によく見られる攻撃の種類（n = 2,907）



エラー

エラーは、間違いなく今年度のベスト攻撃サポート賞を受賞しています。エラーは、現在ではソーシャルエンジニアリングと同じくらい一般的でマルウェアよりも一般的であり、実際にほぼ全ての業界に行きわたっています。ハッキングだけが依然として上位を占めていますが、これまでにも触れたように、これは認証情報の窃取と使用によるものです。図14を見ると2017年度以降、設定ミスが増加しています。セキュリティ研究者や無関係の第三者が発見した事実ですが、これにはオンラインストレージが大きく関わっていると考えられます。誤公開は減少しているように見えますがこれは単に、以前は組織のインフラストラクチャ上で非公開のドキュメントを誤って公開したことが原因だった誤公開が、現在ではシステム管理者が最初の設定でストレージを公開に設定していたということで、設定ミスのカテゴリーに該当するためということではないでしょうか。

最後に、リストに入っていないものにも注目しておきましょう。2010年度には30%を超えていた紛失が今年度は一桁台に減少しています。誤廃棄も昨年と変わりありません。行政や医療など報告義務のある業界では、DBIRのエラーの数値は常に高い状態です。現在、他の業界でもエラーが顕在化しているのは、ミスを隠蔽しようとするのではなく、ミスを公にできるような職場環境になってきているということなのかもしれません。

もちろん、これらのミスの多くがセキュリティ研究者や第三者によって捕捉されているため、被害者は過失を認めざるを得ないということもあります。エラーによるデータ漏洩/侵害については、セキュリティ研究者が最も優秀な発見手段であり、昨年の6倍以上となっています（図15）。しかし、弊社のDBIRチームは楽観的な性格なので前者の結論に従うことにします。

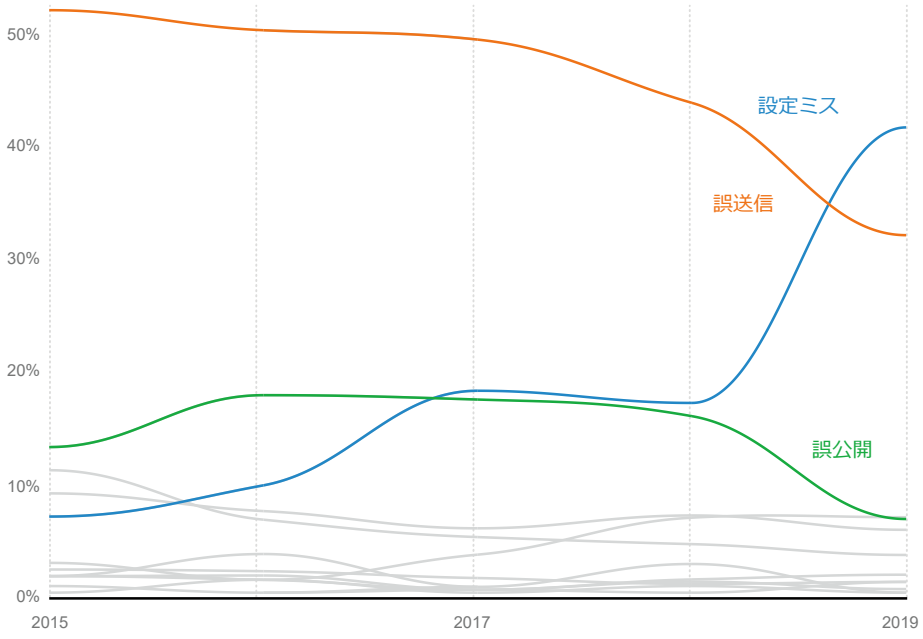


図14. . 漏洩/侵害によく見られるエラーの種類の経時的変化

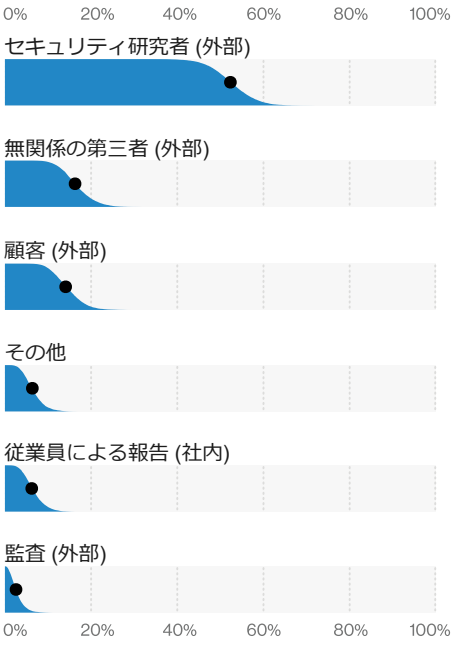


図15. 漏洩/侵害によく見られるエラーの発見手段（n = 95）

マルウェア

弊社のマルウェアの調査結果は、データ漏洩/侵害に関してフィッシングや認証情報の窃取の傾向がさらに強まっています。図16に示すように、データ侵害マルウェアの種類については（甘い、甘い認証情報を取得するための）パスワードダンパーがトップの座を占めています。侵入経路については、メール（通常はフィッシングに関連している）と直接インストール（普通は認証情報を必要とするが、そうとは限らない場合もある）が上位を占めています。

ランサムウェアは、マルウェア攻撃の種類の中で3番目に多く、マルウェアのインシデントの種類では2番目に多くなっています。ダウンローダーはランサムウェアのすぐ後を追い、ランサムウェアだけでなくトロイの木馬も移動させるなど活発な働きを見せています[13]。暗号通貨マイニングがトップ10に入っていないという事実にも触れておくべきでしょう。HODLの読者を失望させることは確実だからです。

しかし、データ漏洩/侵害やインシデントに見られるマルウェアの相対的な割合は、組織全体でのマルウェアとの戦い、クリーニング、検疫で体験した割合とは一致しない可能性があることを認識しておいてください。このことを念頭に置いて、バイアス、厳密にはマルウェアの生存バイアスについてお話したいと思います。

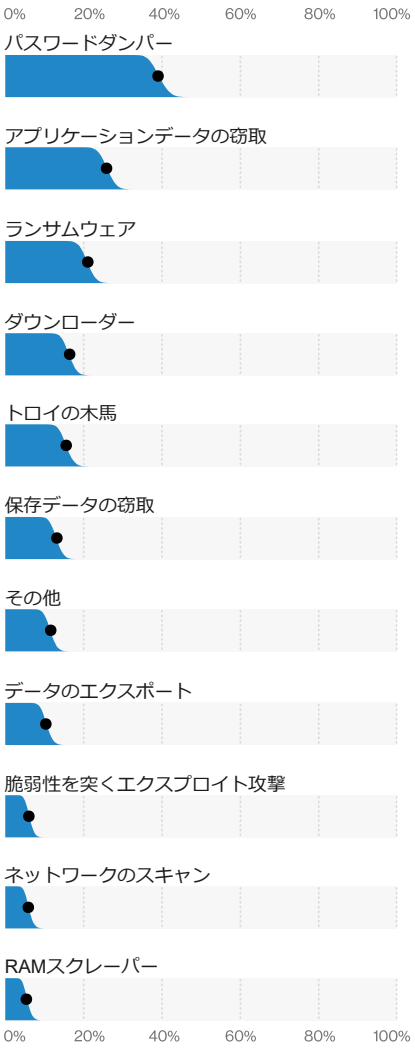


図16. 漏洩/侵害によく見られるマルウェアの種類（n = 506）

図17. 漏洩/侵害によく見られるマルウェアの侵入経路 (n = 360)

パスワードダンパー（攻撃者にとって非常に旨味のある認証情報の窃取に使用される）は、データ漏洩/侵害マルウェアの種類の中でトップの座に就きました。

13 複数の種類のマルウェアの組み合わせ：RAT、トロイの木馬、C2、バックドア、スパイウェア/キーロガー

生存バイアス

生存バイアス（またはより正式には選択バイアス）については巻末の「方法論」セクションで説明していますが、ここでも注意喚起のために触れておきます。誰もが多くのマルウェアデータを見ています。弊社のインシデントコーパスは、生存バイアスの逆の現象に苦しんでいます。データ漏洩/侵害やインシデントの記録は、生き残れなかった被害者の記録です。

一方で、保護コントロールによってブロックされているマルウェアは、潜在的な被害者がマルウェアを入手しなかったという生存バイアスの例です。DBIRでは両方のタイプのデータを自由に利用できるため、可能性のある4つの状況を示すことができます。

1. **ブロックとインシデントの両方で数値が高い：**これは何か大規模のものです。ブロックされていますが、同時に大量に発生しています。
2. **ブロックではなくインシデントで数値が高い：**これは、捕捉されている以上に潜在的に発生しています。
3. **ブロックの数値は高いがインシデントの数値は低い：**検出が良好に行われています。通過数よりも捕捉数のほうが多くなっています。
4. **ブロックとインシデントの両方で数値が低い：**あまり発生していません。

ランサムウェア

従来ランサムウェアはDBIRではデータ漏洩/侵害ではなく、インシデントとして扱っています（特定の業界（医療など）では法規制上のガイダンスに従い、報告目的でデータ漏洩/侵害とみなしています）。弊社がインシデントとしているのは、データを暗号化したからといって、必ずしも機密情報が開示されるわけではないからです。しかし今年はランサムウェアの攻撃時に認証情報の漏洩が確認されたこともあり、ランサムウェアによる侵害がより顕著になっています。また、マルウェアのインストールに加え、個人情報へのアクセスが確認されたことで「データ漏洩/侵害」とされたケースもあります。

ランサムウェアは、分析にかけられたマルウェアの固有サンプルの3.5%を占めており、全体としてはそれほど大きな数字ではありません。インシデントのシミュレーションデータでは82%というかなり良好な検出率を示していますが、1年間で少なくとも1つのランサムウェアが18%の組織でブロックされています[14]。しかし、前述したように実際のインシデントやデータ漏洩/侵害ではランサムウェアの存在が大きく現れています。

これは、左のコラムの生存バイアスのカテゴリー2に該当します。これは大きな問題であり、データはこの種のマルウェアからの保護が組織内に不足していることを示していますが、阻止することは可能です。このマルウェアが成長を続けている理由の1つとして、攻撃者がランサムウェア攻撃を容易に開始できることがあげられます。ハッキングフォーラムや闇市場のランサムウェア関係のスレッドでは、「サービス」という言葉が出てくるスレッドが7%あり、これは攻撃者が自ら開発する必要がないことを示唆しています。彼らは単にサービスをレンタルし、くつろいだり、猫のビデオを見たりして戦利品が入ってくるのを待つだけなのです。

大きな問題がさらに大きくなっています。

ドロッパーとトロイの木馬

先に指摘したようにトロイの木馬は、いまだにマルウェアの上位5種類には入っているものの、時間の経過とともに減少しています。しかし、そのバックドアや遠隔操作機能は高度な攻撃者が操作し、複雑なキャンペーンで目的を達成するための重要な機能であることに変わりはありません。ダウンローダーは、ネットワークからこの種のマルウェアを取り込むためによく使われる方法であり、マルウェアサンプルの19%を占めていました。19%はバックドアに分類され、12%はキーロガーでした。

ドロッパーとトロイの木馬は、生存バイアスのコラムではカテゴリー3に分類されるようです。これらはマルウェアではかなり頻繁に目にしますが、必ずしもインシデントやデータ漏洩/侵害の件数が多いとは限りません。この理由として、この種のマルウェアのうちコモディティ化された粗悪なバージョンをブロックできるようになったことで、素質のない攻撃者がスマッシュ＆グラブ戦術に移行してきているということが考えられます。さらに、産業界のサービスのほとんどがWebインターフェースに移行したことで、トロイの木馬の攻撃対象が狭くなったということも考えられます。

14 ランサムウェア攻撃につながるようなインシデントは、マルウェアが顕在化する前に阻止することができるので、これは過小評価の可能性があります。

脆弱性を悪用したマルウェア

ドロッパーやトロイの木馬がカテゴリー3の例だとすると、脆弱性を悪用するマルウェアはカテゴリー4に該当します。それらは、図16のマルウェアの種類においては最下位にランクされています。図25（後述する「ハッキング」セクション）では、脆弱性を悪用するマルウェアは、すでに比較的少なくなっているハッキングよりもさらに稀であることを示しています。この脆弱性を突いたエクスプロイト攻撃は現在も発生していますが（特に、「ハッキング」セクションの図22に示す数値の低い個所に対して）、組織が合理的なパッチプロセスを実施していて、国家レベルの攻撃者の標的にされていないのであれば、他の種類の脅威に時間を割いた方が良いかもしれません。

暗号通貨マイニング

暗号通貨マイニングのマルウェアは、カテゴリー4に分類されます。データ漏洩/侵害の全体でマルウェアの占める割合はわずか2.5%、インシデントで占めるマルウェアの割合はわずか1.5%でした。約10%の組織は、1年のうちどこかの時点で暗号通貨マイニングを受け取り、ブロックしています[15]。

データ漏洩/侵害のシミュレーションデータによると、暗号通貨マイニングマルウェアのブロック率の中央値が非常に高かったことを示しており、何が起きているのかを知る手がかりとなっています。もう1つの有効な理論は、認証情報が盗まれたクラウドインフラ上で実行されているインスタンスでない限り、暗号通貨マイニングの発生が「インシデント報告」のレベルにまで達していないということです。このようなケースでは、組織に多大なコストがかかる上、攻撃者が自宅で見つける小銭よりも稼ぐことができません。

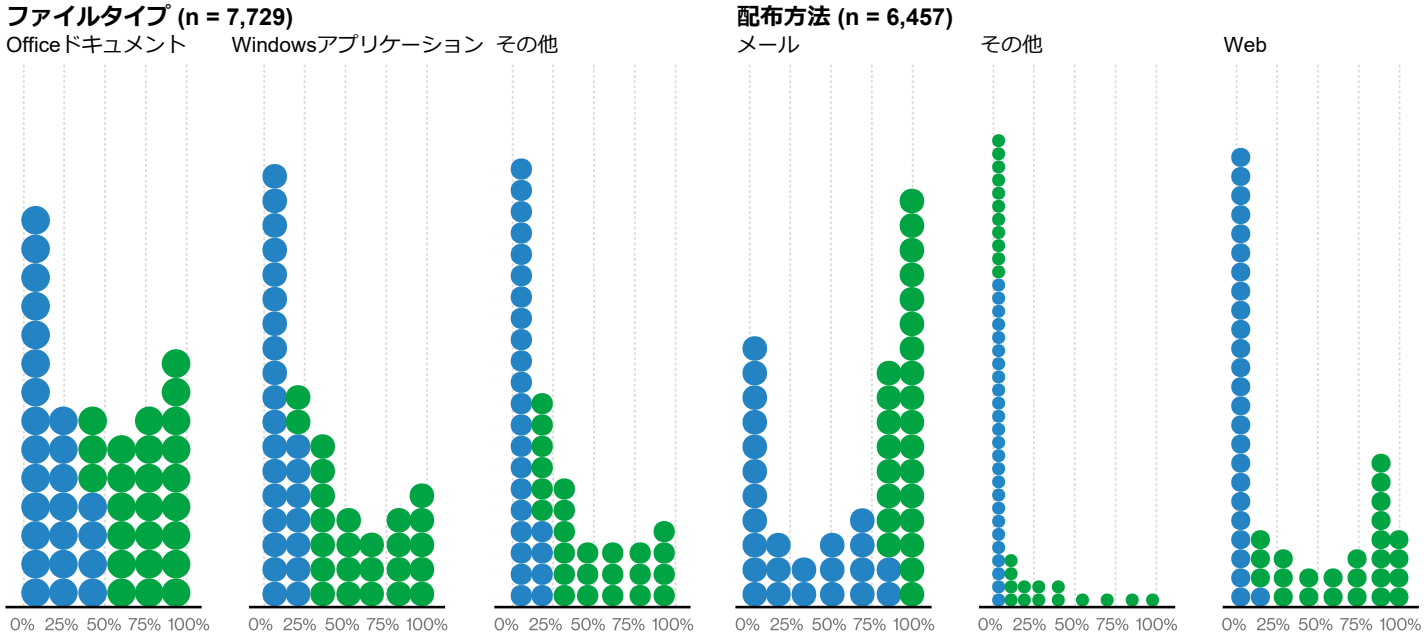


図18. よく見られるマルウェアのファイルタイプと配信方法

15 マルウェアが顕在化する前にインシデントを阻止することで潜在的な過小評価があると思われます。

マルウェアの配信

最後に、今年度はマルウェアの配信方法についてもう少し掘り下げてみました。マルウェアのファイルタイプとしては、依然としてOffice文書やWindows®アプリが選択される傾向にありますが、「その他」のカテゴリーも比較的大きくなっています。マルウェアのほとんどは依然としてメールで配信されていますが、Webサービス経由で配信されるものは少なく、その他のサービスで配信されるものはほとんどありません（検出した限り）。

図18から分かることは、「平均」は実際にはそれほど多くの企業を表しているわけではないということです。例えば、約22%の企業では、メール経由でマルウェアを取り込んだ企業はほとんどなく、一方、約46%の企業では、ほとんど全てのマルウェアがメール経由で取り込まれています。マルウェアのファイルタイプのグラフでOffice文書の箇所を見ると、約0%の組織が急増している以外、他のドットの積み上げ高さはほぼ同じであり、このタイプのマルウェアがほぼ一様に分布していることが分かります。組織がOffice文書として受け取るマルウェアの割合を決定しようとする場合、データに基づいてそれを求めるのは、その数字にダーツを投げつけて当てるのと同じ程度の確率になるでしょう[16]。これは確率が低いということではなく、地図上のどこにでも存在していることを示しています。

地図といえば、図19からは、組織がよく遭遇するマルウェアの他のファイルタイプを垣間見ることができます。図18のような詳細さには欠けますが、マルウェアはさまざまな形で侵入し、そのほとんどがフローリング板のようだということを視覚的に思い出させてくれます。ありがたいことに、先に述べたように、マルウェアがインシデントやデータ漏洩/侵害をもたらすことは頻繁にはありません。したがって、マルウェアに対しては可能な限りブロックができる優れたセキュリティツールを入手すれば、より差し迫った他の問題に注意を傾けることができます[17]。

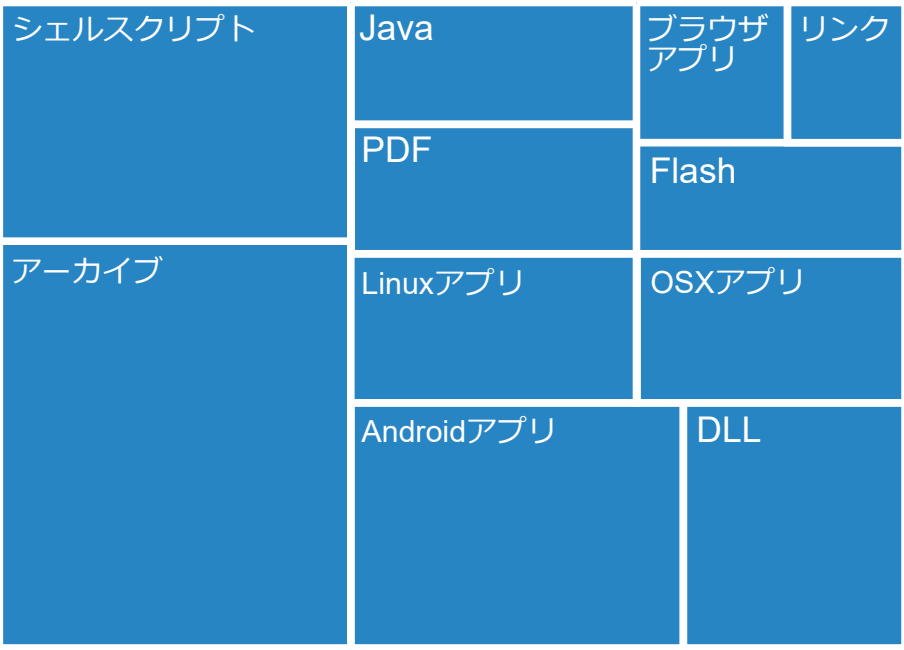


図19. その他のマルウェアファイルタイプ（n = 1,360万）

16 もちろん、確率はゼロではありません。試してみる際は、同僚や家族、ペットの周りでは鋭利なものの取り扱いに十分注意してください。
17 認証情報の窃取と使用、フィッシングとエラー。

ハッキング

ハッキングは大まかに3つのグループに分類されます。1） 盗まれた認証情報またはブルートフォース攻撃された認証情報を利用するもの、2）脆弱性を悪用するもの、および 3）バックドアおよびコマンドアンドコントロール（C2）機能を利用する攻撃です。

しかし、ハッキングや一般的なデータ侵害は（少なくとも弊社調査のデータセットに見る限り）窃取された認証情報によって引き起こされていると言わざるを得ません。ハッキングによるデータ漏洩/侵害の80%以上は、ブルートフォースか紛失または窃取された認証情報の悪用に関係しています。これらのハッキング（以下の図20）は脆弱性を突いたエクスプロイト攻撃（SQLiを含む）を始め、図21に示すようにWebアプリケーションと大きく関連しています。弊社では昨年、この問題の調査に時間を費やしてきましたが、Webアプリケーションがこれらの攻撃のベクトルとなる傾向が衰えていないことを改めて認識する必要があります。これは、メールアカウントや業務関連のプロセスなど貴重なデータをクラウドに移管することに関連しています。

バックドアまたはC2（第3位にランキング）の使用は、どちらもより高度な脅威と関連しています。なぜなら、複雑な攻撃キャンペーンやデータ抜き取りは、人手による操作に勝るものはないからです。良くも悪くも、完全自律型のAHI（Artificial Hacking Intelligence）が実現するのは空飛ぶ自動車と同じく、まだ少なくとも15年は先のことです[18]。

ハッキングによるデータ漏洩/侵害の80%以上で、ブルートフォースや紛失または窃取された認証情報が使用されています。

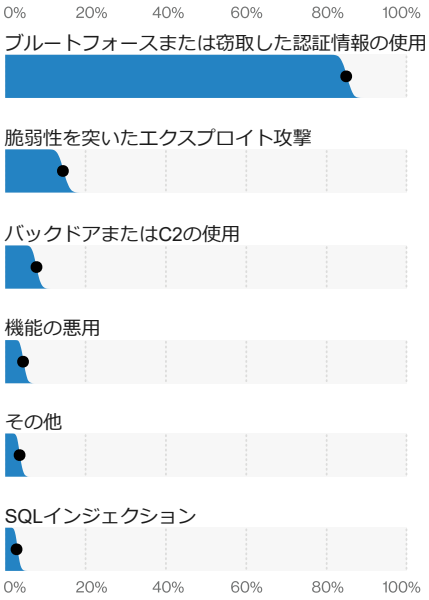


図20. 漏洩/侵害によく見られるハッキングの種類（n = 868）

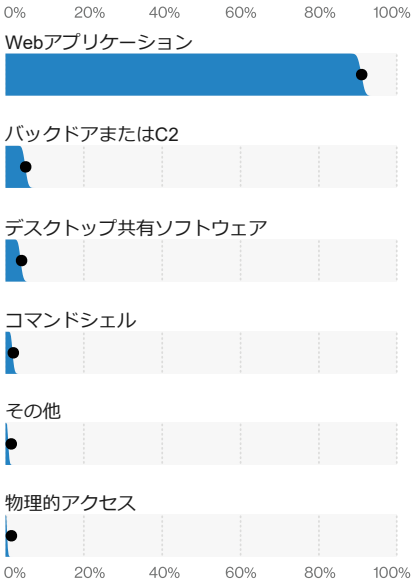


図21. 漏洩/侵害によく見られるハッキングの侵入経路（n = 1,361）

18 [引用が必要]私はこれを確かどこかのベンダーのマーケティング資料で読みました。まあ、実は読んでいないのですが、私が読んでいそうな情報じゃないですか？

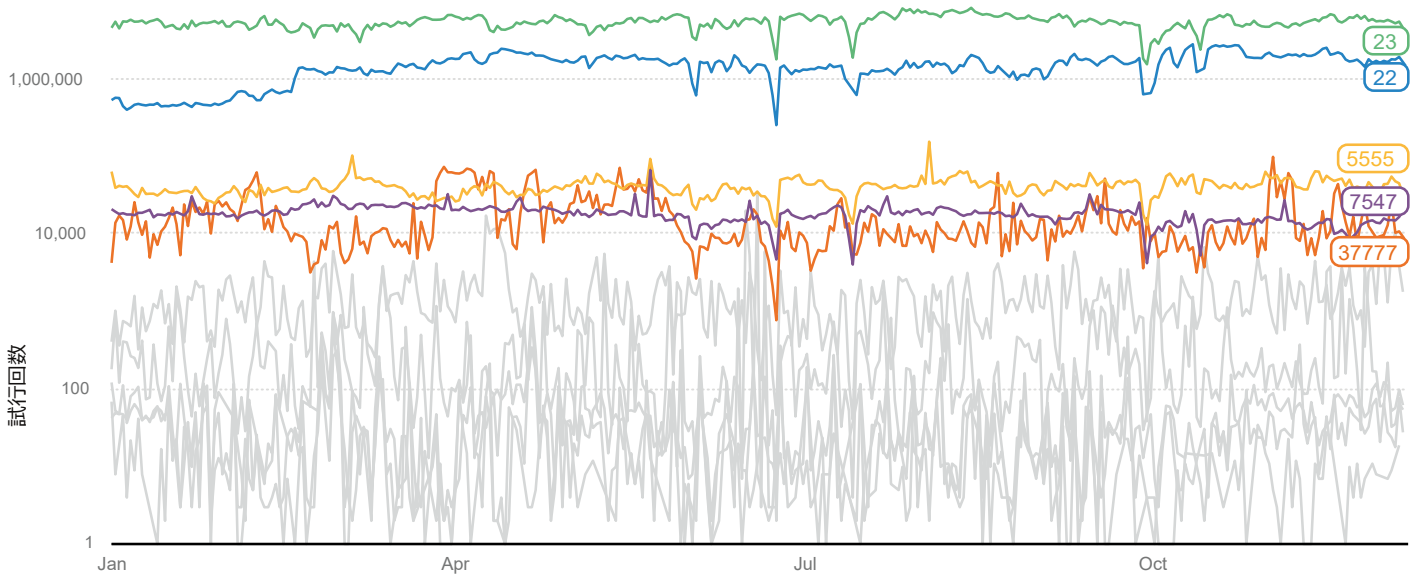


図22. ハニーポットデータにおけるポート別接続試行の経時的変化（n = 25.5億）

認証情報の使用と悪用

犯罪者は明らかに認証情報の窃取に執着していますが、認証情報があると犯行がずっと楽になるからです。「結果と分析」のセクションの冒頭にある図6からは、認証情報の悪用が急激に増加していることがはっきり見て取れます。図22は、情報提供者のハニーポットデータに基づいたポート別の攻撃者の接続試行を時間の経過とともに示しており、このトピックについて別の見解を提供しています。図が示すように、SSH（ポート22）とTelnet（ポート23）での接続試行は、次位のサービスのクラスタよりも2桁も上になっています[19]。ここでは、まずクレデンシャルスタッフィング攻撃の状況を確認してから脆弱性を突いたエクスプロイト攻撃の状況に移ります。

犯罪者が試みるクレデンシャルスタッフィング攻撃については、別の情報提供者のデータが明らかにしてくれています。図23[20]は、クレデンシャルスタッフィング攻撃を受けたことが認められる組織への攻撃の試行回数を示しています。お分かりの通り922,331件の中央値をピークに比較的滑らかなベルカーブが描かれています。もちろん、試行されたログイン/パスワードの組み合わせの大部分は、「admin/admin」や「root/hunter2」のような複雑なものですが、弊社のインシデントデータセットによると、これらの持続的な攻撃は時間が経つにつれ成功率が上がっています。

認証情報の漏洩がクレデンシャルスタッフィング攻撃をもたらしているのでないかという疑問を抱かれる方もいらっしゃるかもしれません。認証情報の漏洩のデータセットと弊社のクレデンシャルスタッフィング攻撃のデータを比較してみました。図24を見ると答えは「いいえ」であることが分かります[21]。認証情報の漏洩とその翌週に発生したクレデンシャルスタッフィングの件数とは基本的に関係がないことが判明しています。むしろ、これは多かれ少なかれ一貫したペースで、以下のようなプロセスをあらゆるところで行っているように思われます：漏洩情報を入手し、ディクショナリに追加し、インターネットでブルートフォースを試し続ける。この手順が何度も繰り返されます。

19 両者は近いように見えるかもしれませんが、それは対数目盛です（https://en.wikipedia.org/wiki/Logarithmic_scale）。
20 このグラフが紛らわしい場合は、「凡例と定義」セクションにあるドットプロットの説明を参照してください。
21 この「いいえ」という結果をもたらした実験が好きな方はどこかにいませんか？同僚の皆さん、科学に乾杯しましょう！

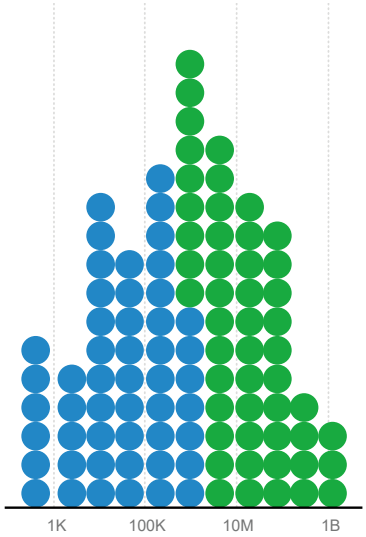


図23. 年間の組織あたりの認証情報の試用 (n = 631)

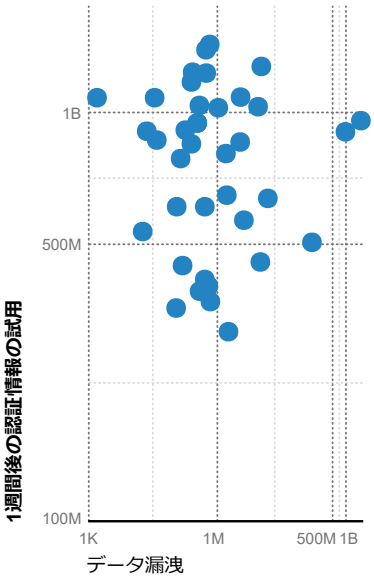


図24. 認証情報の漏洩と1週間後の試用との関係。R^2 = 0.006 (n = 37)

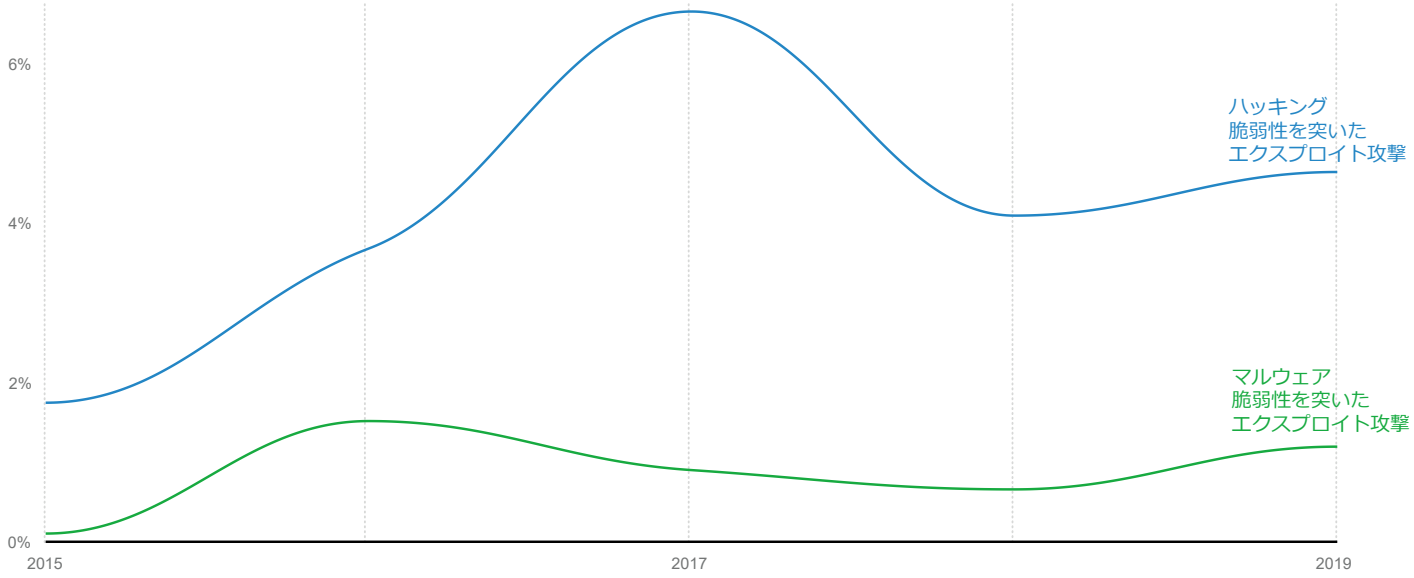


図25. 漏洩/侵害における脆弱性を突いたエクスプロイト攻撃の経時的変化

脆弱性を突いたエクスプロイト攻撃

脆弱性は、情報セキュリティにおいて高い占有率を示します。しかし、「マルウェア」セクションでの生存バイアスに関する話を思い出してみると、脆弱性はカテゴリー1よりも3の状況の方が多いのです。多くの脆弱性が発見され、また多くの脆弱性が組織のウイルススキャンやパッチ適用によって検出されていますが実は、図25に示すように、データ侵害に脆弱性が悪用されている割合はそれほど多くはありません。脆弱性を突いたエクスプロイト攻撃は、データ侵害ハッキングの種類では2位ですが、過去5年間でDBIRが判明したインシデントの中では大きな役割を果たしていませんでした。実際、2017年にハッキングの種類としてのピークは5%強でした。ベライゾンのセキュリティ情報とイベント管理（SIEM）のデータセットでは、ほとんどの組織において脆弱性を突いたエクスプロイト攻撃に関わるアラートは2.5%以下でした[22]。

しかし、だからといって攻撃者が脆弱性を突いたエクスプロイト攻撃を試してみないわけはありません。明らかに攻撃者はそこら中にいるわけで、パッチが適用されていないものをインターネット上に放置しておけば、攻撃者はそれを見つけて彼らのインフラストラクチャに取り込んでしまいます[23]。インターネット上でも組織内でも、新しい脆弱性とその蔓延についてよく耳にします。新しい脆弱性が発見されるたびに、インターネット全体が脆弱になるのでしょうか[24]？また、問題を拡大させているパッチ未適用の脆弱性は、各社のそれぞれのシステム内にも存在している可能性が高いのでしょうか？

これらが本当かどうかを検証するために昨年の夏、弊社でちょっとした調査を行いました[25]。公開IPアドレスについて、2019年に発見されたEximの脆弱性に脆弱なIP[26]とランダムに選ばれたIPでホストされている2台のサーバーを調査しました。図26にあるようにEximの脆弱性に晒されているホストは、10年前のSSHの脆弱性について、ランダムに選ばれたサンプルよりもはるかに高い頻度で脆弱性が認められました[27]。

これから分かることは、これらのサーバーでパッチが適用されていなかったのはEximの脆弱性だけではなかったということです。何もパッチが当てられていなかったのです。ほとんどの場合、インターネット全体としては、新しい脆弱性が見つかるたびに安全性が低下しているようには見えませんが、少なくともパッチ管理に長けた組織がシステムを更新した後は安全性が低下することはありません[28]。Usenetのh4x0rの友人からもらった10年前のl33tの脆弱性を悪用するのと同じくらい簡単にこれらの脆弱性のあるサーバーを悪用できるのです。

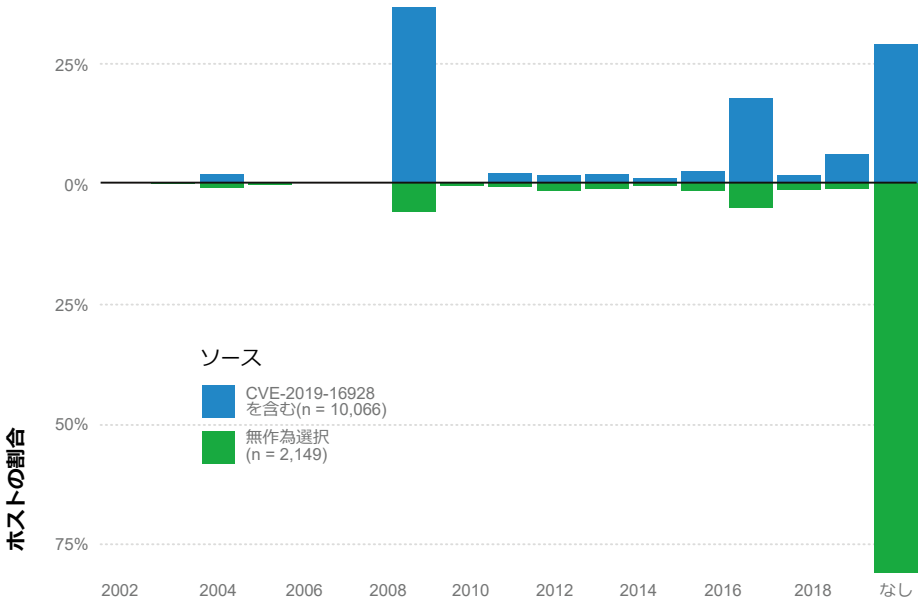


図26. その他の古い脆弱性についてEXIM CVE-2019-16928を含むインターネット接続ホストと無作為に選択したホストを比較

22 買い手がリスクを負うのです。このために、MITRE ATT&CKに既存の協力者マッピングを使用し、付録Bで説明したVCAFマッピングにトレースしました。

23 もっとも、CPUのサイクルを盗むことが従来のサービスとしてのインフラストラクチャ(IaaS）よりもはるかに安価なことを示す研究はありませんが、私のクラウドサービスの最新の請求書のことを考えると、これができないわけがありません。

24 TL;DR：ほとんどの場合、そうではありません。いずれにしても長続きはしません。

25 新しい脆弱性が発見されるたびに、インターネット全体が脆弱になるのでしょうか？

26 CVE-2019-16928

27 そして基本的には、それ以降の全ての脆弱性

28 この調査をしてくれた夏季インターンのQuinnan Gillさんに感謝します。あなたは素晴らしい方です。

しかし、2つ目の質問についてはどうでしょうか。現在運用しているシステムに脆弱性がある可能性が高いのでしょうか[29]？ これを検証するために、脆弱性スキャンデータから2つのサンプルを採取しました。システムに「Eternal Blue」の脆弱性[30]がある組織と脆弱性がない組織です。図27[31]も、図26と同じ結果を示しています。Eternal Blueの脆弱性が存在していたシステムは、過去10～20年のあらゆるものに対しても脆弱性がありました。繰り返しになりますが、新しい脆弱性があるからといって、そこまで脆弱性が高くなるわけではありません。パッチを当てている組織は優先順位をつけた良好なパッチ管理体制を維持しているようです。

それでも、ここでは生存バイアスのカテゴリー4の状況にはなっていません。攻撃者は、インターネットを巡回しているときに簡単に攻撃できる脆弱性に遭遇すると、まず攻撃を試してみます。「認証情報の使用と悪用」のセクションを読んだばかりの方は図22を覚えているかもしれませんが、グラフのSSHとTelnetの線の下にあるのはポート5555（最近流行のAndroid Debug Bridge（ADB）、ポート7547（一般的なルータのRPCポート）、ポート37777（IPカメラやDVRによく使われる）の3つのサービスです（見やすくするためにハイライトしています）。比喩を交えて言えば、この場合クマは全て一括で3Dプリントされ、人間を狩るために自動化されているのでクマを追い抜くことはできないというわけです。

ですから、そのまま先へ進み現在やっていること（パッチ適用）をやり続け、「資産」のセクションにスキップして、恐らくあなたが見落としている可能性のあるものについてヒントを得てください。

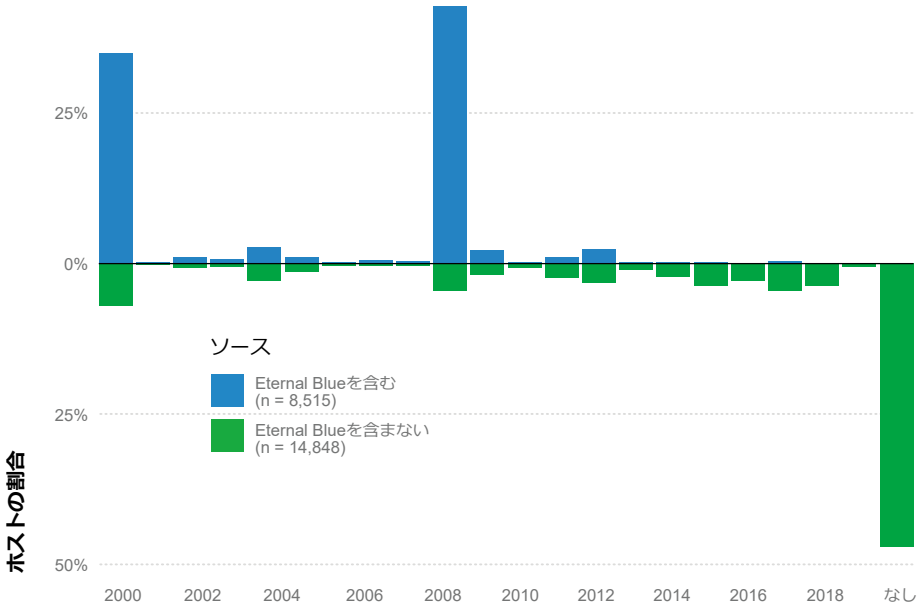


図27. その他の古い脆弱性についてEternal Blueを含むホストと含まないホストを比較

29 TL;DR：繰り返しになりますが、恐らくそうではないでしょう。パッチを当てているのであれば可能性は低いでしょう

30 CVE-2017-0144

31 ここではEternalBlueを使用し、図26ではEximの脆弱性を使用しています。なぜなら、図27のデータはCVE-2019-16928以前の可能性がある昨年度のものであるのに対し、図26の分析は夏に行われたものだからです。

ソーシャル エンジニアリング

攻撃のタイプが人間の場合、危険な臭いがするのでハッキングやマルウェア、エラーとは関わらないよう身構えることでしょう。しかし、それらに比べると「ソーシャルエンジニアリング」は、はるかに気楽な感じがします。留守番の代わりをお願いしたり、Buncoゲームの仲間に入れてもらったり、近所のバーベキューパーティに招かれたりするのと同じくらいに。しかし、その考えは間違いです。ソーシャルエンジニアリングには油断ならない態度に胡散臭いヘアスタイルがつきものです。図28は、ソーシャル攻撃のインシデントの種類が主に「フィッシング」と「なりすまし」の2つであることを示しています[32]。データ漏洩/侵害に関しては、その割合はほとんど変わらず数字が若干低くなっているだけです。

ソーシャル攻撃は、96%がメールで届き、3%はWebサイトから届きました。電話やSMSによるものが1%強で、これは「Officeドキュメント」で観察されたものと同程度です。図29を見てみるとフィッシング詐欺の被害に遭ったのは認証情報が最も多いですが、その他のデータソースも多く含まれています。フィッシングは、これまで（そして今も）攻撃者にとって成果を上げられる手法なのです。幸いなことに、クリック率がかつてないほど低く（3.4%）、報告される割合は増えてはいますが急激ではありません（図30）。

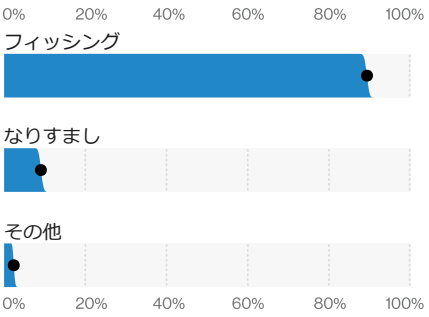


図28. インシデントによく見られるソーシャル攻撃の種類（n = 3,594）

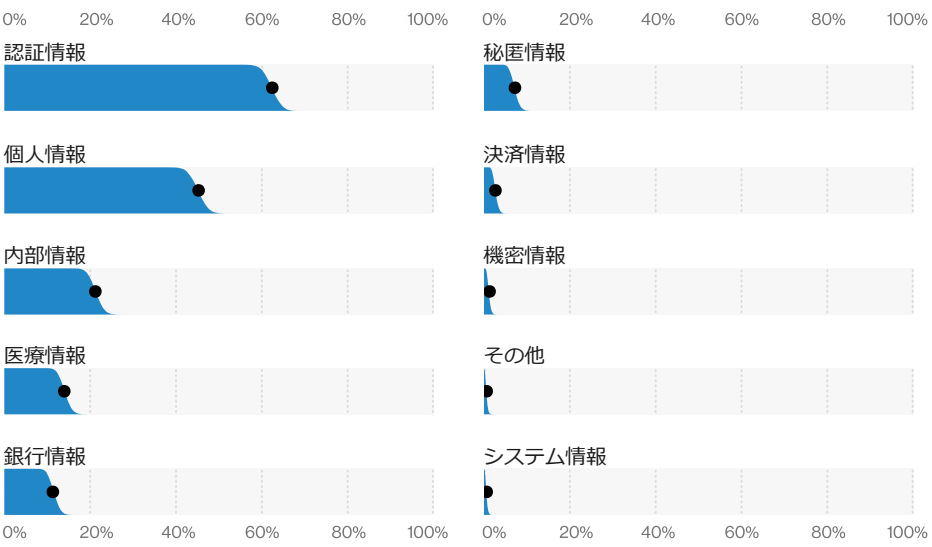


図29. フィッシングの漏洩/侵害によく見られるデータの種類（n = 619）

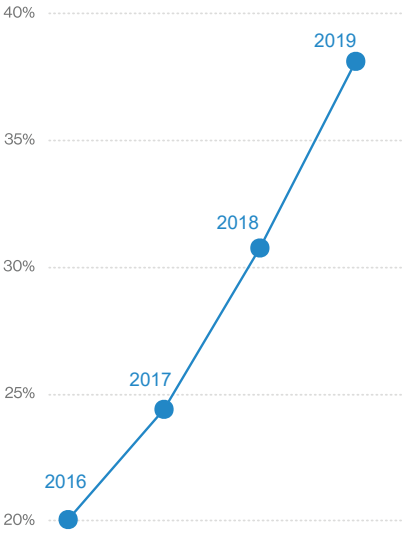


図30. フィッシングテストキャンペーンが1回以上報告された数

32 大抵はビジネスメール詐欺（BEC）ですが、メールアドレスを侵害していなくても動作することを考えると、「金銭を目的としたソーシャルエンジニアリング（FMSE）」の説明を参考にできるかもしれません。

金銭を目的としたソーシャルエンジニアリング攻撃

金銭を目的としたソーシャルエンジニアリング攻撃（FMSE）は前年に比べて増加し続けており（図31）インシデントに占める割合は少ないものの、今年度の生のデータセットでは500件以上発生しています。これらの攻撃は、純粋にソーシャルな性質を持つため、通常は「その他全て」のパターンに分類されます。国家が関与する高度な攻撃シナリオに見られるようなマルウェアの要素はなくまた、被害者のネットワークを足がかりにして執拗に攻撃を繰り返す姿勢も見られません。これらは単に「できるときにできるものを手に入れよう」という類の攻撃なのです。

これは、成果を上げるためにどこまで手を広げるかという点で攻撃者が洗練されていないわけではありません。以前はCEOやその他の役員になりすまして、従業員のW-2データを要求していました。今では戦術を大きく変え、現金を直接要求するようになってきました。何故わざわざデータを現金化して時間を無駄にするのか？非常に非効率的です。なりすましのシナリオを工夫してその試みに信憑性を持たせようとしているのは、彼らがどれだけ仕事に長けているかの現れです。

昨年、FBIのインターネット犯罪苦情センター（FBI IC3：Internet Crime Complaint Center）に報告されたインシデントについて、被害額の中央値を調べたところ、ビジネスメール詐欺（BEC：Business E-mail Compromise）に関しては、ほとんどの企業が1,240ドルか44,000ドルの損失を被っており、後者の損失額の方がやや頻度が高くなっていました（図32）。

また、昨年のDBIRで、「IC3のリカバリーアセットチーム（RAT）がBEC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詐欺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」と述べました。RATはこの指標の記録を継続しており、今年度はわずかに改善し、52%が99%以上の被害額を回収し、回収できなかったのはわずか8%でした。

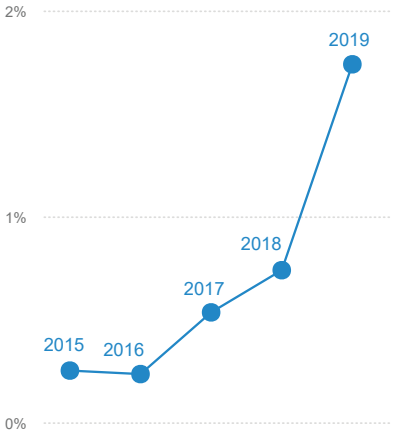


図31. インシデントにおける金銭を目的としたソーシャルエンジニアリング（FMSE）の経時的変化

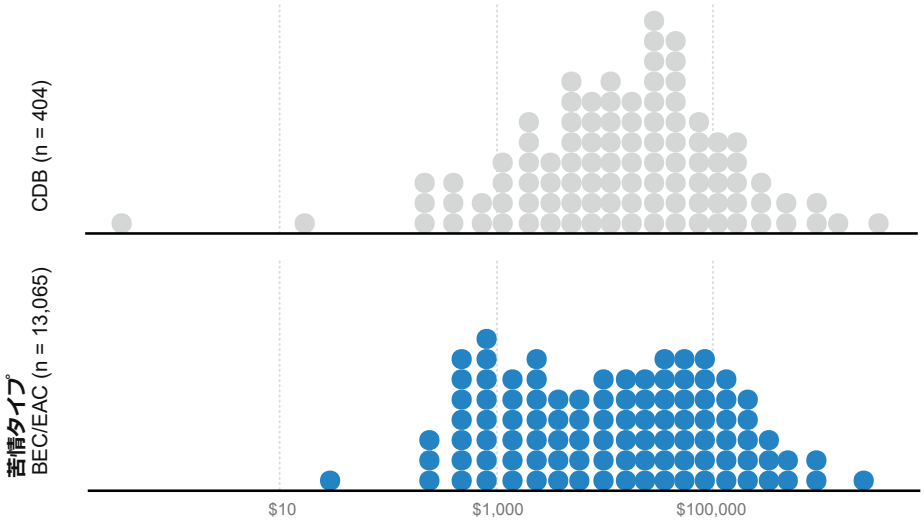


図32. 企業のデータ漏洩/侵害 (CDB) およびビジネスメール詐欺/(個人の)メールアカウント詐欺(BEC/EAC)による損失額(損失ゼロの苦情を除く)

資産

図33は、資産の状況の概要を示しています。サーバーが中心となって増加が続いています。これは主に産業界がWebアプリケーション（図34では最も一般的な資産の種類）へとシフトし、SaaS（Software as a Service）として提供されるシステムインターフェースを持つようになったことによるものです。会計のボブが作成した素晴らしいマクロを備えた7年前のスプレッドシートは過去のものとなりました。「人[33]」が2年連続で2位を獲得していますが、この期間にソーシャル攻撃がいかに関わり続けているかを考えると、驚くことではありません。

キオスクと端末は昨年に引き続き減少しています。これは主に攻撃者が実店舗ではなく、「カードを提示しない」小売店に攻撃の焦点を移したことによるものです。

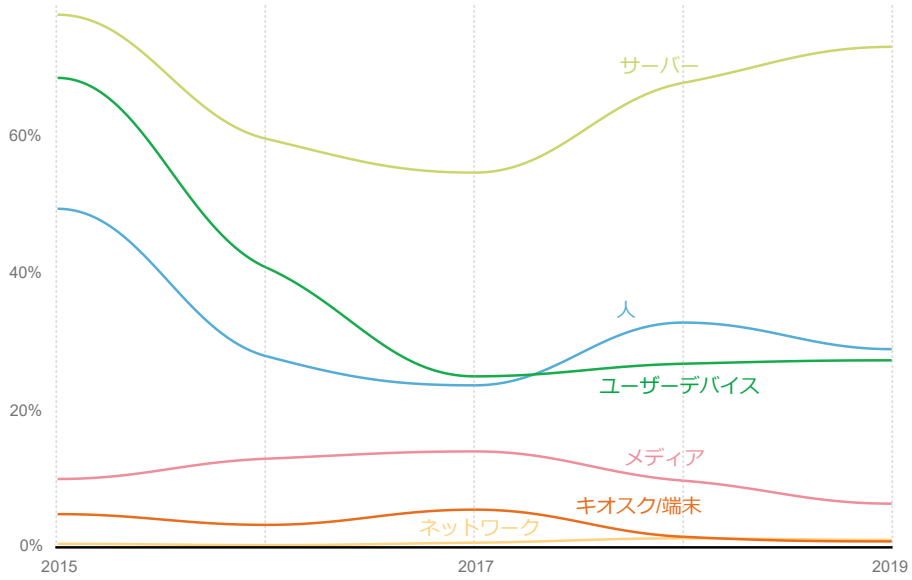


図33. 漏洩/侵害における資産の経時的変化

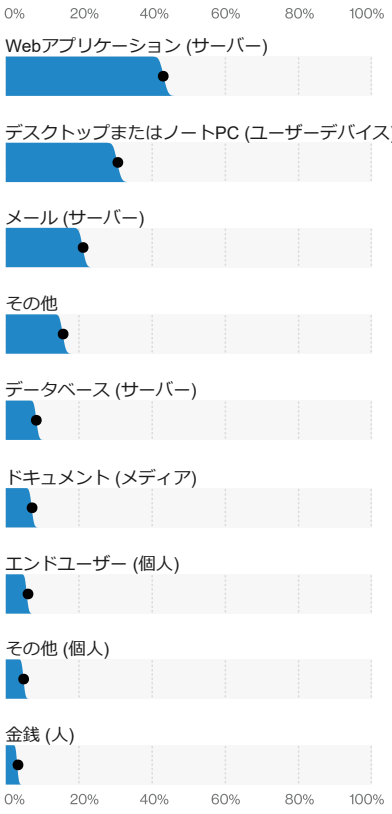


図34. 漏洩/侵害によく見られる資産の種類（n = 2,667）

33 人を資産と考えるのは奇妙で、人間性を奪うようなものかもしれませんが、これはソーシャルエンジニアリングの要素を持つ攻撃の影響を受けた当事者を表すものです。人にもセキュリティ属性があります。

非現実的な考え

クラウド資産が今年度のデータ漏洩/侵害に関与したのは約22%ですが、インシデントデータセットの報告では依然とオンプレミス資産が71%[34]を占めています。クラウド資産のデータ漏洩/侵害では、73%がメールサーバーやWebアプリケーションのサーバーに関係していました。さらに、これらのクラウド侵害の77%は、認証情報の漏洩/侵害に関わるものでした。これは、クラウドの現状のセキュリティに落ち度があるというよりは、サイバー犯罪者が被害者への最短のルートをすばやく見つけ出す傾向にあるということを示しています。

情報技術と運用技術との比較

昨年、含み資産の追跡を開始しましたが、予想よりもインサイトが浅かったことが分かりました。そこで今年度は、インシデントに関係する資産の情報技術（IT）と運用技術（OT）の比較の追跡を開始しました。来年以降、より包括的な分析ができるようになることを期待していますが、今のところ弊社の調査結果には特に驚くようなものはありませんでした。データ漏洩/侵害の96%がITに関係していたのに対し、4%がOTに関係していました。4%という数字は大きくないように聞こえるかもしれませんが、生産手段をOT機器に依存している業界においては、相当の懸念材料となることは間違いありません。

モバイルデバイス

今年度は、弊社のデータセットにおいて1000以上の紛失ケースがモバイルデバイスに関わっていたことが分かり、冷蔵庫で見つけたプラムをいくつか食べながら、自分たちのビジネスのことに気をもんでいました。インシデントでのこの信じられないほどの急増をこの重要な調査結果の1つにすることになりますが、かなり確信しているのは「流行りのコーヒーショップで仕事用の携帯電話を忘れる」のは、何も2019年に発明された新しい技術ではないということです。どうやら、データ収集の一部がここで非難されているようです。数人の外部協力者の下、データ収集プロトコルを更新しました。その結果がこれです。これらのエラーのケースは、モバイルデバイスで発生したインシデントの約97%を占めていました。

残りの3%は非常に興味深いものです。これらのインシデントは、スパイ活動の動機と金銭的動機とほぼ均等に分かれています。しかし弊社データの全体の内訳では、金銭的動機が64%、スパイ活動が5%です。金銭的動機のものは窃盗からなりすましのためのツールとしてのデバイスの使用までさまざまですが、スパイ活動に関連するケースは、マルウェアをベースとしたモバイルデバイスの侵害から国家が関与する高度で執拗に繰り返される攻撃やデータ抜き取りまでのケースに限られています。

34 あとの残りは、人的資産など、クラウドが適用できないようなデータ漏洩/侵害でした。

資産管理

「ハッキング」のセクションで、大きな新しい脆弱性の影響を受けやすいホストは多くの古い脆弱性に対しても無防備である傾向があることを述べました。この発見は、パッチ適用に効果があるように見える一方で、資産管理ができていない可能性があることを示唆しているという点でやや両刃の剣のようなものです。弊社が見つけた中で最も多いケースでは、インターネット上で見えるパブリックIPの約43%を組織が1つのネットワークで運用していました[35]。しかし、組織が占有しているネットワークの数は5つが最も多く、全体の半数が7つ以上のネットワークに存在していることが分かりました（図35）。これらのネットワークを全て掌握していないと資産管理に問題が出るかもしれません。したがって、単純に資産管理の問題ではなく把握していない資産の脆弱性管理の問題なのかもしれません。

90%以上の組織ではインターネットに接続しているホストの10%未満に重大な脆弱性がありました。また、半数の組織ではインターネットに接続しているホストに脆弱性があったのは1%未満でした（図36）。つまり脆弱性は、一貫した脆弱性管理をゆっくりと行った結果ではなく、むしろ資産管理の欠如が原因である可能性が高いことを示唆しています。

図35. 組織あたりのネットワーク追加数 (n = 86)

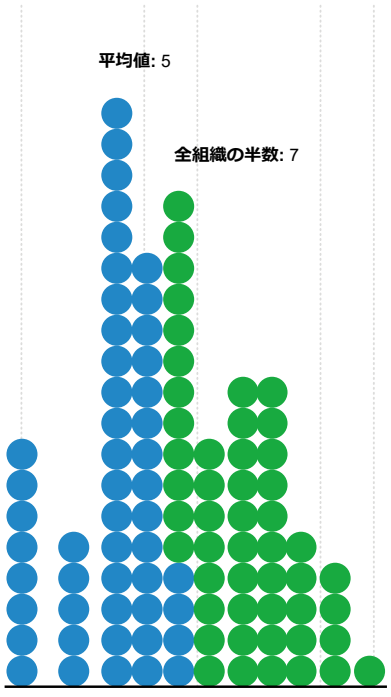
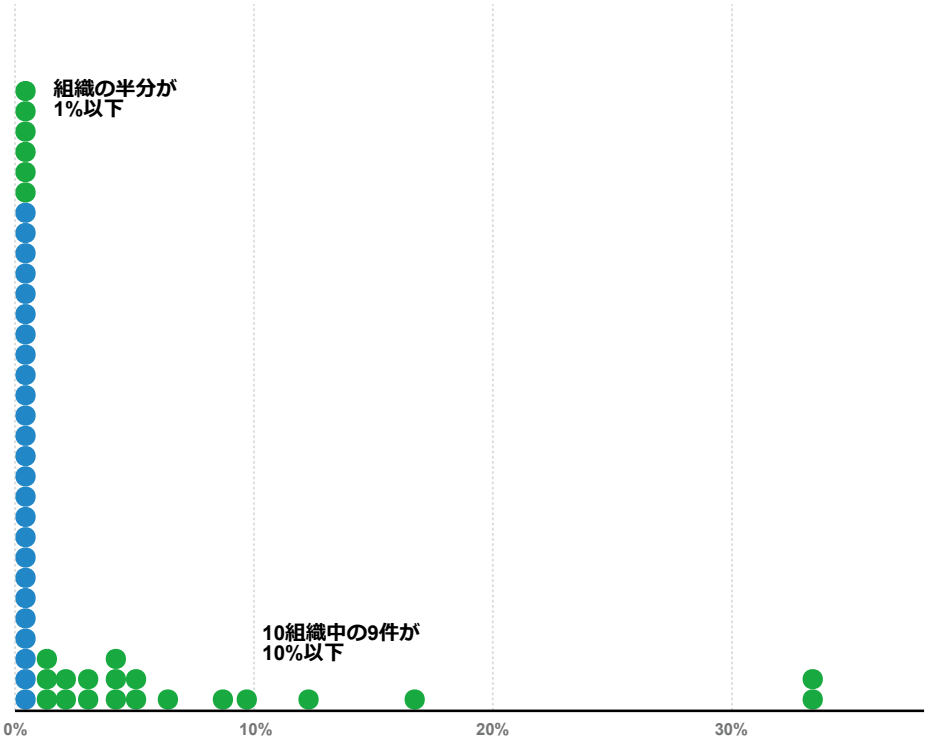


図36. 重大な脆弱性がある組織のパブリックIPの割合 (n = 110)



35 「ネットワーク」とは、自律システム番号（ASN）で表される自律システムを意味します。https://www.apnic.net/get-ip/faqs/asn/

属性

図37に示すように個人の機密データへの侵害は、侵害で影響を受けた属性の中でも群を抜いています。しかし、これにはメールアドレスが含まれており、悪意のあるデータの流出だけでなく、「良性の」エラーによるものも含まれていることに留意してください。ハッキングとエラーのワンツーパンチでメールアドレス（ひいては個人情報）が先頭に立っているのです。確かに個人情報は単なるメールアドレスをはるかに超えるものですがメールアドレスは個人情報が存在する場所を示します。

2位には認証情報が入っていますが、このトピックについてはすでに十分に説明しているので驚くことではありません。次に登場するのは「行動の変化」で、これは被害者の個人資産の完全性に影響を与えるソーシャル攻撃がもたらす結果です。最後にソフトウェアインストールの完全性に影響を与えるマルウェア関連の侵害が見られます。

図37のもう1つの注目すべき観察は、銀行情報と決済情報がほぼ同じくらいであることです。5年前は決済情報の方がはるかに多かったのですが、銀行情報の漏洩は比較的横ばいで推移しており、決済情報はそれと同じレベルまで減少し続けた結果です。

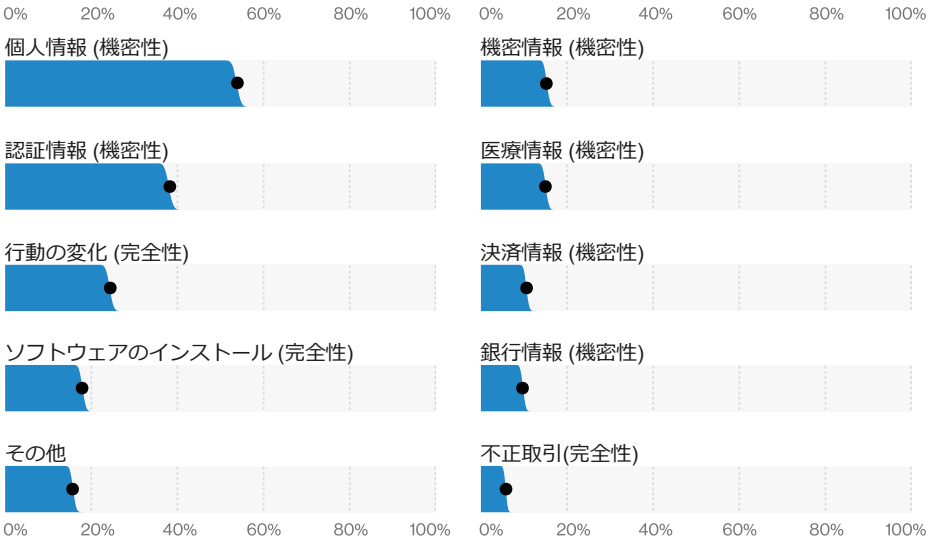


図37. 漏洩/侵害によく見られる攻撃を受けた属性の種類（n = 3,667）

メールアドレスの漏洩

今年度の報告書では、メールアドレスが個人識別情報（PII）であり、個人情報が侵害の最も多いデータの種類であることを考慮して、過去10年間に見られたメール漏洩についていくつかのケースをもう少し詳しく調べてみました。図38では、最も侵害されているメールのトップレベルドメイン（TLD）を知ることができます。ちなみに、「その他」のカテゴリーには1%未満のメールのTLDが含まれています。

.comは流出したメール全体の約59%を占めているドメインなので、その部分に少し注目してみました。最初の150のドメインを調べたところ、ほとんどがメール登録サービスであることが分かりました。これは侵害の約97%を占めており、侵害されたメールのほとんどが従業員の会社のアドレスではないことを示唆しています。しかし、重要でない残りの3%は、数千万のメールアドレスで構成されていました。

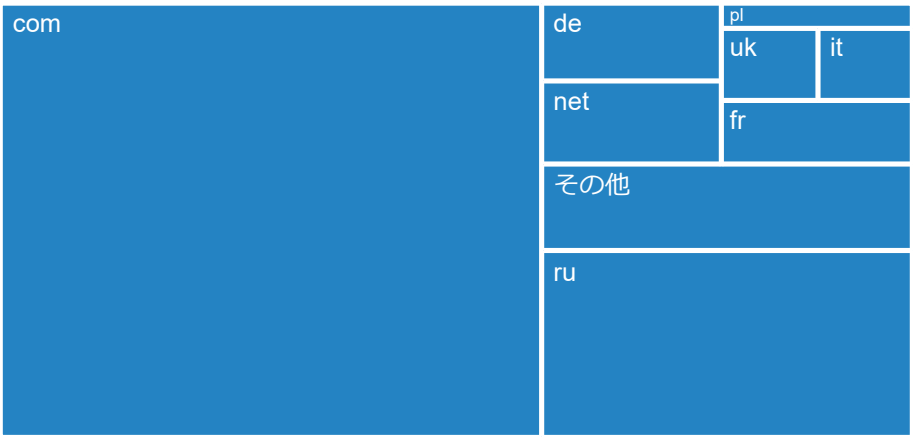


図38. 漏洩したメールにおけるトップレベルドメイン（TLD）の普及率 (n = 39.4億)

その属性は何を犠牲にしているのか？

FBIのIC3への苦情で報告されているように、今年度被害額が最も多かったのは32,200ドルで、昨年度の約29,300ドルから増加しています。それはまだ基本的には中古車の範囲内であり、誰もが大金を失うことを望んでいませんが、この数字はさらに悪くなる可能性があります。

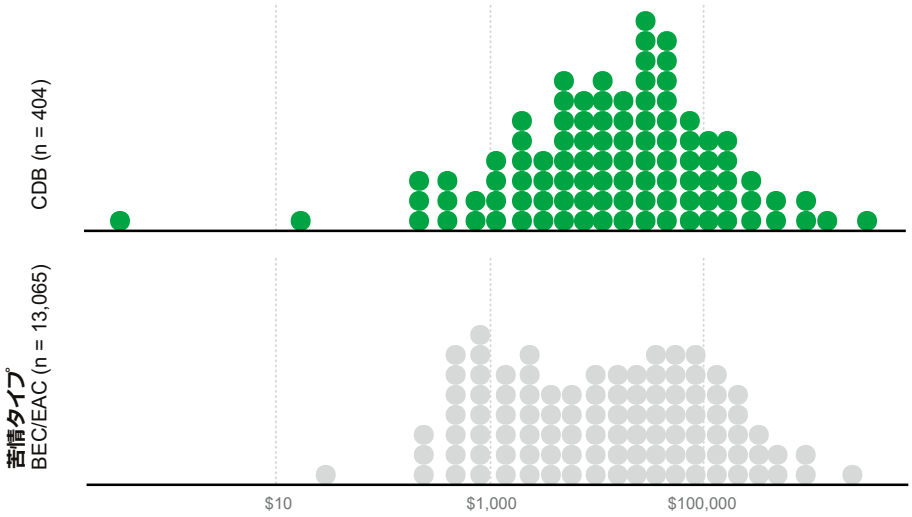


図39. 企業のデータ漏洩/侵害 (CDB) およびビジネスメール詐欺/(個人の)メールアカウント詐欺(BEC/EAC)による損失額(損失ゼロの苦情を除く)

攻撃パスはどれだけあるのか？

私たちは、インシデントやデータの漏洩/侵害をある時点での出来事と考えがちです。指を鳴らすと攻撃者の攻撃は全て完了し、盗まれたデータは攻撃者のサドルバッグの中にあり、彼らは町を去って夕日の中へと消えていくのではないかと。しかし、実際はそうでないことも分かっています。本報告書で調査された攻撃の多くは、複雑さの点ではピストル強盗と大列車強盗の間に位置します。幸いなことは、防御側がこれを有利に利用できるということです。

図40を見れば分かるように、攻撃にはさまざまな形状や規模のものがありますが、そのほとんどは短いものでステップ数が少ないものが多いです（図40から、攻撃のステップ数が4から6の間で少なくなっているのが分かります）。長いものは、ハッキング（青）とマルウェア（緑）による侵害であり、攻撃者が組織的にネットワーク経由で侵入し、持続性を延ばしていくため、機密性（真ん中）と完全性（下位）が侵害される傾向があります。攻撃者が侵害に至るまでの径路で通過しやすい「領域」（脅威・攻撃は色、侵害されている属性は位置）を知ることの利点は、攻撃者を迎撃する場所を選択することで先に優位に立てることです。攻撃者の最初の攻撃や最後の攻撃を阻止したい場合もあるでしょう。彼らの側に近づきたくはないので、「オールドタウンロード」を聞く必要はありません。これらの選択肢は、いずれも対応戦略に応じて理解できます[36]。

36 あるいは、どこにでもいるイヤーワームに感染しやすいかどうか。

図40. インシデントの攻撃経路 (n = 652。2件の漏洩/侵害でそれぞれ77ステップと391ステップ。図示なし)

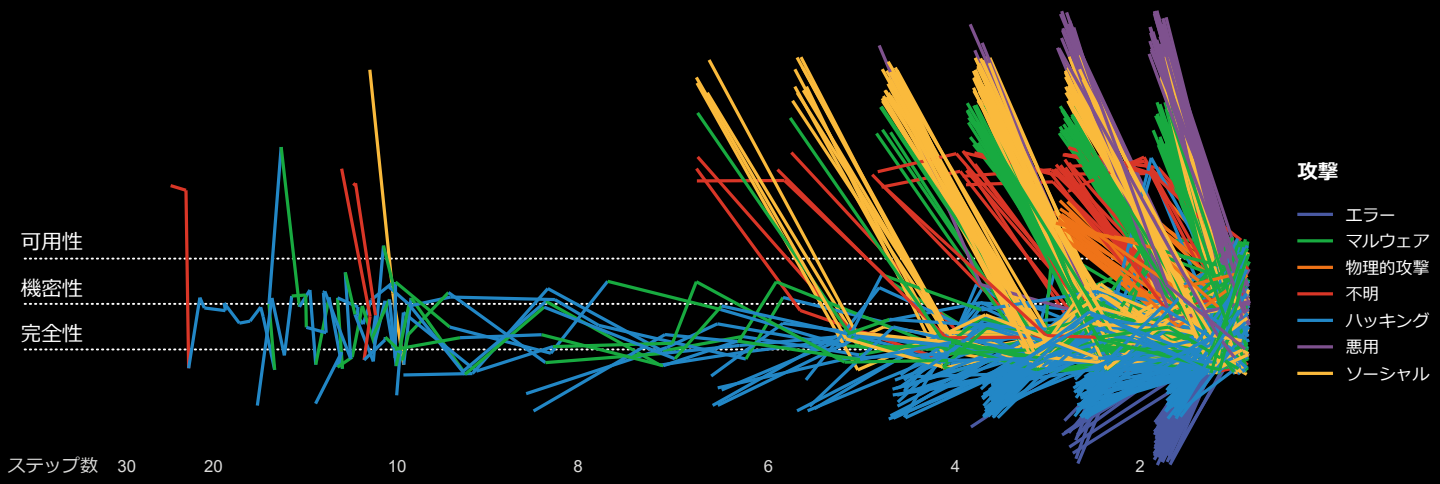


図41と42は、次の防御のための優位性を私たちに教えてくれています。攻撃者は短い攻撃パスを好み、長いものを試すことはほとんどありません。つまり、攻撃者が取らなければならないアクションの数を増やすための策を私たちが簡単に投じることができれば、それによってデータが持ち出される機会を大幅に減らすことができるのです。ここまでで認証情報の盗難と使用の重要性と普及率については理解していただけたでしょうか。二要素認証が不完全であることは認めますが、攻撃者にステップを追加することは役立ちます。2つのステップ（テキサス・ツー・ステップ）と3つまたは4つのステップ（ワルツまたはタンゴ）の違いは、防御戦略において重要になるでしょう。

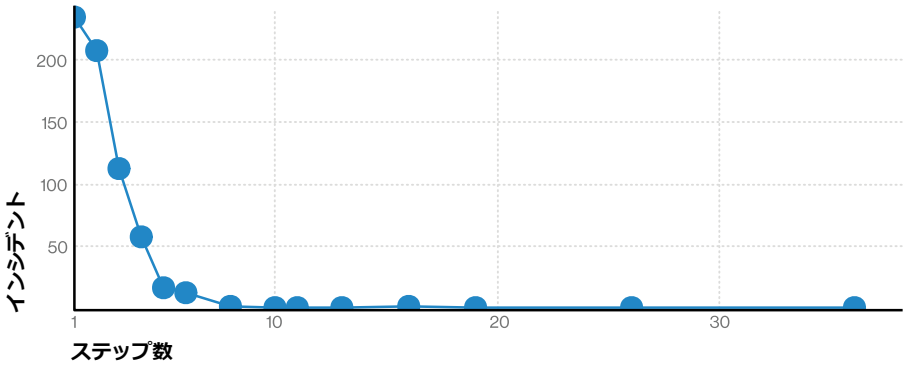


図41. インシデント1件あたりのステップ数 (n = 654。2件の漏洩/侵害でそれぞれ77ステップと391ステップ。図示なし)

2ステップ（テキサスツーステップ）と3ステップまたは4ステップ（ワルツ）の違いが防御戦略では重要になります。

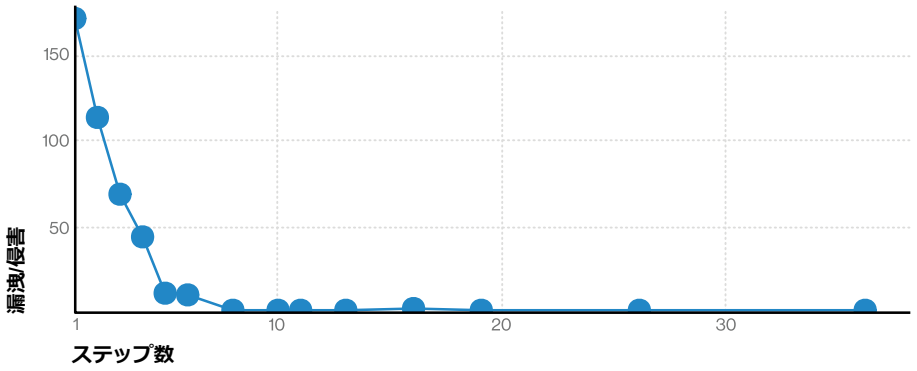


図42. 漏洩/侵害1件あたりのステップ数
(n = 429。2件の漏洩/侵害でそれぞれ77ステップと391ステップ。図示なし)

ではここで深呼吸をして図40を見てください。これは、蝶が報告書の上に何か吐いたのではありません。この図が伝えたいことを全て理解しようとしなくても構いません。その代わりに、この図のコンセプトを解説いたします。この抽象的な芸術作品には、数百の侵害行為のそれぞれについての線（「攻撃パス」）が含まれています。数字を棒グラフで視覚化するように、このグラフは攻撃者が取った攻撃パスを簡単に表したものです。

各色の付いた線分（「ステップ」）は、侵害された関連属性とともに、攻撃者が取った行動を表しています。各ステップの色はそのステップのVERIS攻撃を表し、ステップが終了する位置は侵害された属性を表します。しかし、この図を理解するための本当のトリックは、攻撃パスが左から始まり右に移動するということです。パスの最初の一歩は、グラフの上または下のいずれかから踏み出され（どこかから来なければならないので）、適切な属性に「着地」します。

例えば、グラフ上方の横軸4から始まり、グラフの下の位置で終わる黄色いステップの場合は、4つのステップのインシデントであり、ソーシャル攻撃を開始して、「完全性」属性を侵害したという意味です。また、エラーアクション（グラフ下方から始まる濃い青の線）は、通常、非常に短いパスの一部を形成し、「機密性」属性に着地していることにも注目してください。

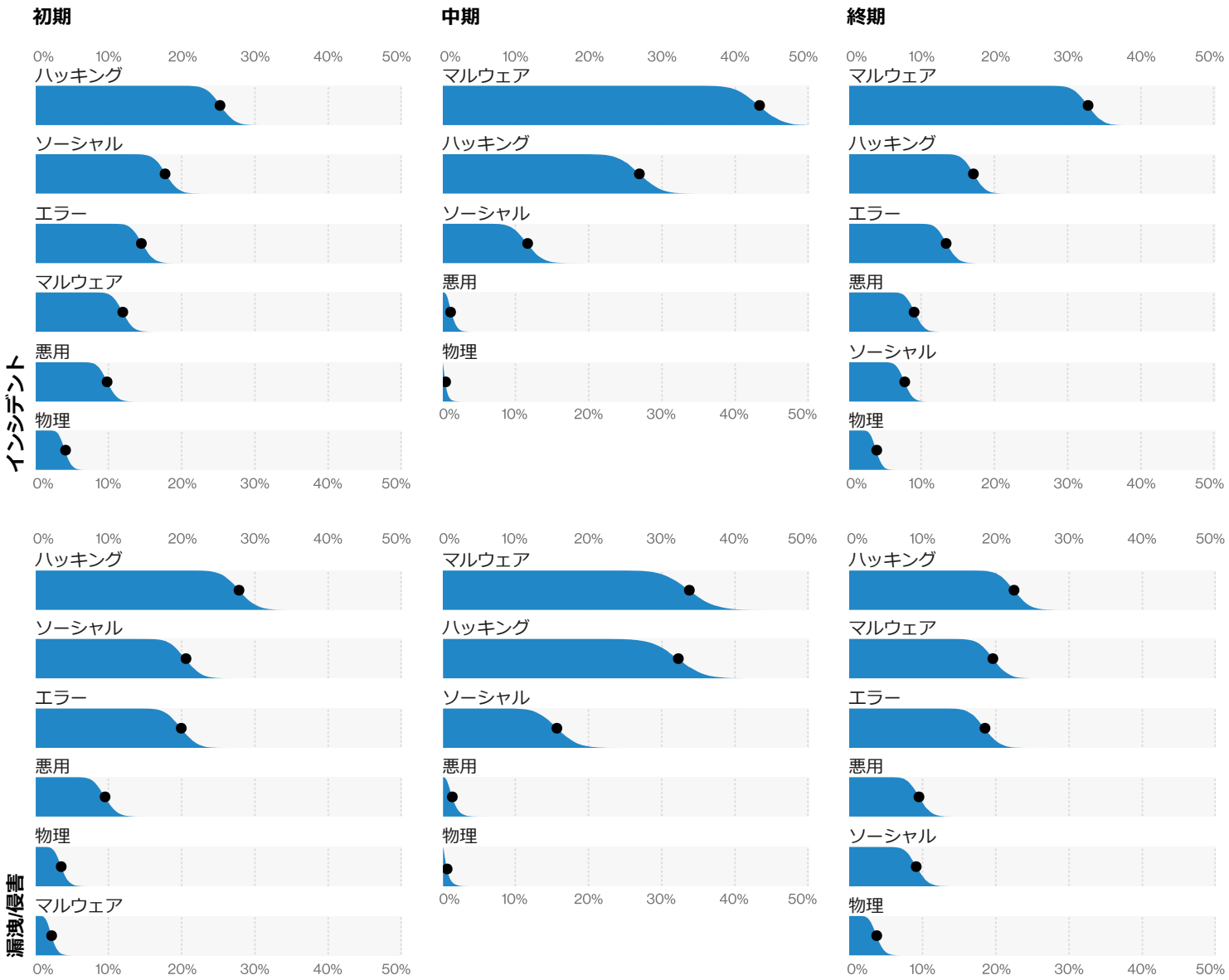
線の位置には少しノイズが含まれていますが、これがないと同じ線がぴったり重なってしまい、このような多くの線を見ることができなくなるためです。しかし、ほとんどはアートのためにやったことです。

最後に、図43を見てください。これは、インシデントとデータ漏洩/侵害の両方において初期、中期、そして終期にどのような行動がとられるかを示しています。興味深いのは、上位にあるものではありません（「ソーシャルエンジニアリングーフィッシング」や「ハッキングー窃取された認証情報の利用」が攻撃の開始に適した方法であることはすでに知っていますし、「エラー」はあまりにも短いため、攻撃パスの始まりが終わりでもあることを示しています）。

興味深いのは、一番下に近いところです。マルウェアが侵害の最初の行動になることはほとんどありません。逆に言えば、ソーシャル攻撃が攻撃を終わらせることはほとんどありません。中期では、ハッキングとマルウェアがデータ侵害をつなぎ止める接着剤となっていることが分かります。そして、3つ目の防御の機会は検出済みのものから未検出のものを推測することです。例えば、マルウェアを検出した場合、過去にさかのぼって見落としていたものが何かないか探す必要がありますが、ソーシャル攻撃を検出した場合は、攻撃者の現在の場所ではなく、向かっている先を突き止めるのです。

全体として、攻撃パスを理解するのは難しいかもしれませんが、一度理解すると攻撃者を理解するだけでなく、自分の防御策を計画するための貴重な機会が生れます。

図43. インシデントと漏洩/侵害の初期、中期、終期のアクション



タイムライン

データ漏洩/侵害のタイムラインが時間の経過とともにどのように展開してきたかを分析すると、数日以内の検出が増加し（図44）、同じタイムフレームでの封じ込めは2017年の歴史的なピークを越えています（図45）。ただし、これは弊社の外部協力者から提供されたインシデントデータのサンプリングに多くのマネージドセキュリティサービスプロバイダー（MSSP）が検出したデータ漏洩/侵害が含まれていることと、攻撃者が開示されたために検出はほぼ「即時」となった場合は、その巻き添え被害として、ランサムウェアによるデータ漏洩/侵害が相対的に増加することが原因である可能性が高いことを覚えておいてください[37]。

発見まで数か月以上要したデータ漏洩/侵害は依然として全体の4分の1以上を占めているうえ、2019年に発生し、まだ発見されていない潜在的なデータ漏洩/侵害がかなり存在することからも、これは年次の報告書であるため、常に実際の件数の遅行指標となっていることを指摘しておく必要があります。

いずれにしても、この1年で検出能力と対応には改善が見られおり、私たちは決して迫り来る虚しさとの戦いに人生の貴重な年月を使っているのではないと考えたいものです。さあ、ローストビーフサンドをご馳走しますので前向きに行きましょう。

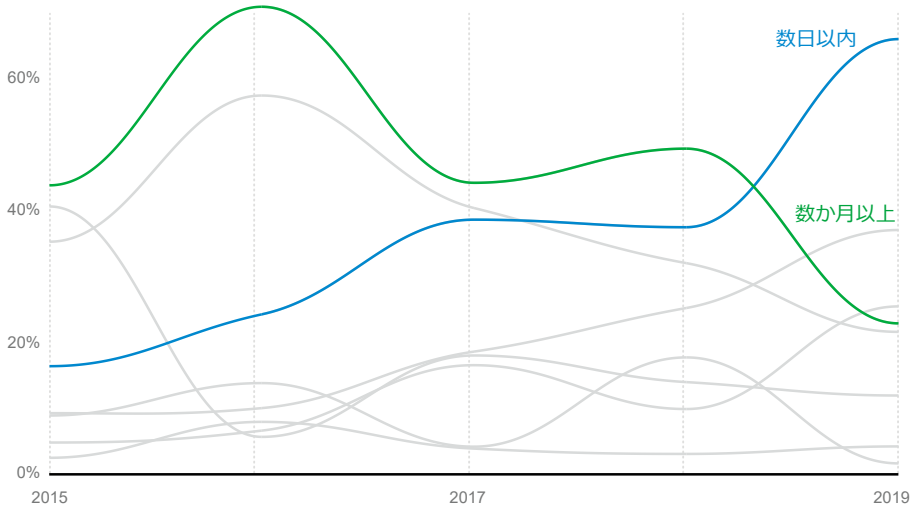


図44. 漏洩/侵害の発見までの時間の経時的変化

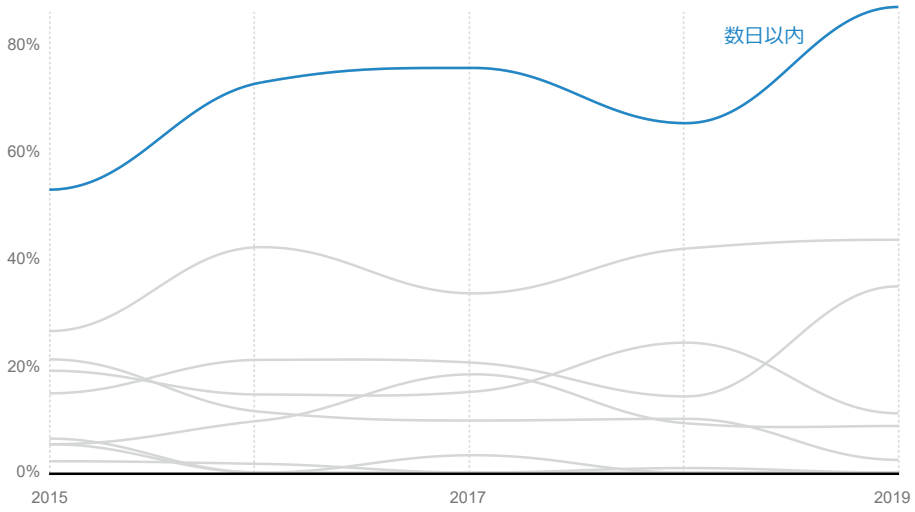


図45. 漏洩/侵害の封じ込めの経時的変化

37 貴社のサーバーに対して暗号通貨を要求し、引き換えにデータ漏洩/侵害を「発見」させる回転する炎のドクロのようなものでは決してありません。

インシデントの分類パターンとサブセット

VERISとDBIRに初めて触れた方は、弊社が所有するデータの量（現在、年間で755,000件以上のインシデント）とそのデータの分析深度（各インシデントで2,400以上の値を追跡可能）の両方を考えると、圧倒されるかもしれません。この膨大なデータをより正しく理解し、伝えるために、2014年に「パターン」というものをデータ分析に導入しました。これは本質的に「同類」で括ったインシデントとは異なるクラスターです。ここではデータサイエンスの専門的な観点からは詳しく触れませんが[38]、このパターンの適用により、「インシデント分類パターン」と呼ばれる9つの中核となるクラスターを特定することができました。これにより、攻撃、資産、攻撃者、属性のさまざまな組み合わせでの傾向ではなく、各パターンにおける傾向をさらに抽象化して説明できるようになりました。

本調査の開始以降に収集した40万9,000件のセキュリティインシデントと重大な約2万2,000件のデータ漏洩/侵害について調べたところ、セキュリティインシデントの94%およびデータ漏洩/侵害の88%が9つのインシデント分類パターンのいずれかにぴったり当てはまっていることが分かりました。しかし、今年度のデータだけを見てみると、その割合はセキュリティインシデントで85%に、データ漏洩/侵害では78%にまで低下しています。

このことは、弊社の「その他全て」というカテゴリーが、予備のUSBケーブルを入れる引き出しとなるように設計されていることからも明らかなように、フィッシングが台頭して上位のパターンに食い込んできたことで、それ以外のパターンのいくつかが当初の量からは激減しています。まるで、パターンのない時代が来て、時とともに変わり続けることだけがデータ漏洩/侵害の不変の真実であるかのようです。

これらのパターンについては、「地域」と「業界」のセクションで詳しく説明しますが、これらのパターンを理解する、あるいは以前の関係を再構築するために、ここで定義しておきます。

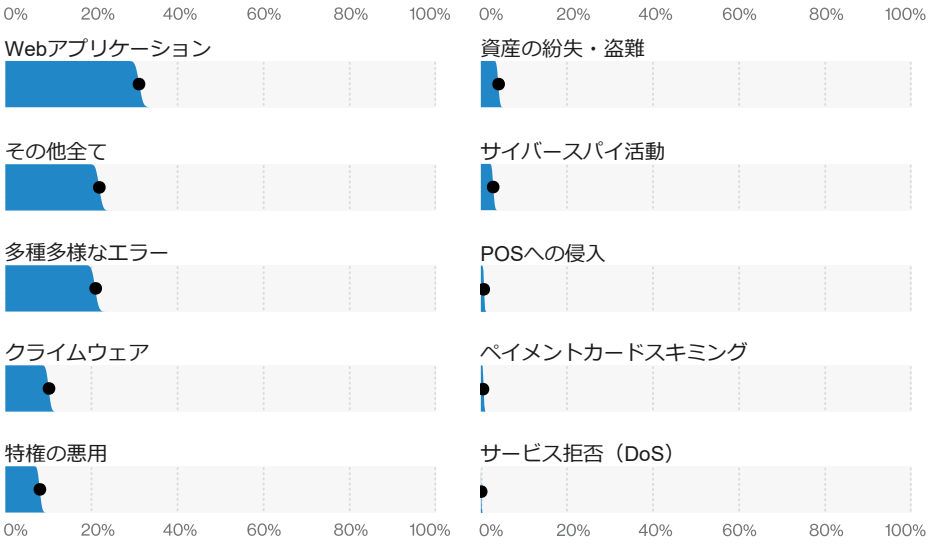


図46. データ漏洩/侵害のパターン（n = 3,950）

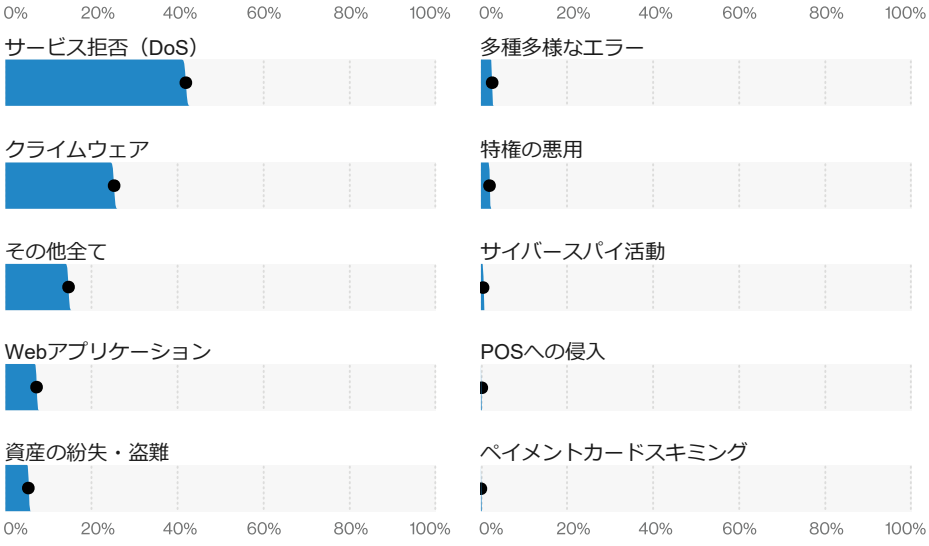


図47. インシデントのパターン（n = 32,002）

38 マニアックな詳細が気になる方は 2014年のレポートをご覧ください。

パターン

クライムウェア

クライムウェアは市中で最も古いゲームの1つです。他のパターンには該当しないマルウェアを含んでいます。これらのマルウェアは、誰もが恐らくファックスや不在着信を装ったメールなどで目にしたことのある、よくあるタイプのマルウェアです。これらのインシデントやデータ漏洩/侵害の動機は、金銭目的の傾向があります。

注目すべき事項：今年度は、クライムウェアに関連したインシデントやデータ侵害の件数が緩やかに増加する傾向が続いており、現時点の累計で約300件に上っています。これは昨年度よりも高く、2014年度に達した最高レベルにほぼ匹敵します。誰もが知っているように、これらのタイプの攻撃の伝播は、通常、リンクまたは添付ファイルを含んだメールを介して行われ、ダウンローダー、パスワードダンパ、トロイの木馬、またはC2機能といった厄介なものを落としていきます。

サイバースパイ活動

このパターンに含まれるのはネットワークやシステムへの不正アクセスを手段とするスパイ活動です。主に国家に関連する攻撃者が、機密性の極めて高い情報を探し求めています。

注目すべき事項：これは今年度減少したパターンの1つです。件数の数字と割合の両方で減少しており、2018年度には13.5%だったデータ漏洩/侵害は2019年度には3.2%になりました。件数の数が減少したのは、報告数が少ないか、これらの攻撃を検出できなかったためかもしれませんが、割合での減少は、他のパターンの量が増加したことが大きく影響しています。これらのタイプの攻撃は、ソーシャルエンジニアリングとマルウェアを組み合わせたベクトルに大きく依存しており、インシデントの81%にはフィッシング、92%には何らかの形のマルウェアが使用されています。

サービス拒否（DoS）

この攻撃は非常に多く発生しており（弊社がどのように対応したかご覧いただけます）、今年度のデータセットでは13,000件以上のインシデントが発生してしています。このパターンの攻撃は、さまざまな戦術を用いており、最も一般的なのは、ネットワークにジャンクトラフィックを送信してシステムを逼迫させて、システムのサービスを拒否させる方法です。システムは、入ってくる不正なトラフィックと正規のトラフィックを峻別することができません。

注目すべき事項：前述の通り、この攻撃のトラフィック量は増加していますが、DDoSについては、単に攻撃の数だけではなく、攻撃の規模を示す毎秒ビット数（BPS）や攻撃の経路を示す毎秒パケット数（PPS）にも注目しています。攻撃の送信に使用されたサービスに関係なく、パケット対ビット比は比較的狭い帯域内に留まっており、時間が経過してもPPSにそれほど変化はなく、最も一般的なモードでは570Mbpsに留まっていることが分かりました（図48）。

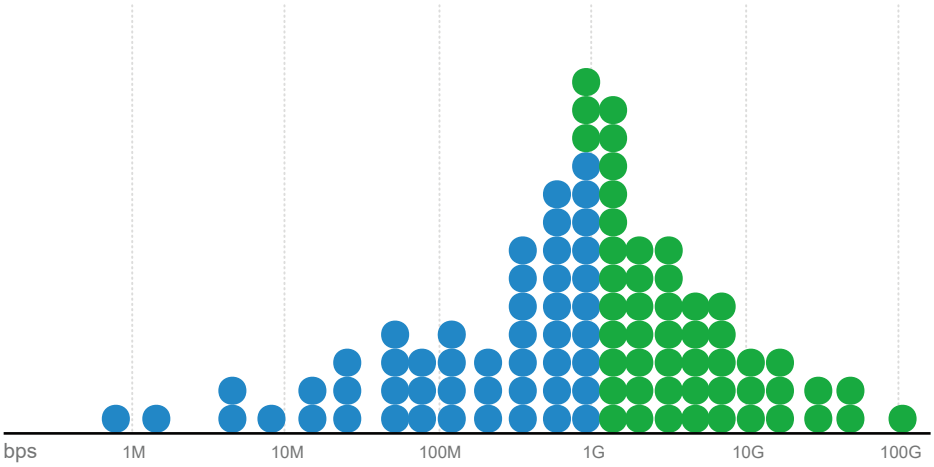


図48. DDoSのビット/秒(BPS)の平均 (n = 195)

DDoSの防御に関しては、攻撃の一部はインターネットサービスプロバイダーがネットワークレベルで緩和し、その他はエンドポイントやコンテンツ配信ネットワーク（CDN）プロバイダーが処理するという階層型のアプローチが最適です。これらの攻撃は、使い勝手がよく、インターネットに接続したインフラストラクチャを標的にすることができるため、広く普及しています。ただし、組織への影響や緩和するかどうかの判断はすべて、その企業にかかっています。

特権の悪用

このパターンは、社内の従業員が悪意を持って行った行為であり、何らかの形でセキュリティインシデントを引き起こす「不正使用」行為で構成されています。

注目すべき事項：インシデントに占める「不正使用」の割合は減少していますが、他のパターンは相関的に増加しています。しかし、これは今年度のデータの粒度が低かったことに起因する可能性があり、2021年には以前のレベルに戻るものと思われます。一方で、データ漏洩/侵害は理にかなった減少を示しており、これはデータへのアクセスや侵害を目的としたデータベースの不正使用が減少したことに関連していると考えられます。

多種多様なエラー

人生はアクシデントに満ちており、あの有名な画家ボブ・ロスのファンを失望させるわけではありませんが、全ての木が「ハッピー・リトル・ツリー」とは限りません。このパターンはまさにそのためのものであり、意図しない（私たちが知っている限りでは）アクシデントがサイバーセキュリティのインシデントやデータ侵害をもたらすイベントとなることを示しています。

注目すべき事項：これらの多種多様なエラーの大部分は、システム管理者によるストレージの設定ミスやエンドユーザーが犯したメールの誤送信といったものが関わっています。どんな攻撃者がどのような攻撃に関わっているのか見てしてみましょう。発見ということでは、こうしたエラーは、例えば情報を検索していたセキュリティ研究者や誤送信メールを受信した無関係の第三者によって発見されることが多いです。「結果と分析エラー」のセクションでは、このような特殊な傾向がある方のために、さらに詳しく説明しています。

ペイメントカードスキミング

このパターンはとても分かりやすく、例えば、ATMやガソリンスタンドの自動清算機などの端末機器から決済情報を抜き取るためにカードスキマーが使用されたインシデントです。

注目すべき事項：弊社のデータによると、POSカードスキマーが関与するインシデントは継続的に減少傾向にあり、現在ではインシデントデータ全体の0.7%にまで減少しています。インシデント数は約30件で、ピーク時の2013年の206件から比較的顕著な減少傾向にあります。この減少は、弊社の外部協力組織の1つである連邦政府への報告が減少していることや、攻撃手法が変化していることなど、様々な要因が考えられます。

POSへの侵入

このパターンには、ペイメントカードを盗むことを目的としたPOSサーバーやPOS端末環境へのハッキングやリモート攻撃が含まれています。

注目すべき事項：ペイメントカードスキミングと同様に、ここ数年で顕著な減少を見せており、今年度はデータ侵害全体のわずか0.8%です。インシデントの大部分は、RAMスクレーパーを使用したものであり、これにより決済システムを実行しているサーバーやエンドポイントのメモリから直接決済カードの情報を抜き取ることができます。しかし、ペイメントカード犯罪の大部分はオンライン小売店に移っています。

資産の紛失・盗難

これらのインシデントには、資産やデータが消えた理由が不明なものも含まれます。盗難として確認されることもありますが、その他は事故の可能性があります。

注目すべき事項：このパターンは、この数年間は比較的一定の傾向にあり、過去2年間のデータ侵害は全体の3%～6%で、今年度は約4%となっています。インシデントは各所で発生していますが、主に被害者の職場や社員の自家用車で発生しています。ドアは必ず施錠してください。

Webアプリケーション

Webアプリケーションを標的とするインシデントです。コードベースの脆弱性を悪用する「ハッキング－脆弱性を突いたエクスプロイト攻撃」など、実際のWebアプリケーションのコードを攻撃するものから、「ハッキング－盗まれた認証情報の使用」などの認証メカニズムを攻撃するものなどが含まれます。

注目すべき事項：Webアプリケーションに対する攻撃を監視している外部協力者によって提供されたデータ（図49）では、SQLインジェクションとPHPインジェクションの脆弱性が最もよく悪用されています。これらのタイプの攻撃は、無防備なシステムを迅速かつ容易に攻撃者の利益になるように変えることができるので、頻度が高いのも納得できます。しかし、脆弱性データでは、悪名高いding型ポップアップ脆弱性であるクロスサイトスクリプティング(XSS)が最もよく検出されており、SQLiへの攻撃頻度はXSSの半分ほどしかありません。

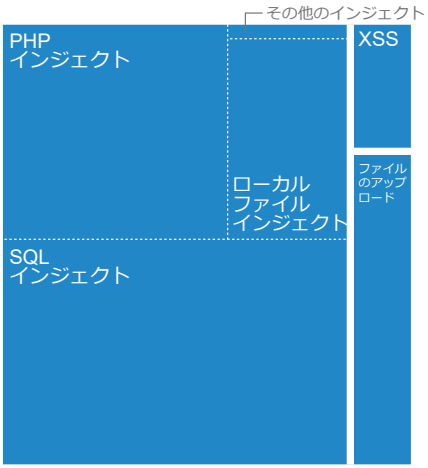


図49. Webアプリケーションの攻撃ブロック（n = 55億）

その他全て

前述のパターンのどれにも当てはまらないインシデントです。言わば「失われたインシデントの魂の墓場」です。

注目すべき事項：これらのインシデントの大部分は、フィッシングや金銭目的のソーシャルエンジニアリングであり、攻撃者はメール詐欺を仕掛けてきます。詳しくは「結果と分析」セクションの「ソーシャルエンジニアリング」の項を参照してください。金銭目的のソーシャルエンジニアリングとフィッシングについて詳しく説明しています。

サブセット

主要な9つのパターンに加えて、極端に詳細情報の少ないインシデントが多い場合などは結果や分析を歪める可能性のある、別の要因があるため別個に検討を要するパターンがあります。今年度も前年度と同様に、これらのパターンを「ボットネット」サブセットと「二次的」動機のサブセットに分けて検討しました。

「ボットネット」サブセット

デスクトップやサーバーに侵入したトロイの木馬やマルウェアのさまざまな事例から得られた103,699件のインシデントから成るサブセットです。大部分は各種のインシデントソースからのもので、質が低く、詳細情報が少ない傾向があります。

注目すべき事項：図50を見ると、ボットネットは主に金融、情報、専門サービスなどの業界に影響が及んでいることが分かります。これらの業界は全て、自社のセキュリティだけでなく、顧客のセキュリティにも力を入れるべきです。このサブセットの絶対数は、前年度の2倍以上に増加しています。また、この種のインシデントはあらゆる人々に影響を及ぼしており、被害者の41%は北米以外の地域であることにも注意してください。

「二次的」Webアプリサブセット

攻撃を受けたWebアプリケーションが別の攻撃のための手段となったインシデントが対象です。侵害されたサーバーがボットネットに利用されたり、他のシステムをDDoS攻撃したりという形でのセキュリティインシデントがよく見られます。

注目すべき事項：二次的サブセットのインシデントは合計で5,831件に上り、そのうちの約90%が何らかの形でハッキング、マルウェア、サーバーへの攻撃に関与しています。「結果と分析」セクションの「攻撃者」の項で指摘しているように、自社のインフラを攻撃者のインフラに取り込む隙を与えれば、相手は躊躇することはありません。

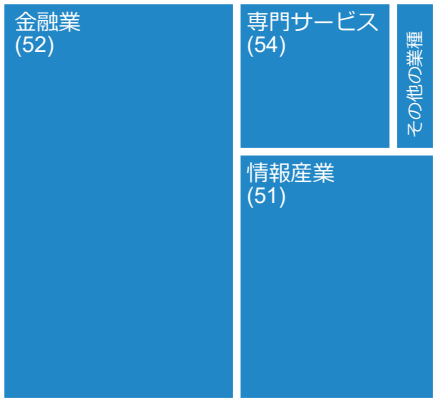
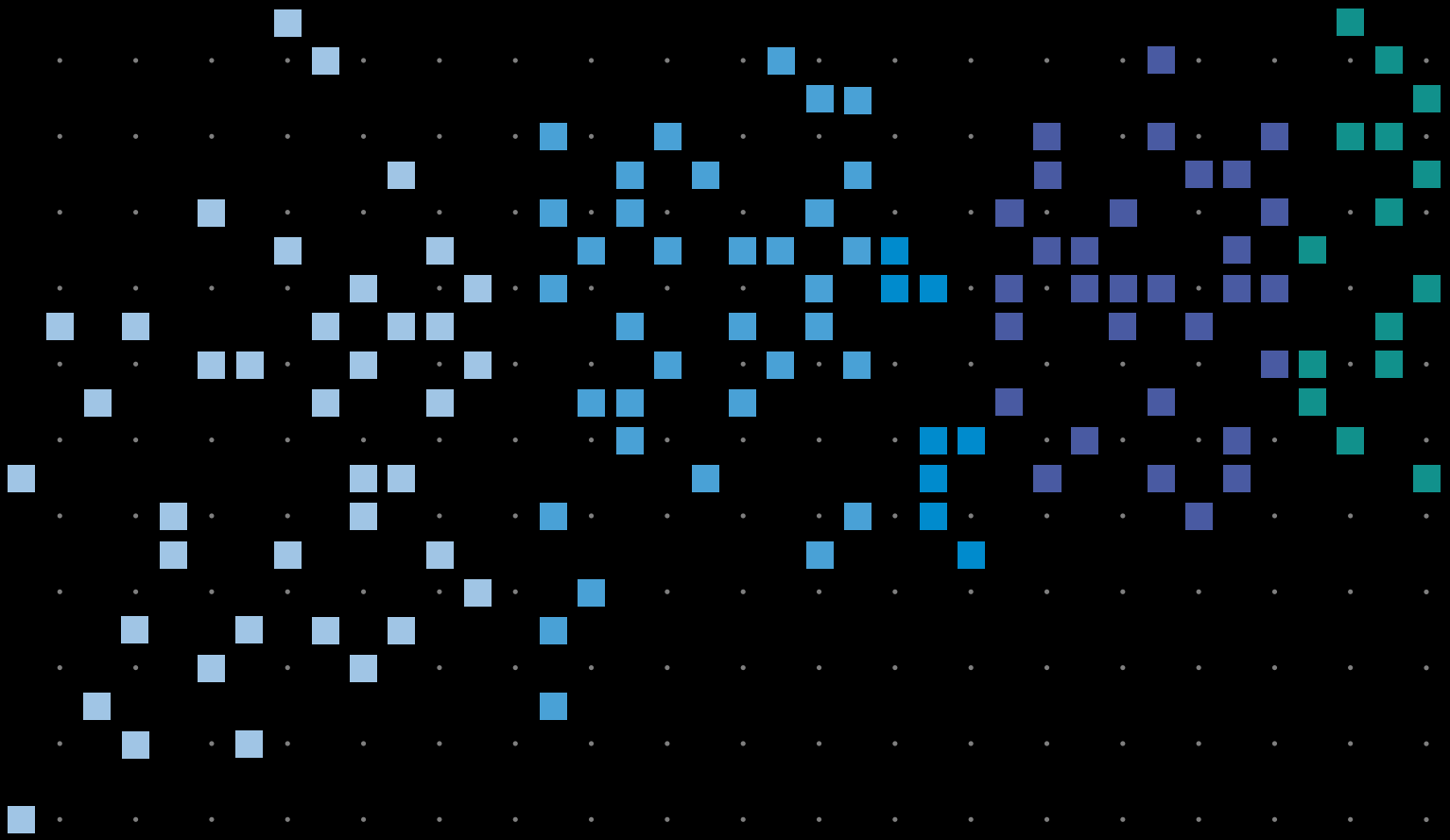
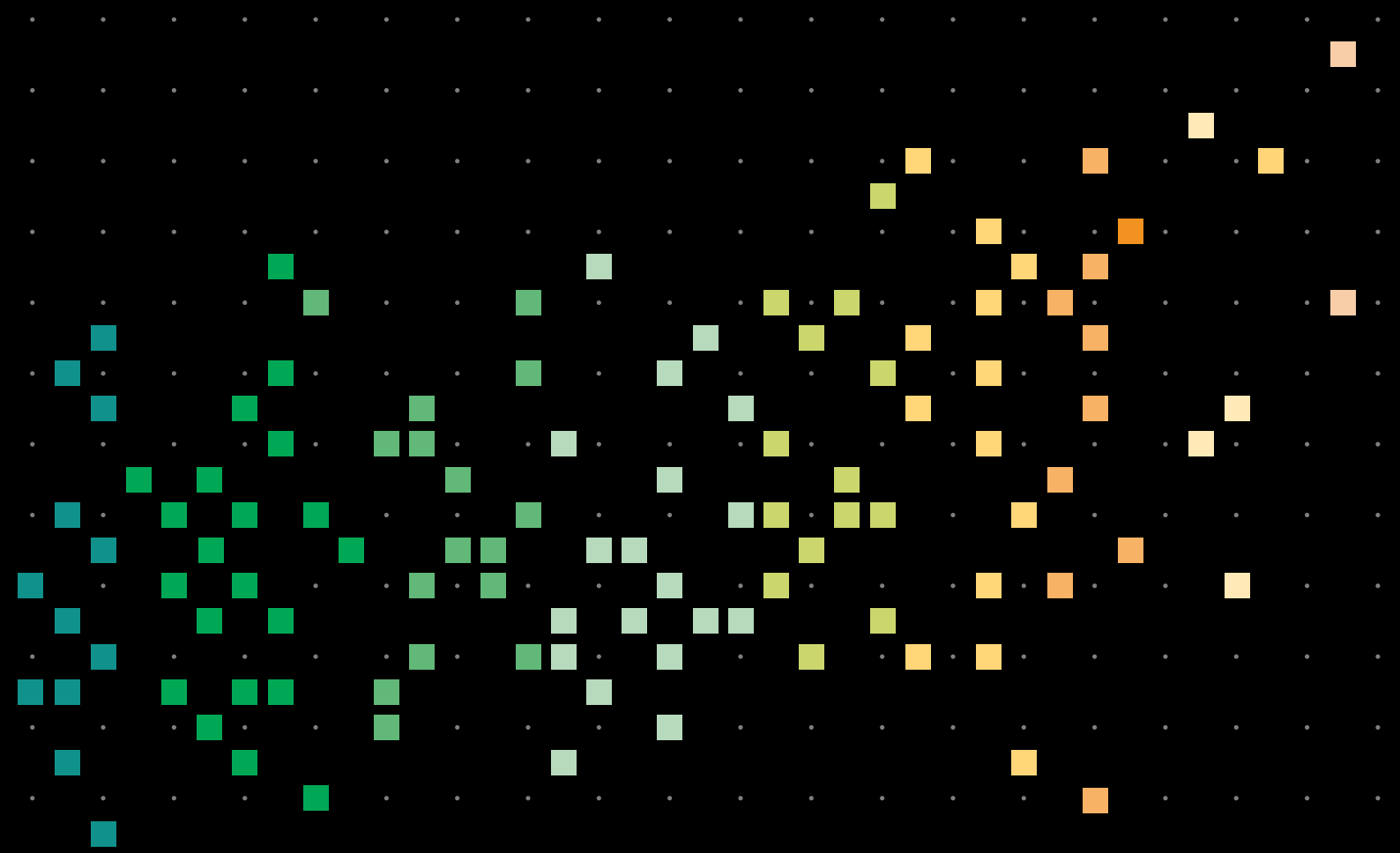


図50. ボットネット感染(n = 103,699)



03



業種別のハイライト

各業種の概要

今年度は157,525件のインシデントと108,069件のデータ漏洩/侵害を収集しました。注目すべきは、このうち10万件以上が、標的にされた銀行口座やクラウドサービスから漏洩した個人ユーザーの認証情報であったということです。弊社ではこれらを「インシデントの分類パターンとサブセット」セクションの「二次的動機」サブセットに分類します。品質のフィルタリングとサブセット化を行った後、インシデントと侵害を表1に示しました。

このブレイクアウトで何をすべきでないか、弊社の今年度の声明は、次の通りです。この調査報告書を利用して、ある業界を基準に別の業界を判断しないでください。管理部門のセキュリティ担当者が金融部門の同僚の目の前で、このDBIRを振りかざして見下したように話すのは、決してあってはなりません。このデータ漏洩/侵害やインシデントの数は、本調査の外部協力者に大きく影響されています。これらの数字は、私たちが「何を使って仕事をしなければならないのか」を知るためのものであり、レポートで使用するデータのソースについて常に透明性を確保するというコミュニティに対する弊社の誓約の1つでもあります。

図51と52には、また別の注意すべきことがあります。ここに示した数字は、業界に関する情報を得ることを目的としたものです。表の数字が小さいほど、その列から導き出された統計の信頼性は低くなります。

インシデント：	合計	小規模	大規模	不明
合計	32,002	407	8,666	22,929
宿泊 (72)	125	7	11	107
行政 (56)	27	6	15	6
農業 (11)	31	1	3	27
建設 (23)	37	1	16	20
教育 (61)	819	23	92	704
娯楽 (71)	194	7	3	184
金融 (52)	1,509	45	50	1,414
医療 (62)	798	58	71	669
情報 (51)	5,471	64	51	5,356
管理 (55)	28	0	26	2
製造業 (31–33)	922	12	469	441
鉱業 (21)	46	1	7	38
その他のサービス (81)	107	8	1	98
専門 (54)	7,463	23	73	7,367
公務 (92)	6,843	41	6,030	772
不動産 (53)	37	5	4	28
小売 (44–45)	287	12	45	230
卸売 (42)	25	2	9	14
運輸 (48–49)	112	3	16	93
公益事業 (22)	148	5	15	128
不明	6,973	83	1,659	5,231
合計	32,002	407	8,666	22,929

漏洩/侵害：	合計	小規模	大規模	不明
合計	3,950	221	576	3,153
宿泊 (72)	92	6	7	79
行政 (56)	20	6	10	4
農業 (11)	21	1	0	20
建設 (23)	25	1	10	14
教育 (61)	228	15	22	191
娯楽 (71)	98	3	1	94
金融 (52)	448	32	28	388
医療 (62)	521	31	32	458
情報 (51)	360	32	32	296
管理 (55)	26	0	25	1
製造 (31–33)	381	5	185	191
鉱業 (21)	17	0	5	12
その他のサービス (81)	66	6	1	59
専門 (54)	326	14	13	299
公務 (92)	346	24	50	272
不動産 (53)	33	3	3	27
小売 (44–45)	146	7	18	121
卸売 (42)	15	1	6	8
運輸 (48–49)	67	3	6	58
公益事業 (22)	26	2	4	20
不明	688	29	118	541
合計	3,950	221	576	3,153

表1. 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

漏洩/侵害

図51. 業界別の漏洩/侵害

インシデント

図52. 業界別のインシデント

例えば、建設業（NAICS 23）のデータ漏洩/侵害に関与する資産は全部で35件です。このうち、1つのデータ漏洩/侵害に複数の資産が含まれている可能性があるため、ここで報告されている資産数よりも実際のデータ漏洩/侵害は少ない（25件）可能性があります。この部門でのデータ漏洩/侵害件数の少なさを考慮すると、そこから得られる統計値の信頼性は比較的低いものと考えられます。しかし、より多くの業界の情報を読者にお届けするために、統計値の範囲を広げています。例えば、「建設業におけるデータ漏洩/侵害の64%はサーバーが関与していた」というような表現ではなく、「建設業におけるデータ漏洩/侵害の44%～82%はサーバーが関与していた」というような表現をとっています。これは控え目な態度ということではなく[39]、単に誤解を招くことなく、このような小さなサンプルを使用する業界では、できるだけ多くの情報を提供したい（すなわち統計に幅を持たせたい）からです。中央値を表す黒のドットを削除した場合の棒グラフと似たような考えです。各業界セクションの「サマリーデータ」の一番下にある「データ分析ノート」にご注意ください。サンプルサイズが小さいことや他の注意点などをここで指摘してあります。本報告書で使用されている統計的信頼性の背景についての詳細は、「方法論」セクションをご覧ください。

報告書の今年度でのもう1つの改善点は、VERISとCIS Critical Security Controls（CSC）とを対応させて、推奨するコントロールを標準化したことです。各業界のサマリーデータには、「上位3つの対策」をリストしています。マッピングの詳細については、「CISコントロールの推奨」セクションをご覧ください。

読者の皆様からいただいフィードバックを拝見する限り、報告書を隅から隅まで目を通す方もいれば、直接関心のあるセクションや業界の業種以外のセクションは読み飛ばす方もいらっしゃるようです。そのため、一部のセクションだけを見ている読者は、他の場所ですでに言及しているかもしれない定義や説明を知らないため、報告書の中でいくつかの定義や説明を何度か繰り返しています。気になる方は、そのような箇所をスキップしていただいてかまいません。

39 ゲームボーイのように

宿泊および飲食業 NAICS 72

サマリー

この業種のデータ漏洩/侵害は、もはや過去にその大部分を占めていたPOS関係の攻撃によるものではありません。漏洩や侵害の要因としては、複数のアクションタイプがほぼ均一に影響しており、具体的にはマルウェアやユーザーのミスに乗じた攻撃、盗み取った認証情報を使ったハッキングなどが挙げられます。この業種では金銭目的のハッカーによるクレジットカードの情報を狙った攻撃が頻繁に確認されています。

頻度	インシデント125件、確認されたデータの暴露92件
上位3つのパターン	「クライムウェア」、「Webアプリケーション攻撃」、「POSへの侵入」がデータ漏洩/侵害全体の61%を占めている
攻撃者	外部（79%）、内部（22%）、複数の関係者（2%）、パートナー（1%）（漏洩/侵害）
攻撃者の動機	金銭目的（98%）、二次的動機（2%）（漏洩/侵害）
侵害されたデータ	決済情報（68%）、個人情報（44%）、認証情報（14%）、その他（10%）（漏洩/侵害）
上位3つの対策	ネットワークポート、プロトコル、およびサービスの制限とおよび制御コントロール（CSC 9）、境界防御（CSC 12）、データ保護（CSC 13）

データ漏洩/侵害を笑顔でサービス

宿泊および飲食業界は、本調査で長い間追いかけてきた業界の1つです。この業界には、何度も追いかけたくなる何かがあります。この業界に費やした時間から学んだことの1つは、この業界ではマルウェアが比較的大きな役割を果たしているということです。今年度の上位3つのパターンのうち2つは、「クライムウェア」と「POS攻撃」（いずれもマルウェアに依存）です。図53に示すように、今年度の攻撃の花形として、「窃取された認証情報の使用」と「脆弱性を突いたエクスプロイト攻撃」の両方をカバーする「Webアプリケーション」が3つ目に加わりました。

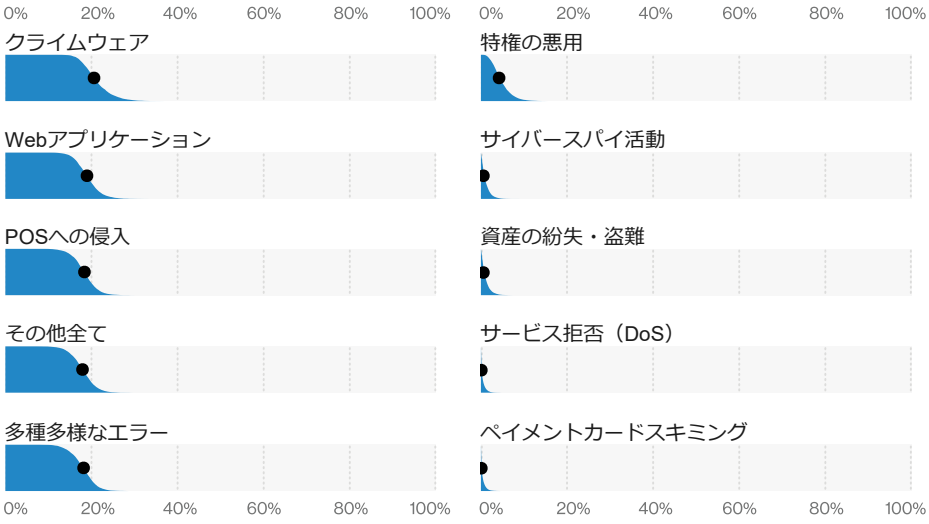


図53. 宿泊および飲食業のデータ漏洩/侵害のパターン（n = 92）

POS攻撃はもうおしまい

昨年の報告書で、POSを標的とする様々な攻撃、つまりマルウェアを使ったリモート攻撃やスキミングが減少していることを報告しましたが、この傾向は今年も続いています（図54）。POS攻撃はまだ比較的一般的で、この業界のデータ漏洩/侵害全体の16%を占めているにもかかわらず、最も高かった2015年に近づいている場所はどこにもありません。これは、攻撃者が環境を揺さぶってマルウェアを拡散するよりも、ランサムウェアを展開して組織内でのアクセスをすばやく収益化しようとする傾向を示している可能性があります（恐らくそうでしょう）。

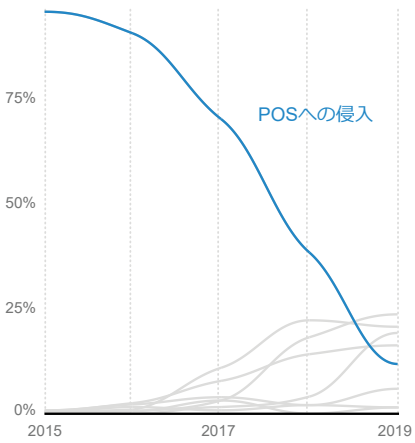
これでマルウェアが必要か?

POS攻撃が減少しているにもかかわらず、弊社のデータセット全体よりも高い割合でペイメントカードやその他のデータを取得するためにクライムウェアが利用されていることが確認されており、今年度のデータ漏洩/侵害の4分の1を占めています。このマルウェアは、デスクトップとサーバーの両方で発見されています。種類別に見ると、図55ではRAMスクレーパーが減少し、トロイの木馬やバックドア、C2など環境へのアクセスを可能にするマルウェアが増加しています。また、すでにある感染を利用して環境への侵入を可能にするランサムウェアの増加も続いています。ランサムウェアは、データ漏洩/侵害においてはマルウェアの上位には入っていませんし、スキャンにおいても増加していませんが、検出度では上位のマルウェアではありませんが、監視を怠ってはなりません。

ドル紙幣だけではありません

この業界は決済情報が豊富にあるため、金銭を簡単に手に入れることができます。しかし、決済情報だけが侵害されているわけではありません。攻撃の副産物として個人情報も侵害されていることが多いので、ペイメントカード周り以外のセキュリティプログラムにも十分に注意を払う必要があります。

図54. 宿泊・飲食業の漏洩/侵害のパターンの経時的変化



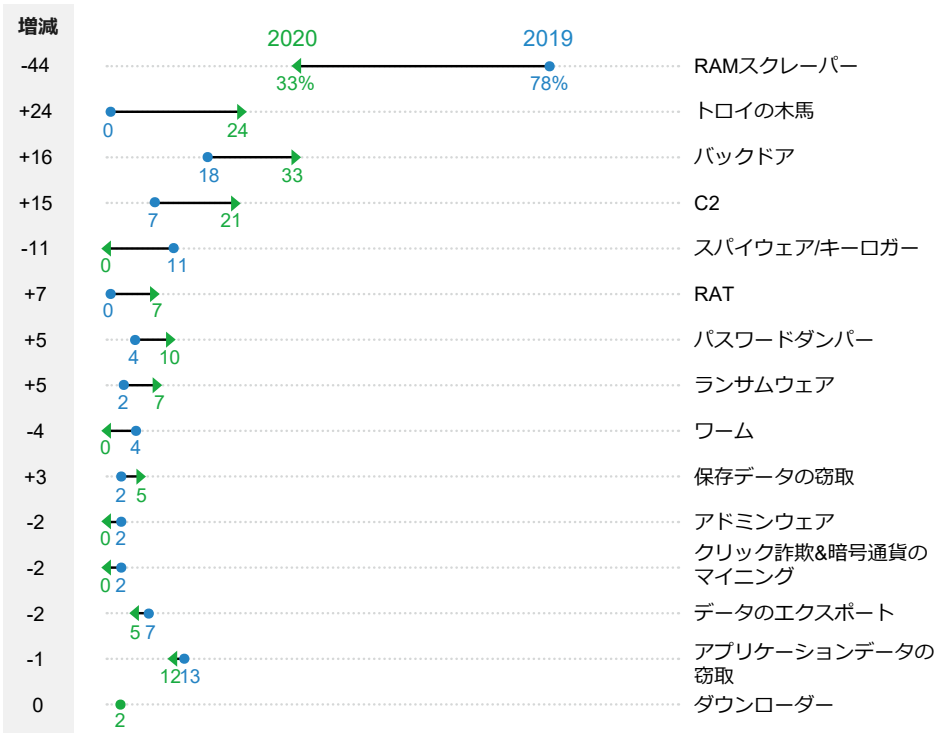


図55. 宿泊および飲食業の漏洩/侵害によく見られるマルウェアの経時的変化：n = 45 (2019)、n = 42 (2020)

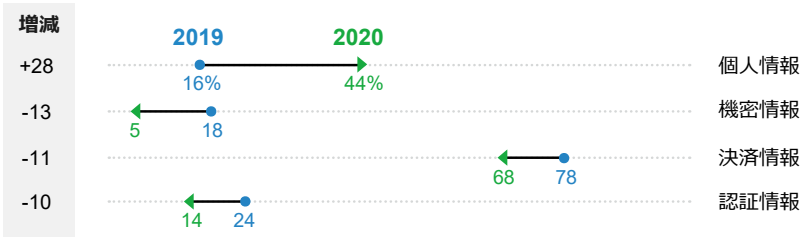


図56. 宿泊および飲食業の漏洩/侵害によく見られる攻撃を受けたデータタイプの経時的変化：n = 51 (2019)、n = 87 (2020)

芸術、娯楽およびレクリエーション業 NAICS 71

サマリー

この業種では、Webアプリケーションを標的とした攻撃によるデータ漏洩や侵害が多く発生しています。また、DoS攻撃における1秒あたりのビット数がデータセット全体と比較して多くなっているほか、ソーシャルエンジニアリング攻撃やユーザーのミスに乗じた攻撃も多く確認されています。

頻度	インシデント194件、確認されたデータの暴露98件
上位3つのパターン	「Webアプリケーション攻撃」、「多種多様なエラー」、「その他全て」がデータ漏洩/侵害の68%を占めている
攻撃者	外部（67%）、内部（33%）、パートナー（1%）、複数の関係者（1%）（漏洩/侵害）
攻撃者の動機	金銭目的（94%）、自己都合（6%）（漏洩/侵害）
侵害されたデータ	個人情報（84%）、医療情報（31%）、その他（26%）、決済情報（25%）（漏洩/侵害）
上位3つの対策	境界防御（CSC 12）、セキュアな設定（CSC 5、CSC 11）、セキュリティ意識向上トレーニングプログラムの実施（CSC 17）

目覚めはすっきり、ハッキング開始

ハッカーはかつて「芸術家のようだ」と表現されていましたが、この業界でその芸術的な攻撃を受けてきた組織は、少し違った意見を持つかもしれません。この業界の特徴は創造性と新規性ですが、データ漏洩/侵害パターンの上位3つが「Webアプリケーション」、「多種多様なエラー」、「その他全て」であることを考えると（図57）、この業界におけるデータ漏洩/侵害の大半は「亜流だ」とか「過去にすでにあった」といった芸術的な批判を受ける可能性があります。

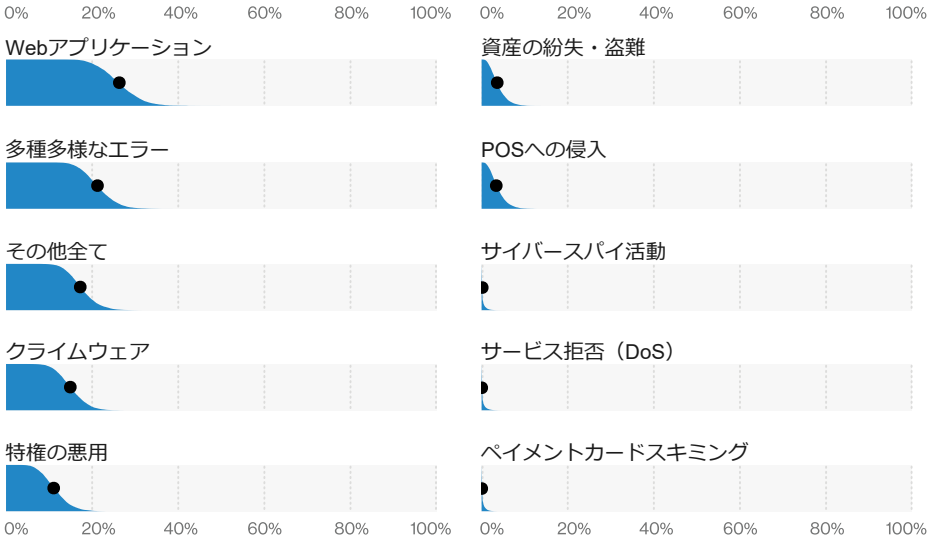


図57. 芸術、娯楽およびレクリエーション業のデータ漏洩/侵害のパターン（n = 98）

詐欺師は何度も騙す

芸術の正統性を確立するのが難しいのと同じように、人間もまた、データ通信の正当性を決定するのに苦労しています。これが、ソーシャルエンジニアリングが主導権を握る「その他全て」のパターンが2番目に多い理由です。2019年には、データ漏洩/侵害全体の約18%でソーシャル攻撃が発見されています。しかし、人間性の話題に戻ると、設定ミスや誤送信などのアクシデントやエラーがこの業界では共通の課題として残っています。図58に示すように、アクシデントによるデータ漏洩/侵害の増加は、ここ数年の間に内部攻撃者と外部攻撃者が集中していることを示しています。この増加はデータ漏洩/侵害報告の変化によるものかもしれませんが、2016年以降は一貫しています。

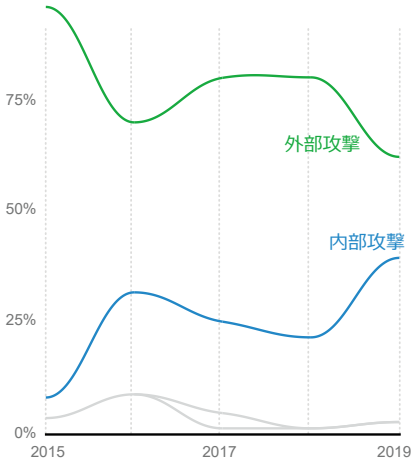


図58. 芸術、娯楽およびレクリエーション業の漏洩/侵害の攻撃者の経時的変化

無題の仕事 II

企業はデータの完全性を維持できるようにしたいと考えており、サイバー犯罪者はそれを知っています。今年のマルウェア（図59）の上位の種類には、「アプリケーションのデータをキャプチャする」などの機能が含まれていました。このような機能を利用する悪質な攻撃者がシステム内に潜入してデータを吸い上げ、ワームを環境に蔓延させたり、ランサムウェアを残すことで、重要なデータをロックしたりすることが可能になります。この場合、脆弱性を利用してWebサーバーに侵入するか、または実証済みメールフィッシングの方法を利用してデスクトップに侵入するかの、いずれかです。

DDoS攻撃者

今年度の調査で非常に興味深い結果の１つとして、この業界でDDoS攻撃の発生率が最も高く（図60）、例年トップであった情報産業を大きく引き離したことが挙げられます。このNAICSコードには、オンラインギャンブル業界が含まれており、これがこの傾向を牽引している可能性が高そうです。どうやら、ビジネスライバルをDDoS攻撃するのは、この業界では当たり前のことのようです。ご存知でしたか?

図59. 芸術、娯楽およびレクリエーション業のインシデントにおける上位マルウェアの経時的変化：n = 14（2015）、n = 35（2020）

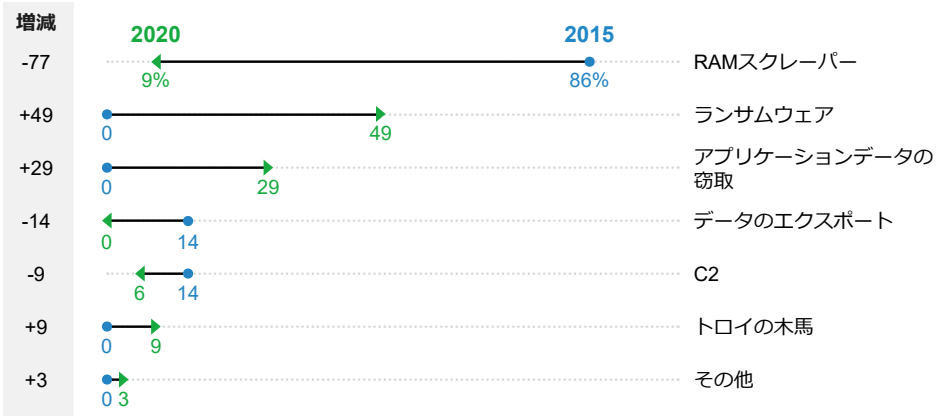
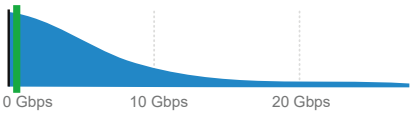


図60. 芸術、娯楽およびレクリエーション業のDDoSの平均的なBPS (n = 5 組織)、全産業のモード (緑色の線)：565 Mbps



建設業 NAICS 23

サマリー

この業種では、Webアプリケーションを標的とする攻撃やソーシャルエンジニアリング攻撃の被害が発生しているほか、窃取した認証情報を悪用する手口も依然として問題になっています。ただし、建設業ではパッチの適用率が全業種の平均よりも高く、従業員のセキュリティ関連のミスの数が驚くほど低く抑えられています。

頻度	インシデント37件、確認されたデータの暴露25件
上位3つのパターン	「その他全て」、「Webアプリケーション攻撃」、「クライムウェア」がインシデント全体の95%を占めている
攻撃者	外部（95%）、内部（5%）（漏洩/侵害）
攻撃者の動機	金銭目的（84%～100%）、怨恨（0%～16%）（漏洩/侵害）
侵害されたデータ	個人情報、認証情報
上位3つの対策	セキュアな設定（CSC 5, CSC 11）、境界防御（CSC 12）、アカウントの監視およびコントロール（CSC 16）
データ分析ノート	攻撃者の動機は、既知の動機によるデータ漏洩/侵害が10件のみだったため、パーセンテージの範囲で表しています。また、漏洩または侵害したデータのパーセンテージを提供することはできません。

ボブとはたらくブーブーズ（Rob the builder）

弊社が取集したデータをさらに深く掘り下げた結果、今年度はいくつかの新しい産業のセクションを追加することができました。建設業がその1つです。データ漏洩/侵害を考えるときに建設業界が最初に思い浮かぶことはないかもしれませんが、この産業は大規模な経済成長を生み出し、国のインフラの維持を支える重要な部門です。その観点から見ると、「この業界を攻撃する動機は何か?」という疑問が浮かぶかもしれません。ほとんどのケースは金銭目的であり、大抵は組織的な犯罪グループによって実行されたものです。これらの攻撃の大部分は狙いを定めたものです（75%）。つまり、攻撃者は、十分に使い慣れたハンマーを手にして、セキュリティの緩い釘を探していたというわけです。

建設業界のテーブルに着くのは誰もが初めてなので、まず左コラムの「サマリー」に示した上位3つの攻撃パターンから説明を始めましょう。「その他全て」パターンは、基本的に他のパターンに当てはまらない攻撃をまとめたものです。このパターンには、なりすまし攻撃（攻撃者の思惑どおりに被害者に実行させるシナリオが考案されている）や一般的なフィッシングなどのソーシャルエンジニアリング攻撃が多く含まれており、手間をかけずに事を済ませたい怠惰な犯罪者からの攻撃がよく見られます。「Webアプリケーション攻撃」はその名の通り、Webサイトをハッキングしてデータを入手する攻撃です。「クライムウェア」は基本的なマルウェア攻撃ですが、ランサムウェアもこの攻撃に該当し、ますます普及しています。ランサムウェア攻撃は通常、データ漏洩/侵害には至りませんが、脅威の主体は、暗号化される前にデータのコピーを取得し、脅して被害者に身代金の支払いを迫るものです。

ブードゥー教の教え

この業界において（データセット全体でも）よくある攻撃方法としてソーシャルエンジニアリングを挙げています。悪意のある者がこの手段を使うのは、単にこの方法が効果的だからです。被害者にWebページに認証情報を入力させたり、さまざまなマルウェアをダウンロードさせたり、あるいは単に現金を送金させるなど、方法は多様ですが、従業員の一定の割合はそれを実行します（図61）。セキュリティ担当者は積極的に何をすべきか？自分が標的にされていることを知ることがどれほど重要であるかは、すでにお話しました。クリック率を見るとこの業界の人々は、わずかな差ですが平均的な人よりも引っかかりやすいことが分かります。つまり、自分たちが標的にされていることを報告することが重要です。この業界では、クリック後の投稿率は非常に低いですが、報告率も同様に低いです。図62のドットプロットでは、積み上げられた全ての企業が0%を示しています。

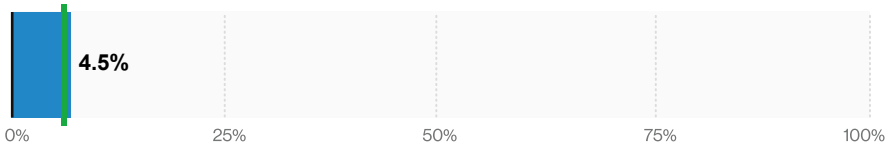


図61. 建設業のフィッシングテストにおけるクリック率の中央値 (n = 532): 全産業の中央値 (緑色の線)：3.6%

Webアプリケーション攻撃では、最も一般的なハッキングの種類は、窃取された認証情報の使用でした。これらはフィッシング攻撃から窃取されたものもあれば、他のデータ侵害の残骸の一部に過ぎない場合もあります。従業員が複数のアカウント（業務用および個人用）で同じ認証情報を使い回していると、データ漏洩/侵害によって窃取された認証情報がクレデンシャルスタッフィングに使用された場合に、組織のリスクが高まります。このリスクを軽減するには、多要素認証方式を導入し、インフラで盗まれた認証情報の効力が失なわれるようにすることが重要です。

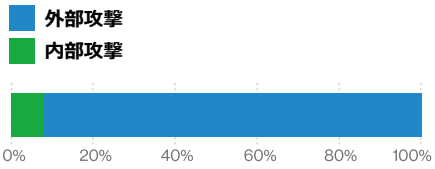


図63. 建設業の漏洩/侵害の攻撃者(n = 25)

従業員を大切に

この業界で目立ったのは、内部攻撃者によるデータ漏洩/侵害が少ないことでした。内部攻撃者によるデータ侵害には2つの種類があります。不正使用（悪意を持った行為）とエラー（偶発的）です。図63に示されているように、この業界では、どちらかに関与したデータ漏洩/侵害がほとんどありませんでした。

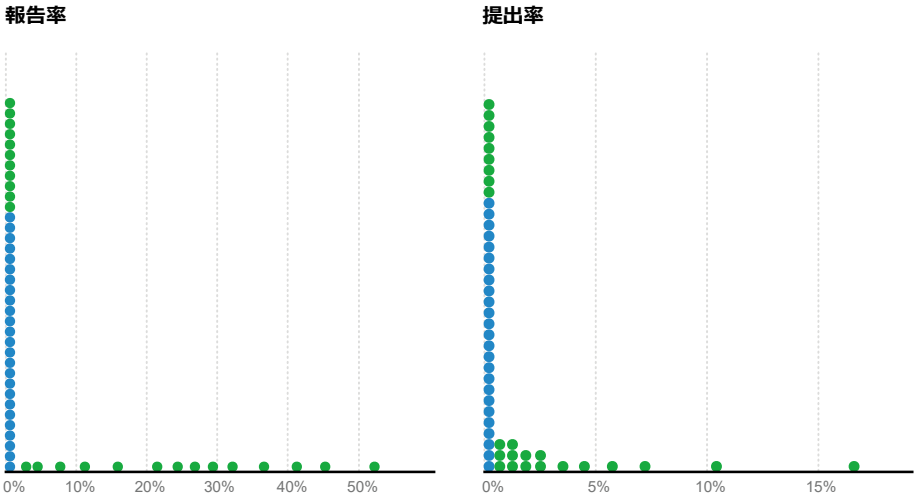


図62. 建設業のフィッシングテストにおける中央値 (n = 532)

教育サービス業 NAICS 61

サマリー

この業種では、データ漏洩/侵害の28%はフィッシング攻撃に起因しており、一方、窃取した認証情報を悪用したハッキングによる侵害が23%発生しています。また、インシデントデータのうち、マルウェア感染の約80%をランサムウェアが占めています。この業種では、フィッシング攻撃を受けた場合の報告の面で不備があり、データ侵害を受けた企業は迅速な対応ができていません。

頻度	インシデント819件、確認されたデータの暴露228件
上位3つのパターン	「その他全て」、「多種多様なエラー」、「Webアプリケーション攻撃」がデータ漏洩/侵害の81%を占めている
攻撃者	外部（67%）、内部（33%）、パートナー（1%）、複数の関係者（1%）（漏洩/侵害）
攻撃者の動機	金銭目的（92%）、愉快犯（5%）、自己都合（3%）、スパイ活動（3%）、二次的動機（2%）（漏洩/侵害）
侵害されたデータ	個人情報（75%）、認証情報（30%）、その他（23%）、内部情報（13%）（漏洩/侵害）
上位3つの対策	セキュリティ意識向上トレーニングプログラムの実施（CSC17）、境界防御（CSC12）、セキュアな設定（CSC5、CSC11）

条件から外れたデータ侵害の島

この業界の中ではトップクラスの「その他全て」のパターンとはいったい何なのかと疑問に思うかもしれません。がらくたがいっぱい詰まった台所の引き出しのように聞こえますが、ある意味ではその通りです。他の攻撃パターンの条件を満たさない攻撃は、クリスマスのプレゼント交換でもらったオリーブ種取り器と一緒にこの引き出しに入れられます。

教育サービス業界では、他の多くの業界と同じく、フィッシングが「その他全て」のパターンを圧倒的に占めています。また、フィッシングの報告率の低さでも目立っています。弊社の外部協力者からのデータによると、全業界の中でフィッシング報告を行っている組織はわずか24%に過ぎず、それらのどれもフィッシング啓発キャンペーンで報告されたメールの50%に達していませんでした。自分の組織がターゲットにされたら報告するようにユーザーベースに働きかけることは非常に重要です。報告がなければ、早期警告システムのアラートを見逃してしまうことになります。

同様に、「Webアプリケーション」のパターンが流行している主な理由は、クラウドのメールアカウントで盗まれた認証情報が使われているためです。これは組織のせいだとは言えませんが、弊社の非インシデントデータを分析したところ、認証情報のダンプが実行された日数は教育サービスが最も多く、1年間に28日となっています[40]。全業界の中央値は8日間です。また、攻撃を受けた認証情報の総数も、今年度の報告書で分析した全業界の中で最も多い部類に入ってます(図64)。

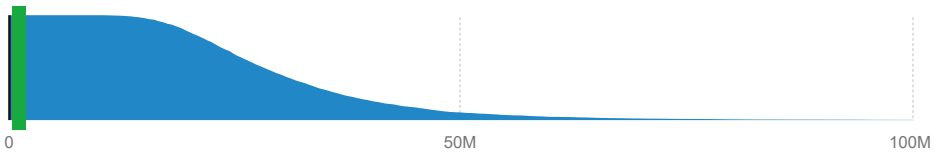


図64. 教育産業のWebブロックにおけるクレデンシャルスタッフィング攻撃 (n = 8)、全産業のモード (緑色の線): 111万

40 業界のモード

この2つのパターン以外でも、残念ながら良い兆候は見られません。ランサムウェアは教育分野のインシデントに大きな影響を与えており、マルウェア関連のインシデントの中では、昨年度の48%から増加して80%を占めています(図65)。これらのランサムウェアのケースは全て、過去2年間に見られた金銭目的によるインシデントの増加にも一役買っています。

弊社の分析によると、その他の懸念事項として、被害者へのマルウェアの配布がメールよりもWebサイト経由の方が多かった唯一の業界であるという事実があります。この情報から、マルウェアは監視されていないメール（BYODデバイスを共有ネットワークに接続した学生の個人メールアカウントなど）を介して配信され、その１つひとつの感染が明らかに大きな組織を危険にさらしていると考えなければなりません。

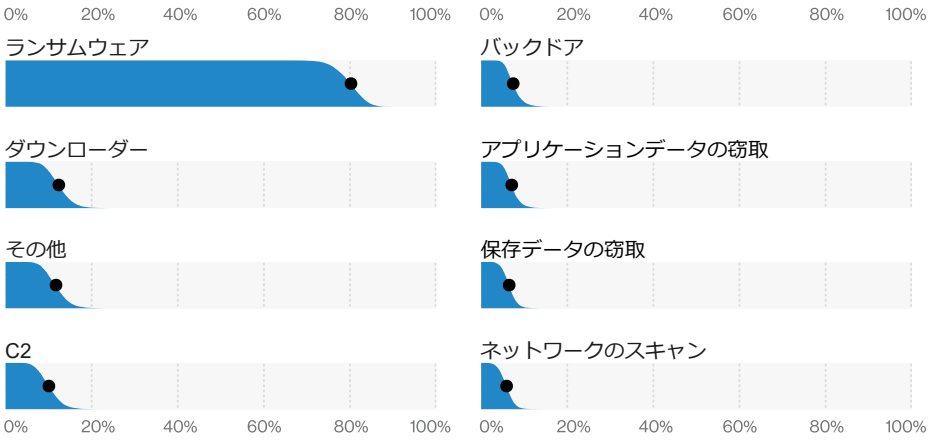


図65. 教育業界のインシデントによく見られるマルウェア の種類 (n = 129)

金融および保険業 NAICS 52

サマリー

この業種でのデータ漏洩/侵害は、金銭目的の外部攻撃者に起因するものが63%を占め、内部の関係者による金銭目的の犯行によるものが18%、内部の関係者のミスに起因するものが9%存在します。また、窃取した認証情報でWebアプリケーションを攻撃する漏洩や侵害も繰り返しこの業種を悩ませています。内部の人間に起因する漏洩/侵害は、悪意のあるアクションによるものから悪意のないエラーによるものへと内容が変わりつつあります。ただし、影響は変わらず大きな被害をもたらしています。

頻度	インシデント1,509件、確認されたデータの暴露448件
上位3つのパターン	「Webアプリケーション攻撃」、「多種多様なエラー」、「その他全て」がデータ漏洩/侵害全体の81%を占めている
攻撃者	外部（64%）、内部（35%）、パートナー（2%）、複数の関係者（1%）（漏洩/侵害）
攻撃者の動機	金銭目的（91%）、スパイ活動（3%）、怨恨（3%）（漏洩/侵害）
侵害されたデータ	個人情報（77%）、その他（35%）、認証情報（35%）、銀行情報（32%）（漏洩/侵害）
上位3つの対策	セキュリティ意識向上トレーニングプログラムの実施（CSC17）、境界防御（CSC12）、セキュアな設定（CSC5、CSC11）

なぜいつも狙われるのか？

金融および保険業界は、顧客から集められるデータというせいで常に標的にされてきました。調査結果によると、今年も金銭を動機とする組織的犯罪分子にとっては、依然として格好の標的 となっています。図66に示すように、業界におけるデータ漏洩/侵害のパターンのトップを争う「Webアプリケーション攻撃」と「多種多様なエラー」の両者がその原因のほとんどを占めています。従業員のミスが、社外からの積極的な攻撃とほぼ同数の漏洩/侵害の原因になっているのは、少し憂慮すべきものです。どうやら、近年は良い支援策がないようです。

2019年の報告書では、「不正使用」はこの業界のデータ漏洩/侵害の原因の上位3つのパターンに挙げられ、全体の21.7%を占めていましたが、今年はわずか8%にまで減少しています。ただし、減少はしているものの、全ての従業員が突如として不正アクセスに対して潔癖になったとは考えられません。これは、従業員の間でモラルが極めて高くなってきている兆候というよりも、単に犯行の可視性の変化を反映した結果と思われます。

図67では悪意のある行為ではなく、意図的ではない行為に注目してみました。最も多いエラーは「誤送信」で、これはその名の通り、間違った相手に情報を送信してしまうというものです。これは「宛先」フィールドに誤った宛先が自動入力されることで、メールなどの電子データが誤送信されることがあるからです。あるいは、一斉メールのように、紙の文書が誤った宛名で大量に送られるケースもあります。メールに添付されていたファイルの内容や配信の規模によっては、どちらも大規模なデータ漏洩/侵害につながる可能性があります。

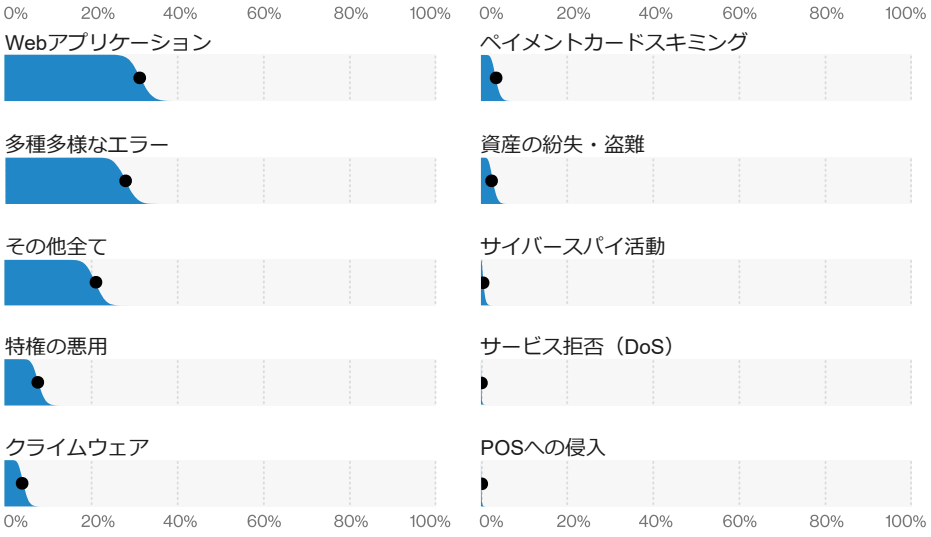
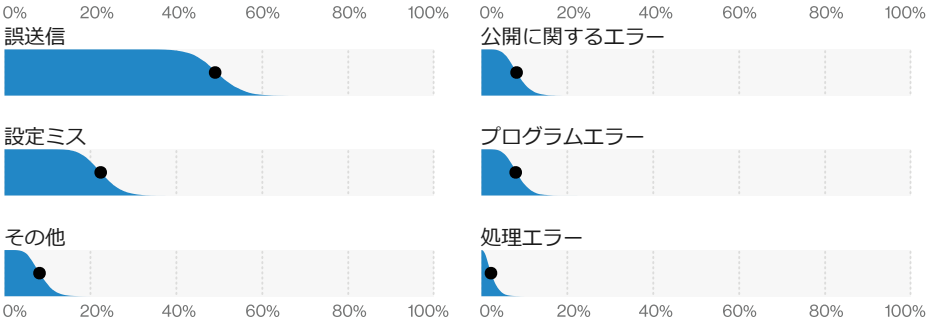


図66. 金融および保険業のデータ漏洩/侵害のパターン（n=448）

図67. 金融および保険業のデータ漏洩/侵害でよく見られるエラーの種類（n=109）



エラーとして2番目に多い「設定ミス」は最近急上昇してきています。これは誰か（多くの場合、システム管理者）がクラウドストレージバケットのセキュリティを確保できなかったり、ファイアウォールの設定を誤ったりした場合に発生します。誤送信と設定ミスの両方のケースにおいては、原因のほとんどが「不注意」でした。有効なセキュリティトレーニングってありますか？　多分誰にもそんなことをしている余裕はありません。

控え目なデータ漏洩/侵害

中学校のダンスの授業で壁際に並ぶ恥ずかしがり屋さんのように目立たず、詳細の判らない攻撃は「その他全て」のパターンに入れられます。ここには、平均的でありながら成功しているフィッシング攻撃や最近ではビジネスメールを標的とする様々な形態の侵害が存在します。その中には、会社の役員レベルの誰かが金銭的利益を要求しているかのようなフィッシングメールもあります。

マインドゲームを一緒にやり続けましょう

また、攻撃者の銀行口座にお金を振り込ませるように仕組まれたシナリオ（なりすまし）も見られます。図68と図69は、これらの一般的なソーシャル攻撃の割合 の高さを示しています。重要なこととして、多くの組織で急所となるのは一般の従業員であるという点です。平均的なユーザー（データへのアクセス状況から標的にされた）が、自分を解雇する権限を持っている人から送られてきたように見える要求を拒むことができるでしょうか？弊社のデータによると答えは「いいえ」です。

この業界での攻撃の大部分は金銭的動機を持つ外部の攻撃者による犯行です。狙いは被害者組織が保存している金銭的報酬を得やすいデータへのアクセスです。この業界には国家機関による「サイバースパイ活動」も少なからず残っていますが、攻撃のほとんどは金の亡者たちによって行われています。

フィルタの適用

過去の調査報告書でも述べているように、弊社の調査では、特定の業界や脅威となる攻撃者のタイプなどに焦点を当てるなど、さまざまな目的でデータ分析にフィルタを利用しています。また、歪曲を減らしたり、見逃してしまう可能性のある傾向を発見したりするために、データの特定のサブセットを除外するときにもフィルタを使用しています。ただし、これらの除外したデータは無視するのではなく、本報告書の他のセクションで個別に分析しています。詳しくは、前述の「インシデントの分類パターンとサブセット」のセクションを参照してください。具体的には、金融業の場合、ボットネットサブセットで数万件のインシデントが発生しており、個別に分析しています。

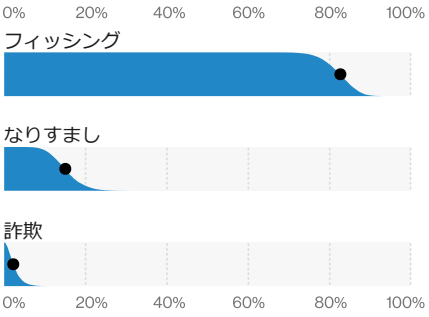


図68. 金融および保険業のデータ漏洩/侵害におけるソーシャル攻撃の種類（n=86）

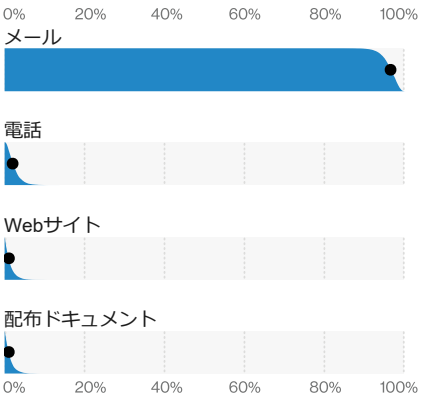


図69. 金融および保険業のデータ漏洩/侵害におけるソーシャル攻撃の経路（n=86）

医療および社会福祉業 NAICS 62

サマリー

この業種では、金銭目的の犯罪者グループによるランサムウェア攻撃が頻繁に確認されています。また、インシデントデータセットを見ると、資産の盗難や消失も依然として問題になっています。基本的なエラーが未だに存在し、その数も少なくありません。エラーのタイプで最も多いのは、誤送信であり、一方で企業内部でのユーザーによるエラーは減少しています。

頻度	インシデント798件、確認されたデータの暴露521件
上位3つのパターン	「Webアプリケーション攻撃」、「多種多様なエラー」、「その他全て」がデータ漏洩/侵害の72%を占めている
攻撃者	外部（51%）、内部（48%）、パートナー（2%）、複数の関係者（1%）（漏洩/侵害）
攻撃者の動機	金銭目的（88%）、愉快犯（4%）、自己都合（3%）（漏洩/侵害）
侵害されたデータ	個人情報（77%）、医療情報（67%）、その他（18%）、認証情報（18%）（漏洩/侵害）
上位3つの対策	セキュリティ意識向上およびトレーニングプログラム（CSC17）、境界防御（CSC12）、データ保護（CSC13）

弊社の外部協力者の交代に伴ってデータセットは変化し、その変化は本報告書に含まれる攻撃の種類とデータ漏洩/侵害の全体的な数の両方に表れます。

今年度は、データセット全体で報告されたデータ漏洩/侵害やインシデントの数が大幅に増加しましたが、その増加は医療業界にも反映されています。実際、確認されたデータ漏洩/侵害の件数は、昨年度の報告書では304件でしたが、今年度は521件に増えています。本書が「データ漏洩/侵害調査報告書」であることから、実際に確認されたデータ漏洩/侵害に焦点が当てられる傾向があります。しかし、医療業界では、例えばランサムウェアのケースに関する保健福祉省（HHS）のガイダンスに従って[41]、データ漏洩/侵害が確認されたものではなく、単に「リスクがある」とする場合でも、他の業界よりもインシデントの関連性が高くなっています。

図70は、医療業界におけるインシデントのパターンの内訳を示しています。クライムウェアのパターンにはランサムウェアのインシデントが含まれており、予想通り、この業界のインシデントの大部分をこのパターンが占めています。このグラフのリストをさらに詳しく調べてみると、坩堝の中で見失いがちなパターンの1つが「資産の紛失・盗難」であることが分かります。これらの資産が手元にないため、データにアクセスされたかどうかを証明するのは簡単なことではありません。したがって、これらはデータ漏洩/侵害が確認されたものとしてではなく、「リスクがある」インシデントに振り分けています。読者の皆様に注意していただきたいのは、弊社のデータセットにおいて「確認されたデータ漏洩/侵害」として表示されていないからといって、業界の規則に従ってその侵害を報告しなくてもよいとは限らないということです。

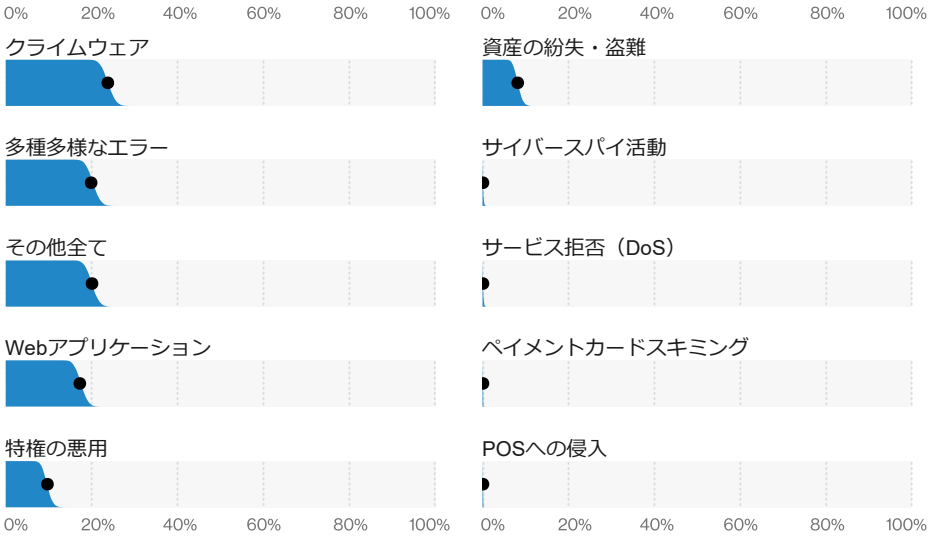


図70. 医療および社会福祉業のインシデントのパターン（n = 798）

41 「対象となる事業体やビジネス・アソシエイトのコンピュータ・システム上にランサムウェア（またはマルウェア）が存在することは、HIPAA セキュリティ規則に基づくセキュリ ティ・インシデントである」 https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf

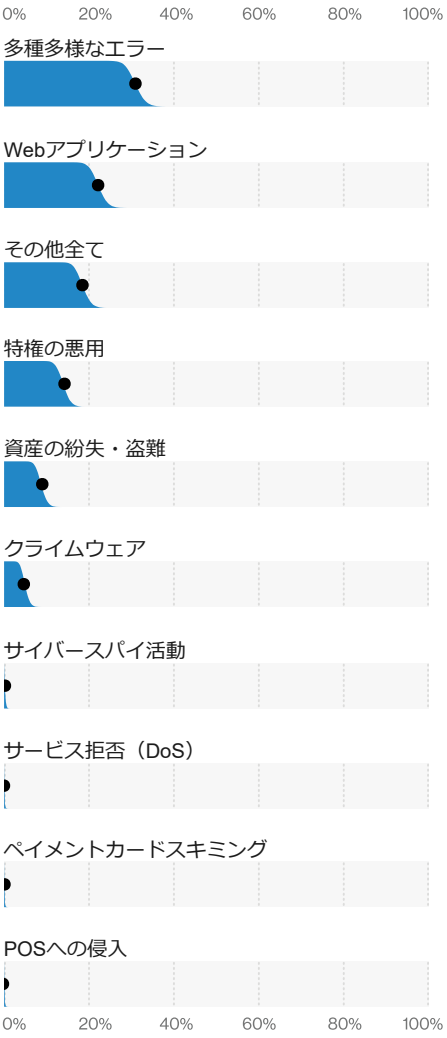


図71. 医療および社会福祉業のデータ漏洩/侵害のパターン（n = 521）

3つのパターンで朝に電話を

以前から医療業界を注視していた方は、図71のデータ漏洩/侵害パターンのランキングに大きな変化があることに気づくかもしれません。「特権の悪用」のパターンが上位の3位内に入っていないことです。これは今年度が初めてです。しかし、このパターンは、医療業界だけではなく、弊社のデータセット全体でも同じように大幅に減少しています。2019年度の報告書では、「特権の悪用」が攻撃の23%を占めていたのに対し、2020年度はわずか8.7%にまで激減しています。これは、内部攻撃者が仕事で付与されたアクセス権を使って悪意のある行為をしなくなったということでしょうか?まあ、そこまではいかないでしょう。しかし、来年度のデータが集まったときに、この傾向が続いているかどうかは興味深いところです。

内部攻撃者の悪用によるデータ漏洩/侵害が減少したことに伴うもう1つの変化は、複数の攻撃者による侵害が減少したことです。これまで医療業界が常にトップだったこの種のデータ侵害は、通常、外部と内部の攻撃者が協力してデータを持ち出し、それが金融詐欺に利用されることで発生します。複数の攻撃者によるデータ侵害は、昨年度は4%でしたが、今年度は1%にまで減少しています。2019年のDBIRでは、医療業界について内部攻撃者によるデータ侵害（59%）が外部攻撃者による侵害（42%）を上回ったという初の報告がありました。今年度は外部攻撃者によるデータ侵害が51%とわずかに多く、一方で内部攻撃者による侵害は48%に減少しています。しかし、この割合の差はわずかなものであり、医療業界は依然として悪質な内部攻撃者が最も多い業界であることに変わりはありません。

人生の多くのことがそうであるように、1つの攻撃が広まると、他の攻撃は減少し始めます。これは「多種多様なエラー」のパターンにも当てはまります。この業界の上位3つのパターンには頻繁にランクインしていますが、今年度は金メダルを獲得しました。では、医療業界の中で一番多いエラーは何だと思いますか?それは、私たちが最もやりがちな誤送信です。

このエラーは、大きく2つのカテゴリーに分類される傾向があります。

- 誰かがメールを送信する際に、間違った（そして大抵は広範囲の）配布先に送信してしまう場合。機密データを含むファイルが添付されていたら、まさにボーナスです。
- ある組織が大量の郵便物（紙の文書）を送る際に、封筒の宛先と封筒の内容がずれてしまう場合。郵送の場合は、そのプロセス全体のサンプリングを定期的に行わなければ、患者の機密情報を守ることはできません。

医療業界といえば、普通は医療データのことを思い浮かべます。そして驚くことではありませんが、この業界では、このタイプのデータが最も頻繁に侵害されています。しかし、これらの攻撃では、個人情報（基本的な人口統計情報からそれ以外の標的とされたデータ要素まで）と認証情報の両方が盗まれています。医療業界で2番目に多いパターンは、Webアプリケーション攻撃です。患者ポータルを開設し、革新的な方法で患者とコミュニケーションする組織が増えるにつれ、攻撃の対象となる箇所もさらに増えています。

最後に、他の攻撃パターンの条件に当てはまらない攻撃のために、遺失物取扱所ならぬ「その他全て」のパターンがあります。このパターンの中に、ビジネスメール詐欺が含まれます。この攻撃をご存知でない方のために、これは通常、なりすまし攻撃（被害者を思い通りに行動させるために考案されたシナリオ）を利用して（電信送金、ギフトカード、またはその他の手段で）送金させることを目的としたフィッシング攻撃です。これらはデータセット全体で共通の攻撃タイプですが、標的にされているのは患者の医療データだけではないことを医療機関に思い出させてくれます。

これらの症状に最初に気づいたのはいつですか?

データを侵害し、データを漏洩させるのに要する時間は、データセット全体で短くなってきています。残念ながら、侵害されたことに組織が気づくまでの時間は、これに追いついていません。これは、給料を得るまでにかかる時間と課税されるまでにかかる時間との関係に似ています。いくつかの攻撃は、その性質上、発生するとほぼ同時に発見されるものもあります。良い例としては、ノートPCを盗まれた場合、車の窓を壊して戦利品を持ち去るのにどれくらい時間がかかると思いますか?(これは修辞的な質問なので、メールでの回答は無用です。正解でも賞品はありません。)同様に、ノートPCの所有者が自分の車に戻ってきて侵入を発見するのにも、それほど時間はかかりません。

犯罪の性質上、どちらの時間も短いものです。対照的に、アクセス権を悪用して毎週データを少しずつコピーして仲間に売り、その仲間がその情報を金融詐欺に利用しているような内部攻撃者の場合は、かなり長い間捕まらないかもしれません。

情報産業 NAICS 51

サマリー

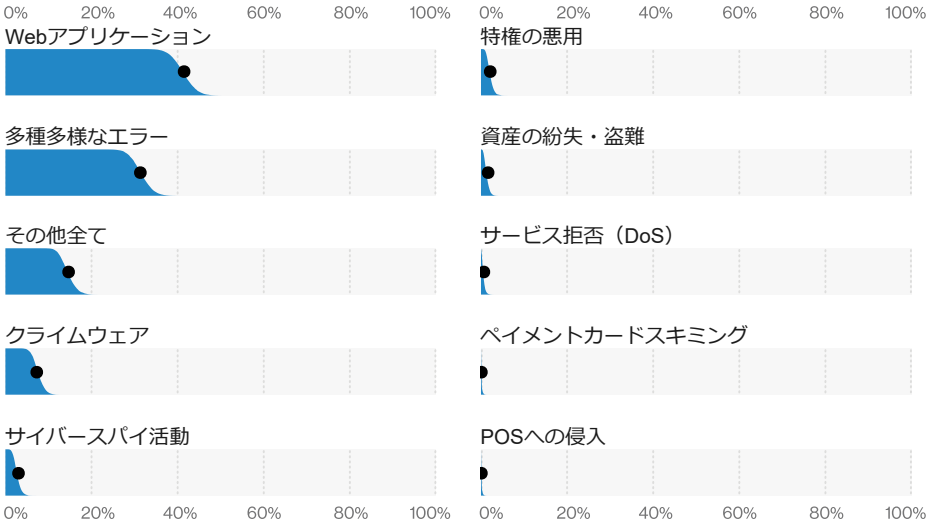
この業種では、Webアプリケーションの脆弱性を突いた攻撃や盗取した認証情報を悪用した攻撃が数多く確認されています。依然としてエラーが漏洩/侵害発生の大きな要因になっており、クラウドデータベースの構成の不備がエラーの大半を占めています。また、この業種では依然として、DoS攻撃の増加が問題になっています。

頻度	インシデント5,741件、確認されたデータの暴露360件
上位3つのパターン	「Webアプリケーション攻撃」、「多種多様なエラー」、「その他全て」がデータ漏洩/侵害の88%を占めている
攻撃者	外部（67%）、内部（34%）、複数の関係者（2%）、パートナー（1%）（漏洩/侵害）
攻撃者の動機	金銭目的（88%）、スパイ活動（7%）、愉快犯（2%）、怨恨（2%）、その他（1%）（漏洩/侵害）
侵害されたデータ	個人情報（69%）、認証情報（41%）、その他（34%）、内部情報（16%）（漏洩/侵害）
上位3つの対策	セキュアな設定（CSC 5、CSC 11）、継続的な脆弱性管理（CSC 3）、セキュリティ意識向上トレーニングプログラムの実施（CSC 17）

一人でも多くの参加を！

DBIRの情報産業セクションへようこそ。どうぞお楽しみください。このセクションでは、Webアプリケーション攻撃から、エラー、フィッシング、マルウェアに至るまで、全てを網羅しています。2019年度のNAICS 51業界で見られた主な3つのパターンは、データ漏洩/侵害全体の40%を超える「Webアプリケーション」、次に「多種多様なエラー」、3番目が「その他全て」でした（図72）。

図72. 情報産業のデータ漏洩/侵害のパターン（n = 360）



2019年以降、Webアプリケーションへの攻撃は、データ侵害での割合とインシデントの件数の両方で大幅に増加しています。これは、この業界の組織が注意すべきことの1つです。なぜなら、攻撃者がWebアプリケーションへのアクセスを得るために、Webエクスプロイトの利用と窃取した認証情報の悪用に等しく労力を割いているからです。この業界では外部サービスやインターネットへの依存度が高いことを考えれば、他の業界に比べてWebアプリケーションの悪用の割合が高いのは、それほど驚くことではありません。ただし、弊社が収集した非インシデントデータによれば情報産業は、タイムリーに脆弱性パッチを適用している割合が最も高い業界の1つでもあります（図73）。

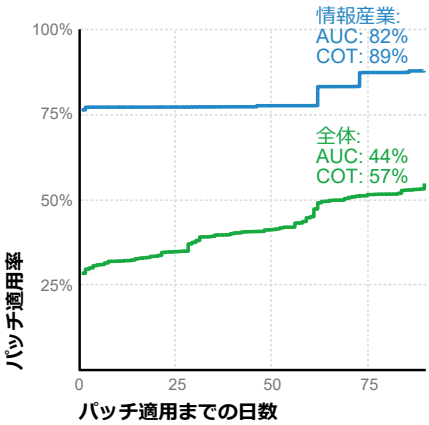
エラーへの賛歌

人的ミスは誰にでも犯す可能性があり、情報インフラを管理する技術者も例外ではありません。このため、エラーはデータ漏洩/侵害の種類の中では2番目に多く、例年と比較的同じレベルを維持しています（一貫性があることは必ずしも良いことではない）。設定ミスは、エラーの中でも圧倒的に多いタイプです。データベースやファイルストレージのセキュリティ保護が不十分なまま、クラウドサービスで直接公開されてしまうことに大きく関係しています。これらのタイプのインシデントについては、セキュリティ研究者がインターネット上に晒されているものを調べるだけで発見するという話を耳にすることがあります。楽観主義者は、これらの新しい技術が普及すれば、人々がこの種の間違いを犯すのを止められる（あるいは少なくとも遅らせられる）と期待します。一方、現実主義者はこのようなことにお金をかけたくないと思うでしょう。

あなたは詐欺師ですね

テクノロジーに支えられているこの業界に影響を与えているのは、技術的な問題だけではありません。この業界の組織も、誰もが影響を受ける同じタイプのソーシャルエンジニアリング攻撃の餌食になっています。これらの攻撃のほとんどは「その他全て」のパターンに該当し、2019年度にはデータ侵害全体の14%を占めていました。ソーシャル攻撃に関しては、フィッシングとなりすまし（メールで情報提供を求めたり、既存の会話を利用して情報を得ようとする）と比較的均等に分かれています。もっとも一般的な技術の1つに、仲間のタイポスクワッティングドメインを使用して既存のメールスレッドを送信させたり、銀行口座情報を更新させたりする手法があります。

図73. 情報産業の漏洩/侵害の脆弱性へのパッチ適用 (n = 36,255)



高速度と広帯域幅

消費者は、動画の読み込みが速く、Webサイトのコンテンツが高速で画像が更新されることを求めているため、帯域幅の広いインターネット回線がこの業界の重要な部分を占めています。残念ながら、サイバー犯罪者はその重要性を知っており、サービスや機能を混乱させるためにDoS攻撃でこの業界を執拗に狙ってきました。2019年度のデータでは、DDoSインシデントの割合が継続的に増加していることが示されています（図74）。この業界は、一人称視点のシューティングゲームのレッドバレル以上に標的にされるだけでなく、BPSの中央値が2番目に高い攻撃にも晒されています。多くの企業にとって残念なことに、これらの攻撃を軽減するためには助けが必要な場合が多いため、セカンドプレイヤーを味方につけておくと力になります。

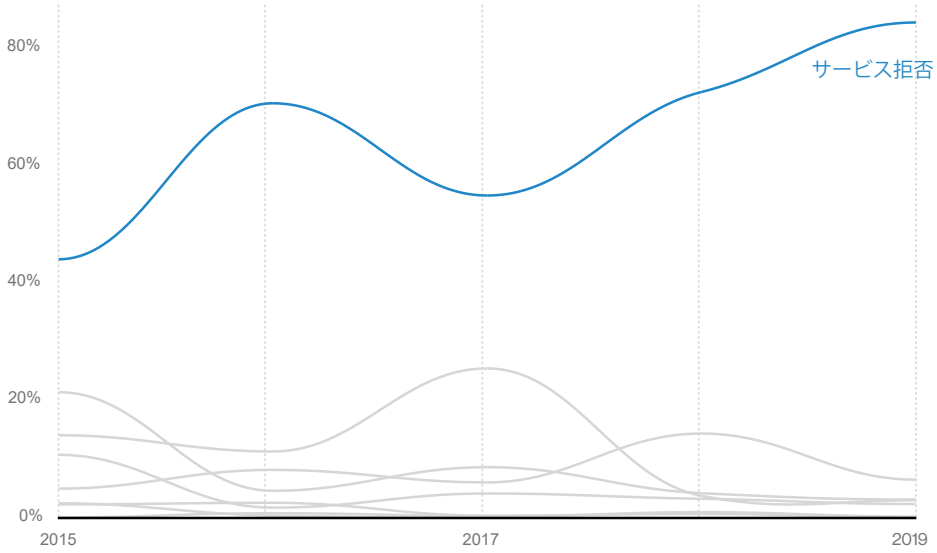


図74. 情報産業のインシデントのパターンの経時的変化

製造業

NAICS 31–33

サマリー

製造業は、パスワードダンパーマルウェアや盗取した認証情報を使用してシステムに侵入したり、データを盗み出したりする外部からの攻撃を受けています。攻撃のほとんどは金銭目的の攻撃ですが、この業種ではスパイ活動を目的とした攻撃も相当な数が確認されています。また、従業員がアクセス権限を悪用してデータを不正に持ち出すケースも依然として問題になっています。

頻度	インシデント922件、確認されたデータの暴露381件
上位3つのパターン	「クライムウェア」、「Webアプリケーション」、「特権の悪用」が漏洩/侵害の64%を占めている
攻撃者	外部（75%）、内部（25%）、パートナー(1%)（漏洩/侵害）
攻撃者の動機	金銭目的（73%）、スパイ活動(27%)（漏洩/侵害）
侵害されたデータ	認証情報(55%）、個人情報(49%）、その他（25%）、決済情報（20%）（漏洩/侵害）
上位3つの対策	境界防御（CSC12）、セキュリティ意識向上トレーニングプログラムの実施（CSC17）、データ保護（CSC13）

「下手な役者、下手な演技、下手なダジャレ」

「人間の正しい研究課題は人間（製造）である」と言われますが、少なくとも我々はそのような金言が当てはまるのを確信しています。このトピックについてはあれこれと考えてきたので、少なくともそうあってほしいと願っています。今年は、製造業においてインシデントとデータ漏洩/侵害の両方が非常に多く見られました。いつもと同じく、大幅な増加が観察される場合は、傾向を示していると言えますが、あるいは単に弊社の事例数を反映しているだけのことかもしれません。今回のケースでは、確かに後者であろうと思われます。

しかし、NAICS 31～33は長い間サイバー攻撃の標的にされてきており、今年も例外ではありません。敵対国の成功を見極め、それを丸々コピーしようとしている国家組織、あるいは競争に参入しようとする新興企業だとしても、この業界には攻撃者が狙う膨大な量の貴重なデータが存在します。そして、それらのデータを窃取する攻撃者が採用する主な手段は図75に示す「クライムウェア」のパターンのいずれかです。つまり、「パスワードダンパー」、「アプリケーションデータの窃取」、「ダウンローダー」などの類です。

パスワードの窃取、ネットワークへの侵入、ソフトウェアのダウンロード、データの窃取などの組み合わせは、製造業界で起きているものを明確に描いていますが、それはこの業界の企業にとっては壁に掛けて眺めたいような絵画ではないことは確かです。しかし、一般的なマルウェアのトピックとは別に、ランサムウェアは（この報告書ではデータ漏洩や侵害とは考えていませんが）、インシデントで発見されたマルウェア全体の23%を占めており、この業界においては依然として危険性が高いことを忘れないでください。

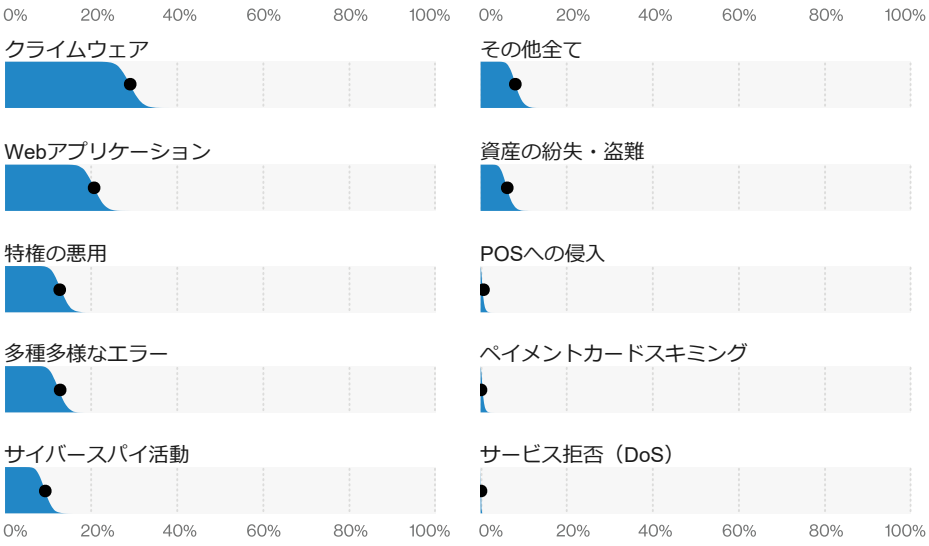
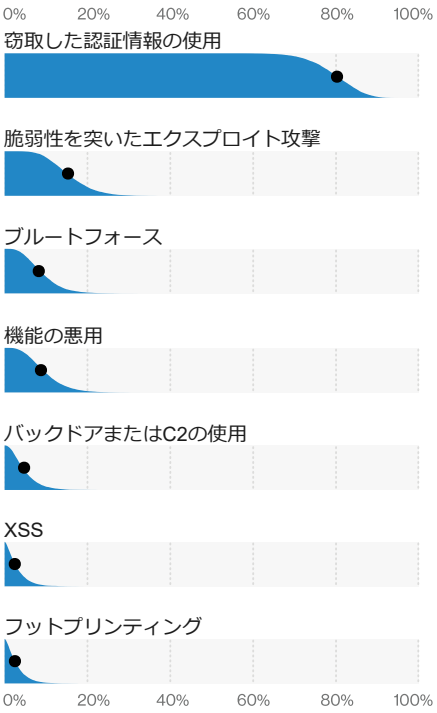


図75. 製造業のデータ漏洩/侵害パターン（n=381）

図 76. 製造業のデータ漏洩/侵害における ハッキングの種類（n=44）



「Webアプリケーション攻撃」は今年第2位となり、主に「窃取した認証情報の使用」によって企業のさまざまなWebアプリを侵害しています。これらの認証情報は、フィッシング攻撃の成功によって提供された悪意のあるリンクを介して窃取されることもあれば、デスクトップPCの共有で盗まれることもあり、また被害者に至るまでの感染経路が不明な場合もあります。侵害の手口にかかわらず、これらの認証情報は多くの場合さまざまな形態のクラウドベースのメールを介したものであり、この業界では目的達成の手段として非常に成功しています（図76）。

製造業の第3位あたりでは、いくつかのパターンが密接にグループ化されています。「不正使用」（13%）は定義上、内部の関係者が関与しており、そのほとんどが「特権の悪用」です。正当なアクセス権を持っている攻撃者がその特権を使って悪質なことをしています。主な例として、データの誤操作、個人のメールアカウントを使って会社のデータを送信する、自宅で仕事をするためにクラウドドライブにデータを保存するなどがあります（図77）。

今年は比較的にエラーが全業種で偏在しており、製造業においても他の業界と同様に誤送信と設定ミスが見られます。最後に、サイバースパイ活動に関連した攻撃について、少し触れておきます。

図77. 製造業のデータ漏洩/侵害における不正使用/悪用の種類

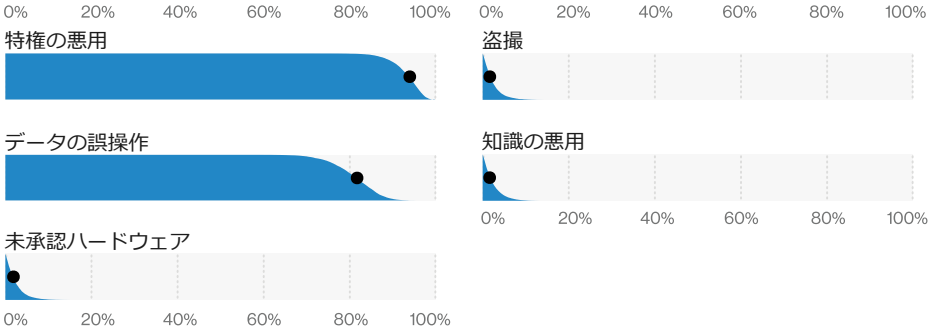


図78と図79からも分かるように、攻撃者の38%は「国家関連組織」であり、データ漏洩/侵害の28%は「スパイ活動」を動機とするものでした。過去の調査報告書でも述べてきたように、何かを一から作り出すよりは他から盗む方が安くて簡単です。また、大規模な組織ではヘルプデスクの機能を外注するケースが多いのですが、原則として知的財産や研究・デザイン設計を海外に持ち出すことは嫌います。

図78. 製造業のデータ漏洩/侵害における外部攻撃者の種類（n=83）

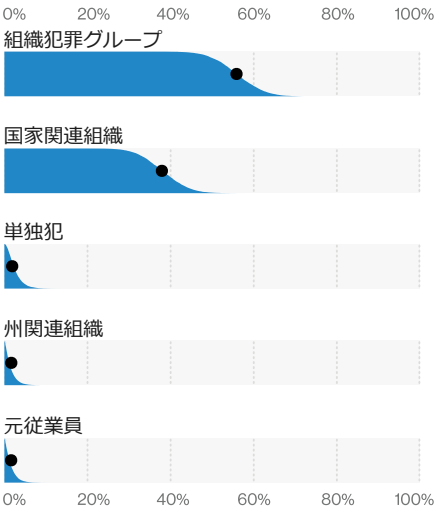
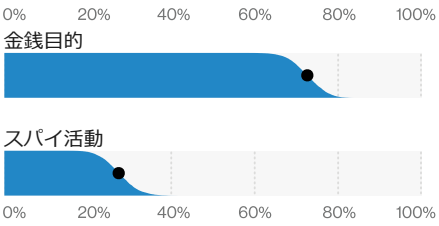


図79. 製造業のデータ漏洩/侵害における外部攻撃者の動機（n=121）



鉱業、採石業、石油・ガス採掘業および公益事業 NAICS 21+22

サマリー

漏洩/侵害のタイプは多岐にわたりますが、インシデントデータの多くはフィッシングやなりすましなどのソーシャル攻撃に関するものです。ただし、データの漏洩は確認されませんでした。オペレーションテクノロジー（OT）資産に関係するスパイ活動を目的とした攻撃やインシデントも、この業種では問題になっています。

頻度	インシデント194件、確認されたデータの暴露43件
上位3つのパターン	「その他全て」、「Webアプリケーション攻撃」、「サイバー諜報活動」がデータ漏洩/侵害の74%を占めている
攻撃者	外部（75%）、内部（28%）、複数の関係者（2%）（漏洩/侵害）
攻撃者の動機	金銭目的（63%～95%）、スパイ活動（8%～43%）、自己都合/その他/二次的動機（各0%～17%）、恐怖/愉快犯/怨恨/イデオロギー（各0%～9%）（漏洩/侵害）
侵害されたデータ	認証情報（41%）、個人情報（41%）、その他（35%）、内部情報（19%）（漏洩/侵害）
上位3つの対策	セキュアな構成（CSC 5、CSC 11）、境界防御（CSC 12）、セキュリティ意識向上トレーニングプログラムの実施（CSC 17）
データ分析ノート	攻撃者の動機は、既知の動機によるデータ漏洩/侵害が21件のみだったため、パーセンテージの範囲で表しています。

NAICSのマッシュアップ

この新しいセクションでは、鉱業、採石業、石油・ガス採掘業（NAICS 21）と公益事業（NAICS 22）を組み合わせて、それぞれに影響を与えたインシデントやデータ漏洩/侵害をまとめています。かなり深く掘り下げてみたものの、今年度の報告書に単独でNAICS 21のセクションを設けるほど、石油を採掘することはできませんでした(有効な統計にするには、最低限のインシデント数が必要です)。しかし、NAICS 22と組み合わせたこのセクションは、読み物としては刺激的な内容であり、退屈させないと信じております。

図80を見てみると、「その他全て」、「Webアプリケーション」、「サイバースパイ活動」がデータ漏洩/侵害の上位3つのパターンであるように見えますが、これらは重複するケースが多いため、どれがより普及しているかを統計的に判断することは不可能です。新しい業種のセクションにこのような多様なデータ侵害があるのは興味深いですが、提言を出す際に「全てのCISOへの注意事項：全てのものにセキュリティを確保しましょう！」以上に的を絞ることが難しくなります。

とはいえ、指摘しておきたいのは、「その他全て」のパターンでは、インシデントとデータ漏洩/侵害のどちらにおいても、明らかにFMSEであると思われるなりすましの攻撃など、金銭的利益を動機としたフィッシングが大半を占めているということです。

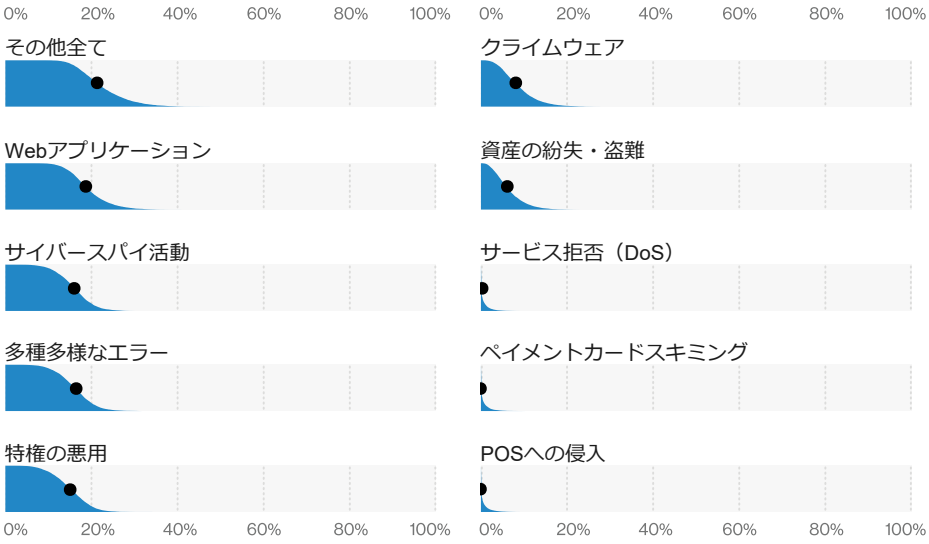


図80. 鉱業、採石業、石油・ガス採掘業および公益事業のデータ漏洩/侵害のパターン（n = 43）

目を閉じていても、データ侵害だったのでしょうか？

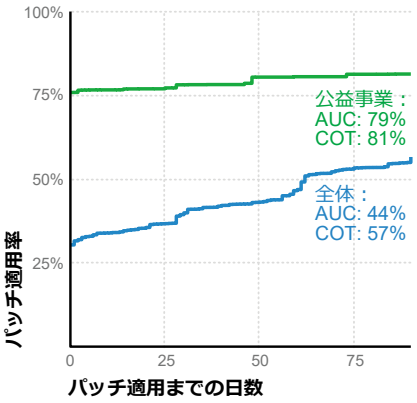
「その他全て」のパターンはインシデント（データ開示の可能性があったが確認されなかったケース）の中で最も大きな割合を占めており、特に注意が必要です。これらの業種では、データ開示の可能性のあるインシデントが、確認されたデータ侵害の数とほぼ同じくらい発生しています。これは、スパイ活動を動機としたデータ侵害の可能性のある割合が8%～43%と幅広い業種の中では特に問題となっていますが、インシデント全体で占める割合は10%です。

上位3つのパターンをまとめると、「Webアプリケーション」では、フィッシングで窃取された認証情報の使用が多く、「多種多様なエラー」では「設定ミス」と「誤公開」が目立っており、どちらも業務プロセスの強化と人材育成によって軽減が可能です。

Webアプリケーションのインフラストラクチャにパッチが適用されていない脆弱性は、脆弱性を突いたエクスプロイト攻撃を自動で行うツールを持っている者に発見される可能性があります。インフラストラクチャのパッチを最新の状態に保つことは、間違いなくセキュリティのベストプラクティスです。パッチ適用までの時間に関する非インシデントのデータ（図81）を見てみると、公益事業部門のスコアが平均よりも高くなっています。これは良い兆候です。弊社の調査によると、リリースされてから最初の四半期以内に適用されないパッチは、ほとんどの場合、全く適用されないからです。これにより、熟練の攻撃者でなくても脆弱性が残るインフラストラクチャの攻撃が可能なツールを構築する時間があるということです。

また、これらの業種が報告の対象となっていることから、最新版のVERISではOT機器に関わるインシデントを追跡するために、OT専用の項目を追加しました。今年度の件数は少ないですが、製造業（NAICS31～33）と並んでこの業種が中心となっています。

図81. 鉱業、採石業、石油・ガス採掘業および公益事業における脆弱性へのパッチ適用(n = 151,658)



その他のサービス業 NAICS 81

サマリー

その他のサービスには、様々な種類のビジネスが含まれており、パーソナルサービスや修理サービス、非営利の宗教法人や公益団体などがあります。金銭目的の外部からの攻撃が最も多く、Webアプリケーションを標的にした攻撃がデータ漏洩/侵害の39%を占めています。この業種では、従業員のミスも問題になっており、特に構成やデリバリーの不備が目立っています。認証情報もよく狙われる標的ですが、最も盗まれることが多いのは個人情報データです。

頻度	インシデント107件、確認されたデータの暴露66件
上位3つのパターン	「Webアプリケーション攻撃」、「多種多様なエラー」、「その他全て」が漏洩/侵害の83%を占めている
攻撃者	外部（68%）、内部（33%）、複数の関係者（2%）（漏洩/侵害）
攻撃者の動機	金銭目的（60%～98%）、スパイ活動（0%～28%）、自己都合/恐怖/愉快犯/怨恨/その他/二次的動機（各0%～15%）（漏洩/侵害）
侵害されたデータ	個人情報（81%）、その他（42%）、認証情報（36%）、内部情報（25%）（漏洩/侵害）
上位3つの対策	境界防御（CSC 12）、セキュリティ意識向上トレーニングプログラムの実施（CSC 17）、セキュアな設定（CSC 5、CSC 11）
データ分析ノート	攻撃者の動機は、既知の動機によるデータ漏洩/侵害が12件のみだったため、パーセンテージの範囲で表しています。また、グラフによっては、期待値を表示するには十分なデータが観測されていないものがあります。

攻撃の対象が広がる

その他のサービス（NAICS 81）も、今年度の報告書で新しく登場した業種です。このNAICSコードは驚くほど幅広く、さまざまな個人サービスや修理サービスから非営利の宗教団体や公益団体までカバーしています。奇妙なことに、このコードには個人世帯のサブコード（814）も含まれているのに、それらのデータはこのデータセットには含まれていません。インシデントを調査対象としてDBIRに含めるには、被害者団体の存在が必要です。そこが法律の焦点であり、規制が効果を発揮する可能性が高いところだからです。他の新しいセクションでも述べたように、この業界を報告書に含めるのは今年が初めてですが、この業界については数年前のデータがあります。

トップの座を争う

この業界の侵害パターンの上位3つは、「Webアプリケーション攻撃」、「多種多様なエラー」、「その他全て」でした。インシデントのパターン（データ侵害が認められないもの）でも、順位は異なるものの、同じパターンが上位を占めています。

この業界の昨年のデータからの大きな変化は、「サイバースパイ活動」のパターンが減少したことです。昨年は徒競走で1位の座を守っていましたが、図82を見ると、他のパターンに「どうぞお先に、後から追いつくので」と息を切らしているかのようです。この変化に合わせて、外部攻撃者のデータ侵害の多様性と動機が、国家が関与する攻撃/スパイ活動から組織的な犯罪/金銭目的へと変化していることが分かります。データを収益化することを純粋に楽しむためにデータを狙うのが好きな攻撃者たちは、この業界で仲間を見つけたようです。

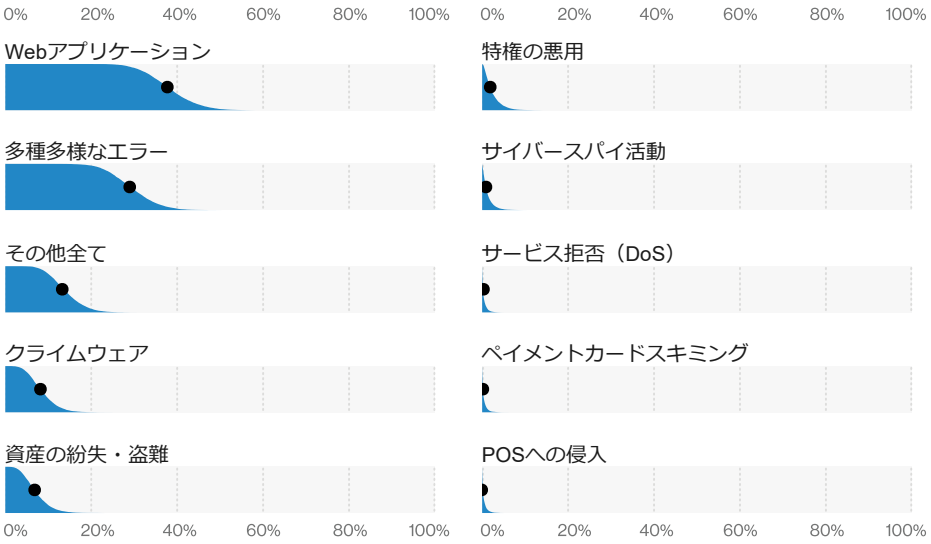


図82. その他のサービス業のデータ漏洩/侵害のパターン（n = 66）

図83. その他のサービス業の漏洩/侵害によく見られるエラーの種類 (n = 21)

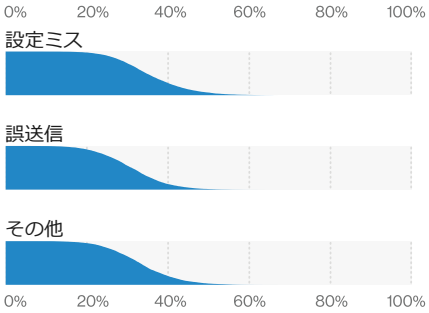
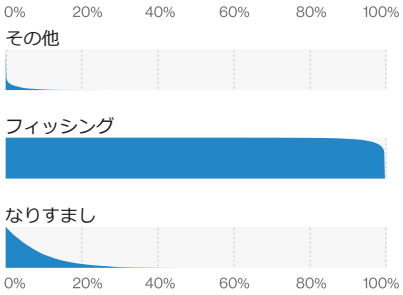


図84. その他のサービス業の漏洩/侵害によく見られるソーシャル攻撃の種類 (n = 12)



「Webアプリケーション攻撃」パターンにはハッキング攻撃が含まれており、好まれる攻撃の種類は、既に窃取されている認証情報の使用です。それはそうでしょう。他人のコンピュータに侵入しようとするときに、認証情報を使いたくない人がいるでしょうか?ただで手に入る鍵を嫌がる泥棒がいるでしょうか?また、バックドアやコマンドアンドコントロール（C2）インフラはいつでも手口として優れていますが、軽快な足取りで簡単に玄関から侵入できるのであれば、わざわざ無理をする理由があるでしょうか？　つまらない質問はこれで終わりにしましょう。

うまくいかないことは、自分の身に起きる

「多種多様なエラー」パターンには、従業員が行うあらゆるミスが含まれます。「その他のサービス」のエラーでは、「設定ミス」と「誤送信」の2つが際立っています（図83）。設定ミスは、情報セキュリティの大敵です。これらのデータ侵害は、内部攻撃者（多くの場合、大量のデータにアクセスできるシステム管理者やDBA）が、データを扱うインスタンスをクラウドに立ち上げながら、アクセスを制限するためのセキュリティ管理を怠っていることが原因で発生します。このような侵害が発生すると、遅かれ早かれ勇猛なセキュリティ研究者が検索ツールを使ってその事実を発見したり、誰かが通報したりします。

この業界で最も一般的なエラーのもう1つは、機密情報が誤った受信者に送られる誤送信です。よくある例としては、メールの「To:」または「cc:」フィールドのオートコンプリートにより、誤った相手に送信される場合が挙げられます。他の例では、メールのアドレスとメールの内容が食い違ったまま、大量のメールを一斉送信することなどがあります。手紙を開いただけで、中に他人の個人情報が入っているのを見つけてしまうのは、決して良いことではありません。

最後に、「その他全て」のパターンがありますが、これは弊社で寄せ集めたものです。他のパターンの条件を満たさない攻撃はここに含めています。これらの攻撃は、セキュリティ侵害で香り高い花ではありませんが、多くのものはフィッシング攻撃（詳細情報が提供されない）で構成されています。

ビジネスメール詐欺もこのパターンに含めています。ビジネスメール詐欺は、一般的ななりすましと経営幹部を騙るなりすましの2つに分けられます。一般的ななりすましとしては、作り話のシナリオがあり、通常は請求書の支払いや、攻撃者が指定する銀行口座への電信送金のいずれかを要求します。上司のメールアカウントを窃取したうえで、本人が旅行中になるのを待ち、緊急の依頼を行ない、本人への確認の連絡をできるだけとらせないようにすることもあります。後者のタイプでは攻撃者が経営幹部レベルのメンバーのふりをして、電信送金ではなくデータを要求することがあります。図84は、フィッシングとなりすましがこの業界ではいまだに盛んに行われていることを示しています。これらのソーシャルエンジニアリング攻撃は、どちらも通常はメールを介して行われます。

専門的・科学的・技術的サービス業 NAICS 54

サマリー

この業種では、金銭目的の攻撃者が認証情報を盗み、それを利用してWebアプリケーションインフラストラクチャに攻撃を仕掛ける事例が後を絶ちません。不正アクセスに利用されるのは、フィッシングやなりすましといったソーシャルエンジニアリングの手口がほとんどです。また、この業種は定期的にDoS攻撃を受けています。

頻度	インシデント7,463件、確認されたデータの暴露326件
上位3つのパターン	「Webアプリケーション攻撃」、「その他全て」、「多種多様なエラー」がデータ漏洩/侵害の79%を占めている
攻撃者	外部（75%）、内部（22%）、パートナー（3%）、複数の関係者（1%）（漏洩/侵害）
攻撃者の動機	金銭目的（93%）、スパイ活動（8%）、イデオロギー（1%）（漏洩/侵害）
侵害されたデータ	個人情報（75%）、認証情報（45%）、その他（32%）、内部情報（27%）（漏洩/侵害）
上位3つの対策	セキュアな設定（CSC 5、CSC 11）、セキュリティ意識向上トレーニングプログラムの実施（CSC 17）、境界防御（CSC 12）

この業界は、主に顧客に直接サービスを提供する多様な企業から成ります。業種は、弁護士、会計士、建築家から研究所やコンサルティング会社まで、幅広く多岐にわたるものの、共通する特徴があります。それは、組織の生計にとってインターネット上での存在感が非常に重要であること、そして、従業員は人間であり、間違いを犯すことがあるということです。

この業界の組織にとって、インターネット上での存在感が重要であることを述べましたが、それゆえに、今年度は「Webアプリケーション攻撃」のパターンが非常に多く見られました（図85）。これらの攻撃は、窃取された認証情報（主にフィッシングで取得されるが、他の企業のデータ漏洩/侵害によってインターネット上に公開され、進取的なハッカーに発見されるのを待つだけの場合もある）を使用することで、ますます活況を呈しています。これらの攻撃は、この業界での個人情報の盗用を促進させます。また、Webインフラがどのような形態であっても、窃取された認証情報を使って運試しをしようとする者が常に存在することを考えると、近い将来にはなかなか終わりそうにありません。

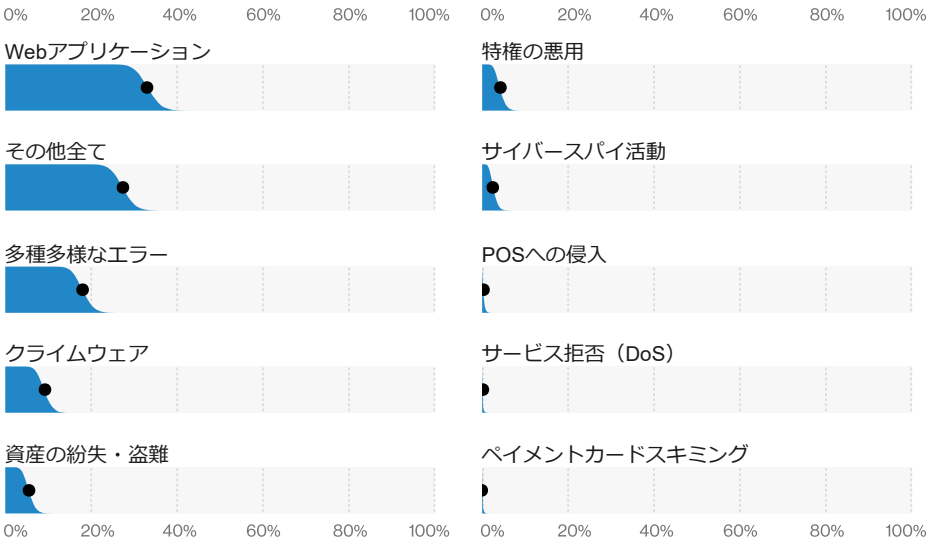


図85. 専門的・科学的・技術的サービス業のデータ漏洩/侵害のパターン（n = 326）

攻撃されているような気がする

それにしても、なぜこの業界の組織が攻撃の標的にされるのでしょう。「場所、場所、場所」という表現を知っていますか ?この業界は有用な個人情報が多く存在します（実際、認証情報とは別に、個人情報はこれらの侵害で最も標的とされているデータタイプです）。この業界は必ずしも金融情報やペイメントカードの記録で溢れているわけではありませんが、個人情報は様々な種類の金融詐欺において相当の利益を得られる可能性があり、それが魅力となっています。図86は、スパイ活動の（さらにはエラーの）動機を退け、金銭的動機によるデータ漏洩/侵害が増え続けていることを示しています。

「その他全て」のパターンには他のパターンの基準に合わない攻撃が集められます。廃れた攻撃のゴミ箱のようです。これらの大半は詳細情報の少ないフィッシング攻撃ですが、ソーシャルエンジニアリングの攻撃者が少し手を加えて、獲物をおびき寄せるためのありそうなシナリオを考案することもあります。ビジネスメール詐欺をよくご存知の方は、フィッシングがそこに存在することも理解できるでしょう。専門サービスは、フィッシング攻撃の標的のまさにど真ん中に位置しています。しかし、この攻撃は単に攻撃を受けるだけではなく、被害者がクリックするかどうか、データを送信するかどうかが重要です。また、フラグを立てて社内のセキュリティ担当者に「やったこと」を知らせるようにしているかどうかにも関係しています。

この業界のフィッシングに関する報告は、やや混同されぎみです。図87では、クリック率が全体の中央値とほぼ一致しています。また、図88では、送信率が低くなっています（右側の送信率の図で0%の企業の数に注目してください）。これは良い兆候です。認証情報を差し出す人の数は少ない方がよいに決まっています。ただし、悪い兆候としては、報告率も低くなっています（左側の報告率の図でも0%の企業の数が高いのが分かります）。つまり、フィッシングの被害に遭ったことを報告する社員がいないということです。2つ目のこの報告率という指標は、組織のセキュリティ対策チームにとっては、データ漏洩/侵害の影響を軽減するために非常に重要な指標です。

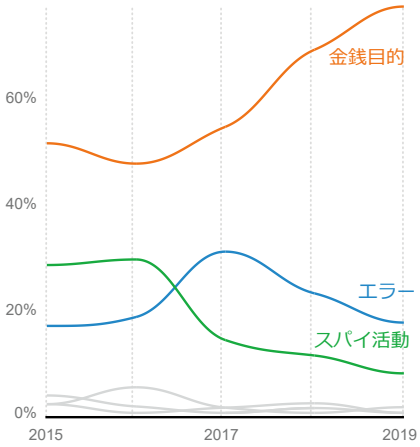


図86. 専門的・科学的・技術的サービス業の漏洩/侵害の動機の経時的変化

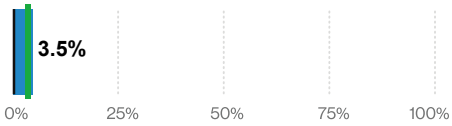


図87. 専門的・科学的・技術的サービス業のフィッシングテストのクリック率の中央値、全産業の中央値 (緑色の線): 3.6%

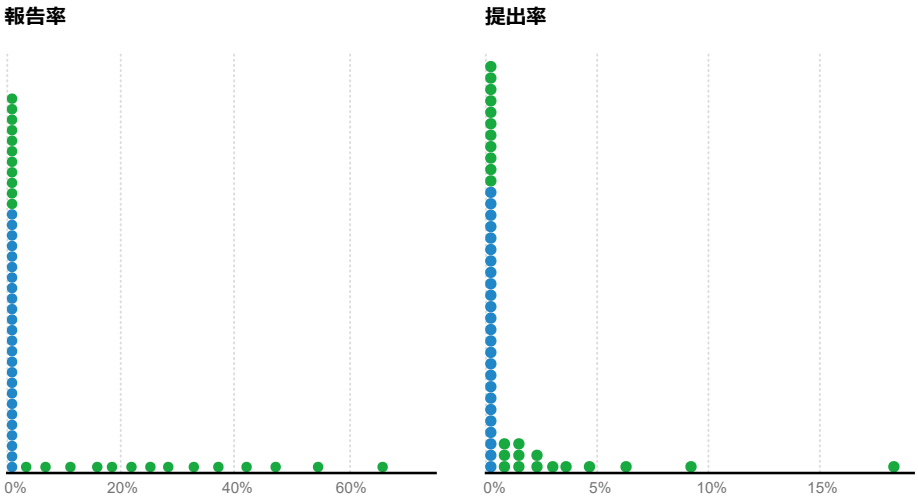


図88. 専門的・科学的・技術的サービス業のフィッシングテストのクリック率の中央値 (n = 2,583)

図89. 専門サービス業の漏洩/侵害のエラーの種類 (n = 67)

こんなことをするべきではなかった

この業界で目立つのは「多種多様なエラー」ですが、実際にはどの業界でも、従業員のミスがデータ漏洩/侵害の原因となっています。図89は、この業界で上位を占める3つのエラー、「設定ミス」、「誤送信」、「紛失」を示しています。設定ミスが報告されるようになったのは、主に、この種のデータ漏洩/侵害を積極的に探している人がいるからです。このエラーは、クラウドデータベースのインスタンスにデータをアップしたときに、何らかの保護措置を講じなかった場合に発生します。積極的にこの種のデータ漏洩/侵害を探している人がいると先ほど言いました。そう、笑えてきますが、そんなことはありません。

誤送信は、多くの場合、紙の書類の郵送で、宛先の間違った書類を受け取ったりすることですが、メールの宛先や添付ファイルを不注意で間違った場合にも当てはまります。紛失はまた、タイプの少し違うエラーです。紛失したものがノートPCなどの電子デバイスである場合、弊社のデータセットではこれはデータ漏洩/侵害としてはカウントされません。これを数に入れるためには、データの機密性が損なわれていることが確認されなければなりませんが、紛失した資産が手元にないため、機密データにアクセスされたかどうか確認することは困難です。紛失のエラーはデータセットには表示されますが、それはデータ漏洩/侵害ではなくインシデントであることがほとんどです。しかし、データ漏洩/侵害では、何が条件になるでしょうか。それは、紙の文書のように、人間が読める形式の資産になっていることです。印刷されたものには保護をかけようがないので、それらはデータ漏洩/侵害としてカウントされます。そのため、プリンターには注意書きがあり、印刷された文書に機密情報が含まれている場合には慎重に扱わなければならないという注意を喚起しているのです。

最終的に得るもの

DoS攻撃はデータ漏洩/侵害のパターンから除外されていますが、これは通常、実際の守秘義務違反には至らないためです。DDoSは専門サービスではインシデントの90%以上を占めており、図90では、この業界のDDoSの帯域(BPS)の平均をわずかに上回っています。

良い兆候としては、図91に示すように、専門サービスのパッチ適用率は平均よりも高く、メーカーによるリリースから最初の四半期に67%のパッチ適用が行なわれています。「結果と分析」セクションの「攻撃」の「ハッキング」の項を読まれた方は、すぐにパッチが適用されないことが問題なのではなく、パッチが適用されない残りの3分の1のシステムの方が問題なのだということをすでに理解されているかと思います。

図90. 専門的・科学的・技術的サービス業のDDoSの平均的なBPS (n = 30 組織) : 全作業のモード (緑色の線): 565 Mbps

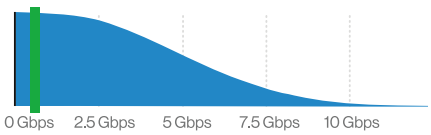
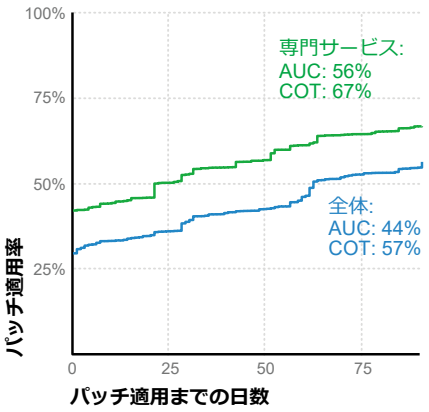


図91. 専門的・科学的・技術的サービス業の脆弱性へのパッチ適用(n = 87,857)



公務 NAICS 92

サマリー

この業種では、ランサムウェアが大きな問題となっており、金銭目的の攻撃者は広範な政府関係機関を標的としてのランサムウェア攻撃を仕掛けています。また、政府・公共機関では誤送信や設定ミスが依然として多く存在します。

頻度	インシデント6,843件、確認されたデータの暴露346件
上位3つのパターン	「多種多様なエラー」、「Webアプリケーション」、「その他全て」がデータ漏洩/侵害の73%を占めている
攻撃者	外部（59%）、内部（43%）、複数の関係者（2%）、パートナー（1%）（漏洩/侵害）
攻撃者の動機	金銭目的（75%）、スパイ活動（19%）、愉快犯（3%）（漏洩/侵害）
侵害されたデータ	個人情報（51%）、その他（34%）、認証情報（33%）、内部情報（14%）（漏洩/侵害）
上位3つの対策	セキュリティ意識向上トレーニングプログラムの実施（CSC17）、境界防御（CSC12）、セキュアな設定（CSC5、CSC11）

はっきりと見えるようになった

この公務のセクションでは、1つの業種について弊社の外部協力者らが明らかにするものがどのようなものかを示しています。この業界の大半のデータは、政府・公共機関のデータ侵害の動向を把握している米国連邦政府内の協力者から提供されたものです。本報告書の他の箇所でも述べているように、データ侵害の定義の閾値を満たすためには、データの機密性が損なわれていることが確認されなければなりません。しかし、政府のデータ侵害の報告要件では、ありふれたマルウェアの感染や単純なポリシーの侵害であっても開示が必要とされています。そのため、インシデントの数が異常に多く、それに反して侵害の数は少なくなっています。

例えば、この業界の攻撃パターンの違いを見ると、データ漏洩/侵害の上位3つは「多種多様なエラー」、「Webアプリケーション攻撃」、「その他全て」となっています。同じデータでインシデントについて見てみると、上位3つのパターンは「クライムウェア（マルウェア攻撃）」、「資産の紛失・盗難」、「その他全て」となっています。

インシデントのデータセットに含まれるマルウェアについては、図92を見ると、「ランサムウェア」が圧倒的に多く、全体の61%を占めています。このマルウェアは、他のマルウェアによってダウンロードされたり、システムへのアクセスを獲得した攻撃者によって直接インストールされたりすることが最も一般的です。しかし、ランサムウェアは通常、機密性への侵害をもたらす攻撃ではありません。むしろ、ソフトウェアのインストールによる完全性への侵害であり、被害者のシステムが暗号化された後の可用性に対する侵害です。したがって、これらの攻撃は通常、データ侵害を論じる際には出てきません。

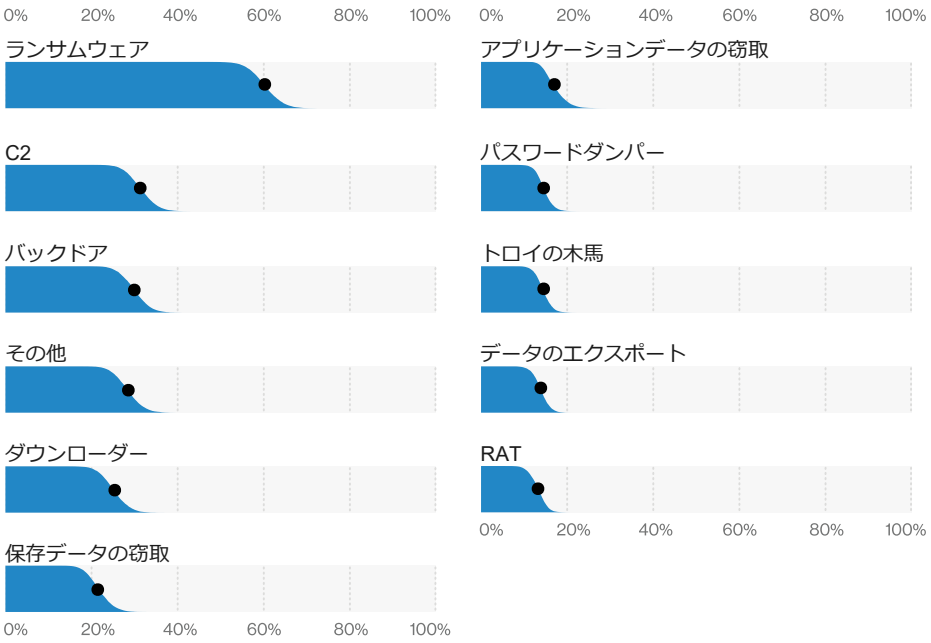


図92. 公務の漏洩/侵害によく見られるマルウェアの種類 (n = 198)

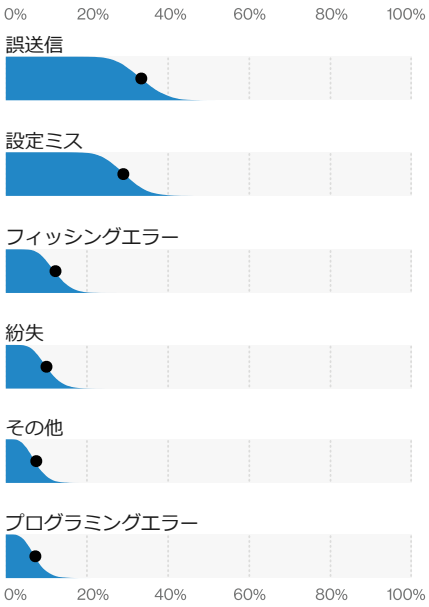


図93. 公務の漏洩/侵害によく見られるエラーの種類 (n = 92)

同じことが、「資産の紛失・盗難」のパターンにも当てはまります。これらの資産は暗号化が行なわれていなかったデバイスであるか、またはデータ侵害のリスクがあったとしても考慮されません。もちろん、復号化キーも同時に人間が読める形式で紛失していたのなら別ですが（野次る前に、私たちが実際にこれを見たことがあるということを心に留めておいてください）。これらのデバイス上のデータはパスワードのみで保護されている可能性が高いため、弊社のデータセットではリスクありと考えられており、確認されたデータ侵害ではありません。

後悔しないこと[42]

確認されたデータ侵害を見ると、赤コーナーの「多種多様なエラー」がこの業界で最も目立つパターンとなっています。図93は、誤送信が依然として政府・公共機関で大きな問題であることを示しています。これは、機密情報が誤った受信者に送られる場合のことです。宛先を間違えたメールなどの電子的な手段を介した場合もあれば、昔ながらの紙の文書の場合もあります。政府や公共機関から送られてくる紙の量には誰もかないませんが、封筒の宛名と中身が一致しない郵便物が大量に送付されたら、深刻な問題になりかねません。

青コーナーでは、最上位のエラーのもう1つの候補である「設定ミス」がデータ漏洩/侵害の30%を占めています。設定ミスによるデータ侵害とは、不正アクセスからデータを保護するためのセキュリティ対策を講じずに、何者か（通常はシステム管理者や他の特権的な技術的役割を持つ者）がクラウド上のデータストアを立ち上げた場合に発生します。世の中には、この種の機会を探すために時間を費やしているセキュリティ研究者がいるのです。構築すれば彼らはやってきます。

昨年度から今年度の変化を振り返ってみると、データ漏洩/侵害の上位3つのパターンの構成がかなり変わっています。2019年の報告書では、「サイバースパイ活動」、「多種多様なエラー」、「特権の悪用」でした。図94でパターンの順位が変わっているのを見ることができます。サイバースパイ活動と特権の悪用の2つは、今年度のデータセット全体において減少しており、この業界での割合は一桁台にまで減少しています。

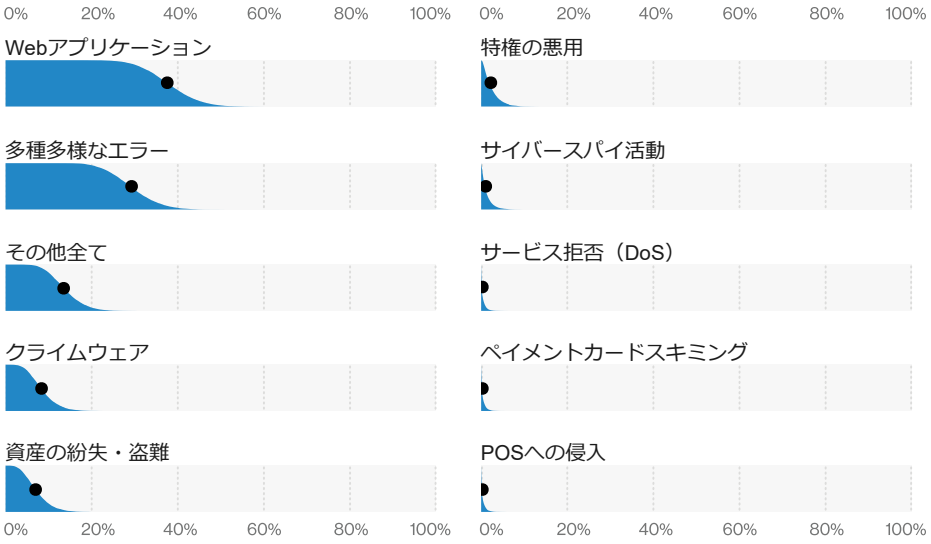


図94. 公務のデータ漏洩/侵害のパターン（n = 346）

42 去年はけしかけられて変なタトゥーを入れてしまいましたが。

不動産業、レンタルおよびリース業 NAICS 53

サマリー

この業種では、盗み取った認証情報を利用してWebアプリケーションを攻撃する事例が頻繁に確認されています。ソーシャルエンジニアリング攻撃も多数確認されており、この攻撃では攻撃者は資産の移転のプロセスに自身の情報を埋め込み、自らの銀行口座に直接金銭を振り込ませようとします。他の多くの業種と同様に、この業種でも構成の不備がセキュリティに影響を及ぼしています。

頻度	インシデント37件、確認されたデータの暴露33件
上位3つのパターン	「Webアプリケーション攻撃」、「その他全て」、「多種多様なエラー」がデータの漏洩/侵害の88%を占めている
攻撃者	外部（73%）、内部（27%）（漏洩/侵害）
攻撃者の動機	金銭目的（45%～97%）、自己都合/スパイ活動（各0%～40%）、恐怖/愉快犯/怨恨/イデオロギー/その他/二次的動機（各0%～21%）（漏洩/侵害）
侵害されたデータ	個人情報（83%）、内部情報（43%）、その他（43%）、認証情報（40%）（漏洩/侵害）
上位3つの対策	セキュアな設定（CSC 5、CSC 11）、セキュリティ意識向上トレーニングプログラムの実施（CSC 17）、境界防御（CSC 12）
データ分析ノート	攻撃者の動機は、既知の動機によるデータ漏洩/侵害が8件のみだったため、パーセンテージの範囲で表しています。また、グラフによっては、期待値を表示するには十分なデータが観測されていないものがあります。

完売御礼!

家を初めて所有したときの感慨に優るものはありません。入居し、塗りたてのペンキの匂いをかぎ、これから作るたくさんの思い出を思い描きます。この業界のデータからは、サイバー犯罪者もまた、家の中にすぐに上がり込んでくつろいでいることが伺えます。「Webアプリケーション攻撃」を利用してデータの展示会に参加したり、「その他全て」のパターンでソーシャルエンジニアリングを利用したり、あるいは「多種多様なエラー」を利用して従業員から立ち寄るように頼まれたりと、サイバー犯罪者は確実に歓迎されています。図95に示すように、これら3つのパターンのうちどれが統計的にトップであるかを明確に示すことは困難ですが、これら3つのパターンは全て有望な候補者であることは間違いありません。

玄関入口マットの下に鍵を置いたままにしないこと

昨年度は、この業界のデータ漏洩/侵害件数はやや少なかったものの、総じて興味深い調査結果がいくつかありました。他の多くの業界と同様に、犯罪者は盗んだ認証情報を積極的に利用してユーザーの受信トレイにアクセスし、悪質な活動を行っています。実際、全ての業界において認証情報の窃取はどこでも行なわれているので、認証情報は所有されているというよりも、時間貸しの共有物と考えた方が正確かもしれません。一方で、ソーシャルエンジニアリングに頼って仕事をこなしている外部攻撃者もいます。これらの攻撃の中には、単にデータを盗むことを目的としたものもありますが、他のケースでは、なりすましを利用した攻撃によく見られるように、これらの攻撃が別の攻撃に利用されることもあります。

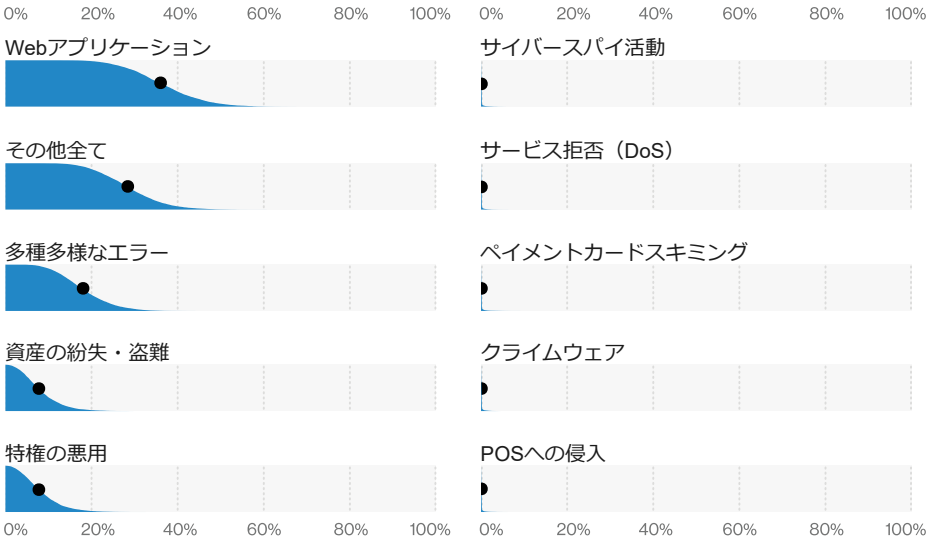


図95. 不動産業、レンタルおよびリース業のデータ漏洩/侵害のパターン（n = 33）

図96. 不動産業の漏洩/侵害によく見られる完全性への影響 (n = 16)

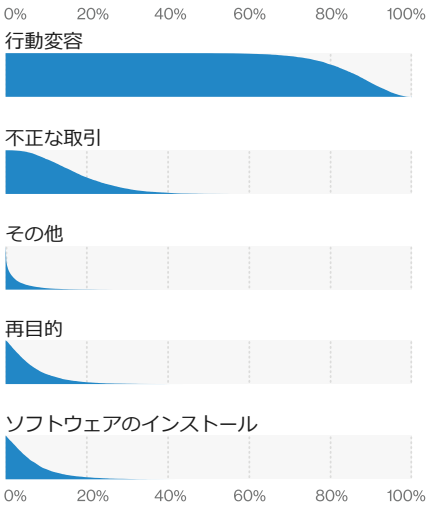


図97. 不動産業、レンタルおよびリース業の漏洩/侵害によく見られるエラーの種類 (n = 7)

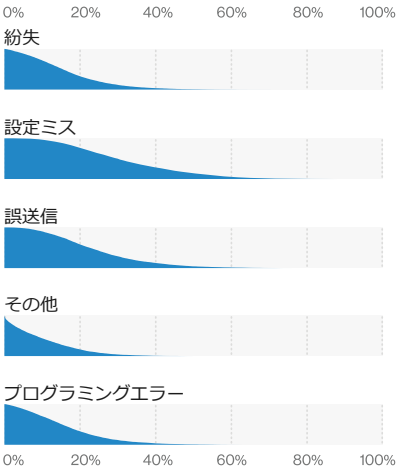


図96は、悪意のある者（Bad Guys[TM43]）が人の善意に付け込み、従業員を騙して目的を達成させる方法を示しています。彼らはなりすましを利用して従業員の行動を変え、機密情報を漏らすようにしたり、知らず知らずのうちに不正行為に手を貸すようにしむけたりします。この種のソーシャルエンジニアリングの例として、新築住宅の売買に関するメールのスレッドに攻撃者が入り込み、攻撃者の銀行口座に購入代金を振り込むように組織を誘導することが挙げられます。この種の重要な取引を行う場合は、電話で詳細を確認することをお勧めします。

誰に送ったのか?

不動産業界のセクションを設けたのは今回が初めてですが、弊社では何年も前からこの業界のデータを収集してきました。したがって、この業界の各パターンが時間の経過とともにどのように推移してきたかを分析することができます。今年度は、興味深い調査結果の1つとして、エラーが継続的に発生したことが挙げられます。これらのエラーに関連したデータ漏洩/侵害には、図97に示すように、「設定ミス」（権限を制限し忘れた）、「誤送信」（メールや紙の文書の宛先を誤った）、「プログラミングエラー」（コーディングのミス）などがあります。これらのエラーは、不動産業界におけるデータ侵害全体の18%を占めています。この業界でビジネスを行う場合は、セキュリティ意識向上のためのトレーニングや健全なポリシーと手順の実施に時間を割くことをお勧めします。

43 確かに誰かがこれを商標登録していますよね？

小売業 NAICS 44–45

サマリー

この業種では、データ漏洩/侵害の主な要因として、eコマースアプリケーションを標的とした攻撃が圧倒的多数を占めています。この業種の企業は主要な業務をWebに移行し続けていますが、犯罪者もその動きに追随しています。この業種で長年にわたり主要な問題になっていたPOS関連のデータ漏洩や侵害は、Webへの移行の影響を受けて減少し続け、2019年のDBIRで最も件数が少なくなりました。標的となるデータタイプとしてはクレジットカードの情報が一般的ですが、個人情報や認証情報も狙われることが少なくありません。

頻度	インシデント287件、確認されたデータの暴露146件
上位3つのパターン	「Webアプリケーション攻撃」、「その他全て」、「多種多様なエラー」がデータ漏洩/侵害の72%を占めている
攻撃者	外部（75%）、内部（25%）、パートナー（1%）、複数の関係者（1%）（漏洩/侵害）
攻撃者の動機	金銭目的（99%）、スパイ活動（1%）（漏洩/侵害）
侵害されたデータ	個人情報（49%）、決済情報（47%）、認証情報（27%）、その他（25%）（漏洩/侵害）
上位3つの対策	境界防御（CSC12）、セキュアな設定（CSC5、CSC11）、継続的な脆弱性管理（CSC3）

「1ドルで買うよ。」

この業界では周知のことですが、小売業は頻繁に金銭目的の標的にされます。小売業自体がほぼ例外なく金銭的動機を持つ業界なので当然のこととも言えます。この業界は、これらの組織が保有する豊富なペイメントカード情報へのアクセスを得ようとする犯罪者グループに狙われています。「対面取引」から「非対面取引」へと移行する昨年の犯罪傾向が続いており、RAMスクレーパーマルウェアの使用は2016年以降、同様に減少しています。個人情報についても小売業は不正アクセスの標的として目立っており、侵害されたデータの種類の上位で「決済情報」とほぼ同数になっています。確かに、決済情報にアクセスできなくても、他のタイプの金融詐欺で金銭的報酬を得やすい個人情報を入手できるなら、攻撃者が文句を言うはずはないでしょう。

Webへの移行

図98からは、商品の陳列ケースのように、小売業界全体の状況を窺い知ることができます。2014年から2019年のここ数年の間に、攻撃はPOS端末やコントローラから「Webアプリケーション」へと移行しています。これは主に業界がWebを中心とするトランザクションインフラに移行している傾向に大いに同調した動きです。このように、インフラの変化に伴い最短の手段でデータへアクセスするために攻撃者も変化します[44]。Webアプリケーションを標的にした44件の攻撃は勢いがあると言えます。2019年の調査報告では、小売業での漏洩/侵害の大半がWebサーバー関連のものと予想していましたが、図99に示すように、実際にこの業界ではそのような状況が起きています。裏表紙に印刷されているラッキーロトの番号を必ず試してみてください。勝った！勝った！夕飯は「ドン勝」だ！

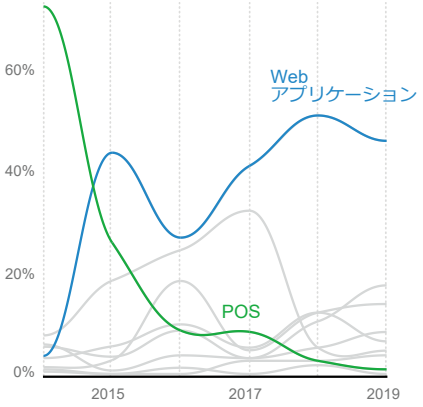


図98. 小売業のデータ漏洩/侵害パターンの経時的変化

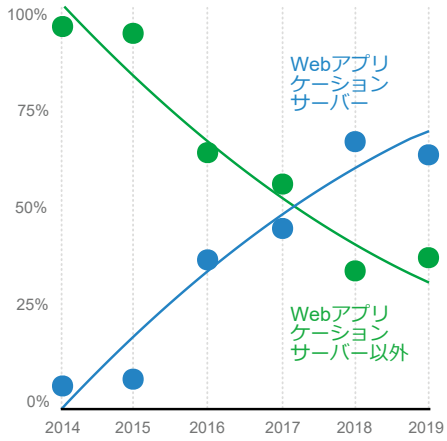
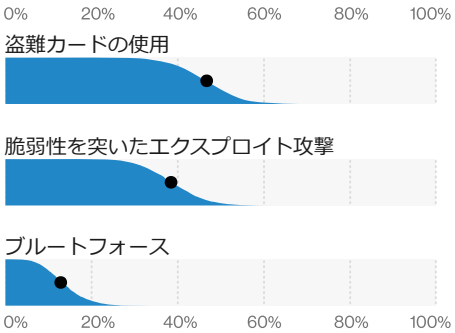


図99. 小売業の決済情報の漏洩/侵害との関係性の経時的変化（Webアプリケーションサーバーと Webアプリケーションサーバー以外）

44 もちろん、この移行を行っていない場合、お客様のPoSインフラはリスクにさらされたままです。

「Webアプリケーション攻撃」パターンは、すでに窃取されている認証情報の使用と、Webアプリインフラの脆弱性を突く攻撃という2つの主要なアクションから構成されています。図100を見ると、脆弱性を突いたエクスプロイト攻撃と盗難カードの使用がハッキングの種類のカテゴリーの1位を僅差で争っており、パーセンテージ的に両者の間には大きな差はありません。理想的なのは、他人のデータが漏洩/侵害されても自分自身のリスクが高まらないことです。しかし、攻撃者は他の被害者から集めた認証情報をデータストアに貯め、新たな犠牲者に対してそれを試しているため、そのケースはますます当てはまらなくなっています。

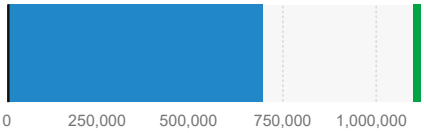
図100. 小売業のデータ漏洩/侵害によく見られるハッキングの種類（n=48）



認証情報が奪われている

弊社の非インシデントデータによると、この業界ではクレデンシャルスタッフィングが重要な問題であることがわかります（図101）。今年は全業種のうちの最も多い値をわずかに下回っていますが、これだけ多くの鍵（認証情報）を手中にしている者が、他の鍵も試すことがないとは考えられません。

図101. 小売業のクレデンシャルスタッフィング攻撃のWebブロック（n=284）、業界全体（緑）：111万



悪意のある攻撃者がインフラに対して他人の認証情報を使用していないとしたら、パッチが適用されていないWebアプリケーションの脆弱性を突いてアクセスをしています。図102の脆弱性に関するデータによると、脆弱性の発見後最初の3か月以内にパッチが適用されているケースは全体の約半数にすぎません。これらのパッチは放置せずにできるだけ早く適用した方が良いでしょう。過去の調査によるとタイムリーにパッチが適用されない場合（単に対処しないまま）、その脆弱性はかなりの期間放置される傾向があることが分かっています。弊社の分析ではSQL、PHP、ローカルファイルインジェクションがこの業界で最も一般的に試みられている攻撃であることが判明しています（図103）。

図102. 小売業における脆弱性へのパッチ適用（n=35,098）

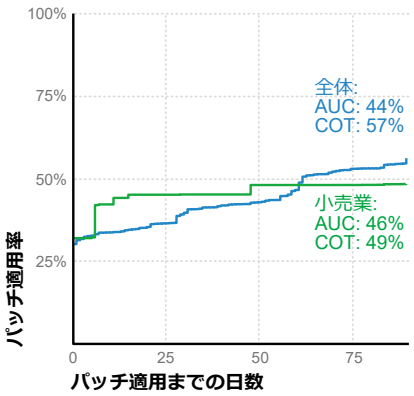
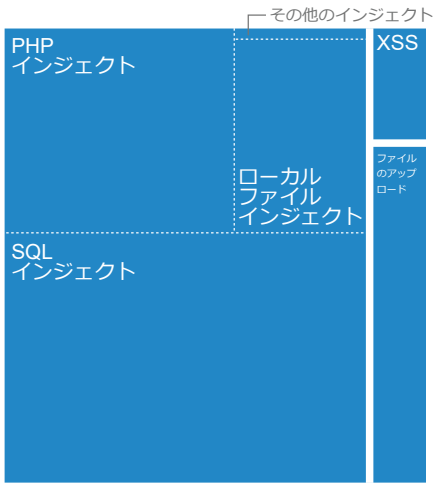


図 103. 小売業のWebアプリケーションの攻撃ブロックの種類（n = 22.2億）



データタイプ

金銭的報酬を最も得やすいデータタイプのランキングを作るとしたら、間違いなくペイメントカード情報がトップになるでしょう。何と言っても、その真新しいクレジットカードを試し、誰よりもいち早く「侵入」したいという衝動を持たない人はいないでしょう。図104は、攻撃者が同じ感覚を持っていることを示しており、恐らく他人の金を使って自分のゲーム機を作りたいと考えていることを示しています。しかし、個人情報も決済情報と同列に悪用の対象になっています。Webアプリがますます攻撃の対象にされるにつれ、被害者の個人情報が決済情報と一緒にパッキングされ、配達されることがあることを忘れないでください。

図105は、犯罪者のフォーラムやマーケットプレイスの投稿に見かけるハッキングデータの中で頻出度の高い用語をリストアップしたものです。犯罪者たちが（他の優れたSEO対策と同様に）用語を最も需要のあるものに合わせるのは当然のことと言えます。彼らのウィッシュリストの上位を占めるのは銀行やペイメントカードの情報であることは言うまでもありません。この種の取引をする者は、そうした願いを叶えるためにわざわざ埃だらけのランプを探す必要はありません。

図 104. 小売業の漏洩/侵害被害によく見られるデータの種類（n=135）

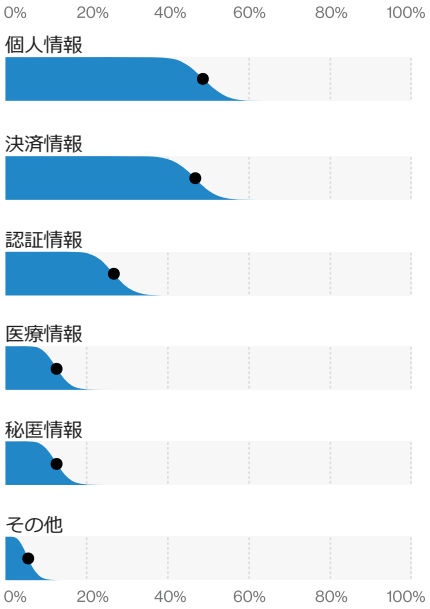
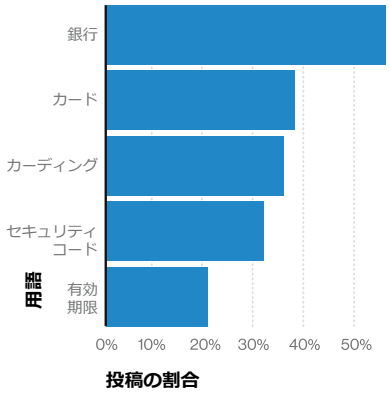


図105. ハッキング関連の犯罪フォーラムの投稿に頻繁に登場する用語（n=335万）



運輸および倉庫業

NAICS 48–49

サマリー

この業種を標的にしているのは、Webアプリケーションに攻撃を仕掛ける金銭目的の犯罪者集団です。一方で、制御機能のない大規模なデータベースを構築してしまうといったような従業員のミスも繰り返し問題になっています。このような要素にフィッシングやなりすましといったソーシャルエンジニアリングの手口を加えると、この業種で発生している大部分の漏洩/侵害の要因がカバーされます。

頻度	インシデント112件、確認されたデータの暴露67件
上位3つのパターン	「その他全て」、「Webアプリケーション攻撃」、「多種多様なエラー」がデータ漏洩/侵害の69%を占めている
攻撃者	外部（68%）、内部（32%）（漏洩/侵害）
攻撃者の動機	金銭目的（74%～98%）、スパイ（1%～21%）、コンビニエンス（0%～15%）（漏洩/侵害）
侵害されたデータ	個人（64%）、認証情報（34%）、その他（23%）（漏洩/侵害）
上位3つの対策	境界防御（CSC 12）、セキュリティ意識向上トレーニングプログラムの実施（CSC 17）、セキュアな設定（CSC 5、CSC 11）
データ分析ノート	攻撃者の動機は、既知の動機によるデータ漏洩/侵害が26件のみだったため、パーセンテージの範囲で表しています。また、グラフによっては、期待値を表示するには十分なデータが観測されていないものがあります。

運輸業と倉庫業は今回初めての登場です。その理由でこの報告書を初めて読まれる方は、ぜひ椅子に座ってじっくりご覧ください。ご存知のように、この業界はある場所から別の場所へ人や商品を運び、必要な期間それらの商品を保管することに関係しています。乗り物で移動した人々は、たいていは自分たちで滞在先を見つけることができますが、それは全く別の業界の話です。

全ての道はPwndにつながる

この業界では何がデータ漏洩/侵害の原因となっているのでしょうか？弊社のデータによると、「Webアプリケーション攻撃」と「多種多様なエラー」は非常に一般的であり、「その他全て」のパターンも一般的ですが、これについては後ほど詳しく説明します（図106）。Webアプリケーション攻撃はデータセット全体に見られ、インターネットに接続するアプリケーションがあれば、いつかは誰かに乗っ取られてコントロールが奪われることになるというのが、この時代の事実です。ハッキングとソーシャル攻撃は、この業界では最も一般的なものであり、これが「Webアプリケーション」パターンの隆盛の下地となっています。

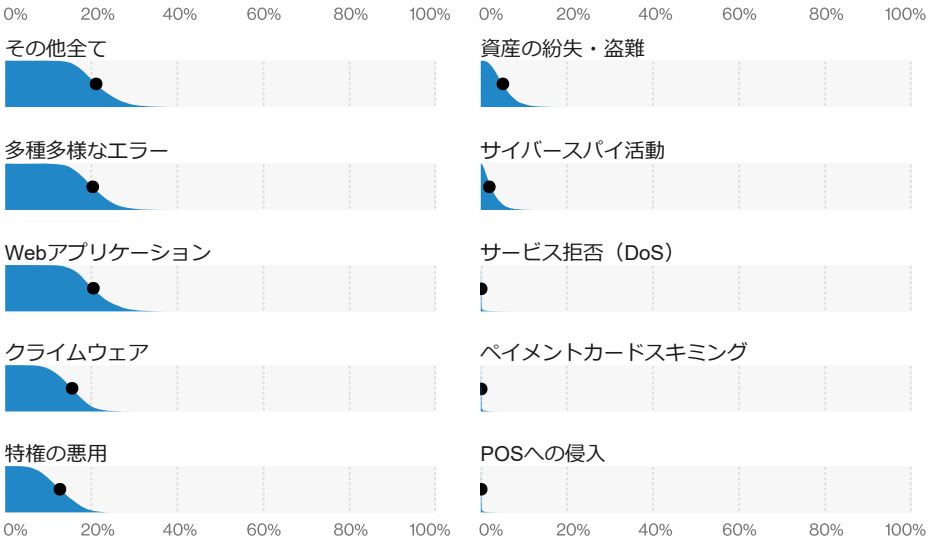


図106. 運輸および倉庫業のデータ漏洩/侵害のパターン（n = 67）

道から目を離さないように

人間は間違いを犯すものです。「多種多様なエラー」は、単に人間であることの副産物に過ぎません。この業界で最も多いエラーは、図107に示すように「設定ミス」です。よくある設定ミスのシナリオは、内部の攻撃者（多くはシステム管理者やDBA）が、機密データに対して一般に行われる手続きの面倒なアクセス制御を全く行わずに、クラウドサービス上にデータベースを構築してしまう場合です。そして、進取の気性に富んだセキュリティ研究者が、保護されていないデータストアを検出するために作られた検索エンジンを使ってそのようなインスタンスを見つけてみると、なんと既にデータ漏洩/侵害が起きているというわけです。

「その他全て」のパターンは、前述したように他の攻撃パターンには当てはまらない雑種の攻撃を集めた場所であり、このパターンの中にはBusiness Email Compromise（BEC、ビジネスメール詐欺）が含まれます。これらの攻撃は、通常はフィッシングメールで行われますが、電話で行われることもあります。攻撃者の目的は、データを入手すること、または適当な銀行口座への振り込みを促すことです。これらの攻撃は、主に金銭的動機を持った犯罪組織によって行われています。

図108は、この部門の外部攻撃者の最も一般的な動機を示しています。スパイ活動を動機とする攻撃者もいますが、金銭的動機を持つ攻撃者と比較すると、その数はごくわずかです。この業界で標的にされているデータの種類は個人情報であるように見えますが、このすぐ後を認証情報が追っています。

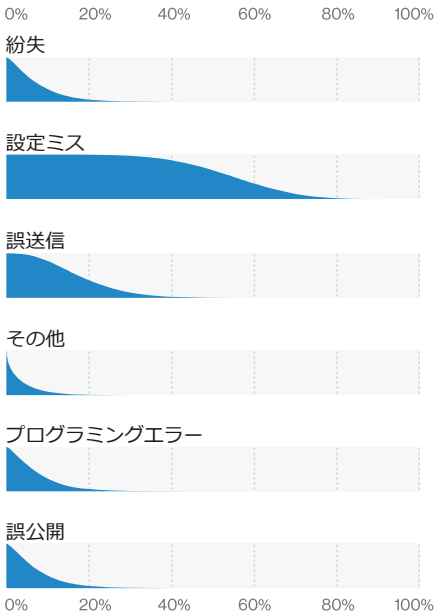


図107. 運輸および倉庫業の漏洩/侵害によく見られるエラーの種類 (n = 15)

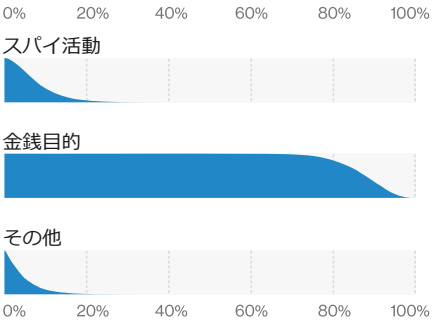
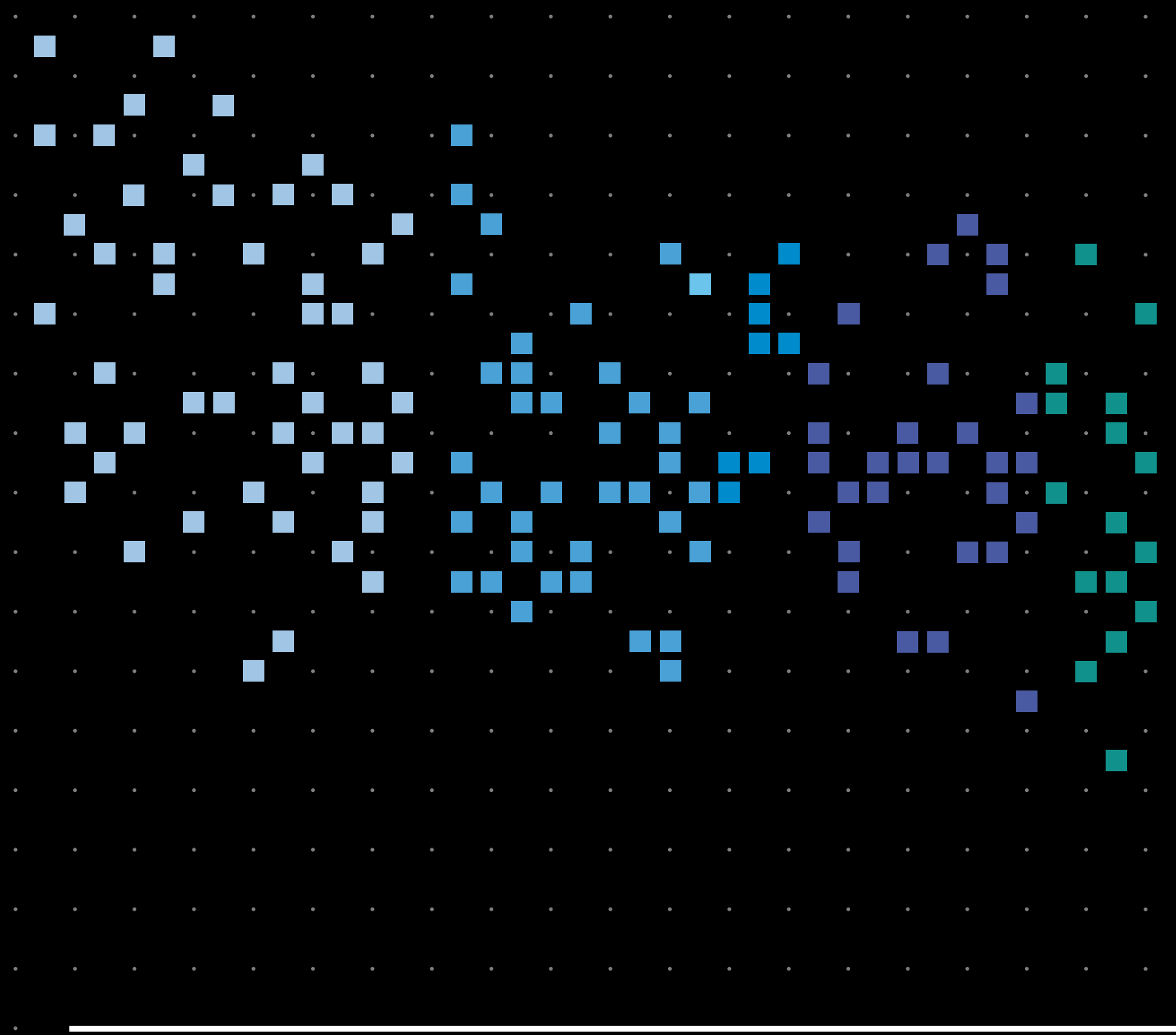
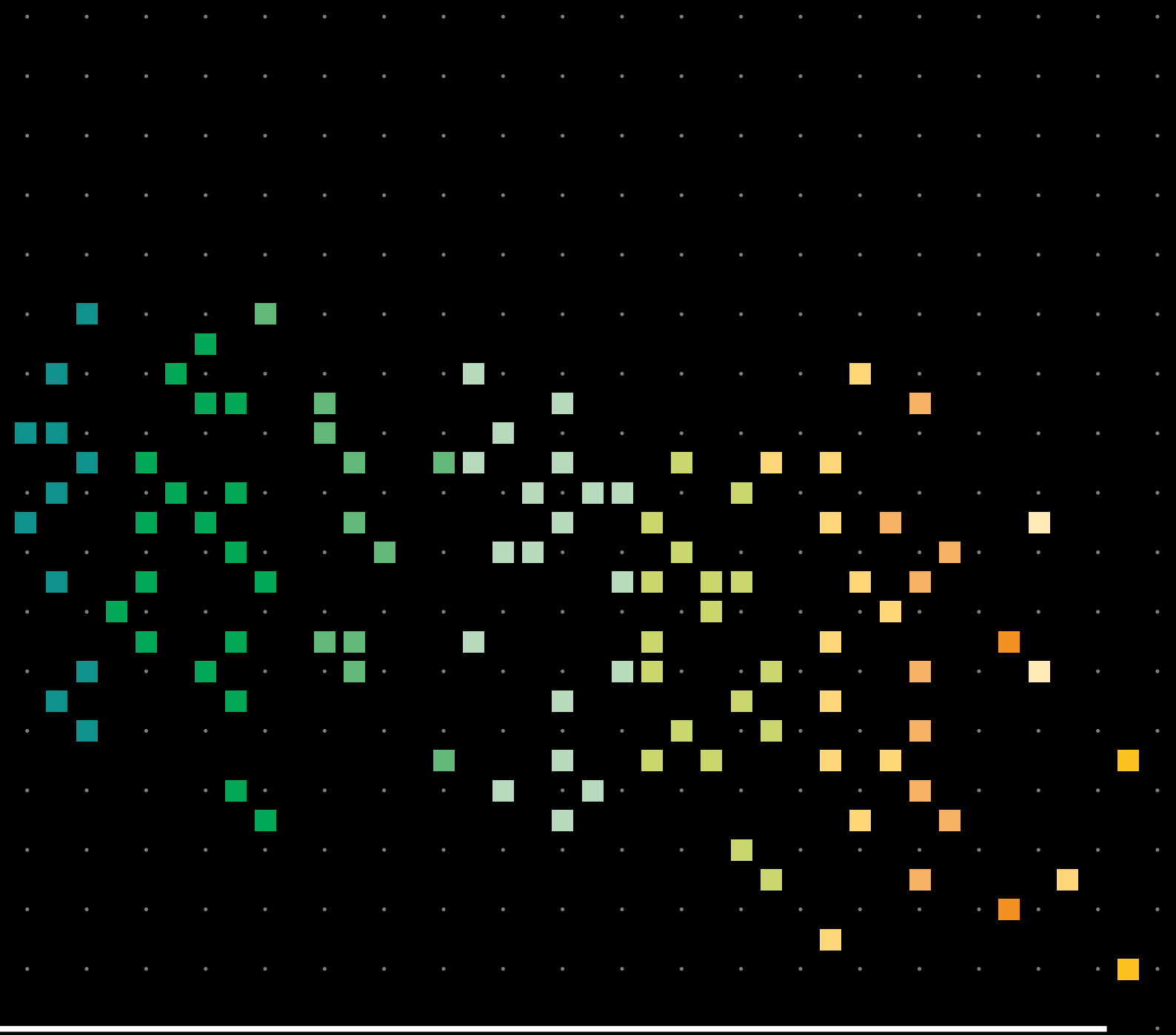


図108. 運輸および倉庫業の漏洩/侵害によく見られる攻撃者の動機 (n = 25)



04



組織の規模は重要か？中小企業におけるデータ漏洩/侵害の実情

組織の規模は重要か? 中小企業における データ漏洩/侵害の実情

サマリー

中小企業（SMB）と大企業ではデータ漏洩や侵害の内容に違いがありますが、クラウドへの環境の移行やWebベースの無数のツールの登場、ソーシャル攻撃の拡大に伴い、その違いは小さくなっています。SMBがビジネスモデルを調整していくなかで、犯罪者も自身のアクションを変更してその歩調を合わせており、最短のルートで最も容易に攻撃を成し遂げられる方法を選択しています。

頻度	小規模 （従業員数1,000人未満）	大規模 （従業員数1,000名以上）
	インシデント407件、確認されたデータの暴露221件	インシデント8,666件、確認されたデータの暴露576件
上位3つのパターン	「Webアプリケーション攻撃」、「その他全て」、「多種多様なエラー」がデータの漏洩/侵害の70%を占めている	「その他全て」、「クライムウェア」、「特権の悪用」がデータ漏洩/侵害の70%を占めている
攻撃者	外部（74%）、内部（26%）、パートナー（1%）、複数の関係者（1%）（漏洩/侵害）	外部（79%）、内部（21%）、パートナー（1%）、複数の関係者（1%）（漏洩/侵害）
攻撃者の動機	金銭目的（83%）、スパイ活動（8%）、愉快犯（3%）、怨恨（3%）（漏洩/侵害）	金銭目的（７９％）、スパイ活動（14%）、愉快犯（2%）、怨恨（2%）（漏洩/侵害）
侵害されたデータ	認証情報（52%）、個人情報（30%）、その他（20%）、内部情報（14%）、医療情報（14%）（漏洩/侵害）	認証情報（６４％）、その他（26%）、個人情報（19%）、内部情報（12%）（漏洩/侵害）

心の旅

数年前に（正確には2013年度版で）、中小企業（従業員数1,000人未満）と大企業（従業員数1,000人以上）の間の違いや類似点をいくつか見てみました。7年も経てば多くのことが変わるので、もう一度この2つを比較対照し、データの変化から何か語れるものがないか見てみたいと思いました。結局のところ、PaaS（サービスとしてのプラットフォーム）やSaaS、その他思いつく限りのあらゆる「サービスとしてのXX」などを含め、クラウド上で日常的に利用可能なサービスがかつてなく普及しており、中小企業にとっては、これまで以上に大企業のように事業を運営できる環境が整っています。そこで私たちは、「セキュリティインシデントの検出と対応に関して、能力の差によって、両者間の競争の場が少しは均等化されたのではないか」と自問してみました。このセクションを読まれている方は、答えが「その通り」であることをすでに推測していらっしゃるでしょう。どのくらい変わったのか、またどのような点が変わっていないのか詳しく見てみましょう。

サマリーの表を作成する際にまず気が付いたのは、インシデントとデータ漏洩/侵害の数に関して、両者間に大きな隔たりがあることです。大企業では小規模企業よりも2倍以上の頻度でデータ漏洩/侵害が発生しています。これは、小規模な組織がレーダーの網にひっかからないということなのか、それとも単に攻撃を受けていることに気付いていないだけなのでしょうか。また、インシデントの件数に関しても、両者の格差に目を見張るものがあります。大企業には「金があれば問題もある」ということが明らかになったということなのでしょうか?あるいは、可視性が高まったことなのか、それとも攻撃範囲が広がったということのなのでしょうか?この事象について、最近、一部のプロスポーツの審判が直面しているのと

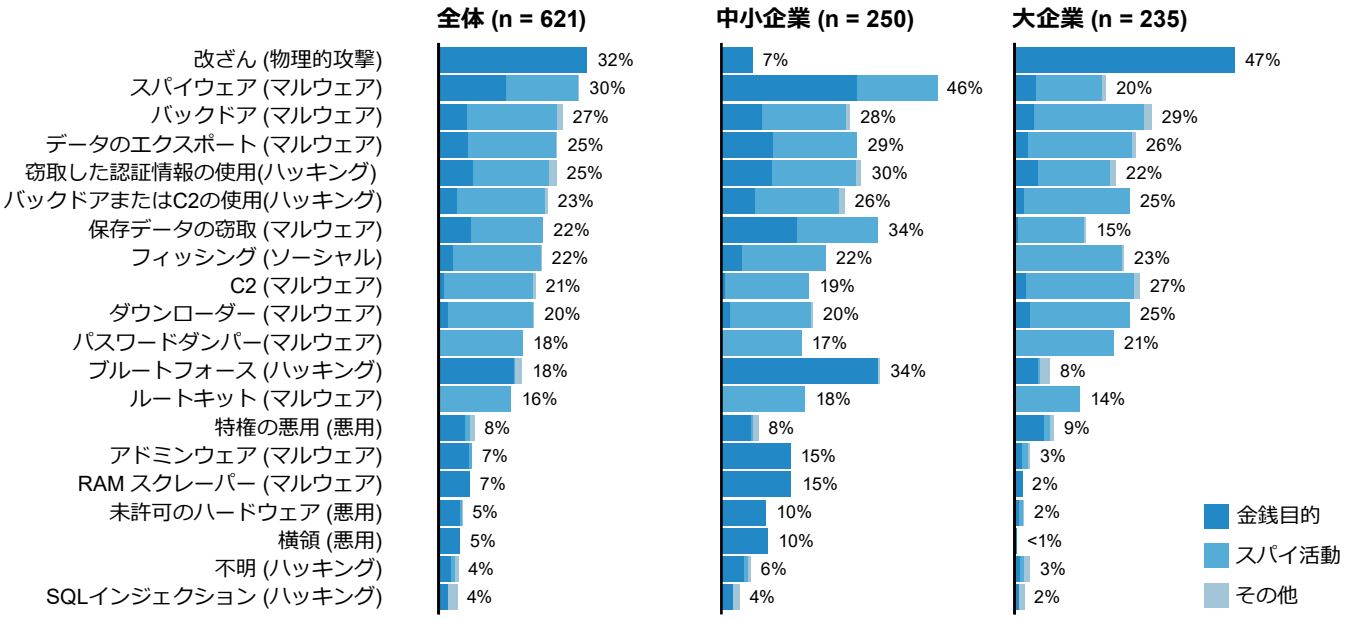


図109. トップ20の攻撃 (2013年度DBIRより)

同じ立場にいることに気付きました。正しい判断を下すのが難しいと実感しているからです（ニューオリオンズでの審判ではなおさらのことかもしれません）。

このセクションの一番上にある表で上位の攻撃パターンを紹介していますが、前回の調査で組織の規模に焦点を当てたときには、このパターンの概念はまだ生まれていませんでした。振り返ってみると、2013年以降、最も頻繁に発生している要因（VERISでは「攻撃の種類」と呼ぶ）にはいくつかの変化が見られます。2013年のDBIRの攻撃上位20では、小規模組織と大規模組織に分けて攻撃をリストアップしています（図109を参照）。

大規模組織では、「物理的改ざん」の攻撃が最上位に上がっています（そんなことがある?）。対照的に、小規模組織では「スパイウェア」が最上位に来ていますが、「ブルートフォースハッキング」や「保存データの窃取」もそのすぐ後に続いています。その後の年度を飛ばして7年後の現在のデータセットを見てみると、大企業(図110)と小規模企業(図111)の両方でフィッシングが最上位の攻撃となっており、窃取された認証情報の使用とパスワードダンパーがどちらの規模でも上位3つに入っています(順位は入れ替わっていますが)。いずれにしても、どちらも同じ3つのパターンが上位を占めているのは、興味深い結果です。フィッシングは、2013年にはかなり下位にランキングされていました。

鍵と財布をよこせ

2013年、最も攻撃の対象にされていたデータのタイプは、ペイメントカード情報でした。当時の犯罪者は、この種のデータを入手するために長い道のりを（裸足で、雪の中で、山を登り続けて）歩いていました（そして、その機会に出合えば感謝していました!）。その後、認証情報が人気を博し、内部情報や機密情報も大流行しました。今日、両規模の組織で盗まれたデータの種類を調べてみると、ペイメントカード情報は去年のものです。2013年の労働倫理に欠けた今日の犯罪者においては、標的にする被害者の組織規模は関係なく、関心を持っているのは主に認証情報の窃取です。個人情報も、組織の規模に関係なく、よく狙われているようです。この2つの大物の後に続くのは、医療情報、内部情報、決済情報のいずれかです。

2013年からのもう1つの変化は、盛んに攻撃される資産の種類です（図112）。大企業（47%）では、攻撃を受けた最上位の資産はATMでした。一方、小規模組織の資産の最上位は、POSコントローラ（34%）でした（POS端末は僅差で29%）。現在では、これらの資産はいずれの組織タイプでもリストから完全に外れています。現在では、組織の規模を問わず、ユーザーデバイス、メールサーバー、従業員（ソーシャル攻撃）への攻撃に悩まされています。

図110. 大企業の漏洩/侵害によく見られる攻撃の種類 (n = 448)

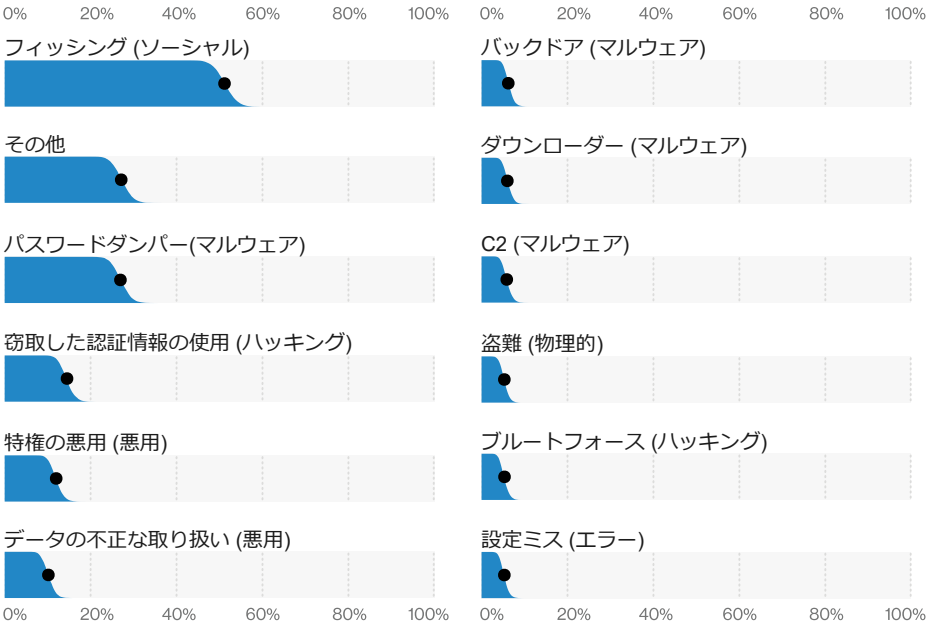
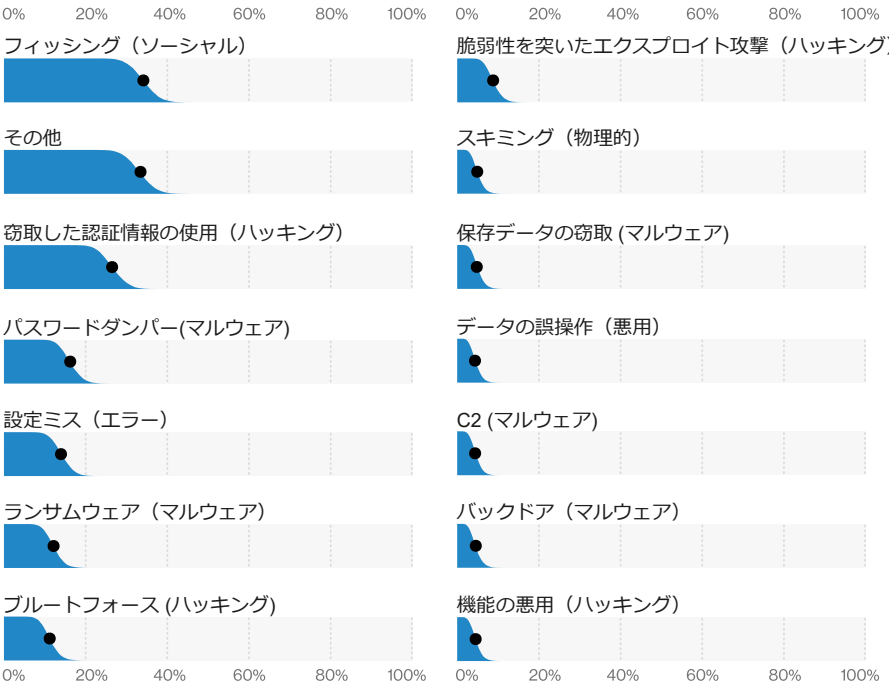


図111. 中小企業の漏洩/侵害によく見られる攻撃の種類 (n = 194)



現在のような時代はない

今年度のデータセットの違いに話を移すと、小規模組織への攻撃パターンの上位は「Webアプリケーション」、「その他全て」、「多種多様なエラー」ですが、いずれもダントツというほどではありません。一方、大規模組織では、「その他全て」、「クライムウェア」、「特権の悪用」が主な課題として挙げられます。「Webアプリケーション」攻撃はその名が表すとおりですが、「その他全て」は、他のどのパターンにも当てはまらない断片的なものを詰め込んだ家具運搬車です。この中には、データや電信送金を要求する上司を装ったフィッシングの形をしたソーシャル攻撃である「ビジネスメール詐欺」などの攻撃が含まれています。「多種多様なエラー」は、従業員が悪意なく組織に害をもたらす多くの手段を網羅した幅広いパターンです（種類は膨大です）。「クライムウェア」のパターンは、ありふれたマルウェアであり、金銭的動機を持つ犯罪者によって展開される傾向があります。最後に、「特権の悪用」とは、内部の攻撃者が企業の日々の営為とブランドの両方を台無しにしてしまう行為です（通常は悪意のある性質のもの）。

タイムラインデータを調べてみると、発見までに数ヶ月から数年かかるデータ漏洩/侵害の数は、小規模な組織よりも大規模な組織の方が多いことが分かります（図113、図114）。これは少し矛盾しているように思えます。大規模な組織は施設の面積が大きく、所有していることを忘れていたインターネットに接続された資産への侵入を見逃す可能性が高いかもしれません。一方、小規模な組織は攻撃対象が小さいため、問題を発見するのが容易なのかもしれません。大企業は大抵、専用のセキュリティスタッフを抱えており、大規模にセキュリティ対策を講じる余裕があるのに対し、中小企業はそうではありません。理由が何であれ、攻撃の検出に関しては、両者の間にはかなり顕著な格差が見られます。

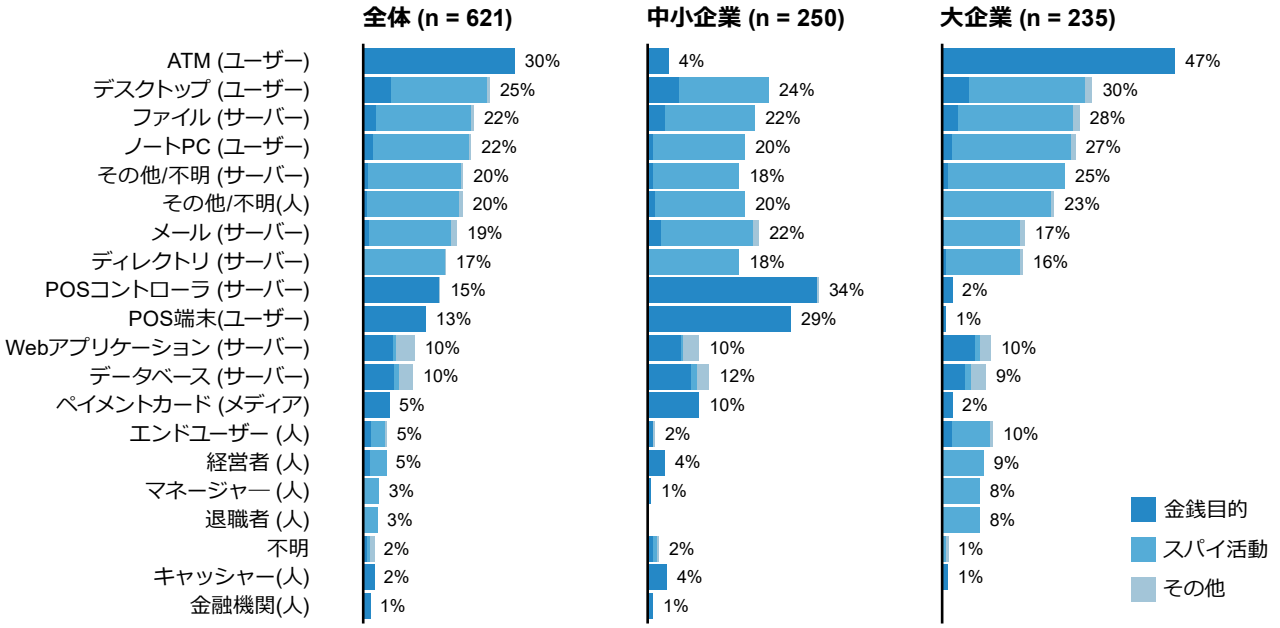


図112. 被害に遭った資産の種類 (2013年度DBIRより)

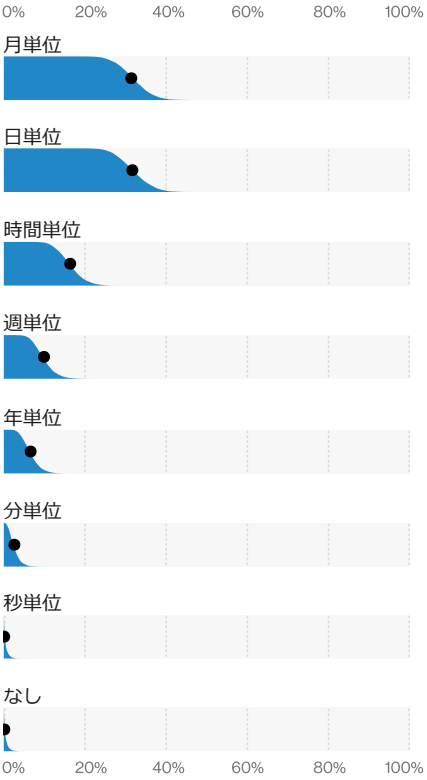


図113. 大企業が漏洩/侵害の発見までにかかった時間 (n = 121)

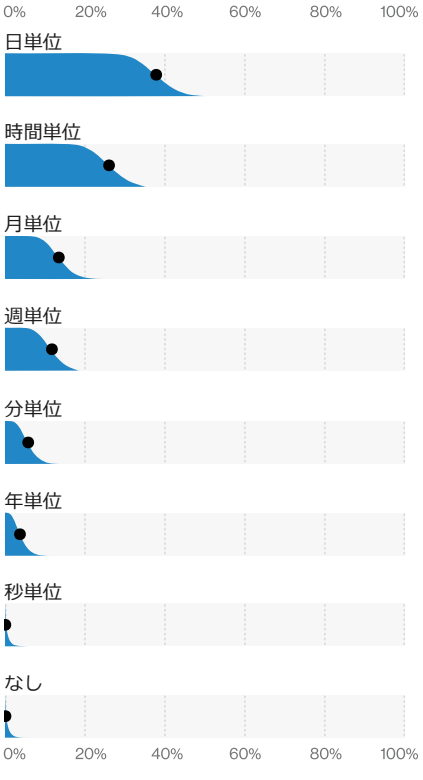
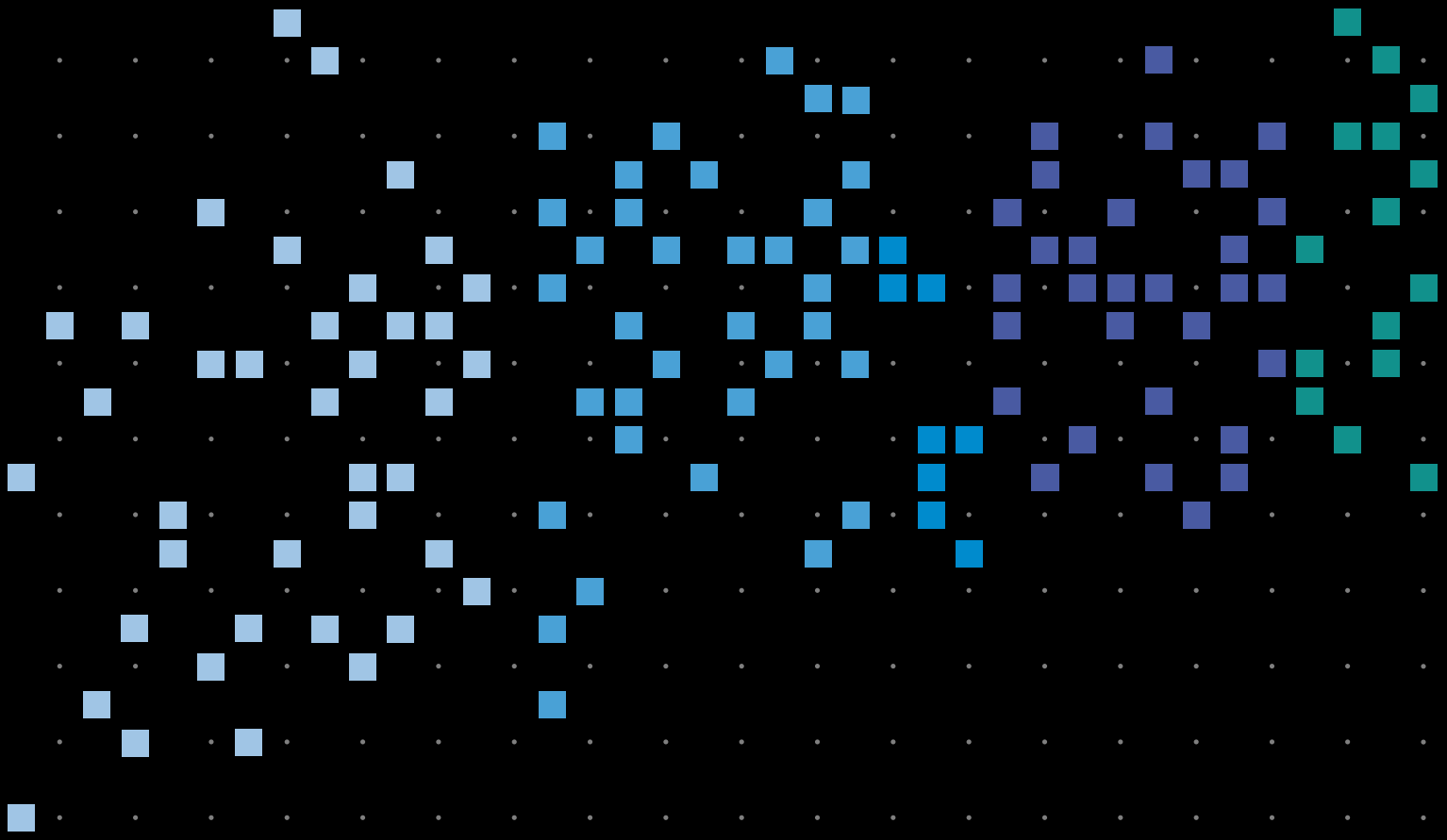
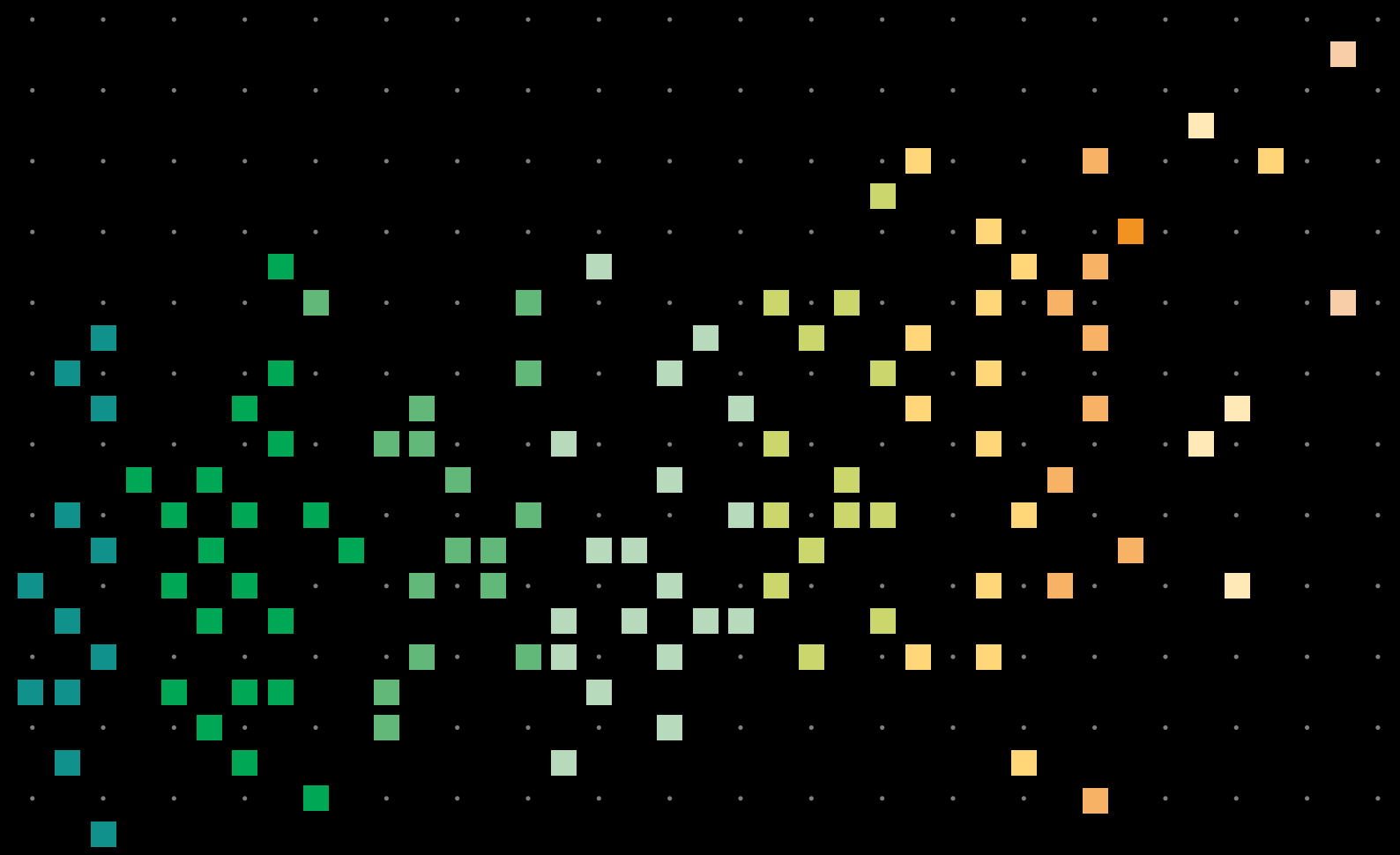


図114. 中小企業が漏洩/侵害の発見までにかかった時間 (n = 102)



05



地域別の分析

地域について

インシデント	合計	小規模 (1〜1,000)	大規模 (1,000以上)	不明
合計	32,002	407	8,666	22,929
APAC	4,055	27	33	3,995
EMEA	4,209	57	88	4,064
LAC	87	14	10	63
NA	18,648	231	6,409	12,008
不明	5,003	78	2,126	2,799
合計	32,002	407	8,666	22,929

データ漏洩/侵害	合計	小規模 (1〜1,000)	大規模 (1,000以上)	不明
合計	3,950	221	576	3,153
APAC	560	22	24	514
EMEA	185	41	53	91
LAC	14	5	5	4
NA	920	130	209	581
不明	2,271	23	285	1,963
合計	3,950	221	576	3,153

表2. 被害を受けた地域および組織の規模から見たセキュリティインシデントの数

データ提供者の多様性を高めるための今年のチームの勤勉な作業と、私たちが導入した精度の高い統計メカニズムのおかげで、世界の各地域に焦点を当てた分析を初めてお見せいたします。

「各業種の概要」で説明したフィルタリングとサブセットの作成を行ったところ、表2のような結果が得られました。世界の各地域を国連のM.49[45]の基準に従って定義し、国のスーパーリージョンとサブリージョンを結合します。これらをさらに組み合わせて、世界を以下の各地域に分けてそれぞれに焦点を当てます。

- **APACー**アジア・太平洋地域：南アジア（034）、東南アジア（035）、中央アジア（143）、東アジア（030）、オセアニア（009）
- **EMEAー**ヨーロッパ、中東、アフリカ地域：アフリカ（002）、ヨーロッパ、北アジア（150）、西アジア（145）
- **LACー**ラテンアメリカ・カリブ海地域（419）：南米（005）、中央アメリカ（013）、カリブ海諸国（029）がエンコーディングが異なる可能性があるため、冗長性のためにも含まれる。
- **NAー**北アメリカ地域（021）：主に米国とカナダ、そして最近何かと忙しくなっているバミューダでのデータ漏洩/侵害で構成される。

表からも明らかなように、いくつかの地域では他の地域よりも領域が広くなっています。しかし、国のとりこぼしがないように努めました。ここで弊社での推定言語とパーセンテージの範囲の多くが役に立つでしょう。

また、弊社が今後より多くのデータ侵害を報告できるように、読者の皆様にデータ共有のお願いをする絶好の機会でもあります。これを、悪意のある意図や偶然によるデータ侵害を作るための誘いだと思わないでください。しかし、読者の皆様がより詳細な分析を希望される地域の新たなデータ提供の候補者を提案し、またその地域の組織にデータ提供を促すことで、弊社は毎年新しい年に向けて調査範囲を拡大し、より良い分析を提供し続けることができます。

サンプル数が少ない場合の注意点は、「各業種の概要」のセクションで説明したのと同じく、図115と図116にも当てはまります。それらのいくつかはあまりに小さいため、子供が床に置いたレゴのブロックのように簡単に踏つけてしまいます。サンプルのサイズ（n値）が小さいことを考慮していない偏った分析結果は、それと同じくらい痛いものです。「小サンプル」であるラテンアメリカ・カリブ海地域のセクションでは、「データ分析ノート」にご注目ください。この報告書全体で使用される統計的信頼の背景に関する詳細については、「方法論」のセクションを参照してください。

読者の皆様からいただいたフィードバックを拝見する限り、報告書を隅から隅まで目を通す方もいれば、直接関心のあるセクションや地域以外の箇所は読み飛ばす方もいらっしゃるようです。そのため、一部のセクションだけを見ている読者は、他の場所ですでに言及しているかもしれない定義や説明を知らないため、報告書の中でいくつかの定義や説明を何度か繰り返しています。気になる方は、そのような箇所をスキップしていただいてかまいません。

45 https://en.wikipedia.org/wiki/UN_M49

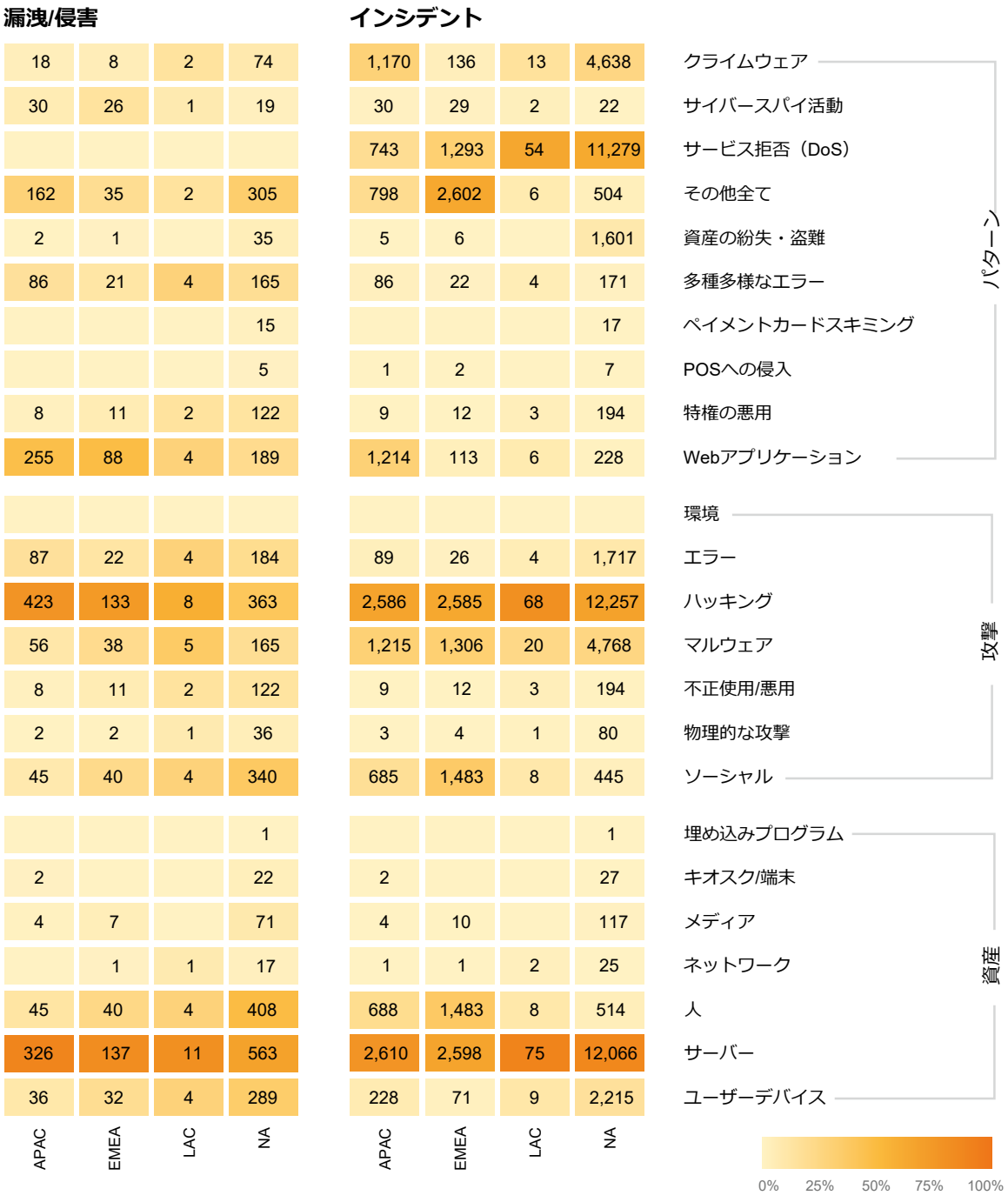
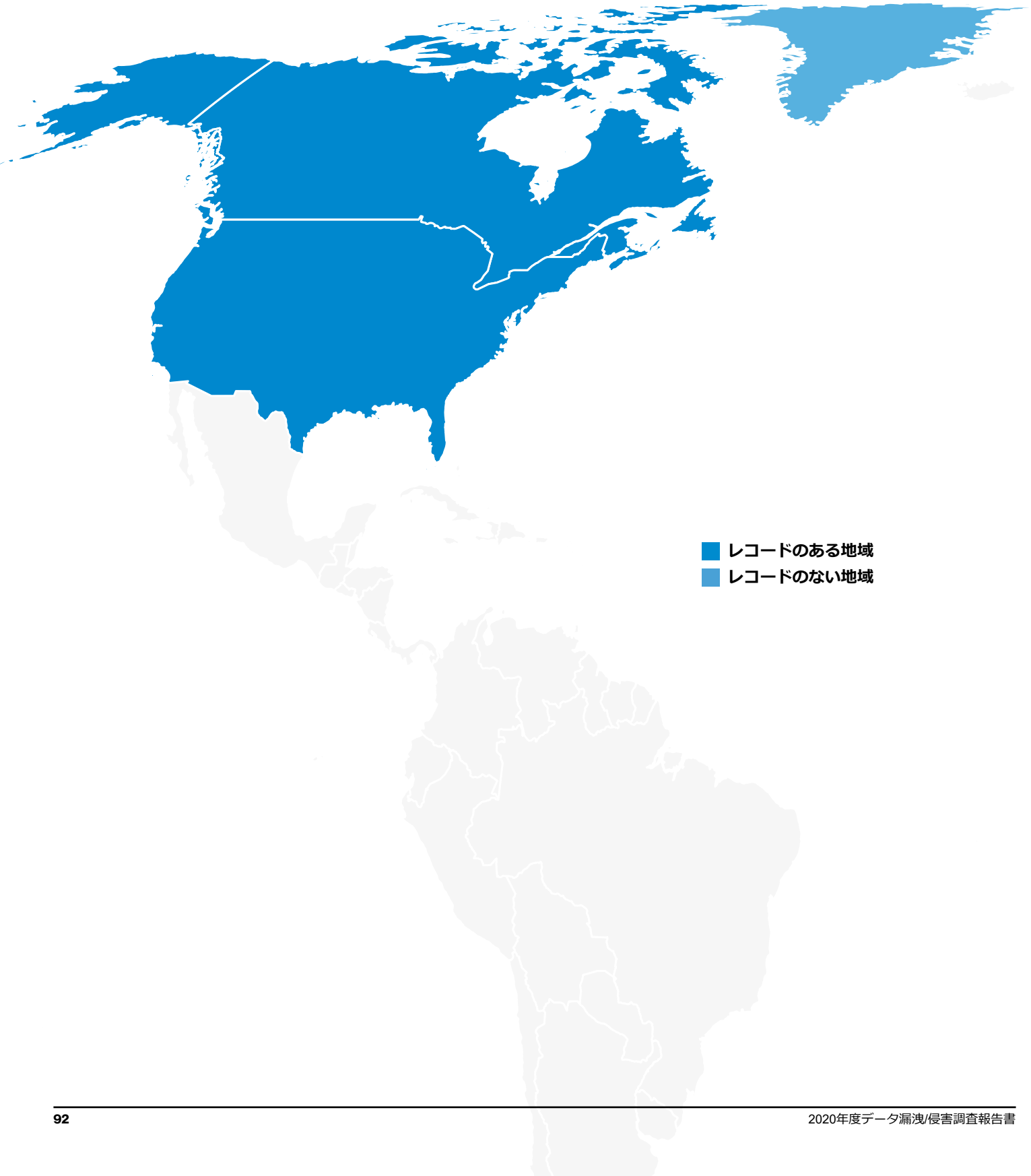


図115. 地域別のデータ漏洩/侵害およびインシデント

北アメリカ（NA）

図116. 北アメリカ（NA）地域



北アメリカ地域に指定されている地域は、アメリカとカナダのほか、バミューダなどの離島で構成されています。

以下の調査結果を見る際には、いくつかの要素に留意する必要があります。第一に、今年度のデータセットでは、この地域が全インシデントの70%を占め、データ侵害全体の63%を占めています。しかし、だからといって、優れたセキュリティ対策がバミューダトライアングルの中に消えてしまったわけではありません。北アメリカ地域は、特に医療と公務の業界では、現存するデータ報告基準[46]の中で間違いなく最も厳しいものをいくつか適用しています。そのため、インシデントやデータ漏洩/侵害の件数は、開示要件がそれほど厳しくない地域よりも多くなる可能性が高いと考えられます。また、本報告書は世界中からの報告が増えてはいますが、データ提供者の多くは北米の組織に所属しており、主に北米の組織を調査の対象にしていることを理解しておく必要があります。これらの要因の結果、北アメリカ地域の調査結果は、データセット全体の調査結果とさほど変わりません。とはいえ、興味深い相違点がいくつかあり、議論に値するハイライトがあります。

フィッシュとホイッスル、ホイッスルとフィッシュ[47]

この地域では「その他全て」が最上位のパターンとなっています（図117）。これは、多くの業界で金銭的な動機によるフィッシング攻撃が多発していることに起因しています（図118）。過去には、セキュリティ意識向上のためのトレーニングを行うことで、フィッシング攻撃の頻度や影響を抑えることができることが確認されています。しかし、このトレーニングが全く実施されていないか、実施されていたとしても不十分か不適切だった可能性があります。理由が何であれ、従業員にフィッシングメールをクリックしないように伝えることは、子供に嫌なことを聞かせたくないときに「耳栓をして」と叫ぶのとくらいの効果があります。

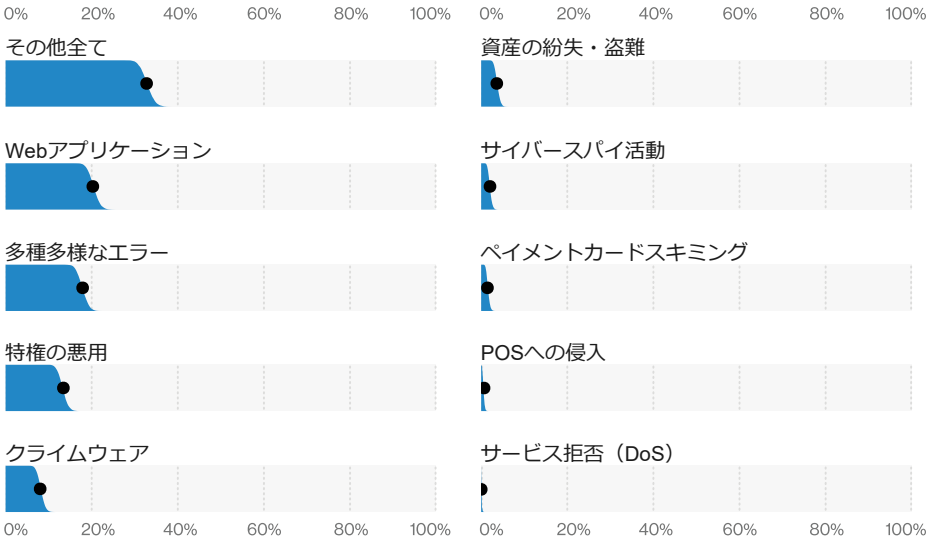


図117. 北アメリカのデータ漏洩/侵害のパターン（n = 920）

サマリー

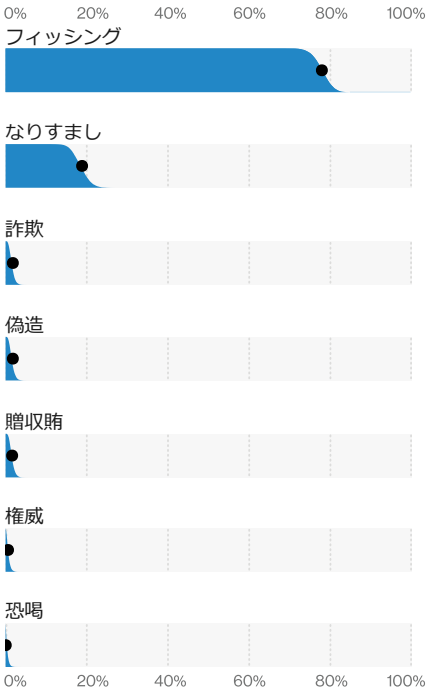
北アメリカの組織は今年、金銭的動機によるWebアプリケーションインフラへの攻撃に大きな被害を受けました。窃取された認証情報の使用によるハッキングが最も多く見られ、これらの認証情報の共有を促すソーシャルエンジニアリング攻撃がそれに続きました。従業員によるヒューマンエラーも弊社のデータセットでは日常的に観察されていました。

頻度	インシデント18,648件、確認されたデータの暴露920件
上位3つのパターン	北アメリカでは「その他全て」、「Webアプリケーション攻撃」、「多種多様なエラー」がデータ漏洩/侵害の72%を占めている
攻撃者	外部（66%）、内部（31%）、パートナー（5%）、複数の関係者（1%）（漏洩/侵害）
攻撃者の動機	金銭目的（91%）、スパイ活動（5%）、怨恨（3%）（漏洩/侵害）
侵害されたデータ	個人情報（43%）、認証情報（43%）、その他（35%）、内部情報（21%）（漏洩/侵害）

46 これは、2002年に可決されたカリフォルニア州の S.B. 1386など、長年にわたって堅固なデータ侵害通知法が制定されてきたことによるところが大きいです。この法律は、米国の他の州の青写真となり、現在ではゴールデンステートのCCPAによって強化されています。

47 偉大なジョン・プラインの言葉を、私たちに言い換えさせていただきたいと思います。彼の死を悼みます。

図118. 北アメリカ地域の漏洩/侵害のソーシャル攻撃の種類 (n = 322)



頭の中を整理しましょう

北アメリカ地域では、Webアプリケーション攻撃もまた大きな脅威となっています。これらの攻撃の大部分は、「窃取した認証情報の使用」によるものであり（図119）、その後、企業が利用するWebメールやその他のWebアプリケーションのハッキングへと続きます（図120）。過去の調査報告書では、ビジネスがクラウドベースのソリューションに移行する傾向が強まっていることから、それに比例して窃取された認証情報の使用も増加すると予想されると述べてきました。これは事実のようです。

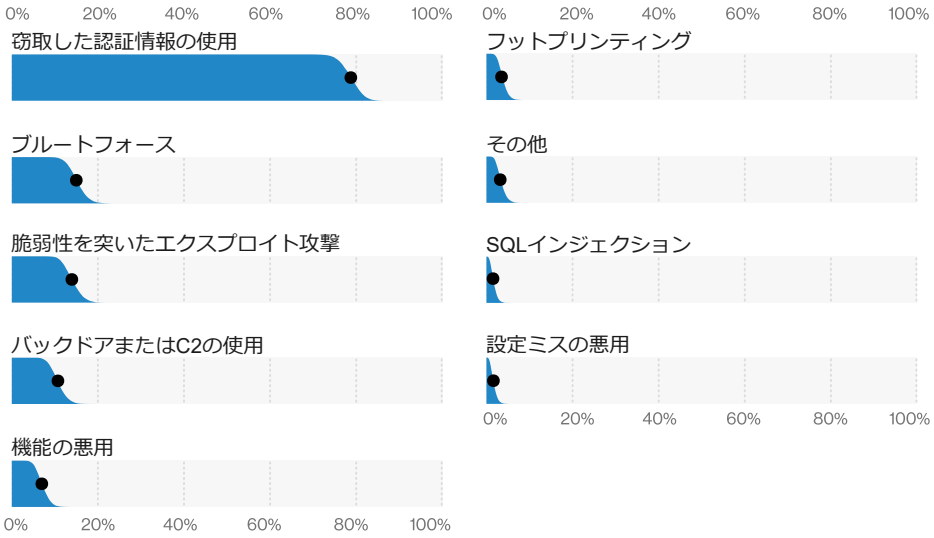


図119. 北アメリカ地域の漏洩/侵害によく見られるハッキングの種類 (n = 268)

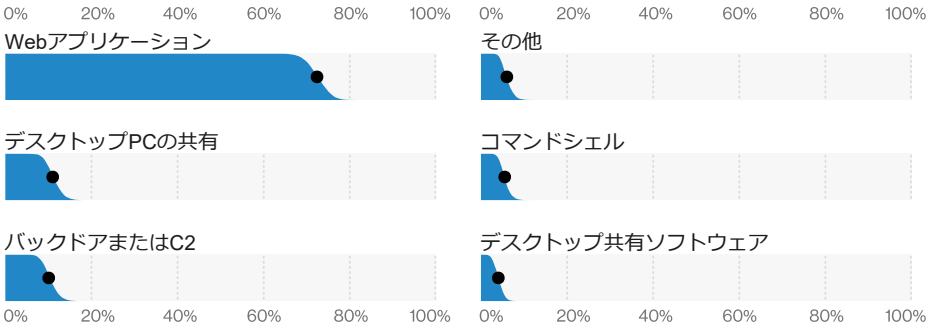


図120. 北アメリカ地域の漏洩/侵害によく見られるハッキングの攻撃経路 (n = 260)

見てください!これが、何もいいことがない理由です

外部攻撃者のために喜んで仕事をしてくれる従業員がいる限り、組織に害を及ぼす外部攻撃者への心配は必要ありません。今年度の内部攻撃者の数は、この地域とデータセット全体ではやや多くなっています（30%）（図121）。これは、「エラー」と「特権の悪用」の攻撃の流行によって説明できます。どちらも内部の攻撃者によって引き起こされ、組織に大きなダメージを与える可能性がありますが、「エラー」は意図的ではないのに対し、「不正使用」は性質からして意図的である可能性があります（多くの場合は故意）。

「エラー」を簡単に見てみましょう。図122に示すように、エラーに関連する全てのデータ漏洩/侵害の大部分は、「誤送信」（誤った受信者へのデータ送信）と「設定ミス」（ストレージバケットへのセキュリティ設定を忘れたなど）によって引き起こされています。理由はどうあれ、これらのエラータイプは、今年度のデータ漏洩/侵害ではピーナッツバターとゼリーのサンドイッチのようにセットになっているようです。恐らく、内部の攻撃者は、最近はTikTokでのレネゲードダンスを完璧にやろうと躍起になっているのでしょう。理由が何であれ、これらのエラーはあらゆる業界や地域で、驚くほど大きな割合で発生しています。この調査報告書の他の箇所でも述べているように、これらのエラーの攻撃径路は、ほとんど全て従業員側の不注意によるものです。

「不正使用」に目を向けると、「特権の悪用」が急増しています(56%)。これは、違法な目的のために合法的なアクセス権を使用することです。さらに下に行くと、「データの誤操作」と「所有権の濫用」がほぼ同じ割合で見られます(図123)。この地域では、どう見ても内部攻撃者の管理を強化することにメリットがありそうです。

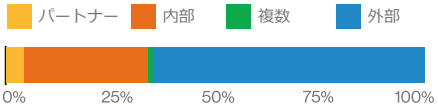


図121. 北アメリカ地域の漏洩/侵害の攻撃者 (n = 908)

図122. 北アメリカ地域の漏洩/侵害によく見られるエラーの種類 (n = 166)

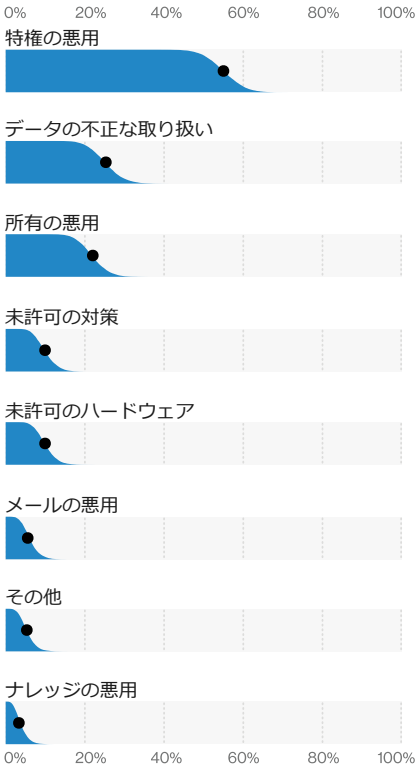
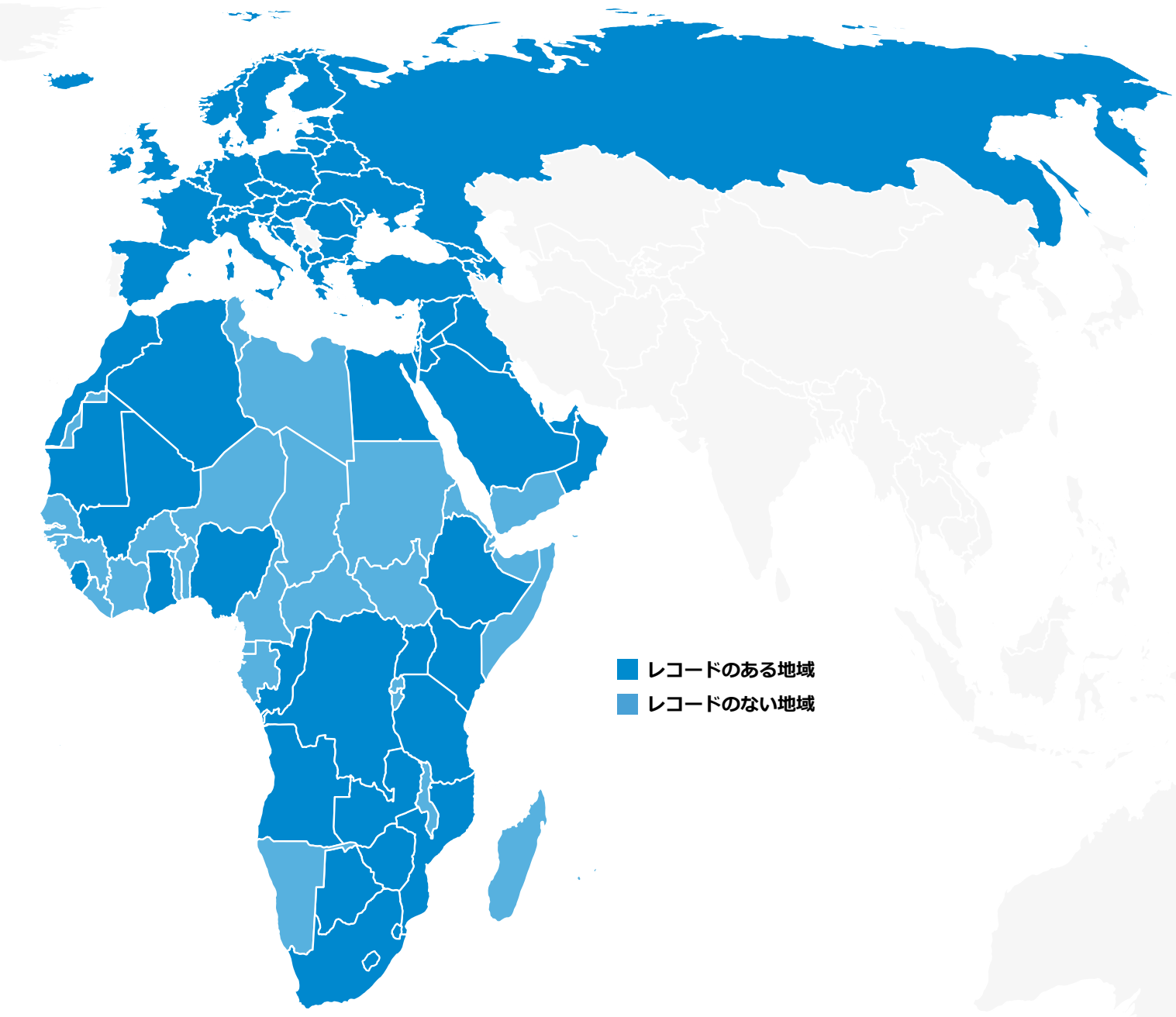


図123. 北アメリカ地域の漏洩/侵害によく見られる悪用の種類 (n = 121)

欧州・中東・アフリカ（EMEA）

図124. 欧州・中東・アフリカ（EMEA）地域



世界は年々狭くなってきているのに、調査報告書の範囲は逆になってきているようです。

このセクションでは、成長と探求の精神でヨーロッパ、中東、アフリカ（EMEA）のデータを見ていきたいと思います。EMEAを「遠い世界」と考える読者もいるかもしれませんが、EMEAの人々が受けている攻撃やサイバーセキュリティインシデントの種類は、北米やその他の地域で観察されているものと非常によく似ています。EMEA地域では、「Webアプリケーション」、「その他全て」および「サイバースパイ活動」が、今年度追跡した185件のデータ漏洩/侵害に関与する最上位のパターンとなっています（図125）。

「Webアプリケーション」のパターンには、この地域に大きな影響を与える2つの主要な攻撃が含まれています。1つ目は、EMEAのデータ漏洩/侵害全体の約42%を占める「窃取した認証情報の使用によるハッキング」です。このシナリオは通常、次のように展開されます。攻撃者は、主にフィッシングやマルウェアによって収集した認証情報を使用して、組織が所有するWebアプリケーションプラットフォームにアクセスし、ある種の悪事を犯します。今年度は、インターネットに接続したメールサーバーなどの資産だけでなく、ビジネス関連のアプリケーションなど、他のプラットフォームも標的にされています。このパターンに関与した2つ目の攻撃タイプは、システムデータに直接アクセスするか、またはサーバーをより悪質な犯罪に再利用するために、インターネットに接続したアプリケーションに対して行うエクスプロイト攻撃です。Webアプリケーション内でのこれらの攻撃は、今年度のEMEAにおけるデータ漏洩/侵害全体の20%近くを占めています。外部へ公開しているWebサイトについて、パッチを適用していないために脆弱性がないか、あるいは多要素ログインが実装されていないかを最近確認していない場合は、早急にチェックした方が良いでしょう。

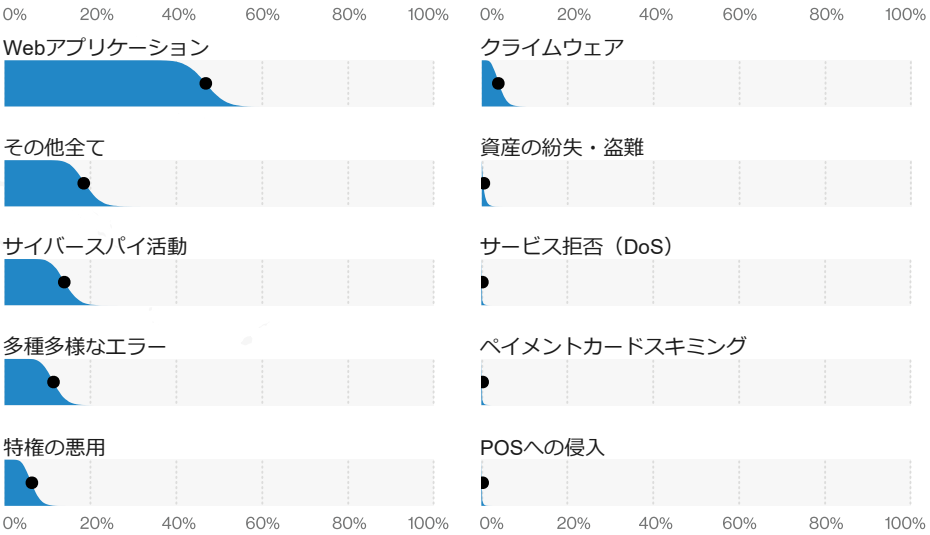


図125. 欧州・中東・アフリカのデータ漏洩/侵害のパターン（n = 185）

サマリー

攻撃者は、窃取された認証情報や既知の脆弱性を利用したハッキング技術を組み合わせて、EMEAのWebアプリケーションを標的にしています。この地域では、これらの戦術を利用したサイバースパイ攻撃が多く見られました。DoS攻撃は、インフラの可用性にも影響を及ぼし続けています。.

頻度	インシデント4,209件、確認されたデータの暴露185件
上位3つのパターン	EMEAでは「Webアプリケーション攻撃」、「その他全て」、「サイバースパイ活動」がデータ漏洩/侵害の78%を占めている
攻撃者	外部（87%）、内部（13%）、パートナー（2%）、複数の関係者（1%）（漏洩/侵害）
攻撃者の動機	金銭目的（70%）、スパイ活動（22%）、イデオロギー（3%）、愉快犯（3%）、怨恨（3%）、自己都合（1%）（漏洩/侵害）
侵害されたデータ	認証情報（56%）、内部情報（44%）、その他（28%）、個人情報（20%）、（漏洩/侵害）

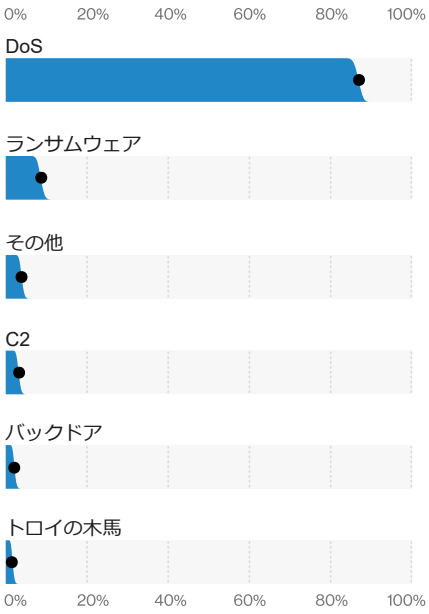


図126. EMEAのインシデントによく見られるマルウェア の種類 (n = 1,298)

次の「その他全て」のパターンは、他のパターンのいずれにも単純に当てはまらないデータ漏洩/侵害やインシデントを対象とした包括的なカテゴリーです。この例では、ほとんどが典型的なビジネスメール詐欺（BEC）から成り、この地域のデータ侵害全体の19%を占めています。このタイプのインシデントでは、ビジネスパートナー、顧客、役員などになりすまして、組織に攻撃者の銀行口座へ現金を振り込ませようとします。これらの攻撃は、スピアフィッシングとなりすまし（悪質な攻撃者が既存のスレッドを乗っ取り、会話の中に入り込むことで、詐欺行為の捕捉をはるかに困難にする）との間で、巧妙さの程度が異なります。

スパイ

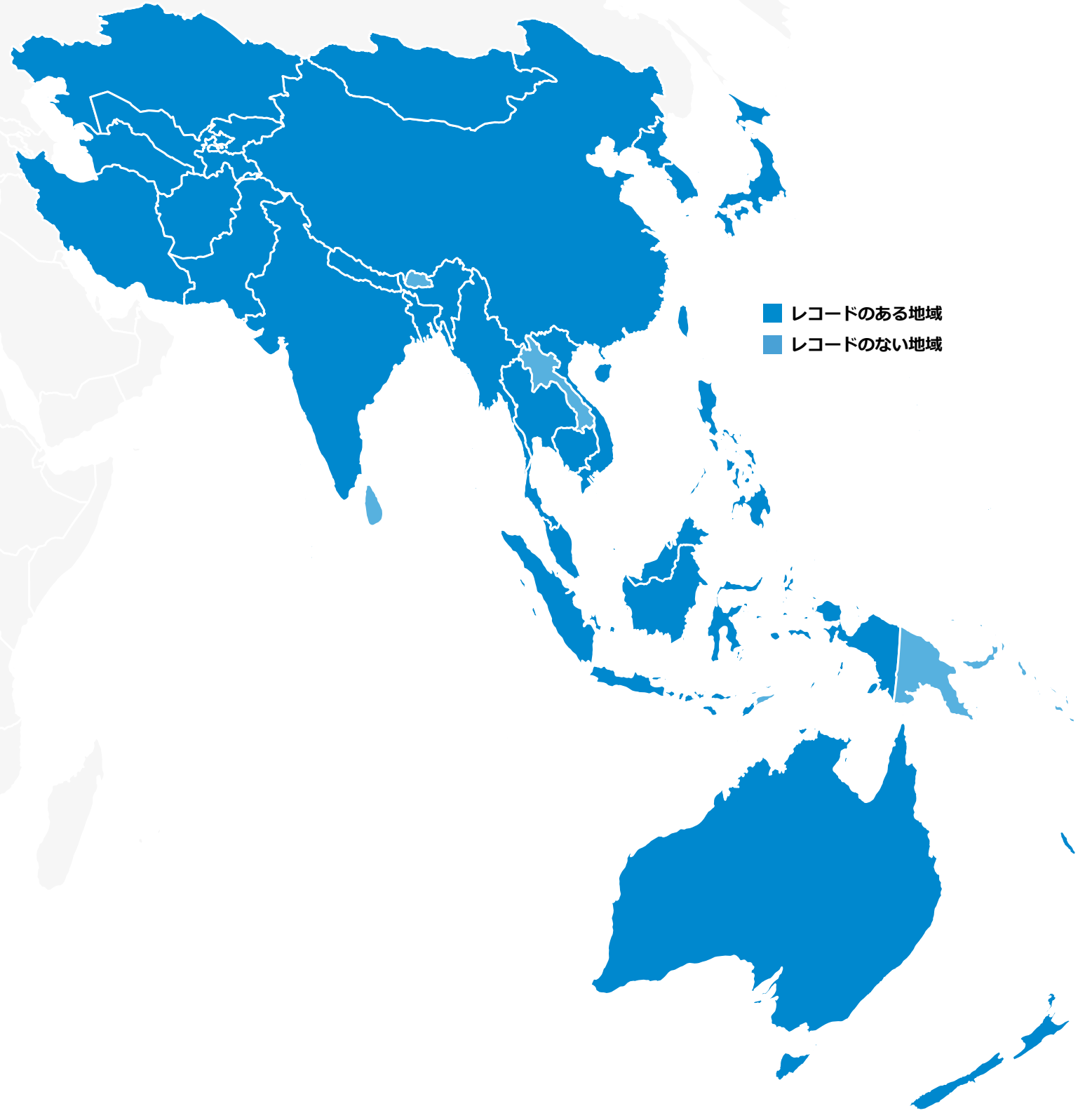
第3位のパターンは「サイバースパイ活動」で、この地域におけるデータ漏洩/侵害全体で14%発生しており、データセット全体の平均3%を大幅に上回っています。これは興味深い結果ですが、はっきりとした理由があるわけではありません。最も可能性の高い説明としては、弊社のデータ提供者の作為的な結果とこの地域で彼らがたまたま遭遇したケースが含まれているかもしれないということです。なにしろ、ジェームスボンドはイギリス人ですからね。このタイプのインシデントでは、APT攻撃の特徴である、アクセス権を獲得するためのソーシャル攻撃（フィッシング）と、持続性を維持し、人目につかないようにするためのマルウェアの投下と環境への配備の組み合わせを期待していることが考えられます。

大局的な観点

一歩下がって、より大きなクラスのインシデントを見てみると、EMEAのマルウェアの種類では「DoS攻撃」が最上位を占めています（図126）。興味深い点は、EMEAの全体的なコーパスに占める「DoS攻撃」のインシデントの割合が非常に高い一方で、実際にはどの地域よりもBPS(ビット/秒)の割合が低いということです。この地域で2番目に多かったインシデントは、現在世界中に広がり続けているランサムウェアです。実際、DoS攻撃を除くと、ランサムウェアはEMEAのインシデント全体の6%を占めており、C2/バックドア、ブルートフォース、パスワードダンパーとの関連が一般的です。だからこそ、エンドポイントにマルウェアが存在しないようにし、サーバーをロックダウンしておく必要があるのです。

アジア太平洋地域（APAC)

図127. アジア太平洋（APAC）地域



サマリー

APAC地域は、アクセスを収益化するためにランサムウェアを展開する金銭的動機を持った攻撃者に狙われています。また、この地域はフィッシング（多くの場合、ビジネスメール詐欺）や従業員によるヒューマンエラーに悩まされており、サイバースパイ活動に関連したデータ漏洩/侵害の発生率が平均よりも高くなっています。Webアプリケーションインフラは、資産の可用性を低下させるDoS攻撃と、窃取された認証情報を利用したハッキング攻撃の両方から標的にされています。

頻度	インシデント4,055件、確認されたデータの暴露560件
上位3つのパターン	APACでは「Webアプリケーション攻撃」、「その他全て」、「多種多様なエラー」がデータ漏洩/侵害の90%を占めている
攻撃者	外部（83%）、内部（17%）、パートナー（0%）（漏洩/侵害）
攻撃者の動機	金銭目的（63%）、スパイ活動（39%）、愉快犯（4%）（漏洩/侵害）
侵害されたデータ	認証情報（88%）、内部情報（14%）、その他（9%）、個人情報（6%）（漏洩/侵害）

アジア太平洋（APAC）地域には、アジアの大部分を含む広大な領域、オセアニアと呼ばれる地域（オーストラリアやニュージーランドなど）、そして太平洋とその周辺にある多数の島国が含まれています。

インシデントとデータ漏洩/侵害の関係性

図128には、この地域のインシデントの大部分を占める主なパターンが示されています。重要なのは、これらのパターンの中には、多く発生するが、通常はデータ漏洩/侵害として確認には至らないものもあるということです。例えば、「クライムウェア」のパターンで2番目に多いマルウェアの種類はランサムウェアのインシデントです。これらの攻撃はデータを暗号化するため、完全性の侵害（ソフトウェアインストール）と可用性の侵害（難読化）の両方にあたりますが、データの閲覧や窃取が行なわれるインスタンス（機密性）は比較的まれな状態が続いています。しかし、来年の報告書[48]に向けてのデータ収集では、被害者に力ずくで身代金を支払わせるために、特定のグループがNaming and Shaming（名前を公表して恥をかかせる）という戦術を用いているケースが表面化しています。また、別のケースでは、身代金を支払うように被害者を煽るために、暗号化する前のデータの一部または全体をコピーし、その抜粋をWebサイトに公開しています[49]。

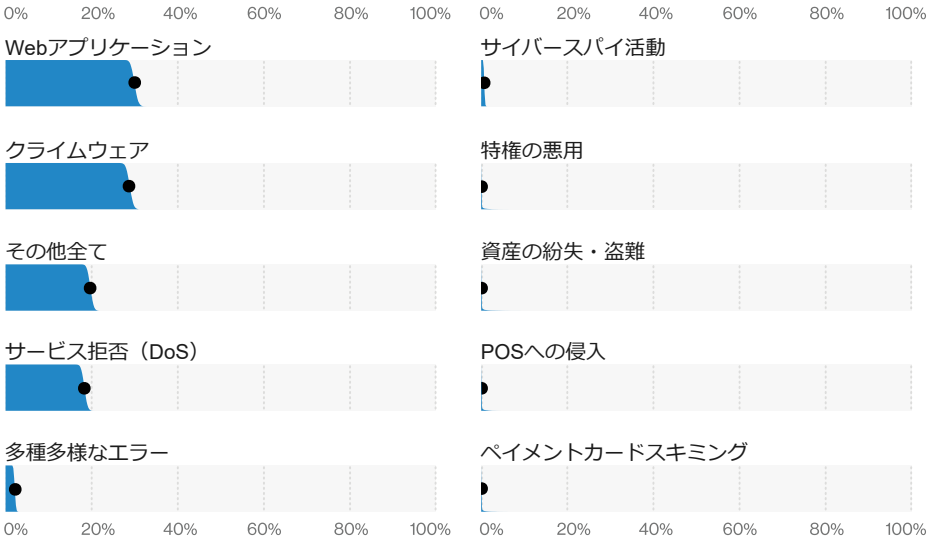


図128. アジア太平洋地域のインシデントのパターン（n = 4,055）

48 シーシュポスもまだ分かっていません！

49 公開されたインシデントの例：https://github.com/vz-risk/VCDB/issues?q=is%3Aopen+is%3Aissue+label%3ARansomeware-N%26S

APAC地域では、インシデントと確認されたデータ侵害のどちらも、最上位のパターンは「Webアプリケーション攻撃」でした。これらの攻撃の多くは、誰かが盗んだ信頼の置ける認証情報のリストをインターネットに接続したインフラストラクチャに対してテストを行い、成功するかどうかを確認するものです。認証情報が再利用され続ける問題と、結果として発生する認証情報ダンプの膨大な宝の山を考えると、もうかり過ぎて笑いの止まらないハッカーが相当な数存在しても不思議ではありません。もしその戦略がハッカー仲間たちに効かない場合は、ソーシャルエンジニアリングを使用することで、大抵の場合、彼らが探し求めている王国への鍵を手に入れることができます。認証情報は、この地域でのデータ侵害で盗まれた情報のトップだったので、明らかに何かが功を奏しているのは間違いありません。

2番目に多かったのは「その他全て」のパターンでした（図129）。これは、他の攻撃パターンの条件に当てはまらないデータ侵害のカテゴリーです。このパターンに当てはまる一般的な攻撃がいくつかあります。そのうちの1つであるビジネスメール詐欺（BEC）は、フィッシングメールで開始される攻撃です。攻撃者は、会社の経営陣の誰かになりすますことが多く、普通に上司からの要求には抵抗しない従業員の行動を支配しようとします。例えば、給与計算担当者は、組織の最高経営責任者からいつものとは異なる銀行口座へ入金するように言われたと思い込み、指示通りに入金を行いますが、後になってその要求が実際にはその役員からのものではなかったことに気付きます。

時には、口実（巧妙なシナリオ）の形で行われることもあります。よくある例としては、今まで使ったことのない特定の口座への電信送金を要求することです。いずれの場合も、権限の高い上司からのこの種の異常な要求に対処するためのプロセスがない限り、組織はインシデントに遭う羽目になるでしょう。

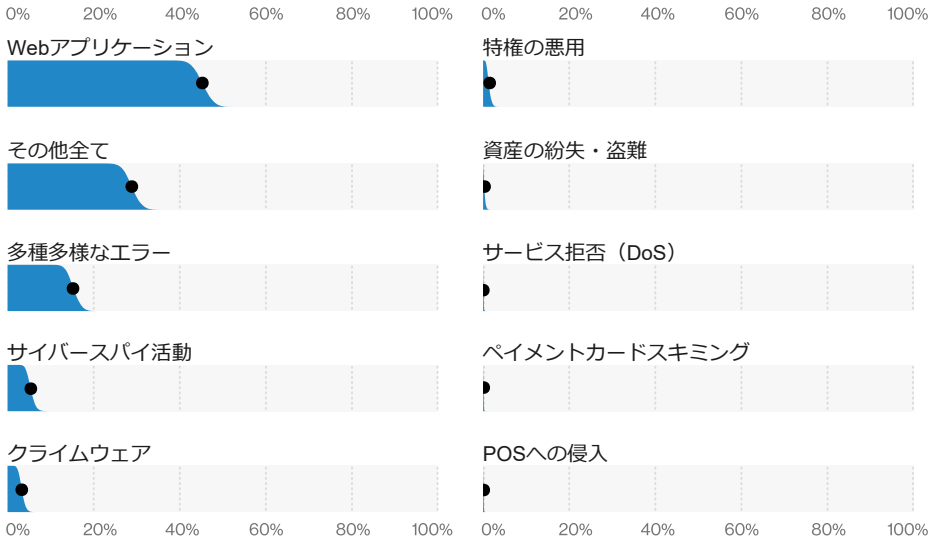


図129. アジア太平洋地域のデータ漏洩/侵害のパターン（n = 560）

おっと、そんなことしたっけ?

あらかじめ警告しておきます。これから述べることにショックを受けるかもしれませんが、人間は完璧ではありません。私たちも最初は信じていませんでした。しかし、弊社のデータセットは確かにそうであることを示しており、組織の種類も地域もあまり違いはないようです。実際、APAC地域のデータでは「多種多様なエラー」のパターンが3位に入っています。いったいこれらのエラーは何なのか?なぜ自分もやってしまうのか?ここでは、組織の構成員が、実際には意図していなくてもデータ漏洩/侵害を引き起こす可能性がある様々な状況を紹介します。

図130は、エラーのほとんどが「設定ミス」であり、不注意によるものであることを示しています。設定ミスのエラーは、このDBIRでもずっととり上げてきています。この種のミスは、通常のセキュリティ管理を行わずにクラウド上のデータベースを立ち上げた従業員、特にシステム管理者や大量のデータに重要なアクセス権を持つ人物が、「これで大丈夫だろう」と思ったときに発生します。「これなら大丈夫。きっと誰もここにはアクセスできないだろう」と自分自身に言い聞かせているのです。あるいは、スペシャルランチが2時に終わってしまうので、後で都合の良い時にセキュリティを管理しようと思って席を離れることもあります。しかし、多くの場合、まさにセキュリティ研究者、あるいはもっと悪いことに攻撃者に発見された時に、その瞬間は訪れるのです。そう、信じられないかもしれませんが、インターネット上に散らばっているデータの金塊を見つけるために雇われている者（フリーランスもいる）は、本当にかなりの数にのぼります。次に何が起きるかは、データを見つけた人の動機にかかっています。セキュリティ研究者であれば、大抵はデータの所有者である組織に通知するでしょう（突き止めることができれば）。しかし、時には、通知という動機を持った人ではなく、ダークウェブ上で見つけたうま味のあるこの情報を収益化しようとする者がいます。

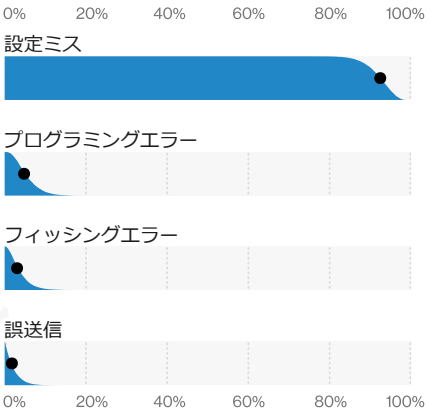


図130. アジア太平洋地域の漏洩/侵害のエラーの種類 (n = 55)

ラテンアメリカとカリブ海地域（LAC)

図131. ラテンアメリカとカリブ海（LAC）地域

サマリー

この地域で記録されたインシデントやデータ漏洩/侵害の件数が比較的少ないにも関わらず、調査結果は明らかに世界全体のデータセットとの整合性を示しています。DoS攻撃は予想以上に多い件数が発生しており、ランサムウェアのインシデントは深刻な問題となっています。

頻度	インシデント87件、確認されたデータの暴露14件
上位3つのパターン	LACでは「DoS攻撃」、「クライムウェア」、「Webアプリケーション攻撃」がインシデントの91%を占めている
攻撃者	外部（93%）、内部（7%）、パートナー（1%）、複数の関係者（1%）（インシデント）
攻撃者の動機	金銭目的（52%～87%）、スパイ活動/イデオロギー（各2%～27%）、愉快犯/怨恨（各0%～15%）、自己都合/恐怖/その他/二次的動機（各0%～8%）（インシデント）
侵害されたデータ	認証情報、個人情報、内部情報、機密情報、システム情報（インシデント）
データ分析ノート	攻撃者の動機は、既知の動機によるデータ漏洩/侵害が22件のみだったため、パーセンテージの範囲で表しています。

法律で定められているかどうか

まず指摘しておきたい重要なことは、メキシコ、ブラジル（データ保護法が2020年2月から施行）、コロンビア（政府のみに通知が義務付けられている）を除くと、この地域の全ての国でデータ漏洩/侵害が発生した場合、通知することが政府または被害者に法的に義務付けられているわけではないということです。したがって、この地域ではインシデントやデータ漏洩/侵害の報告がかなり不足していることは間違いありません。新しい開示法が可決されている世界の他の地域のように、報告が急増し、以前に報告されていたのが氷山の一角に過ぎなかったことが明らかになるどうかは興味深いところです。うまくいけば、本調査のデータの精度を高めるために、この地域の新たな協力者を誘い込むことができます。(読者の中にそのような方がいらっしゃれば、ぜひご相談させてください。)

全てのことを考慮すると、この地域から得られるデータが明らかに世界のデータセットに反映されていることが分かります。全てのインシデントにおける攻撃者の大半は外部者であり、この地域での93%という割合はデータセット全体の92%と非常に近いものです。同様に、LACのインシデントの52%～87%が金銭的動機によるものであるのに対し、世界全体のデータでの金銭的動機は64%でした。

インシデントの上位パターンは、より大きなデータセットと一致しており、「DoS攻撃」が50%～70%を占めており、「クライムウェア」、「Webアプリケーション」、「その他全て」は互いに密接にグループ化されています（図132）。「クライムウェア」は、主にランサムウェアに関連したインシデントで構成されており、他の攻撃の種類と比較して、この地域では非常に強い傾向を示しています。

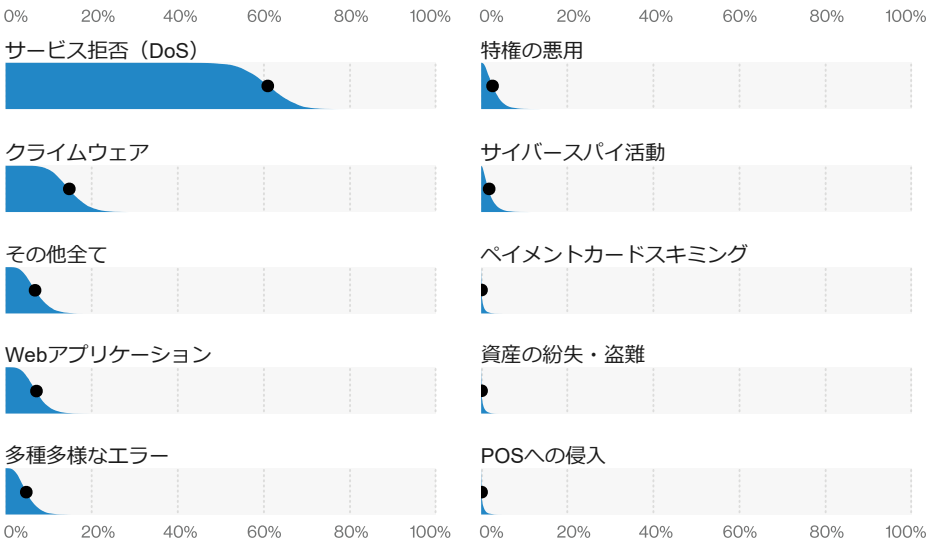
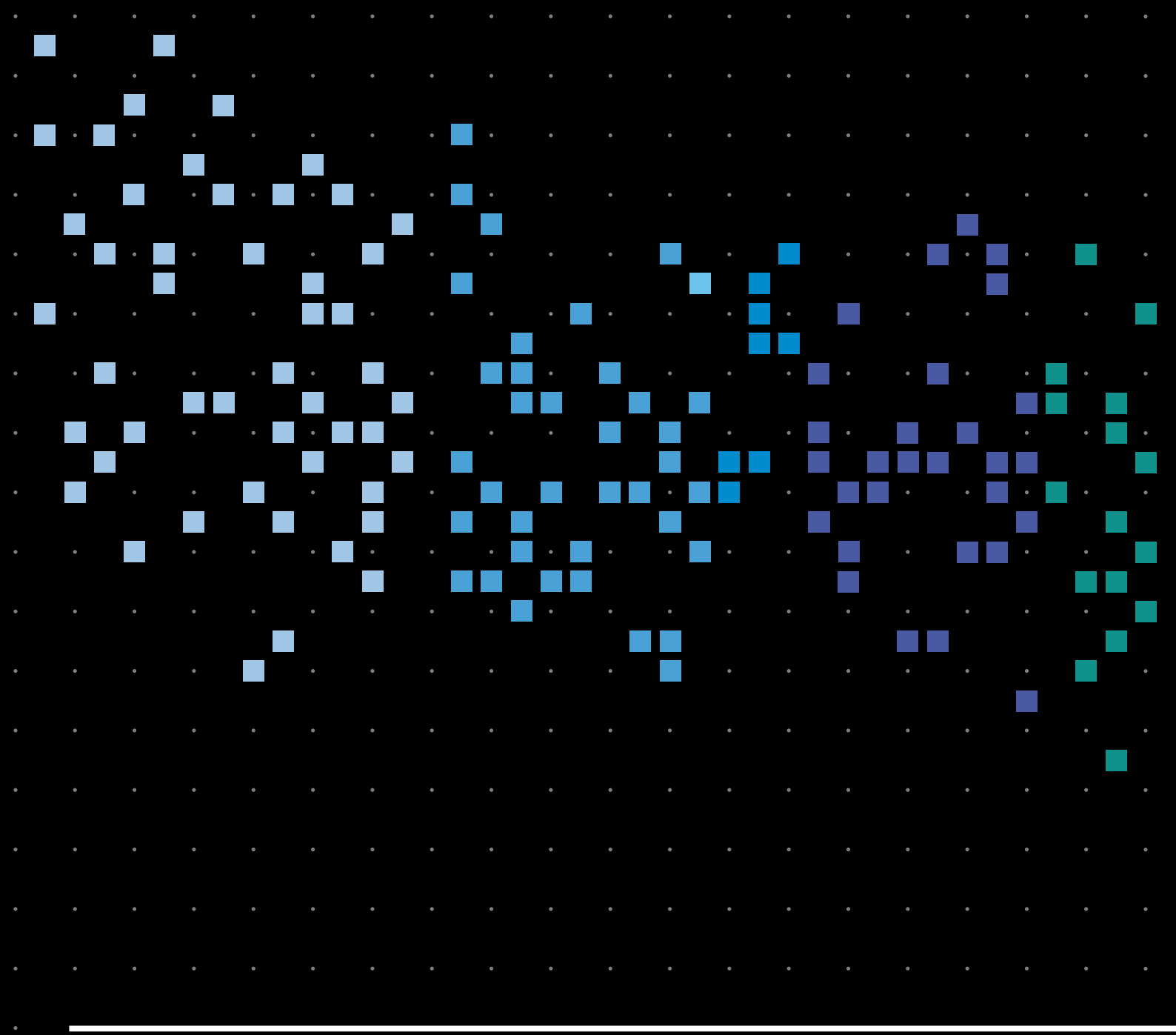


図132. ラテンアメリカとカリブ海地域のインシデントのパターン（n = 87）

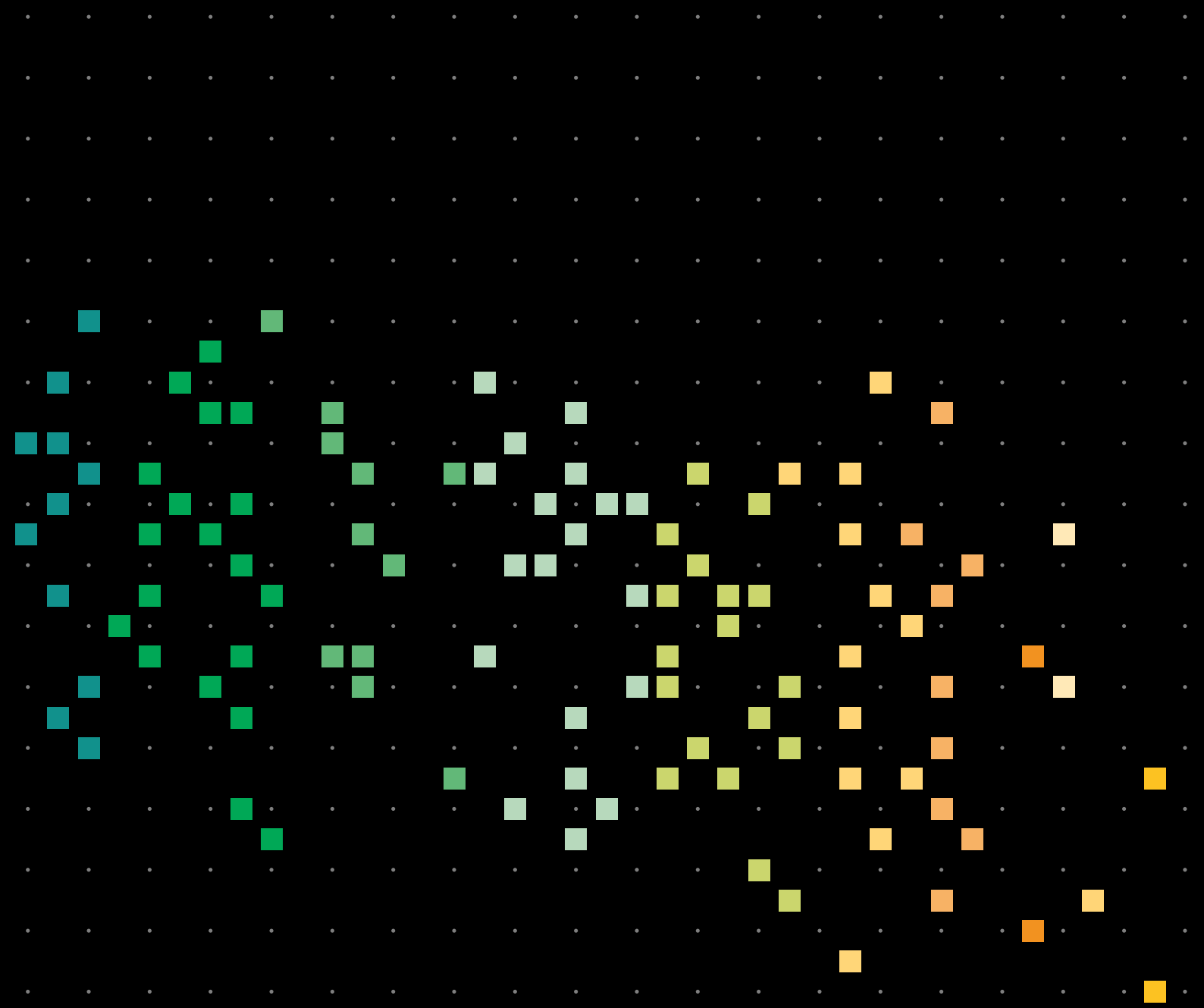
このような類似点があるにもかかわらず、この地域ではビット/秒（BPS）の中央値が最も大きく、世界の中央値が500Mbps強であるのに対し、この地域では9Gbpsとなっています（図133）。この値の高さは、この地域のDDoSデータで大きな比率を占めていた、金融機関に対するDoS攻撃から予想される結果と一致します。

各地域のデータを分析する中で確実になったことの1つは、年によって特定の国がデータセットに含まれているかどうかに関わらず、全ての国で同じようなタイプの攻撃が見られるということです。被害者の地理的な位置に基づいて攻撃者が戦術を変えているわけではないことは何度も確認されています。彼らは、不正アクセスを可能にするために必要なものに基づいて攻撃を調整しています。このように、地域によって多少の違いはあるものの、攻撃の種類は全ての国で共通していることが一貫して見られます。

図133. ラテンアメリカとカリブ海地域におけるDDoSの平均的なBPS
(n = 52 DDoS)：全地域のモード(緑色の線): 565 Mbps



06



まとめ

皆様、これで報告は終わりです。今回もご参加いただきありがとうございました。本報告書をお読みいただき、ご参考にしていただける内容であったことを願っております。いつものように、読者の皆様、サポーターの皆様、データ提供者の皆様に心より感謝申し上げます。この仕事は、時として大変なこともありますが、愛情のこもった仕事でもあります。このレポートを作成し、皆様と調査結果を共有することができたことは、大変幸運なことだと感じております。この努力の報告書に時間と資産を割いてサポートしてくださった皆様、改めてありがとうございました。来年もまたここでお会いできることを楽しみにしています。それまでは、どうかお元気でご盛栄に、そして何事にも準備を怠らずに。

CISコントロールの推奨事項

CISのCritical Security Controls（CSC）：

CSC 1	ハードウェア資産のインベントリとコントロール
CSC 2	ソフトウェア資産のインベントリとコントロール
CSC 3	継続的な脆弱性管理
CSC 4	管理権限のコントロールされた使用
CSC 5	モバイルデバイス、ラップトップ、ワークステーションおよびサーバーに関するハードウェアおよびソフトウェアのセキュアな設定
CSC 6	監査ログの保守、監視および分析
CSC 7	電子メールとWebブラウザの保護
CSC 8	マルウェア対策
CSC 9	ネットワークポート、プロトコル、およびサービスの制限およびコントロール
CSC 10	データ復旧能力
CSC 11	ファイアウォール、ルータ、スイッチなどのネットワーク機器のセキュアな設定
CSC 12	境界防御
CSC 13	データ保護
CSC 14	Need to Know（情報は知る必要のある人のみに伝え、知る必要のない人には伝えない）に基づいたアクセスコントロール
CSC 15	無線アクセスのコントロール
CSC 16	アカウントの監視およびコントロール
CSC 17	セキュリティ意識向上トレーニングプログラムの実施
CSC 18	アプリケーションソフトウェアセキュリティ
CSC 19	インシデントレスポンスと管理
CSC 20	ペネトレーションテストおよびレッドチームの訓練

長年の努力の結晶として、DBIRはようやく標準化されたコントロールを手にすることができるようになりました。

ただし、公平に言えば、これは単に古いアプローチを新しいものに変えただけです。ほこりを被った2014年度版のDBIRを取り出してその調査結果に目を通せば、防御対策とコントロールについての弊社のアプローチを標準化するために行った努力がどのようなものかお分かりいただけるでしょう。

この取り組みの中で、弊社は、私たちの知見をCISのCritical Security Controls（CSC）（当時はバージョン6）と整合させ、DBIRの熱心で忠実な読者に、この知見を読者のセキュリティ対策に一致させる方法を提供しました。これまでの試みを再検討して、読者の皆様に同じタイプの統合を提供することで、それぞれのセキュリティプログラムの優先順位を弊社のデータに結びつけられると聞いて、喜んでいただけるかもしれません（そうでないかもしれません）。

CISを推奨する理由

私たちのほとんどは、恐らく、セキュリティフレームワークおよびガイダンスに関して独自の好みを持っており、本報告書の執筆者たちも確かに独自の好みを持っているが（ある時点または別の時点でCIS Controlsに貢献している者がいるかもしれない）、弊社がこの特定のコントロールを選択したのは、経験からの理由がいくつかあります。簡単に言えば、これらのコントロールは、我々の調査対象である攻撃と攻撃径路の間を意味のある形で結びつけるのに十分なレベルの情報を提供しており、また、CIS Controlsと他の標準規格との間にはオンラインで自由に利用できる多数の様々なマッピングが存在します。また、彼らの非営利のコミュニティのアプローチと一致していることも助けになっています。

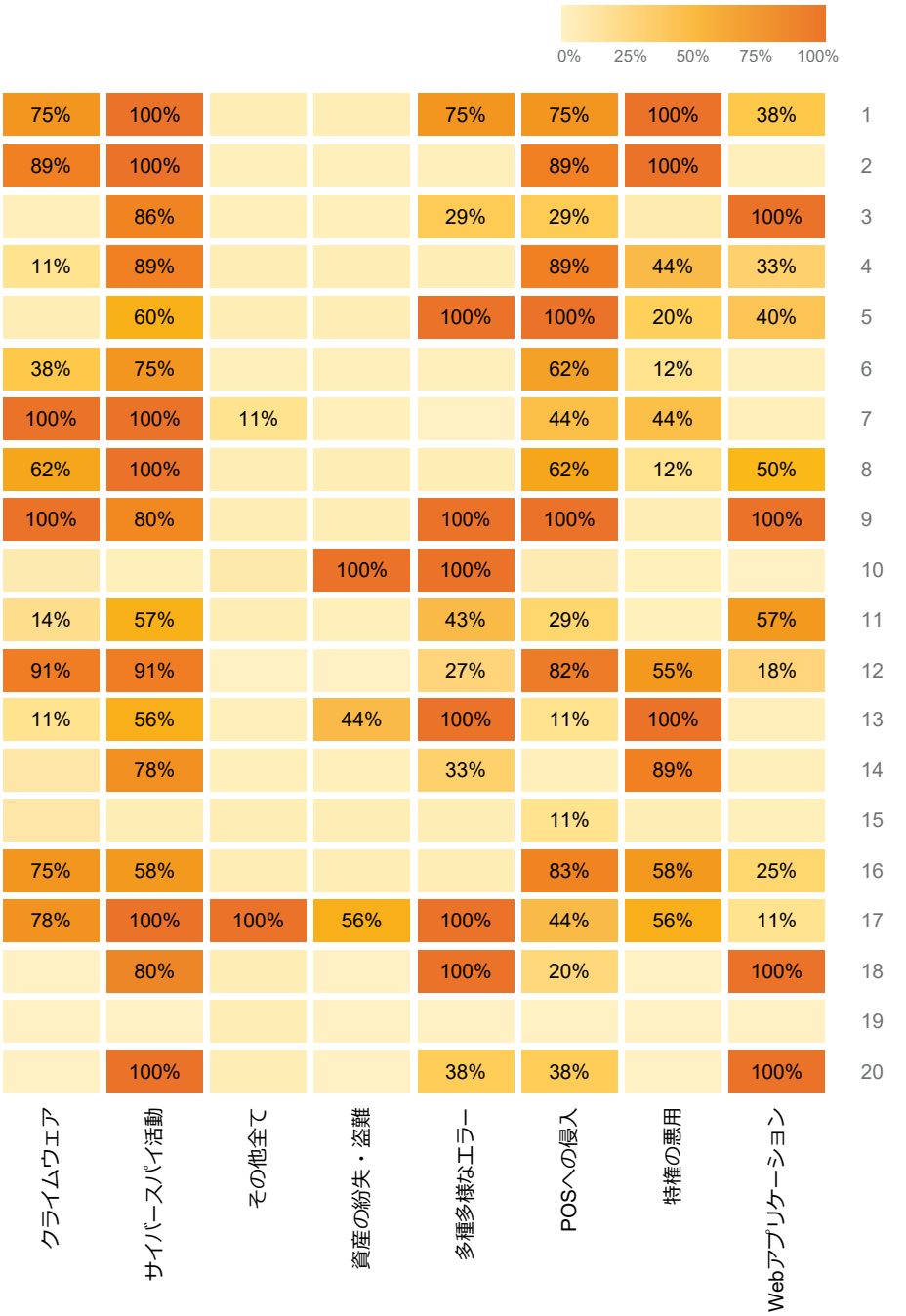


図134. CSC規定の防御対策がパターンに対応する割合

CIS Controlsを知らない人のために説明すると、CIS Controlsはコミュニティで構築され、攻撃者の情報に基づいて優先順位付けされたサイバーセキュリティのガイドラインであり、上位20のコントロールに編成された171の防御対策で構成されています。CIS Controlsのユニークな点の1つは、組織がセキュリティプログラムをどこから始めるべきかを理解できるようにすることに重点を置いていることです。この優先順位付けは、次の2つのように表されます。

- CSCの順序付けにより、緩い優先順位付けを可能にしている（Control 1のハードウェアのインベントリは、Control 20のペネトレーションテストよりも恐らく優先される)
- バージョン 7.1[50]で導入された実装グループの概念では、組織が直面しているリソースの規模とリスクに基づいて防御対策が171のグループに分けられている。すなわち、リソースの少ない小規模な組織（実装グループ1）では、たとえCSC 1の範囲内であっても、パッシブな資産検出ツールのようなリソースおよびプロセス集約的なコントロールを実施することを期待すべきではないが、リソースが多い組織やリスクレベルが高い組織では、そのようなコントロールの検討が考えられる。

50 https://www.cisecurity.org/blog/v7-1-introduces-implementation-groups-cis-controls/

どのように使用したか

観察力の高い方は、特定の業種で発見されたデータ侵害に対し、上位3つの対策を特定する業種セクションのサマリーに新しい項目を追加したことにお気づきかもしれません。これらの上位3つの対策を特定するために、弊社はVERISアクションとサブコントロールのマッピングを作成し、CSCレベルで集約しました。これにより、セキュリティプログラムに優先順位をつけることを検討すべき対策の大まかな概要を知ることができます。

図134は、私たちが行った最初のマッピングに基づいており、特定された攻撃パターンを緩和する役割を果たす防御対策の割合をCSC単位で示します[51]。分析した全ての業種で確認された上位対策のいくつかを、以下に簡単に説明します。実際のCSCに関する追加情報は、CISのWebサイトに掲載されています[52]。

継続的な脆弱性管理（CSC 3）

悪用されているWebアプリケーションに見られるようなコードベースの脆弱性を発見して修復する素晴らしい方法であり、設定ミスを発見するのにも便利です。

セキュアな設定（CSC 5、CSC 11）[53]

システムが、その機能を最大限活用するために必要なサービスとアクセスのみで構成されていることを保証し、検証します。インターネットに接続したオープンで全ユーザーに読み取り権限があるデータベースは、恐らくこれらのCSCに従っていません。

電子メールとWebブラウザの保護（CSC 7）

ブラウザとメールクライアントは、ユーザーが「ワイルドウエスト」(インターネットのこと)とやりとりする主要な方法であるため、これらをロックしてユーザーに防衛のチャンスを与えることが重要です。

ネットワークポート、プロトコル、およびサービスの制限およびコントロール（CSC 9）

Control 12がトラストゾーン間の相互認証を知ることを目的としているのと同じように、このコントロールは、システム上で公開すべきサービスやポートを理解し、それらへのアクセスを制限することを目的としています。

境界防御（CSC 12）

ファイアウォールだけでなく、このコントロールにはネットワーク監視、プロキシ、多要素認証などが含まれており、さまざまな攻撃への適用が増えています。

データ保護（CSC 13）

情報漏洩を制限する最良の方法の1つは、その機密情報へのアクセスを制御することです。このリストには、機密情報のインベントリの管理、暗号化、および許可されたクラウドおよび電子メールプロバイダーへのアクセスの制限が含まれます。

アカウントの監視およびコントロール（CSC 16）

組織全体のユーザーアカウントをロックすることは、窃取された認証情報が悪意のある者に使用されないようにするための鍵となります。特にここにも現れている多要素認証を使用します。

セキュリティ意識向上トレーニングプログラムの実施（CSC 17）

悪意のある攻撃や不注意から発生する漏洩/侵害に関するトレーニングをユーザーに実施します。

未来はコントロールできる

継続的な改善と透明性を高めるために、VERIS GitHubページ（https://github.com/vz-risk/veris）にコントロールのマッピングを追加します。皆様にもぜひご利用いただき、改善点などをフィードバックしていただきたいと思います。これは、コントロールをよりアクセスしやすく、他の人が利用しやすいものにするための第一歩であり、この最初のバージョンには改善の余地があることを認識しつつ、迅速に改良を加えていく予定です。共通の言語を共有すればするほど、協力しながら環境と組織の安全性を強化していくことが容易になります。

51 注意すべき点としては、CISコントロールはサイバーセキュリティのベストプラクティスに焦点を当てており、物理的なセキュリティ（ペイメントカードスキミングのパターン）や可用性のプラクティス（サービス拒否のパターン）のようなものには触れていないため図には含めていません。

52 https://www.cisecurity.org/controls/cis-controls-list/

53 私たちは、デスクトップ、サーバー、およびワークステーションのセキュアな設定（ CSC 5）とネットワーキングデバイスのセキュアな設定（CSC 11）の両方を組み合わせましたが、これには2つの潜在的な理由があります。1つは、侵害の最終的な原因がネットワークの問題なのかシステムの問題なのかを知ることが困難であること、もう1つは、特定の環境でネットワークとデバイスを分離することがますます困難になってきていることです。

年間総括[54]

1月

2019年の最初の情報収集は、クラウドベースのマネージドサービスプロバイダーを標的としたAPT10侵入攻撃に関するFBI Liaison Alert System（FLASH）でした。月間を通して、Verizon Threat Research Advisory Center （VTRAC）の情報収集は、2018年のトレンドを一部引き継ぎ、新年を通じて忙殺されかねない新しいトレンドを反映していました。新しい情報は、APTグレードの2人のロシア人攻撃者、GreyEnergyとAPT28（Sofacy）のにつながりました。「DNSpionageキャンペーン」の追跡を開始してから2ヶ月、新たに収集した情報は、それの世界的な広がりと複雑さを明らかにしました。1月にGandCrabとRyukのランサムウェアが急増したのは、SamSamの運営者が起訴されて活動を停止した後に残された空白を埋めるためでもあります。VTRACは、2019年にさらに増加して再浮上した電子小売業者に対するMagecartペイメントカードスクリプティングスキミング攻撃を追跡し、報告し続けています。ミラノに本拠を置くTecnimont SpAのインド子会社は、中国のハッカーによって1860万米ドル（13億ルピー）が盗まれた後、詐欺の餌食になりました。攻撃者はムンバイ支店の電子メールシステムに侵入し、ビジネスの「リズム」を学び、主要人物、語彙、習慣を学習しました。イタリアの幹部やスイスの弁護士との一連の電話会議の演出により、インド支店長は香港の銀行に資金を送金するように説得されました。

2月

オーストラリア議会は、コンピュータネットワークが特定できない「セキュリティインシデン」によって侵害されていたことを明らかにしました。ノルウェーのクラウドコンピューティング企業であるVisma社は、侵害の原因をmenuPass攻撃者にあるとしています。捕鯨キャンペーンが観測され、恐らくビジネスメール詐欺に利用するためにOffice 365の認証情報を狙ったと思われます。マルタのヴァレッタ銀行は1300万ユーロの詐欺にあいました。APACでAPT級の攻撃者が武器として使用した文書を分析にかけ、共有された「デジタルクォーターマスター」が複数の攻撃者に提供されているかどうかを調べたところ、その中に国家機関と提携した攻撃者が複数いました。一部の中国の攻撃者間のリンクを発見しましたが、「攻撃的なサイバーツールの現状でのやり取りは不透明なまま」であり、さらなる調査が必要です。

3月

Cisco Adaptive Security Appliances、Cold Fusion、Drupal、Microsoft Exchange Server、Windowsカーネルなどの脆弱性を含む、新しい脆弱性に対するエクスプロイト攻撃の成功が3月に繰り返し問題になっていました。2つの「ゼロデイ」脆弱性に対する攻撃は、「Patch Tuesday」の36パッチの中で緩和されました。中国のWinnti攻撃者による「Operation ShadowHammer」攻撃は、PCメーカーASUSTeK Computerのソフトウェアアップデートを改ざんし、被害者のコンピュータにマルウェアをインストールしました。アルミニウムメーカーのNorsk Hydroは、ランサムウェア「LockerGoga」の攻撃を受けた。シトリックスは、攻撃者が足がかりを得るためにパスワードスプレー攻撃を使用した可能性が高いとFBIから警告された後、データ侵害を開示しました。弊社は、POSシステムを標的とした3つのキャンペーンに関する情報を収集しました。

54 VTRACのDavid M.Kennedyに感謝します。

4月

製薬会社バイエルは、機密性の高い知的財産を狙ったWinnti攻撃者による攻撃を阻止したと発表しました。インドの大手ITサービス会社のWiproは、同社の顧客への攻撃のために侵入されました。攻撃の背後にあるグループの究極的な目的は、ギフトカード詐欺にあるようです。ベトナムに拠点を置くAPT32（オーシャンロータス）の攻撃者は、外国の自動車会社を標的にしてIPを取得していました。米国エネルギー省は、カリフォルニア州ロサンゼルス郡とユタ州ソルトレイク郡の送電事業者がDDoS攻撃を受け、業務に支障をきたしたが、停電は発生しなかったと報告しました。US-CERTは、複数のVPNアプリケーションが認証情報やセッションクッキーをメモリやログファイルに安全でない形で保存していると警告しています。Cisco、Palo Alto Networks、F5 Networks、Pulse Secure製品が影響を受けました。主に中東および北アフリカに所在する民間および公的組織を標的とした新しいDNSハイジャックキャンペーン「Sea Turtle」が発見されました。

5月

5月の「Patch Tuesday」には、「BlueKeep」の愛称で親しまれているリモートデスクトッププロトコルの脆弱性、CVE-2019-0708に対するパッチが含まれていました。喫緊のWannaCryのようなワームを避けるためにパッチを当てようという声は、大げさなものになってしまいました。メリーランド州ボルチモア市は、RobbinHoodランサムウェアによって麻痺状態になりました。新しいランサムウェア「Sodinokibi」は、パッチが適用されていないOracle WebLogicサーバーから拡散しているように見えました。Magecartグループは、ペイメントカードのスクレーピングスクリプトを展開し続けていました。標的にされたプラットフォームはMagentoだけでなく、PrismWebやOpenCartなどのeコマースプラットフォームにまで拡大していました。3月にパッチを当てたMagentoの脆弱性が、大量スキャンやSQLinjection攻撃の対象となりました。

6月

LabCorpは、サードパーティの請求書回収会社によるデータ漏洩を開示し、770万人のアメリカ人の個人情報の流出を暴露しました。中国の諜報機関がオーストラリア国立大学をハッキングし、学生が公務員に採用される前に、学生を情報提供者に育てるために使用できるデータを収集しました。米国の送電網規制当局NERCは、ロシアとの関係が疑われる大手ハッキンググループ「Xenotime」が電力会社のネットワークへの偵察を行っているとの警告を発表しました。中国の諜報活動攻撃者APT10は、7年間にわたって「Operation Soft Cell」を実行してきました。彼らは、反体制派、役人、スパイの疑いのある人物を追跡するために、世界30カ国にサービスを提供している国際的な携帯電話プロバイダー10社にハッキングしました。GandCrabランサムウェアの背後にある事業者は、閉鎖を発表しました。しかし、ほとんどのアナリストは、彼らは単にGandCrabからSodinokibiに移行しただけだと評価しました。

7月

Capital Oneは、ハッカーが社会保障番号や銀行口座番号を含む1億枚のクレジットカード申請データにアクセスしたことを明らかにしました。不適切に保護されたAmazonのクラウドストレージが、1人の犠牲者による30GBのクレジット申請データの盗難の中心でした。マイクロソフトは、世界中のシンクタンクやNGO、その他の政治団体を標的としたサイバー攻撃を過去1年間で800件近く検知したことを明らかにしましたが、攻撃の大部分はイラン、北朝鮮、ロシアに端を発していました。BASF、シーメンス、ヘンケルなどドイツの大手工業企業数社は、中国のWinntiグループによる国家主導のハッキング攻撃の犠牲になったと発表しました。

8月

8月16日（金）、テキサス州の22の町がTrickbotに続いてSodinokibiランサムウェアに感染し、攻撃者がマネージドサービスプロバイダーであるTSM Consultingに侵入し、MSPのリモート管理ツールConnectWise Controlを使用してマルウェアを配布したことが判明しました。翌週、マルウェア研究者は、Emotetの配布ネットワークで活動が復活したことを確認しました。6月には、Emotetの一団は攻撃を停止しているように見えました。9月中旬までには、Emotetは完全に活動しているように見えました。Emotetは、Mummy Spider、TA542、TA505を含む複数のロシアの攻撃者とリンクしていました。Emotetのマルウェアスパムは、Dridex、Ursnif、Trickbot、Ryukなどの他のマルウェアペイロードを配信していました。

9月

8月末から9月初旬にかけて、複数の情報筋が、iOSとAndroidのトロイの木馬を使って、チベット人の権利活動家や少数民族のウイグル人をターゲットにした戦略的なWeb侵害の報告を始めました。6月に報告された「Operation Soft Cell」は、恐らくこのキャンペーンの一部だと思われます。もう1つの新たな中国のAPT級の攻撃者「APT5」が出現し、脆弱性のあるVPNサーバーを攻撃していることが判明しました。9月の「Patch Tuesday」にはWindowsの2つの「ゼロデイ」脆弱性の対応が含まれていましたが、月末前にマイクロソフトは3つ目のゼロデイに対応した定例外パッチをリリースしました。ソーシャルビデオゲーム開発会社「Zynga」への侵害は、1億7500万人以上のプレイヤーに影響を及ぼしました。

10月

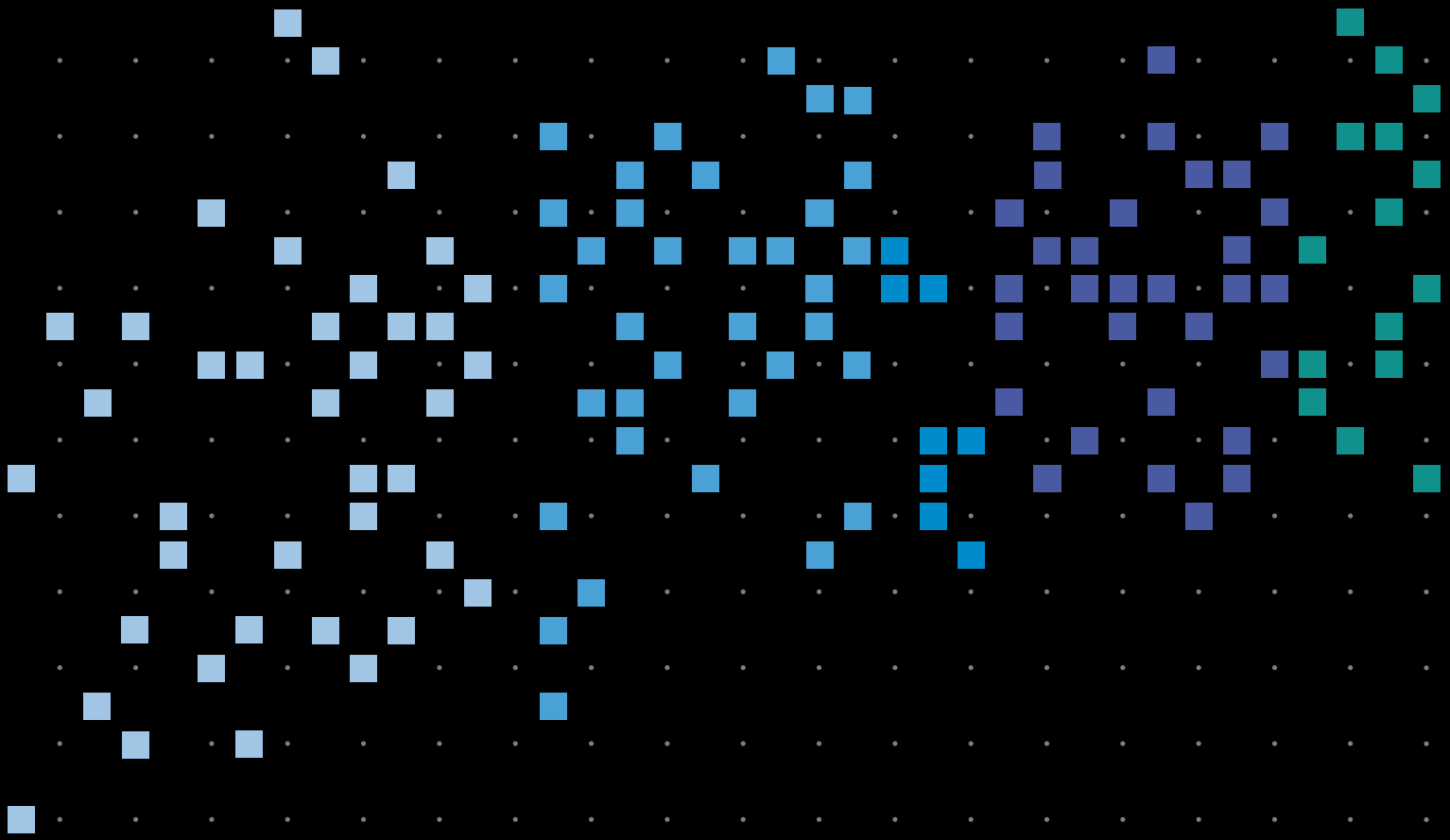
10月、VTRACは、TA505、FIN6、FIN7、RTMサイバー犯罪者を含むAPT級の攻撃者による諜報活動に振り回されました。FIN4、FIN6およびCarbanakは、さまざまなMagecartグループにリンクされていました。サイバースパイ活動やサイバー犯罪の攻撃者に関する情報には、Charming Kitten、Turla、Winnti、APT29の攻撃者が含まれていました。9月にインドのクダンクーラム原子力発電所（KNPP）に対するLazarusグループによる攻撃について報告を受けました。この攻撃は、原子力発電所の制御システムや発電所の制御システムのいずれにも影響を与えませんでした。ビジネスメール詐欺が新たに流行り出し、「ベンダーメール詐欺」と呼ばれるようになりました。

11月

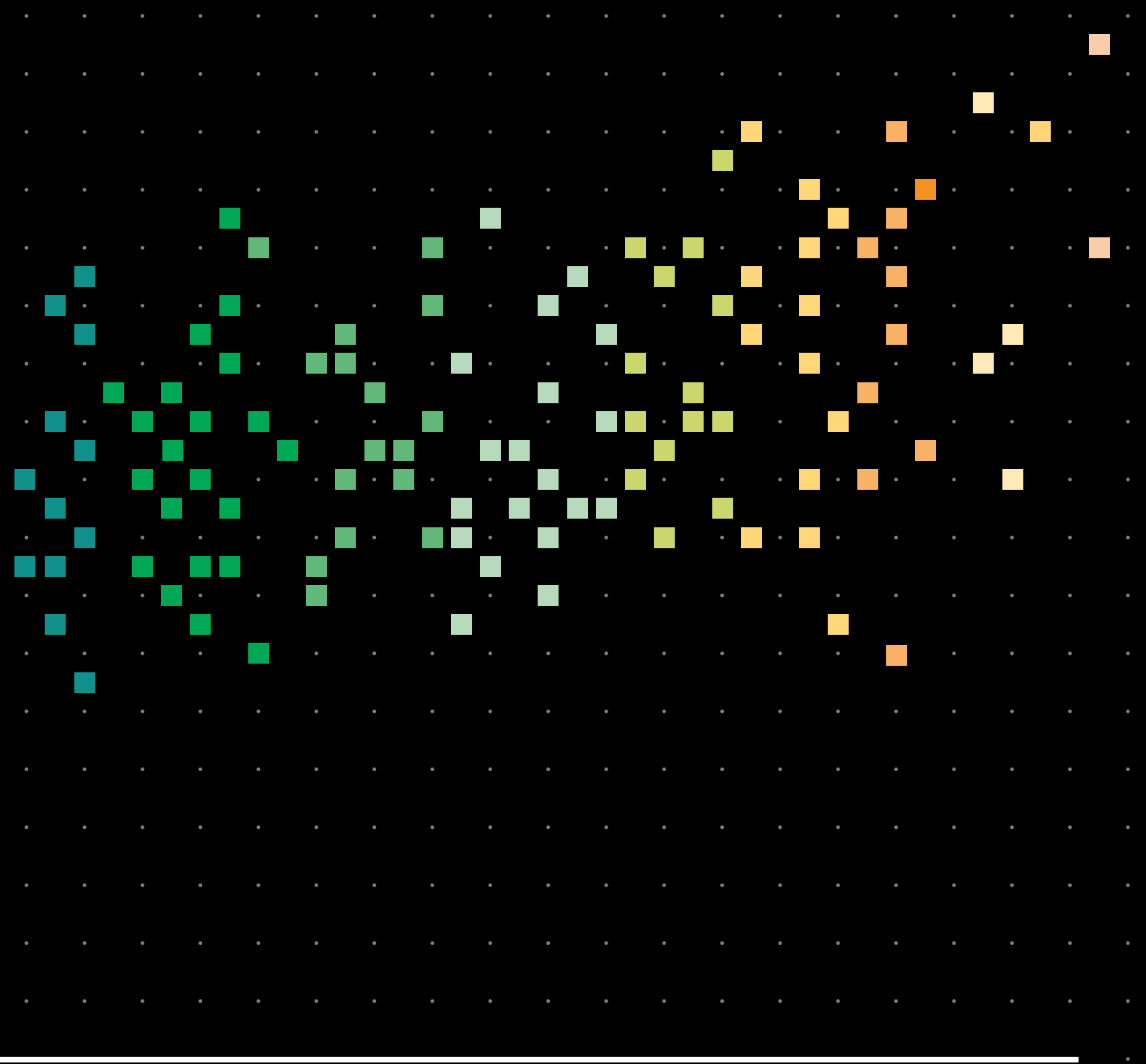
設備サービス会社のAllied Universal社は、Mazeランサムウェアに感染しました。犯人はビットコインで約200万米ドルを要求し、支払いがなければ盗難に遭った5GBの機密ファイルを公開すると脅迫しました。彼らは少なくとも700MBを公開しました。年末前には、少なくとも4つのランサムウェアファミリーの背後にいる犯罪者が、ファイルが暗号化される前に機密ファイルの漏洩を開始していました。彼らは、被害者に支払いをさせるためにデータを公開すると脅していました。イランのAPT33は、石油精製所、電力会社、製造業で使用される産業用制御システム（ICS）機器を標的にしていました。

12月

米国政府は、悪質なスパムを拡散するDridex銀行のトロイの木馬が、BitPaymerランサムウェアでネットワークを感染させるための足がかりを得るために使用されたことについて警告しました。Petróleos Mexicanos (Pemex)は、DridexとBitPaymerの亜種であるDoppelPaymerの被害に遭いました。マイクロソフトがパッチを適用した36の脆弱性のうちの1つが、12月の「Patch Tuesday」の前に「Watering Hole（たまり場）」攻撃に悪用されていました。マイクロソフトは、SharePointの脆弱性が悪用されていたという別の定例外のセキュリティ速報とパッチを公開しました。Gallium攻撃者は、Operation Soft Cellやチベット人やウイグル人へのたまり場攻撃に関与していました。



07



付録

付録A：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1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密性と完全性のレベルです。

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。我々の作業の透明性を高め続けるために、今回のレポートにはいくつかの新機能を導入しています。

まず前提として、我々は間違いを犯します。コラムが入れ替わっていたり、数字が更新されていなかったりなど、修正すべき点がいくつか見つかるかもしれません。その際にはその都度、以下の修正ページにリストアップします。
https://enterprise.verizon.com/resources/reports/dbir/2020/report-corrections/

次に、自分たちの作業をチェックします。DBIRで挙げた数値の根拠となるデータはGitHubリポジトリ[55]で見ることができますが、今回初めてファクトチェックレポートもそこで公開します。これは非常に技術的な内容ですが、ご興味のある方のために、本報告書に含まれる全ての事実をテストしてみました[56]。

免責事項

繰り返しますが、本報告書の調査結果は、全ての組織における全てのデータ漏洩/侵害を表すものではありません。全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。

我々自身は完全ではないかもしれませんが、可能な限り真実に近い最良の情報を入手し、そのうえで有用なものを皆さまにお届けしているものと自負しております。その方法の詳細については、後述の「バイアスの認識と分析」のセクションをご覧ください。

DBIRの作業プロセス

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全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 EventRecording 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。本報告書冒頭にVERISリソースへのリンクが含まれています。

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

全ての協力機関には、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 ObjectNotation（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。

55 https://github.com/vz-risk/dbir/tree/gh-pages/2020
56 テスト方法に興味がありましたら、ModernDiveの第9章「仮説のテスト」を参照してください（https://moderndive.com/9-hypothesis-testing.html）。

インシデントデータ

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。ただし「その他」の場合はサンプルサイズに含まれます。数値は分かっているがVERISの一部ではない、または「上位」の数値ではないという意味です。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。

今年は、信頼区間を自由に使用したことで、小さなサンプルサイズが分析できるようになりました。我々は、そのようなデータを読む際のバイアスをできるだけ小さくできるルールをいくつか採用しました。ここでは、「小さなサンプル」を30件以下のサンプルと定義します。

1. 5件より小さいサンプルは、分析するには小さすぎます。

2. 小さなサンプルの場合は、カウントやパーセンテージの話はしません。これは数値についても同様で、中央値の頻度のドットがない数値があるのはそのためです。

3. 小さなサンプルの場合、値がある範囲内にあることや、値が相対的に大きい/小さいことについて話すことがあります。これらは全て上述の仮説のテストと信頼区間のアプローチに従っています。

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。

1. 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。

2. インシデントには既知のVERISの攻撃カテゴリー（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2019年10月31日まで）である必要があります。本報告書では2019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[57]。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Trickbot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。それが、後述のサンプリングバイアスに関わってくるためです。

57 弊社の折れ線グラフは、インシデントが発生した暦年を連続的に使用していますが、ダンベルチャートは順番通りにDBIR報告書の年を使用しています。

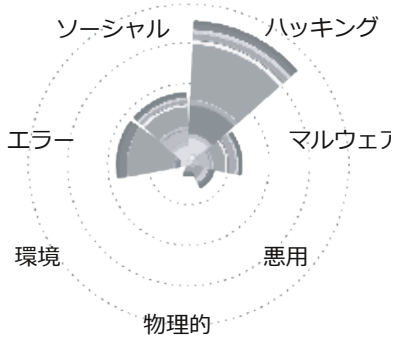


図135. 攻撃別の各貢献度

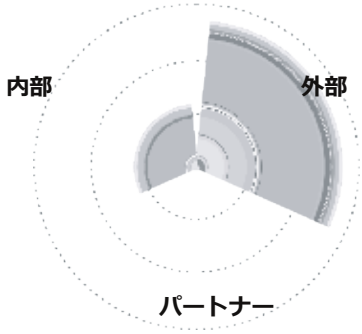


図136. 攻撃者別の各貢献度

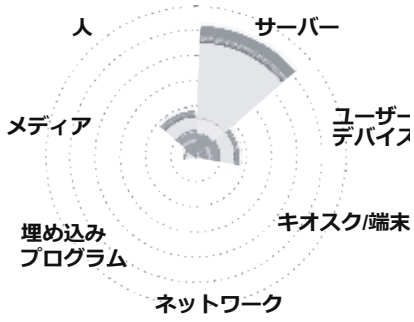


図137. 資産別の各貢献度

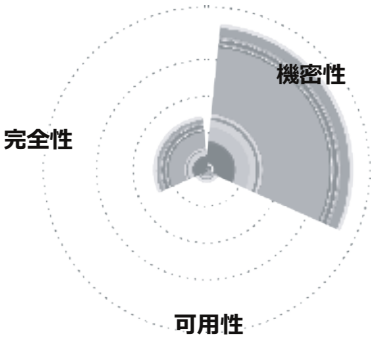


図138. 属性別の各貢献度

バイアスの認識と分析

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。したがって、我々（あるいは誰か）が毎年全世界で発生しているデータ漏洩/侵害（私たちの調査対象人口）を全て網羅した国勢調査を実施できるようになるまでは、サンプリングを利用しなければなりません[58]。ただし、このサンプリングプロセスではいくつかのバイアスが発生します。

1つ目のバイアスは、サンプリングによってもたらされるランダムバイアスです。今年のデータサンプルでは、信頼区間は、インシデントでは±1.5%[59]、データ漏洩/侵害では±0.5%でした。これはサンプルサイズに関係しています。サンプルサイズが小さいサブセットでは、この範囲が広くなります。弊社では、2019年の報告書から使用している条件付き確率の棒グラフ（「斜め」の棒グラフ）でこの信頼度を示しています。

2つ目のバイアスは、サンプリングバイアスです。弊社では、さまざまなデータ提供者からデータ漏洩/侵害を収集することで、可能な限り真実に近い最良の情報[60]を皆様にお届けできるように努めています。それでも、サンプリングが偏っていることは明らかです。例えば、公に開示されているデータ漏洩/侵害のようなものは、弊社のデータベースに登録される可能性が高いですが、機密情報の侵害のようなものは登録される可能性が低くなります。

58 サンプリングに興味がありましたら、ModernDiveの第7章「サンプリング」を参照してください（https://moderndive.com/7-sampling.html）。

59 これと全ての信頼区間は、ブートストラップシミュレーションによって決定された95%の信頼区間です。詳細は、ModernDive第8章「ブートストラップと信頼区間」を参照してください（https://moderndive.com/8-confidence-intervals.html）。

60 エリック・ブラック氏の『Carl Bernstein Makes the Case for 'the Best Obtainable Version of the Truth'』の下地になっているのは、アルベルト・カイロ氏による『How Charts Lie』（それでも、おそらく読むべき良書）。

図135～138は、潜在的なサンプリングバイアスを可視化する試みです。各半径方向の軸はVERISの列挙で、データ提供者を表す棒グラフを積み重ねています。全ての軸に沿って積み重ねられた棒グラフのデータ提供者間で、データ漏洩/侵害の分布がほぼ等しくなるのが理想的です。単一のソースのみで表された軸は、バイアスが偏る可能性が高くなります。しかし、貢献度は本質的に太い尾を引いており、少数の協力者がデータを数多く提供し、多数の協力者が特定の領域内で少数のデータを提供しています。それでも、ほとんどの軸には大量のデータを提供する協力者が複数存在し、その軸に沿って大量のデータを提供する協力者がインシデントの合計にかなりの割合追加されていることが見て取れます。

多くの軸では、大量のデータ提供が1つ存在することに気づくでしょう。全体として気になるところですが、これは他のソースを複数集約したデータ提供を表しており、実際に提供されているのは1つのデータだけではありません。また、これはほとんどの軸に沿って発生しており、間接的なデータ提供者のグループ化によってもたらされるバイアスを制限します。

3つ目のバイアスは、確認バイアスです。弊社では、データセット全体を探索的分析と仮説検証の両方に使用しているので、本質的には仮説を立てるために使用したのと同じデータで仮説を検証しています。宇宙中のデータ漏洩/侵害やインシデントデータを収集できる方法が開発されるまでは[61]これが最善の方法であると考えています。

上述のように、弊社では多様なデータ提供者からデータを収集することで、これらのバイアスの緩和に努めています。一貫した複数のレビュープロセスに従い、「蹄の音が聞こえたら、シマウマではなく馬だと思え」方式で考えます（一般的な要因から考える）[62]。また、調査報告の発表前に、特定の分野の専門家と一緒に調査結果をレビューするようにしています。

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、目立たないトレンドを隠してしまう可能性のある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つのサブセットは過去3年間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内の全ての分析に使用しました。これには前述したクオリティインシデントのみが含まれ、前述の2つのサブセットは含まれていません。

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ー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、DoS、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、企業が貢献したデータ数を加重することですべての企業が平等に扱われています）。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。

61 DBIRは「クライシス・オン・インフィニット・アース」以前の職場環境です。
62 ユニークな発見は、予想外の結果というよりも、データ収集の問題のような平凡なものである可能性は高そうです。

付録B：VERIS Common Attack Framework（VCAF）

インシデントとデータ漏洩/侵害データを分析するには、これらのデータについて一貫した定義が必要であり、VERISはそれを解決するために開発されました。

VERISは、DBIRやデータ分析と密接な関係があることから、データ漏洩/侵害関連の用語に内在する曖昧さを取り除き、主要なデータ漏洩/侵害を定量化できるデータ駆動型の構造を提供することを目的として開発されました。VERISは、被害者の人口統計やタイムラインなど、インシデントに関するさまざまな詳細情報を網羅していますが、VERISの中核をなすのは、インシデントのActor（攻撃者）、Action（攻撃）、Asset（資産）、Attribute（属性）の4つです。頭字をとって「4つのA」と呼ばれます。

しかし、VERISは、攻撃者の手口、選択された持続性の方法、攻撃対象の資産で悪意のあるコードを実行するための方法論など、戦術的・技術的な細かい部分を正確かつ詳細に表現するように設計されているわけではありません。ありがたいことに、そこまでする必要はありません。なぜなら、その必要性を満たすために、他のもので補えるからです。

大規模なATT&CK（の採用）

MITRE社は、攻撃行為を体系化する手段として2013年から独自の「Adversarial Tactics, Techniques and Common Knowledge (ATT&CK)」フレームワークの開発を秘かに進め、2015年に公開しました[63]。ATT&CKは、攻撃者が使用する戦術的攻撃を記述するための方法として定着しています（高度な脅威に重点を置いたものを含む）。VERISと同様、ATT&CKはいくつかの重要な要素に細分化されていますが、フレームワークの核となるのは、攻撃者がどのようにして「戦術」と呼ばれる目的を達成するかという不可分な手段を記述した「テクニック」です。「ATT&CK for Enterprise」に含まれる260以上のテクニックは、それに対応する11の戦術とともに論理的にグループ化されており、侵入の一部として攻撃者が狙う可能性のある様々な攻撃対象が説明されています。

互いに補えば心強い

VERISとATT&CKは、インシデントの体系化を目的としたVERISと攻撃技術の体系化を目的としたATT&CKという、それぞれ異なるニーズと目的から生まれたものですが、両者の間には間違いなく重複する部分があり、それを活用することで両規格の価値を向上させることができます。この2つのフレームワークの関係をより深く理解するためにチームは、VERISのフレームワークをATT&CKの技術に対応させることができないかどうかを調査しました。その結果を示したものが図139です。

これはクロスオーバーの話?

このギャップを埋め、ATT&CKとVERISの関係を運用面で結びつけるための解決策として、「VERIS Common Attack Framework (VCAF)」と呼ばれる拡張機能の開発を行ないました。

VCAFはATT&CKとの橋渡し役となり、全体的なフレームワークの構築を目的として、ATT&CKにはないVERISの部分をカバーしています。VCAFの中核となる部分は、2つのコンポーネントで構成されています。1つはVERISとATT&CKの間の概念的なマッピングであり、もう1つはATT&CKを拡張したもので、VERISに存在する可能性のある攻撃を全てカバーする技術が含まれています。ATT&CKのデフォルトのテクニック「空から降ってくる流星」を活用したいところですが、このような事が起きるのは非常に稀です[64]。

このアプローチは、ランサムウェアのようなVERISに見られる一般的なカテゴリーと、VERISかATT&CKに見られるより特殊な攻撃タイプの両方に対応できる柔軟性を持っています。VCAFを使用することで、対象となる範囲や追跡可能な範囲が広がるだけでなく、これらのインシデントの本質的なコンテキストを理解することができます。以下に、この強力な組み合わせを活用することで得られるさまざまなメリットを列挙します。

- インシデントに関連する技術情報を理解する
- 過去に発生した全てのインシデントの種類（マルウェアやハッキングの種類だけでなく）に基づいて、緩和策に優先順位をつける
- 標的化と能力の接点をよりよく理解する
- 技術的な成果物を超えたインシデントの状況を把握する
- サイバーセキュリティの概念についてサイバーセキュリティの専門家ではない方とのコミュニケーションが容易になる

63 https://www.mitre.org/sites/default/files/publications/pr-18-0944-11-mitre-attack-design-and-philosophy.pdf
64 しかし、確かにインパクトは大きいです。

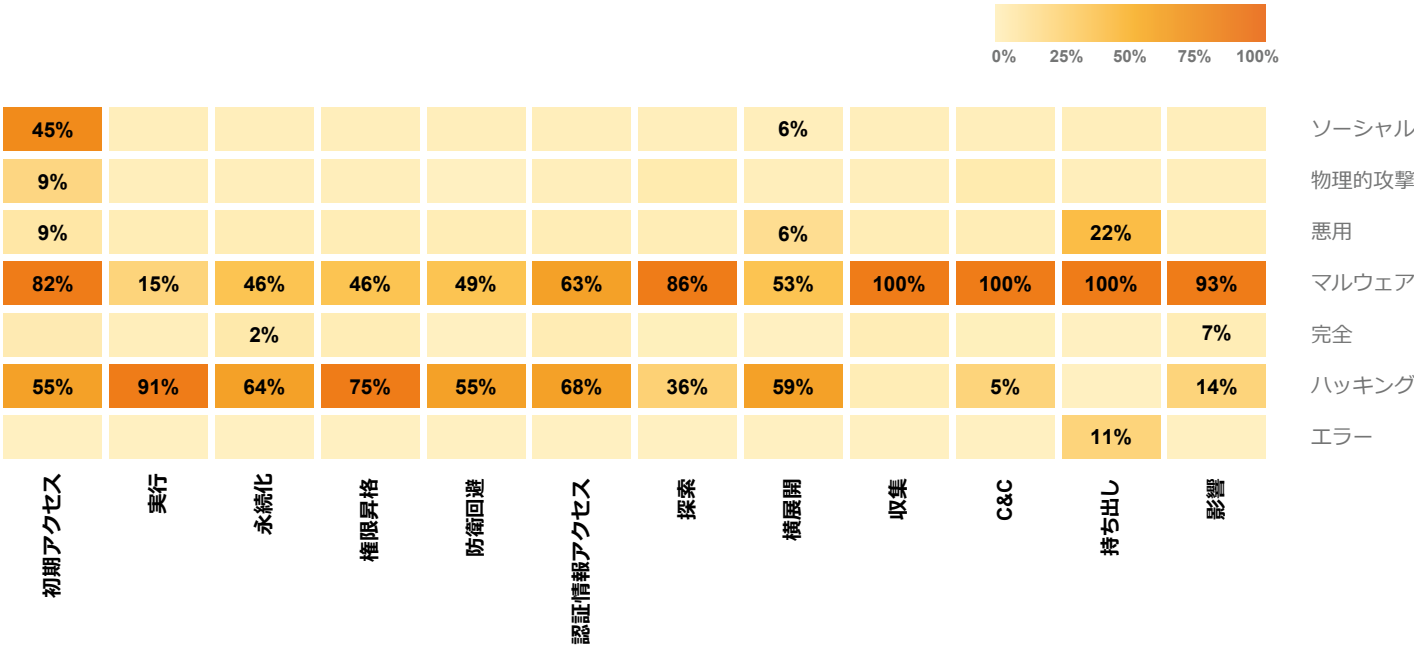


図139. MITRE社規定のテクニックに対するVERISのカバー率

今回のDBIRでは、VCAFを使用して、模擬侵害データ、SIEMデータ、マルウェアの特徴をVERISのアクションカテゴリーにマッピングし、弊社のインシデントデータベースと比較して結論を導き出しました。

偉大なものの始まり

明らかに、VCAFはサイバーセキュリティフレームワークの全てを網羅するものではありません。コミュニティがセキュリティインシデントや攻撃者について議論できるよう、1つに統合された方法を持つことへのささやかな一歩です。サイバーセキュリティフレームワークの数が増え、サイバーセキュリティの各トピックを取り巻く知識の分野が深まるにつれ、私たちコミュニティとして、サイバーセキュリティの専門家ではないより大きなコミュニティとコミュニケーションできるように、私たち自身の言語と理解を統合していく必要があります。VCAFの今後の開発や詳しい情報については、VERISのGitHubページ（https://github.com/vz-risk/veris）をご覧ください[65]。

65 そして、「いいね！」と「購読」ボタンを押すのを忘れずに!

付録C

マイケル・ダンブロージオ氏
アシスタントディレクター
米国シークレットサービス

ジョナ・フォース・ヒル氏
サイバー政策アドバイザー
米国シークレットサービス

金の流れを追うことが、サイバー犯罪者を捕まえるための鍵となる

今年のDBIRでは、悪質なデータ侵害の大半における主な動機として利益の追求が再び浮き彫りになりました。これは、全国的な規模で発生しているセキュリティ関連の侵害がメディアで大々的に報道されているので驚いている方もいると思いますが、実際はそれほど驚くべきことでありません。悪質なサイバー攻撃者の多くは、国家安全保障や地政学的な目的ではなく、むしろ単純な貪欲さが動機となっています。彼らは主に詐欺や恐喝によって利益を得ています。金融システムや決済システムを標的とし、様々な詐欺の計画に使用する情報を盗み出し、ランサムウェアやその他の手段を使ってITシステムを人質にします。その犯罪計画がどのようなものであれ、最終的には、資金移動やロンダリングの機関に頼り、その収益を送金したり、清算したりします。

そのため、米国シークレットサービスは、サイバー犯罪が「サイバー」と呼ばれる前の1980年代初頭に初めてサイバー犯罪の捜査を担当することになり、引き続き現在も捜査を担当しています。シークレットサービスの捜査官は、金融犯罪の捜査官であり、「金の流を追う」だけでなく、犯罪者がその活動から利益を得るのを妨げ、被害者の盗まれた資産を回収することに長けています。サイバーインシデント、データ漏洩、「無制限のATM現金引き出し」の陰謀、ランサムウェア攻撃、その他インターネットを介して行われた様々な金銭的動機による犯罪を捜査するにあたり、シークレットサービスのアプローチの中心は「金の流れを追う」ことです。

被害者から犯罪者へ、犯罪者間で、そしてマネーロンダリングの処理へといった一連の資金の動き追うことで、捜査官が最大の洞察力と犯罪の手がかりを引き出せるということが、何十年にもわたって分かってきました。マルウェアのサンプルや指標の共有は有用であることは間違いありませんが、逮捕、資産の押収、詐欺被害者から盗まれた資産の回収につながるのは、資金とその移動先です。

例えば、典型的なビジネスメール詐欺（BEC）の手口では、被害者は、通常は電信送金で、犯罪者が指定する銀行口座に支払いするように指示されます。この犯罪の詐欺の部分で使用される手法は、高度に洗練されたもの（オーダーメイドのマルウェアを配備するなど）から、驚くほど単純なもの（電話で業者になりすますなど）まで多岐にわたります。重要なのは、詐欺師がどのようにして被害者を騙すかということではなく、その収益をどのように動かし、清算するかということです。

賢い犯罪者は盗んだ資金の移動に使用する口座やペーパーカンパニー、資金移動プロセスには、位置情報やその他の情報が豊富に含まれており、逮捕につながることを知っています。その結果、犯罪者は、自分たちの犯罪に関連する可能性のある全ての口座や機関から自分たちの身元や身分を隠そうとします。

犯罪者がこれを行う方法はいくつかありますが、主要なメカニズムの1つは、外部の個人（「ミュール」(運び屋)と呼ばれる）を雇い、犯罪の手口に招き入れることです。ラバは、犯罪の片棒を担ぐことを承知している場合もあれば、まったく知らない場合もあります。一部のミュールは、自分が関与する犯罪について完全な知識を持って参加しており、そうでないも者は、合法的な求人情報のように見えるものを介して募集されています。また中には、恋愛詐欺などの付随的な詐欺被害者であることも多く、実際には詐欺師のためにお金を動かしているだけなのに、恋人に送金していると信じ込まされています。

ランサムウェアやその他の犯罪でも、暗号通貨が資金に使われるケースでは、同様の動きが見られます。例えば、組織がITシステムのロックを解除するために身代金を要求される場合、犯罪者は一般的に被害者にビットコインの支払いを暗号通貨のウォレットに送るように指示します。これらのウォレットは、合法または違法のいずれかの暗号通貨取引所か、または犯罪者や仲間が操作するデバイス上のいずれかでホストされています。ここでも犯罪者は、ウォレットの場所を不明瞭にし、特定のウォレットやアカウントに自分たちの活動を結びつける可能性のある他の情報へのアクセスを制限しようとします。

ランサムウェア攻撃に従事する犯罪者は、BEC詐欺師と同じ手法の多くを採用して痕跡を隠蔽しています。彼らは、ミュールにお金を払って暗号通貨ウォレットをセットアップさせるかもしれませんし、ミュールを騙して暗号通貨業界で合法的な仕事に就いたと思わせるかもしれません。ブロックチェーン上での動きを法執行機関に追跡させないようにするために、1つの暗号通貨フォームから別の暗号通貨（例えば、ビットコインからビットコイン）に資金を交換するために、暗号通貨タンブラーとミキサーを使用することがあります。またペーパーカンパニーを設立したり、海外に銀行口座を開設したり、国から国へ頻繁にお金を移動させたりしますが、これらは全て、金の動きの追跡を可能な限り困難にさせることを目的としています。

しかし、そこには常に難点があります。サイバー犯罪者が犯罪の成果を味わいたいのであれば、法執行機関に追跡されることなく、その利益を実際に使える金銭の形に変えなければなりません。この難点が、サイバー犯罪者の活動に対抗する最大の機会を生み出すのです。

シークレットサービスはこれらの難点に焦点を絞り、明らかに違法なサービスであっても、犯罪者が悪用する合法的なビジネスであっても、これらの資金の流れを遮断させるために活動しています。潜入捜査、機密情報提供者、業界やより広範な法の執行当局とのパートナーシップを通じて、シークレットサービスはこれらの不正な金融フローを特定し、妨害することに秀でています。2019年、シークレットサービスは71億ドルのサイバー犯罪の損失を防ぎ、盗まれた資産を3,100万ドル以上回収し、詐欺被害者に返還しました。

産業界への教訓は簡単なものです。ネットワークの防衛に投資すること、そして侵害が発生した場合には、できるだけ多くの証拠を収集することです。その証拠を法執行機関のパートナーと共有すれば、犯罪者の逮捕だけでなく、その資産を差し押さえることにもつながります。多くの場合、回収したお金は被害者に返還されます。このようにして、サイバー犯罪者が罪に問われず活動するのを防ぐことができるのです。これは集団的な闘いです。みんなで協力しましょう。

付録D

ディエゴ・カート氏
最高法令遵守責任者（CCO）
アイダホ州知事室、情報技術サービス担当

アイダホ州、VERISを利用してインシデント対応プログラムを強化

私たちは常に「意思決定を改善するためには、インシデント情報やデータ漏洩/侵害情報の共有が必要」であると聞かされています。アイダホ州も同じ問題に直面しており、意思決定の改善と効果のあるサイバー防衛投資のために、さまざまな機関にインシデント情報やデータ漏洩/侵害情報を共有させようとしていました。この問題に対処するために、アイダホ州はプログラムを企画し、法務部を含むさまざまな利害関係者の承認を得ました。このプログラムは、2つの基本的な構成要素と3つの中核的な構成要素から構成されています。

2つの基本的な構成要素は以下の通りです。

1 **Cyber Kill Chain®[66] ロッキード・マーチン社による開発。**実行可能なインテリジェンスプロセス思考を促進するために使用され、効果的なサイバーセキュリティプログラムを構築するための設計図の役割を果たす。

2 **National Institute of Standards and Technology (NIST) Cybersecurity Framework[67]** – 企業全体のサイバーセキュリティ対策の準備態勢と成熟度を評価するために使用されるリスク報告フレームワーク。

3つの中核的な構成要素は以下の通りです。

1 **NIST SP 800-53[68] Incident Response Control Family**—全てのコントロールプロセスを管理し、継続的に対処・成熟させるために使用する。

2 **イベント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)** – インシデントやデータ漏洩/侵害から情報を収集し、より良い意思決定や情報共有を行うために使用される、使いやすく体系的に構成された言語/分類法。

3 初期対応者、緊急管理者、国家警備隊、サイバーインシデントレスポンスの担当者などを1つのプラットフォームに統合し、VERIS言語/分類法を実装した商用Webアプリケーション。

66 https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html
67 https://www.nist.gov/cyberframework
68 https://nvd.nist.gov/800-53

このプログラムの中心となるのは、VERIS分類法です。VERISは、多くの組織が懸念する「部外者との機密データの共有」という問題を乗り越えるための言語/分類法です。インシデント情報を共有するために設計された共通言語（VERIS）を実装できなければ、アイダホ州は、インシデントやデータ漏洩/侵害情報を省内（他の部署）と省外（DHS、FEMAなど）の両方で共有することについて、法務部を含む様々な利害関係者から承認を得ることはできませんでした。

VERISがアイダホ州の情報共有能力の向上に貢献した分野としては、以下のようなものがあります。

- 随時対応している有害事象からの情報収集と活用の方法を改善できるという意識と関心が生まれている。
- 他のインシデント対応フレームワークと連携するオープンソースのフレームワーク。
- 短期間で組み込みと実装ができるように設計された使いやすいフルスキーマの分類法/言語。
- 企業経営者が組織のサイバーセキュリティへの取り組みに関与するための方法を提供し、4つの基本的な質問を繰り返し行うことで情報収集を簡素化します。誰の攻撃が資産に影響を与えたのか? どのような攻撃が資産に影響を与えたのか?どの資産が影響を受けたか?資産はどのような影響を受けたのか?

VERISは、インテリジェンス主導のインシデント対応プログラムを構築するための強固な言語基盤を提供します。これに他のオープンソースフレームワークを組み合わせることで、優れたインシデントレスポンスプログラムを構築することができます。

付録E：協力機関

A

Akamai Technologies

Apura Cyber Intelligence

AttackIQ

B

BeyondTrust

Bit Discovery

Bit-x-bit

BitSight

C

CERT European Union

CERT Insider Threat Center

CERT Polska

Chubb

Cisco Talos Incident Response

Coalition（旧称：BinaryEdge）

Computer Incident Response Center Luxembourg (CIRCL)

CrowdStrike

Cybercrime Central Unit of the Guardia Civil（Spain）

D

Dell（旧称： EMC-CIRC）

DFDR Forensics

Digital Shadows

Dragos, Inc.

E

Edgescan

Elevate Security

Emergence Insurance

F

Financial Services Information Sharing and Analysis Center（FS-ISAC）

G

Government of Telangana, ITE&C Dept., Secretariat

Government of Victoria, Australia—Department of Premier and Cabinet（VIC）

GreyNoise

H

Hasso-Plattner Institut

Hyderabad Security Cluster

I

ICSA Labs

J

JPCERT/CC

K

KnowBe4

L

Lares Consulting

LMG Security

M

Malicious Streams

Micro Focus（旧称：Interset）

Mishcon de Reya

mnemonic

Moss Adams（以前のAsTech Consulting）

MWR InfoSecurity

N

National Cybersecurity and Communications Integration Center（NCCIC）

NetDiligence

NETSCOUT

P

Paladion Networks Pvt Ltd.

ParaFlare Pty Ltd

Proofpoint（旧称：Wombat Security）

Q

Qualys

R

Rapid7

Recorded Future

S

S21sec

SecurityTrails

Shadowserver Foundation

Shodan

SISAP—Sistemas Aplicativos

SwissCom

T

Tetra Defense（旧称：Gillware Digital Forensics）

Tripwire

V

VERIS Community Database

Verizon DDoS Shield

Verizon Digital Media Services

Verizon Managed Security Services—Analytics（MSS-A）

Verizon Network Operations and Engineering

Verizon Threat Intelligence Platform Service（VTIPS）

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

Vestige, Ltd.

VMRay

W

Wandera

WatchGuard Technologies

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）

アメリカ国防防諜保安部（DCSA）

インターネットセキュリティセンター

オーストラリア連邦警察

か

カスペルスキー

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）

た

チェック・ポイント・ソフトウェア・テクノロジーズ

は

パロアルトネットワークス

米国コンピュータ緊急事態対策チーム（US-CERT）

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）


MOSSADAMS

Akamai

CROWDSTRIKE

EMERGENCE

apura

MALICIOUS STREAMS


CERT-EU

Mishcon de Reya

VICTORIA


CyberSecurity
MALAYSIA
An agency under MOSTI

GREYNOISE

AFP
AUSTRALIAN FEDERAL POLICE

CHUBB

kaspersky

ICSAlabs

edgescan

bit-x-bit

IRISS

F-Secure

digital shadows_

KnowBe4

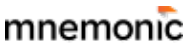
FS-ISAC

ATTACKIQ

DELL

NASK
CERT.PL

CIRCL
Computer Incident
Response Center
Luxembourg

HSC

mnemonic

BeyondTrust


MICRO
FOCUS

JPCERT CC®

Coalition

LMG
SECURITY

BIT
DISCOVERY

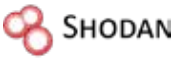
Check Point

HPI
Hasso
Plattner
Institut

DFDR
CONSULTING


LARES

WatchGuard

SecurityTrails

SHODAN

S21

BITSIGHT
The Standard in SECURITY RATINGS

paloalto
NETWORKS

RAPID7

CIS
Center for Internet Security

Qualys


zscaler

swisscom

VESTIGE
Digital Investigations

SHADOWSERVER

TALOS
INCIDENT
RESPONSE

proofpoint.
Security Awareness Training

Elevate Security

PALADION

VMRAY


TETRA
DEFENSE

NETSCOUT


SISAP
Sistemas Aplicativos

DRAGOS

NetDiligence

wandera

CISA
CYBER+INFRASTRUCTURE

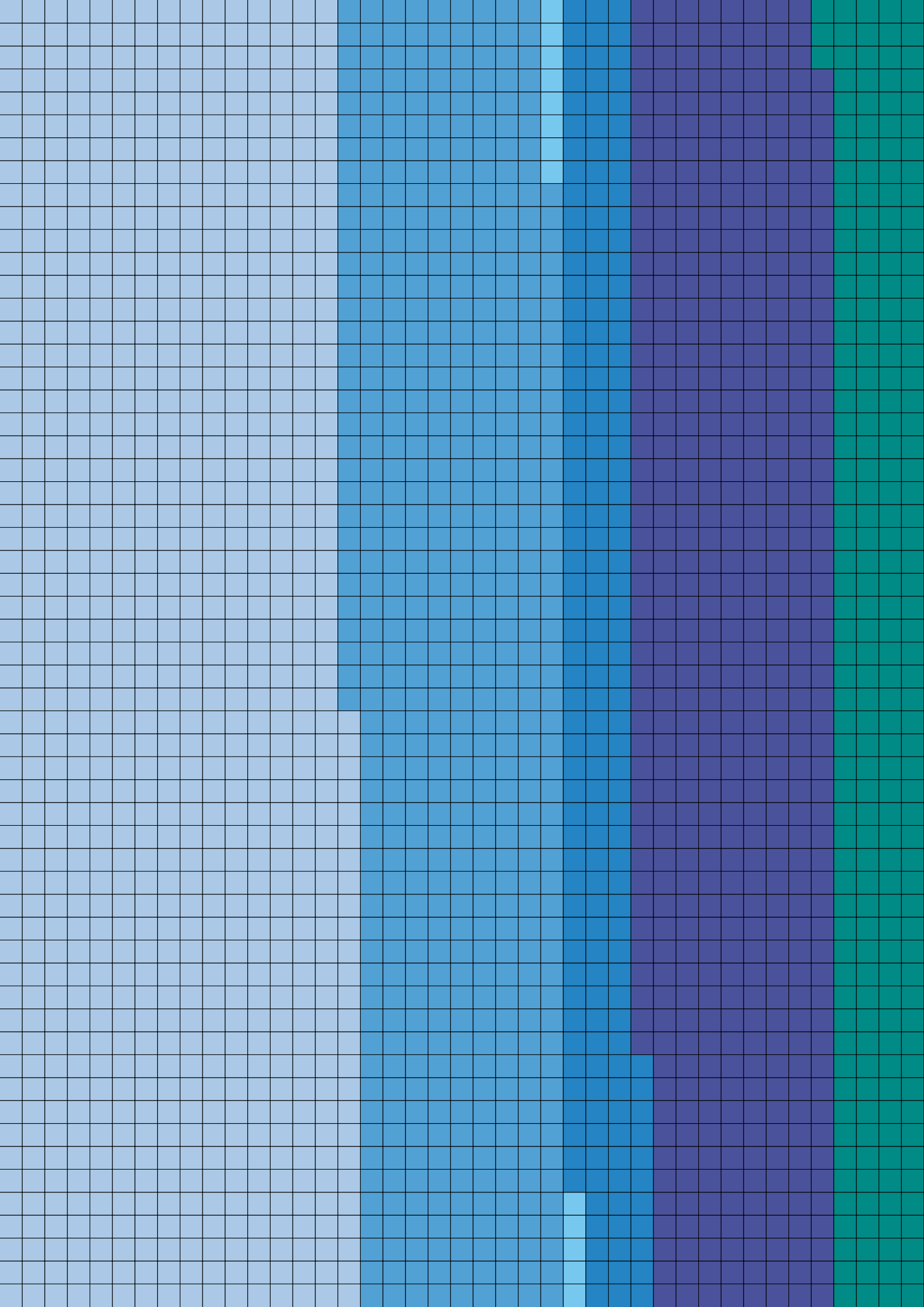
tripwire

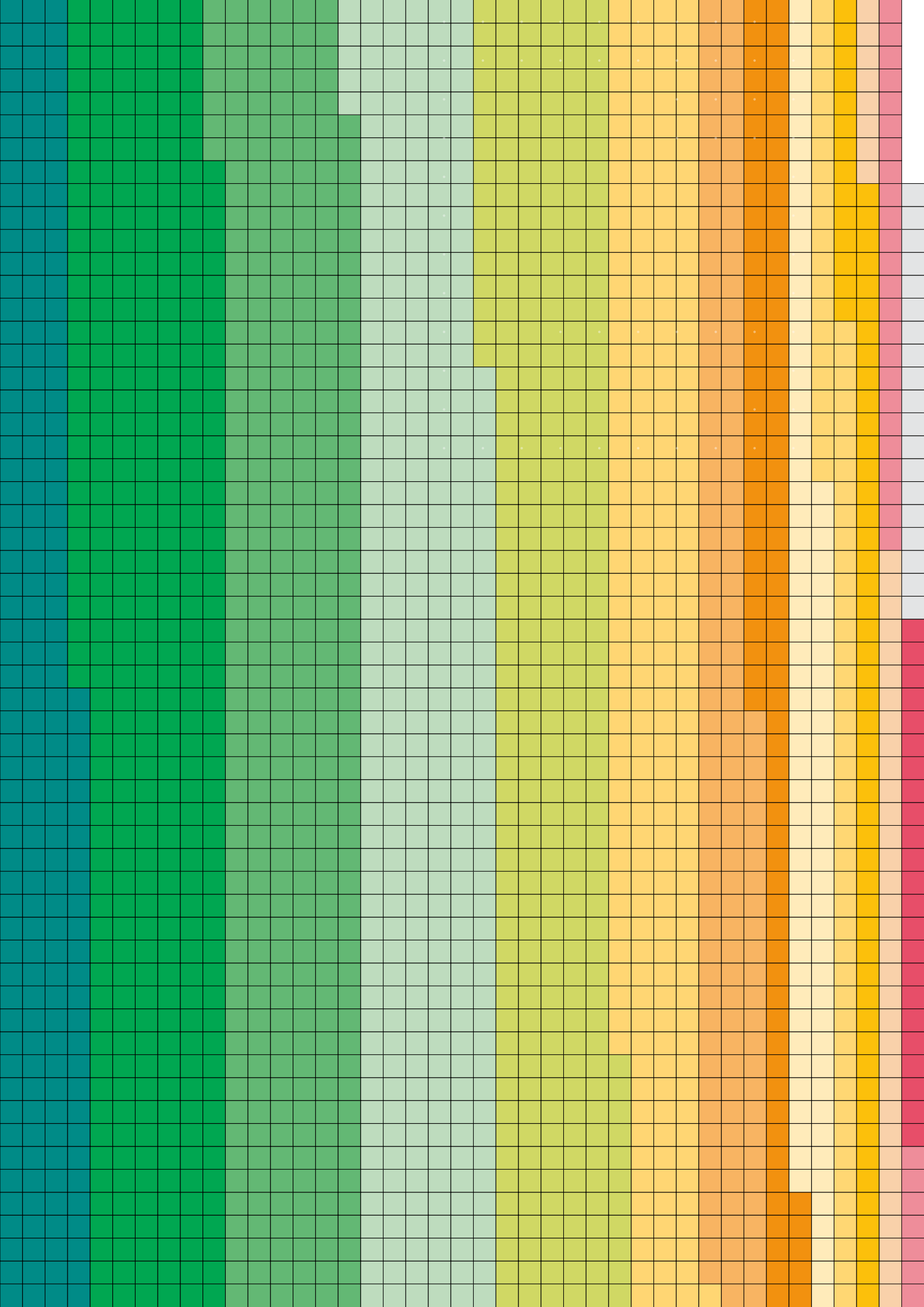
Carnegie
Mellon
University
Software
Engineering
Institute

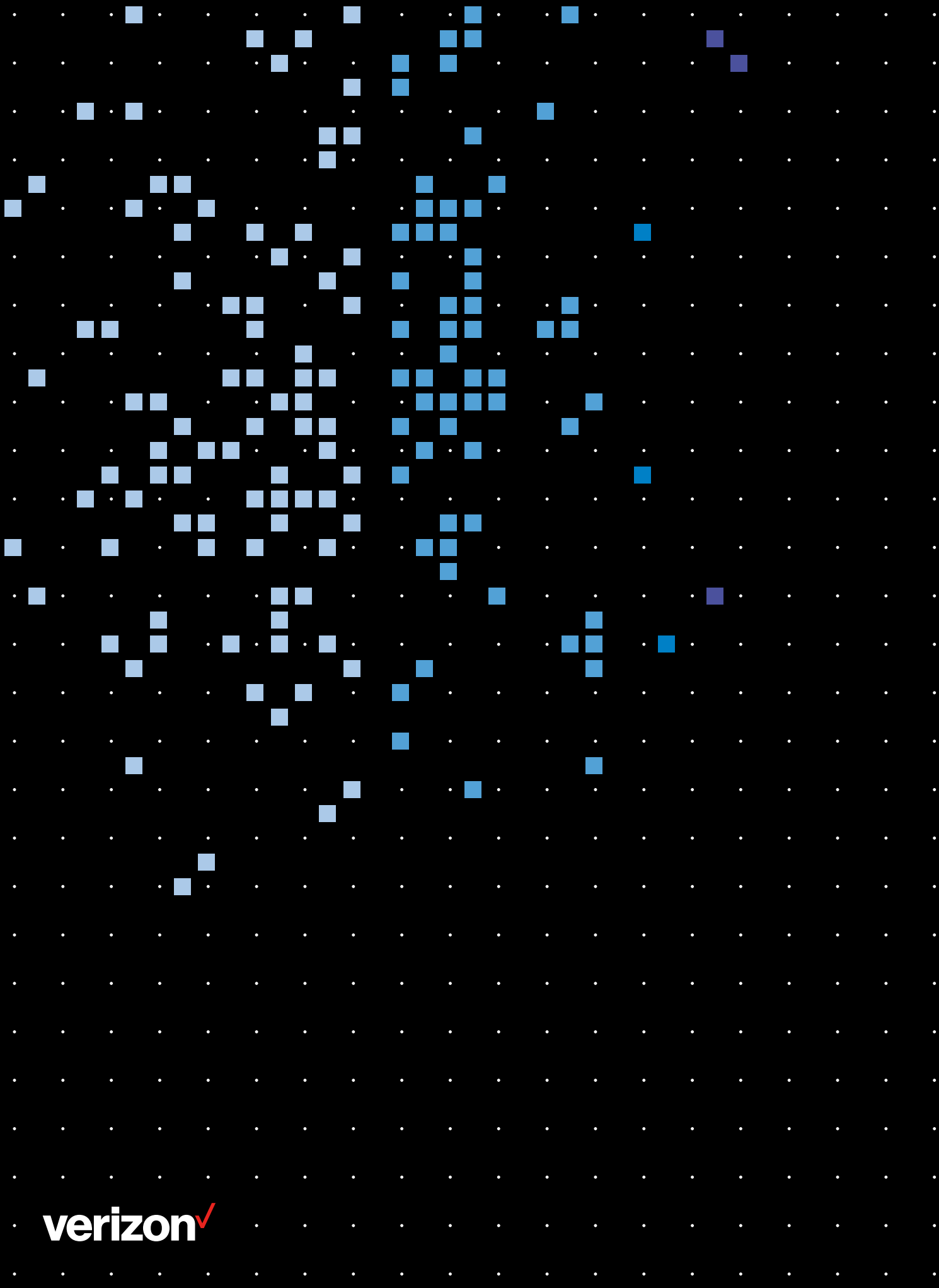
PARAFLARE

Recorded Future

NCCIC






verizon