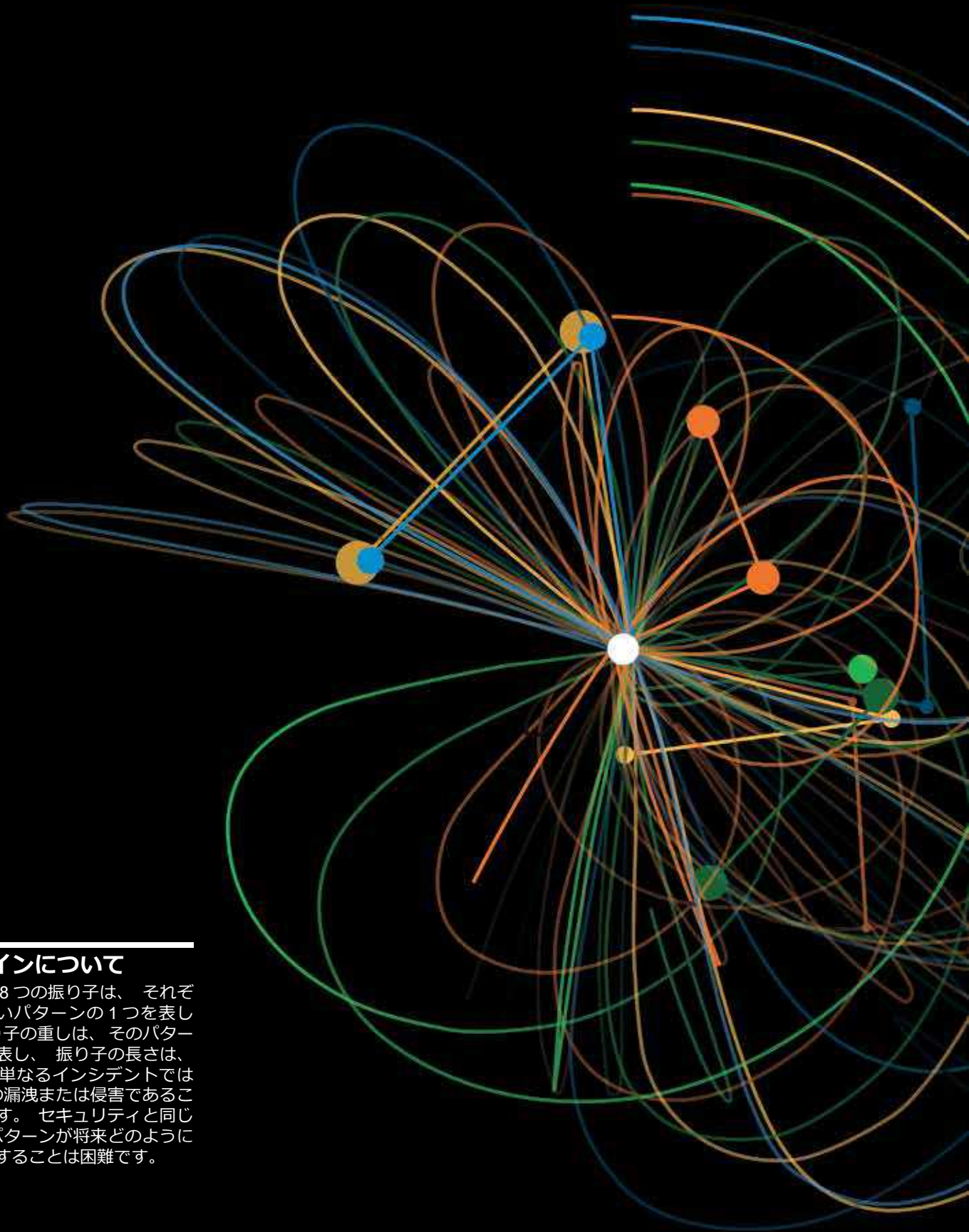
DBIR

2021年度 データ漏洩/侵害調査報告書

verizon



表紙のデザインについて

表紙に描かれた 8 つの振り子は、 それぞれ DBIR の新しいパターンの 1 つを表しています。 振り子の重しは、 そのパターンの発生頻度を表し、 振り子の長さは、 そのパターンが単なるインシデントではなく、 データの漏洩または侵害であることを表しています。 セキュリティと同じく、 これらのパターンが将来どのように現れるかを予測することは困難です。

目次

01

凡例と定義 4
イントロダクション 6
分析の要約 7
結果および分析 8

02

攻撃者 12
攻撃 15
資産 19
属性 22
タイムライン 24
影響 25

03

インシデントの分類パターン 29
サービス拒否（DoS） 35
資産の紛失・盗難 41
多種多様なエラー 43
特権の悪用 46
ソーシャル
エンジニアリング 49
システム侵入 54
基本Webアプリケーション攻撃 58
その他全て 62

04

業種別のハイライト 64
各業種の概要 65
宿泊および飲食サービス業 69
芸術、娯楽、レクリエーション業 71
教育サービス業 73
金融および保険業 75
医療および社会福祉業 76
情報産業 77
製造業 79
鉱業、採石業、石油・ガス採掘および
公益事業 81
専門的・科学的・技術的サービス業 82
公務 84
小売業 86

05

中小企業 88
中小企業のデータ漏洩/侵害が増加 89

06

地域別の分析 91
地域について 92
アジア太平洋地域（APAC） 93
欧州・中東・アフリカ地域（EMEA） 95
北アメリカ（NA) 97

07

まとめ 100
年間総括 102

08

付録 105
付録A：方法論 106
付録B：CISコントロール 110
付録C:米国シークレットサービス 113
付録D:協力企業 115

凡例と定義

2021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（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（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/2021** – 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/侵害に関するベライゾンのデータベース「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

ベライゾンのコーパス（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、私たちでは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/naics/?58967?yearbck=2012

自分たちのデータに自信を持つ

2019年に斜めの棒グラフをDBIRに導入して以来、情報セキュリティについて唯一確かなことは、確かなものは何もないということであると訴え続けてきました。すべてのデータが揃っていても、絶対に正しいと言えることはありません。しかし、データの少ない環境では何も測定ができないと諦めたり、最悪の場合、単に作り話をしたりするのではなく、私たちのチームは仕事に取り掛かります。今年度の本報告書でも、引き続きこの不確実性を数値で表現しています。

図1～図4はいずれも、真実となりうる現実の範囲を示しています。棒グラフの傾き、スパゲティチャートの糸、ドットプロットの点、バイオリンチャートの色など、いずれも独自の方法で業界の不確実性を表現しています。

棒グラフの傾きは、そのデータポイントの95%の信頼水準に対する不確実性を表しています（これは統計的検定のごく標準的なものです）。平たく言えば、2本（またはそれ以上）の棒グラフの傾きが重なっている場合、片方がもう片方より大きいとは言えないということです（そんなことをしたら、数学の神様たちに激怒されます）。

ドットプロットもよく使われますが、このグラフを理解するコツは、ドットが組織を表していることです。例えば、図3の200個のドットがある場合、各ドットは1ドットが組織の0.5%を表しています。これは、組織間の分布を理解するのに非常に適した方法であり、平均値や中央値よりも多くの情報を提供します。今年は、さらに情報量を増やすために、色や吹き出しを追加しました。

新しく登場したのは、スパゲティチャートとバイオリンチャートです。どちらも斜めの棒グラフと同じように不確実性を捉えようとするものですが、それぞれ、時間的に可視化されたデータや、特定の期間における変化の割合を示すのに適しています。これらのチャートでは、色の濃い部分が正しい値である可能性が高くなります。

ご覧になった感想をぜひお聞かせください[1]。この複雑なデータセットの分析が少しでも楽になることを願っています。

責任の明記

この報告書の内容を引用したいという方が多く、どのようにすればいいのかという質問をよく受けます。

本報告書に掲載された統計、数字、その他の情報を自由に引用いただいて構いません。ただし、(a) 出典元に「ベライゾン2021年度データ漏洩/侵害調査報告書」と明記すること、(b) 内容をいかなる形でも変更しないことを条件とします。正確な引用は認められますが、言い換えは審査が必要です。報告書のコピーを他の人に提供したい場合は、PDFではなくverizon.com/dbir/へのリンクを提供するようお願いします。

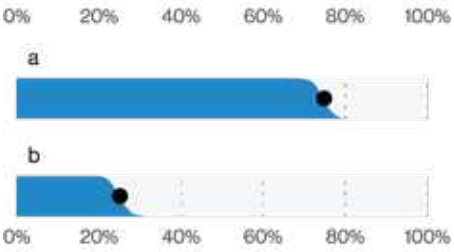


図 1. 棒グラフの傾きの例（n=402）

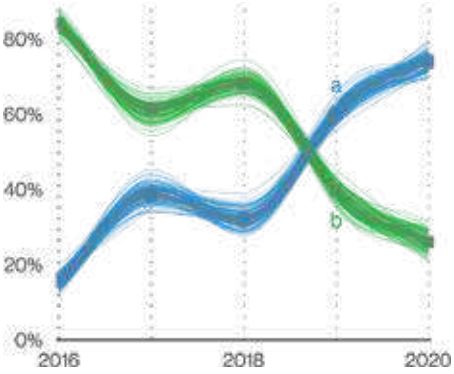


図2. スパゲティチャートの例

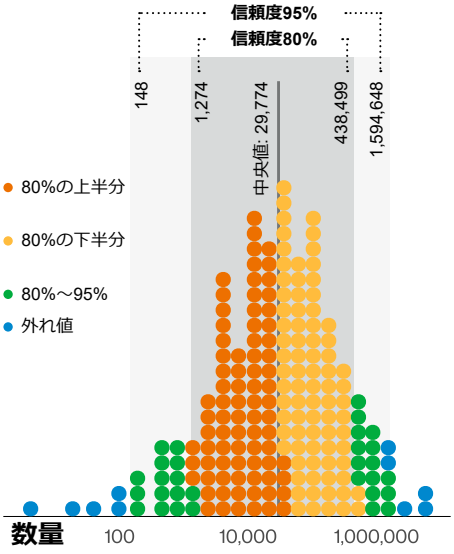


図3.ドットプロットの例（n=672）
1ドット=組織の0.5%

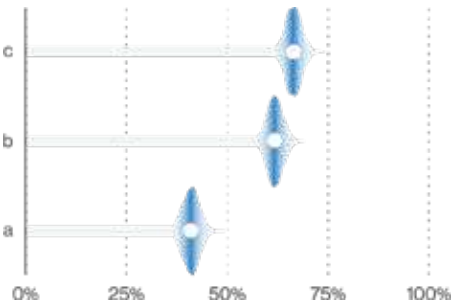


図4. バイオリンチャートの例（n=581）

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？AR/VR版のDBIRがないことにお困りですか？[2]

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のベライゾンのページまでご連絡いただくか、@VerizonBusinessに、ハッシュタグ「#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。

1 ただし、好きな人に限ります。DBIRの図担当者はとても気難しいのです。
2 本当にあればよいと我々も思っています。

イントロダクション

また今年も私たち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。読者の皆様にはいつも感謝しておりますが、とりわけ今年は「ただ読んでいただけるだけでも感謝です」と言いたいです。2020年はしばしば恐怖を感じる、常に予測不可能な悲惨な年でした。この2020年を乗り切り、さらに世界をより安全な場所にすることに関心とエネルギーを持ち続けてくれたことに感謝いたします。皆様がこの報告書を目にする頃には、世界が平穏さを取り戻していることを切に願っています。

世界中に広がっている最近の状況によって、多くの人がそれぞれの優先順位を見直すことになりました。同様に、私たちも一歩下がって、過去数年間に行ってきたことを見直すことにしました。その結果、これまでのパターンを刷新する中で、新しいパターンをいくつか追加し、一部のパターンを再調整しました。こうすることで、どこに危険が潜んでいるのか、どうすれば組織が起こり得るその危険を回避できるのか、という意識が高まることを期待しております。私たちは、想像以上のことが起こり得るということを2020年に学んだのですから、起こり得る危険というよりも「起こる可能性の高い危険」と言った方がよいかもしれません。不可能なのは、何が起こるのかを正確に予測することです。ですから、ここでは「起こり得る」とは言わずに、「起こる可能性の高い」という言葉で通します。

今年度は、世界88ヶ国から抽出した79,635件のインシデントを分析し、そのうち29,207件が適格性の基準を満たし、5,258件がデータ漏洩/侵害と確認されました。今回も、主要11業種と中小企業部門の詳しい分析結果を掲載しているほか、前回の報告書で調査したさまざまな地域についても、昨年の状況を再確認しています。また、Center for Internet Security（CIS）Controls®の推奨マッピングも掲載しています。予測不可能な不確実な世界だからといって、セキュリティ戦略もそうでなければならない言われはありません。

いつものように、データをご提供いただいた新旧83名の協力者の方々に感謝の意を表したいと思います。このレポートは皆様のおかげで完成したものであり、皆様の継続的なご支援に常に感謝しております。同様に、読者の皆様にも、この旅を共にしてくださることに改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

分析の要約

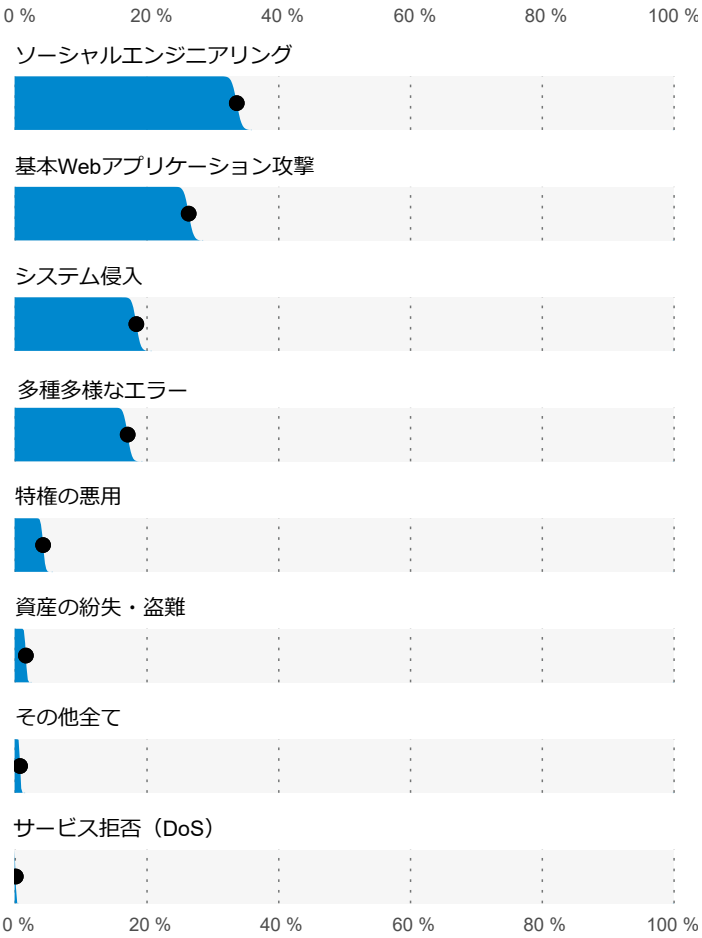


図5. データ漏洩/侵害のパターン（n=5,275）

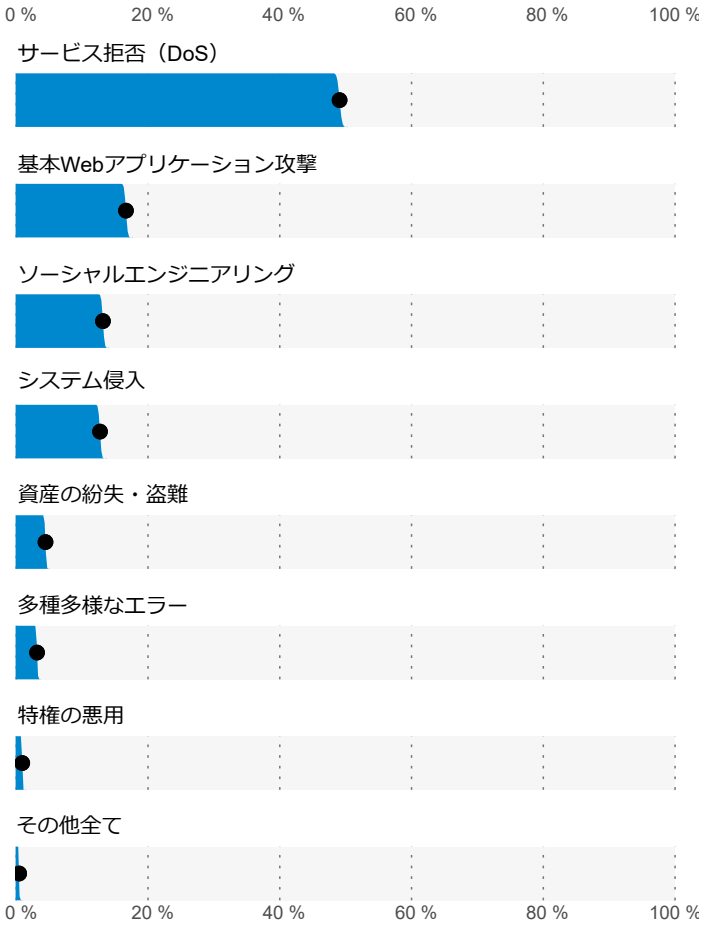


図6. インシデントのパターン（n=29,206）

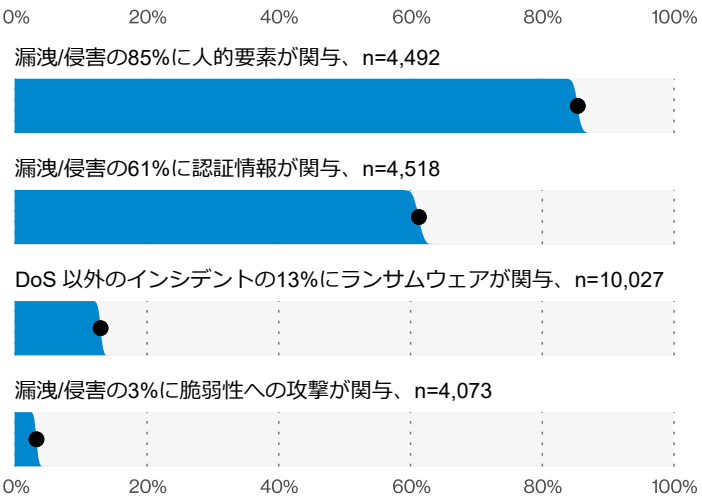


図7. データ漏洩/侵害及びインシデントにおける要因の種類（n=4,073）

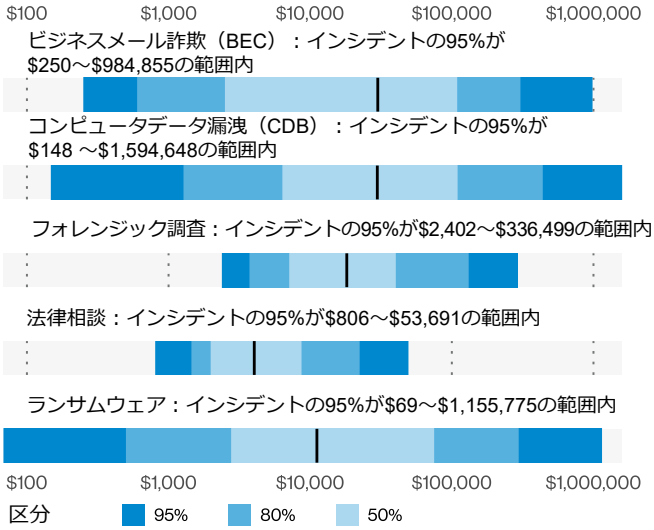


図8. インシデント別の金額的影響

02 結果および分析

結果および分析：イントロダクション

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）から提供されたケース、並びに外部協力者から提供されたレポートなど、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ています。これは私たちが、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[3]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。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。

DBIRは予測を目的としたものではありませんが[4]、不確実な未来に直面したときの対策を戦略として立てておくのに大いに役立ちます。

2020年に得た教訓は、「未来を予測しようとしても無駄なことが多い」というものでした。しかし、未来が予測できないとはいえ、組織の体制を最善にするためのシナリオの計画や準備を断念するわけにはいきません。DBIRは予測を目的としたものではありませんが[4]、不確実な未来に直面したときの対策を戦略として立てておくのに大いに役立ちます。

たとえば、図9の不正使用のグラフを見てみましょう。これは一般的なDBIRチャートですが、すべての棒グラフの先に傾斜を付けて見やすくしています[5]。いくつかの大きなものが上位にあり、下位にはさまざまなものがあります。

これを解釈する1つの有効な方法は、一番上や2番目のもの（この例では「特権の悪用」と「データの誤操作」）が起こりやすい基準と考えることです。これらは、最も一般的な「攻撃」の種類であり、もしこれらによってデータ漏洩/侵害が発生した場合、「あの組織はもっとよく知っているべきだった！」と（某SNSあたりで）つぶやく人が出てくるでしょう。

図9. データ漏洩/侵害における不正使用の種類（n=178）

3　非ランダムサンプリングの一種であるコンビニエンスサンプリングとは、母集団の中で身近にある、あるいは入手可能な部分からサンプルを抽出する方法です。詳細は「方法論」の項を参照してください。

4　3つ目の「先駆者」に賭けることをお勧めします。

5　内部の攻撃協力者はどこへ行った？おーい、おーい！

つまり、攻撃によって発生頻度にはかなりのばらつきがあるのです。短いほうの棒グラフ群は、起こる可能性はあっても、起こりそうにない例外的な滅多にない攻撃です。攻撃を受けた被害者は「高度な攻撃だった。誰にもできない攻撃だった」と主張するでしょう[6]。

ジニ係数とは、統計的分散の指標であり、国家やその他のグループ内の所得や富の格差を表すために最も一般的に使用されています[9]。

しかし、短い棒で表された攻撃の種類を１つにまとめて、その発生頻度を足すと、図10のようになります。こうなると、滅多にない攻撃とは言い難いのではないでしょうか？実際、この例では、2番目に可能性の高い攻撃のタイプが原因であるとして、多くの例外が原因でデータ漏洩/侵害が発生する可能性が高いようです。

しかし、データ漏洩/侵害は常にこのような傾向を示すのでしょうか？たくさんの棒グラフをお見せするのではなく[7]、この概念を1つの数値に凝縮してみましょう。図11と図12は、異なるレベルのばらつきのあるデータを示しています。ここで「ばらつき」という言葉を使ったのは、偶然ではなく、このロングテールのふるまいを表すジニ係数[8]を計算できるという事実を紹介するためです。

ジニ係数とは、統計的な分散を表す指標で、国家やその他の集団における所得や富の格差を表すのによく使われます[9]。難しい数学がたくさん使われていますが、最終的には、誰もが同じ所得を得られる完全に平等な結果（つまり、「一人当たりの所得」のグラフは水平線になります）を0とし、一人の個人がすべての所得を得られる世界（つまり、グラフ上ではどこかに巨大な垂直の突起があるだけです）を1とします。

これを援用して、セキュリティ関連のデータを見てみましょう。たとえば、SIEM（Security Information and Event Management）が直ちにレビューを必要とする重要なアラート群を生成する頻度などです。何となく、まさに「オンコールになるたび」に発生していることを証明できてしまうかもしれませんが、しばらくお付き合いください。図11では、シミュレートされたサンプルデータを生成しました。このデータは完全に滑らかで、チャート上では水平に見えます。このデータの均等性スコアは0（完全に等しい）です。図12は、重大なSIEMイベント間の時間間隔を表す実際のデータですが、極端にでこぼこしています[10]。ジニ均等性スコアは0.95で、イベント間の時間差が非常に大きいことを示しています。重大なSIEMイベントは、誰にでも無差別に発生する現象です。

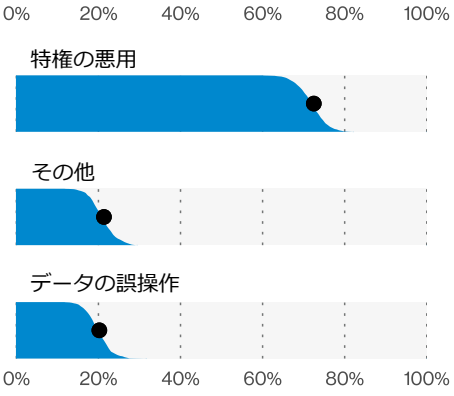


図10. データ漏洩/侵害における上位の不正使用の種類（n=178）

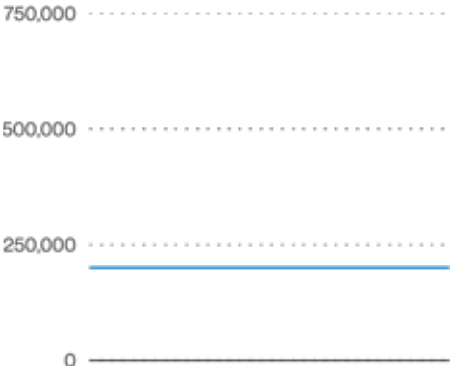


図11. シミュレーションによるSIEMイベント間の時間（n=1,335,343）

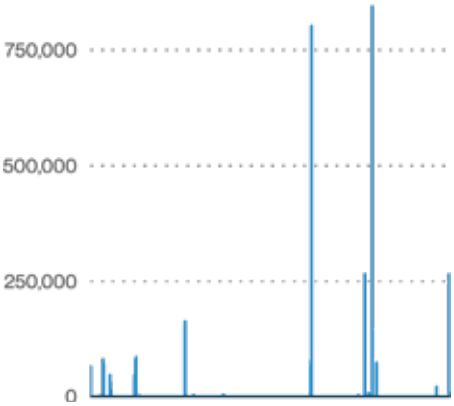


図12. SIEMイベント間の時間（n=1,335,343）

6 本報告書は、このような記述の有効性について主張するものではありません。ベライゾンの公式スポークスマンおよび法律顧問にご相談ください。当社は読者のデータプライバシーの保護を最重要としています。

7 そして、本報告書のページ数の予算を完全に消し去ります。

8 https://en.wikipedia.org/wiki/Gini_coefficient

9 あまり知られていないことですが、富の再分配を望む声から、「Gini in a bottle」（「魔法のランプの精」ジーニーのもじり）という言葉が生まれました。実際には富が再分配されることはありませんが、もしそうだったら素晴らしかったでしょうね。

10 データサイエンスの専門用語だと確信します。

この複雑な数学的設定は、DBIRデータ（インシデントと非インシデントを問わず）が非常に不均衡であるという現実を伝えるためのものですが[11]、少なくともそれを測定することはできます。図13は、過去7年間の攻撃、攻撃者、資産、および属性の種類と攻撃パスの均等性スコアを示しています。スコアの範囲は約0.73～0.94で、ここでは「高い」と言えます。データ漏洩/侵害は常に同じようなものになりそうな気がしますが、攻撃の種類によっては均等性が高いものもあります。

実際問題、基準[12]について水晶玉やニューラルネットワーク、次世代AIに教えを乞う必要はありません。自分で調べて、それに合わせて計画を立てることができます。一方、ロングテールから抜け出す方法はありません。ロングテールは、ごくまれにしか起こらない小さなことの塊で構成されており、それらは基準に対する例外です。ただし十分な資金があれば抜け出すことができます。また社会的に重要な立場にある組織では、資金を出してでもそうせざるを得ないこともあるでしょう。しかし、純粋に金銭的な価値から考えると（「影響」のセクションでデータ漏洩/侵害のコストを見てみると）、起こる可能性のある例外のすべてに対してリソースを使ってソリューションを設計することは賢明ではありません[13]。

何が基準で何が例外かという知識があれば、理想的に最適化されたソリューションは、基準に対応するソリューションを開発し、例外に対処できるようセキュリティ運用チームを訓練することになるでしょう。人間はかなり柔軟に問題を解決することができ、ときには適切な範囲でチャレンジをしたいと思うものです。

今後いつか、パラダイムシフトを起こすような、これまでの基準を覆すようなデータ漏洩/侵害に直面したとき、青い鳥のSNSユーザたちが「この脅威から逃れるためにパッチ管理やアクセス制御を行うことはできない」などと頻繁に騒々しくつぶやくのを聞かないようにしましょう。現実的に、「基本的なことを行う」ことが、組織に影響を及ぼす可能性の高い問題領域の大部分に対して有効なのです。

本報告書を読むことで、通常の攻撃者がこの1年間に何をしてきたかを知り、基準と例外の両方に対して改善できる箇所を選ぶことができます。なぜなら、未来を予測する唯一の方法は、自分自身で未来を変えることだからです。

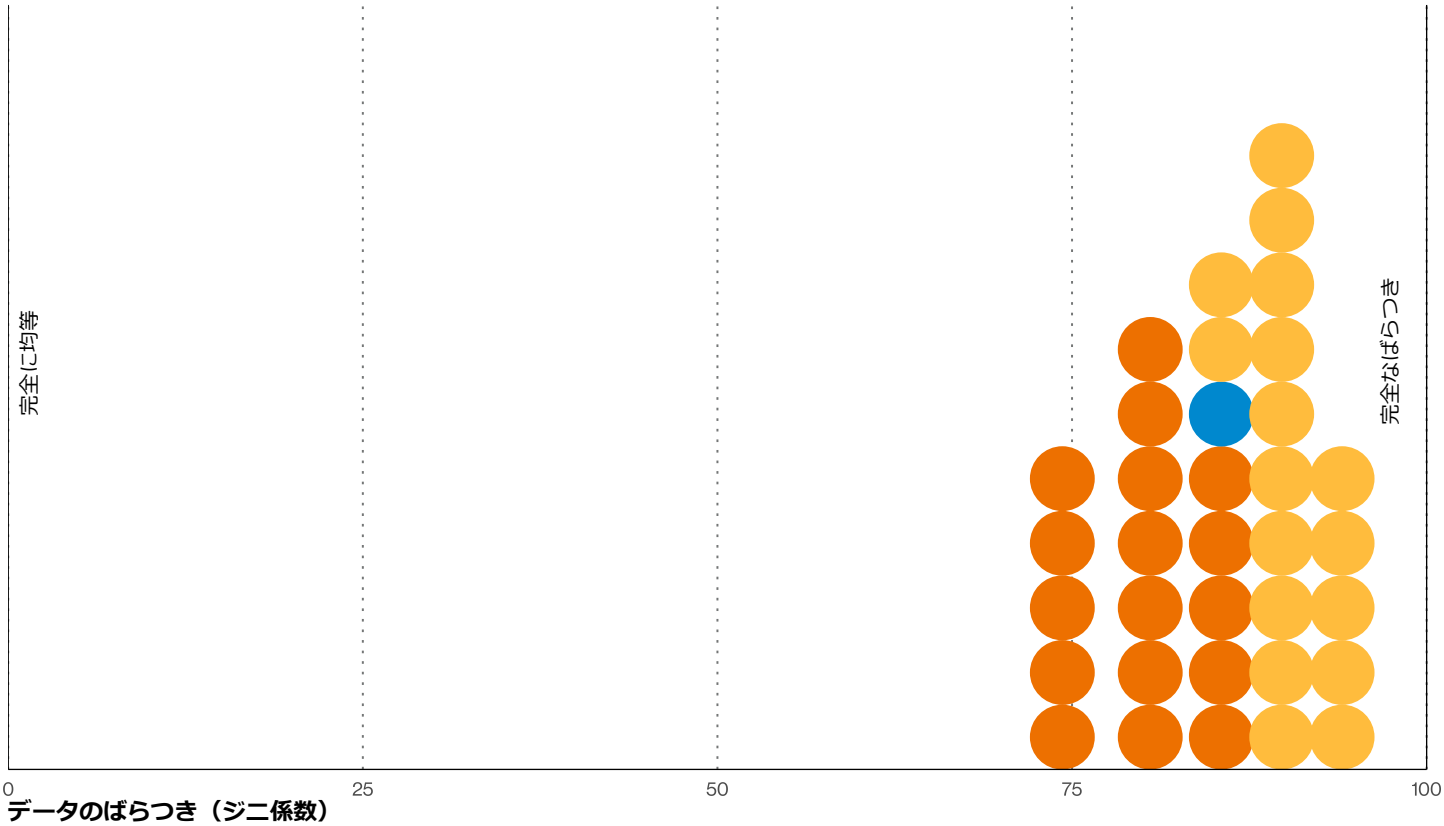


図13. 過去7年間のDBIRの攻撃の種類と経路における項目のばらつき

11 バーモント州出身の新人米国上院議員に、上位3%の攻撃パターンがデータ漏洩/侵害の87%を占めていることを深くお詫びします。

12 DBIRを読むのは、正しい方向への大きな一歩と言ってもいいでしょう。

13 ここでの議論では、人命の死傷や個人のセキュリティに関わる潜在的なインシデントは考慮していません。それらに金銭的価値を割り当てることは意味がなく、実際には冷酷で残酷なことだからです。

攻撃者

攻撃者にとって「この世はすべて舞台」であり、攻撃者には「それぞれに退場と登場の場面がある」のです。また彼らが舞台登場の合図を極めて正確に知っていることも認めざるを得ません。しかし、ここから先、シェイクスピアのこのセリフは少し崩れます。攻撃者は「様々な役をこなす」[14]のではなく、まるでストリーミングサービスでミュージカル劇場の舞台録画を延々と再視聴させられるかのように、同じ演技を何度も繰り返しているようです[15]。

図14に示すように、外部攻撃者は、データ漏洩/侵害の攻撃者タイプを毎年独占しており、世間の注目を浴びることを諦めていないことは明らかです。読者の皆様に注意していただきたいのは、ここで示されている内部攻撃者のタイプには、不正使用行為（分類法上で空想の内部脅威とされる）とエラー行為（不注意）の両方によるデータ漏洩/侵害が含まれます。

もちろん、不正に取得した認証情報やその他の不正なアクセスを利用して組織に侵入し、内部で活動する外部の攻撃者は、詳細なインシデントフォレンジック調査を行う前は、最初は内部攻撃者に似ているかもしれません。しかし、電話が社内からのものであったとしても、電話をかけてきたのは社内の者とは限らないのです。

例年どおり、金銭的な動機による攻撃が引き続き最も多く（図15）、同様に、組織犯罪に分類される攻撃者が引き続き1位となっています（図16）。

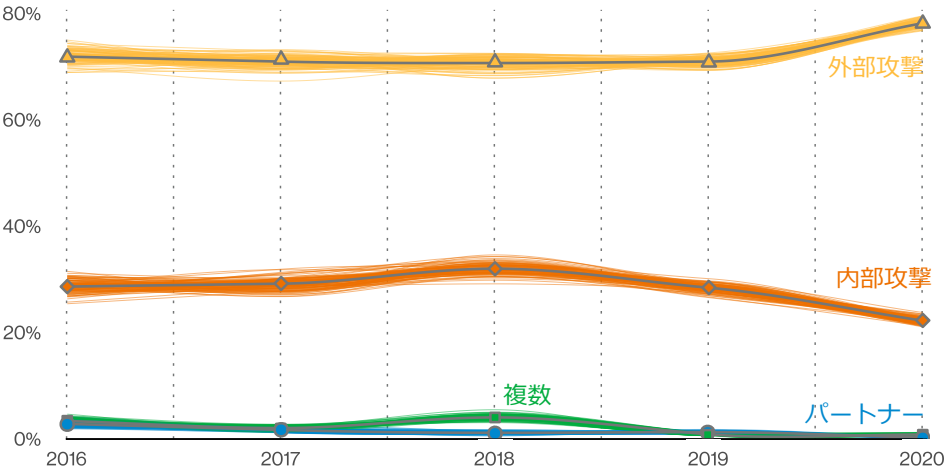


図14. データ漏洩/侵害の攻撃者の経時的変化

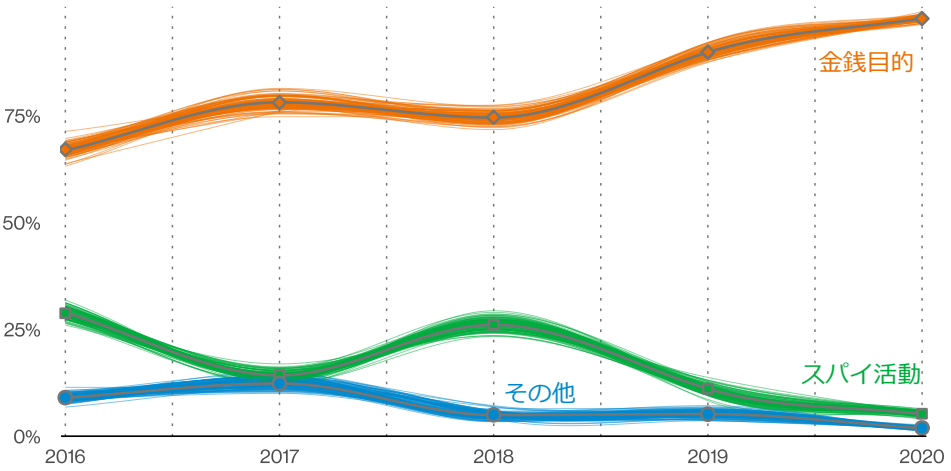


図 15. データ漏洩/侵害の攻撃者が持つ上位の動機の経時的変化

例年どおり、金銭的な動機による攻撃が引き続き最も多く（図15）、同様に、組織犯罪に分類される攻撃者が引き続き1位となっています（図16）。

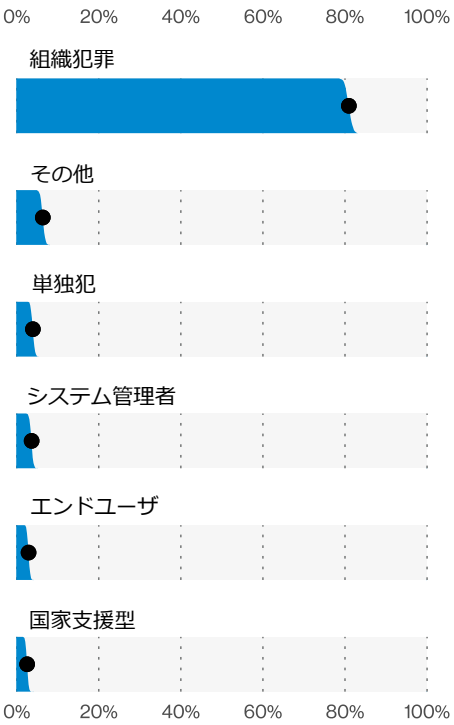


図16. 上位のデータ漏洩/侵害の攻撃者の種類（n=2,277）

14 ウィリアムシェイクスピア作「お気に召すまま」
15 「サイバー～」を商標にできるかどうか、ご存知の方はいますか？

しかし、2015年以降は、国が支援する攻撃者も現金を欲しがることが比較的多くなっています[16]。これらの攻撃者の金銭的動機は、記録されたデータ漏洩/侵害件数の6%から16%の間で変動しています。この結果を受けて図17を見ると、犯罪者フォーラムで最もよく見られるサイバー犯罪用語は、銀行口座とクレジットカード関連の2つであることがわかります。

ここ数か月の間にサプライチェーン攻撃の検出件数が増えているにもかかわらず、被害者のアクセス、インフラ、その他の資産を利用して他のインシデントを実行することがインシデントの最終的な目的であるという二次的な動機を持つインシデントの全体的な割合は、昨年と比較してわずかに減少しています。ここで、注意していただきたいことが2つあります。1つは、金銭目的の攻撃が前年比で増加していること、もう1つは、DBIRチームに報告された二次的動機の攻撃のほとんどが単純なものであることです（つまり、誰もが心配しているような大惨事はまだ、例外的なものであるということです）。

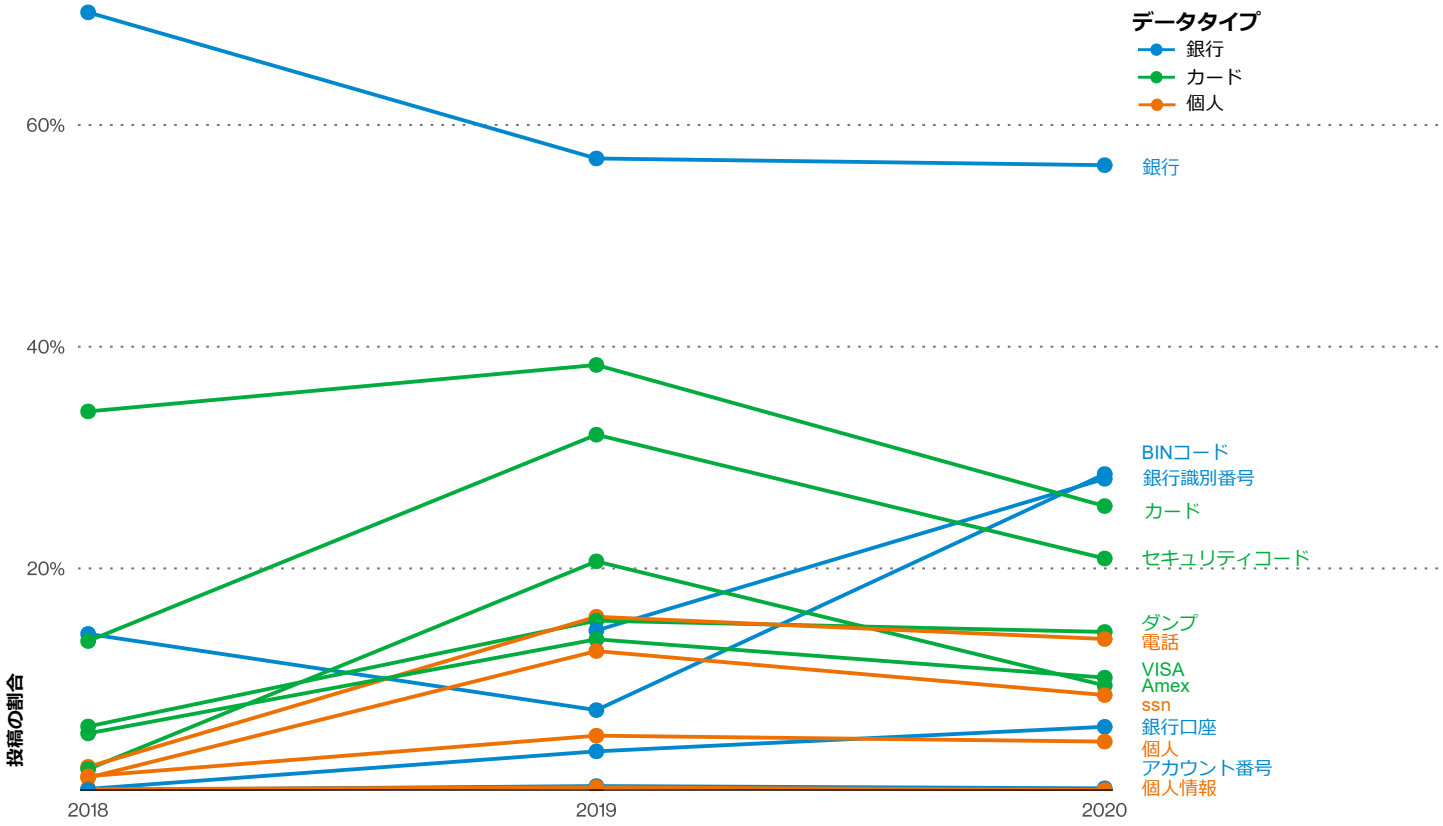


図 17. 犯罪者フォーラムやマーケットプレイスに出現する用語の経時的変化

16 または話題のエセ暗号通貨など。

しかし、図18が示すように、攻撃者の動機としては、二次的動機が依然として2位に位置しています。もしあなたがソフトウェア開発者やサービスプロバイダーで、そのような再利用が可能な資産を持っているのであれば、組織の運営方法に適切な注意を払うようにしてください。

自動化は、防御の規模拡大に役立つのと同じように、攻撃者の攻撃の規模拡大にも役立つ可能性があります。図19は、ハニーポットのデータにおける攻撃の種類の相対的な出現率を示しています。常に臨戦態勢にある攻撃者のセールスファネルの最上部にはスキャナがあります。下の方には、リモートコード実行（RCE）攻撃が存在します。図中のどの位置でも、自動化は、攻撃者が潜在的な被害者をファネルの上部から下部に移動させるのに役立つと考えられます。そのため、資産管理、防御境界、およびインテリジェントなパッチ適用などによって、企業の公共領域への攻撃を制限することが重要です。

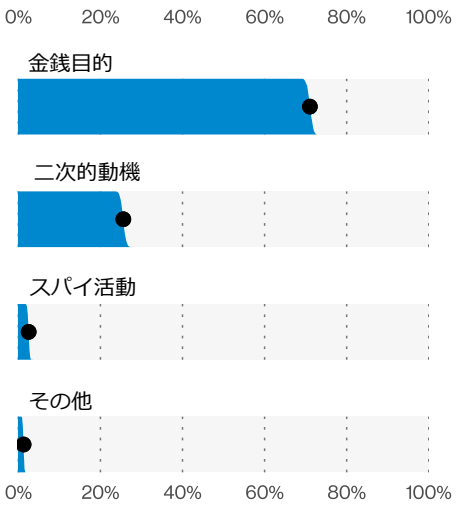


図18. 上位インシデントの攻撃者の動機（n=5,085）

自動化は、防御の規模拡大に役立つのと同じように、攻撃者の攻撃の規模拡大にも役立つ可能性があります。

二次的動機のサブセット

「二次的動機」のサブセットには、24,913件のインシデントが含まれており、そのうち既知のデータ漏洩/侵害は1件のみでした。これらのインシデントのすべてにおいて、外部の攻撃者による二次的な動機でWebアプリケーションが攻撃されていました。それ以上のことは、ほとんど分かっていません。

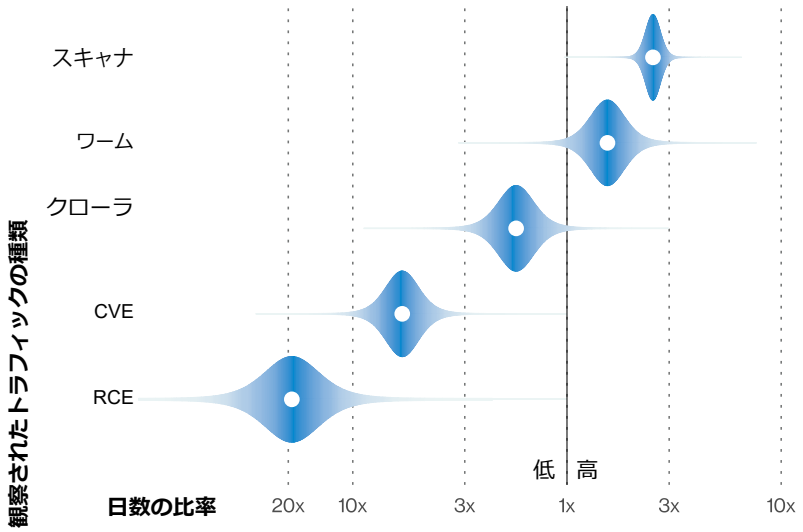


図19. ハニーポットデータにおける検知率の高い日と低い日の割合

攻撃

このセクションでは、攻撃についてたっぷりと説明します。全員に見えるよう、前に詰めて後ろに間を空けてください。図20と図21を見れば、過去1年間の攻撃の種類ごとの頻度がすべてわかります。

しかし、せっかくの新しいインシデントパターンから目をそらしてはいけません。そこで、攻撃がどのような形で現れたのか、その詳細を保存していますので、そちらをご覧ください。

話をすることと行動すること

誰も口にしたくない最悪な問題について[17]私たちが取り上げないわけにはいきませんので、本セクション「攻撃」の初期分析では、パンデミックに襲われた世界での生活への適応が脅威の状況にどのような影響を与えたかを評価することに重点を置きました。昨年半ばにDBIRチームは新型コロナウィルス感染症による脅威の状況の傾向に関する記事[18]を発表しましたが、私たちの推測（「予測」という言葉を避けたのを見てください）の内容についても再検討していきます。

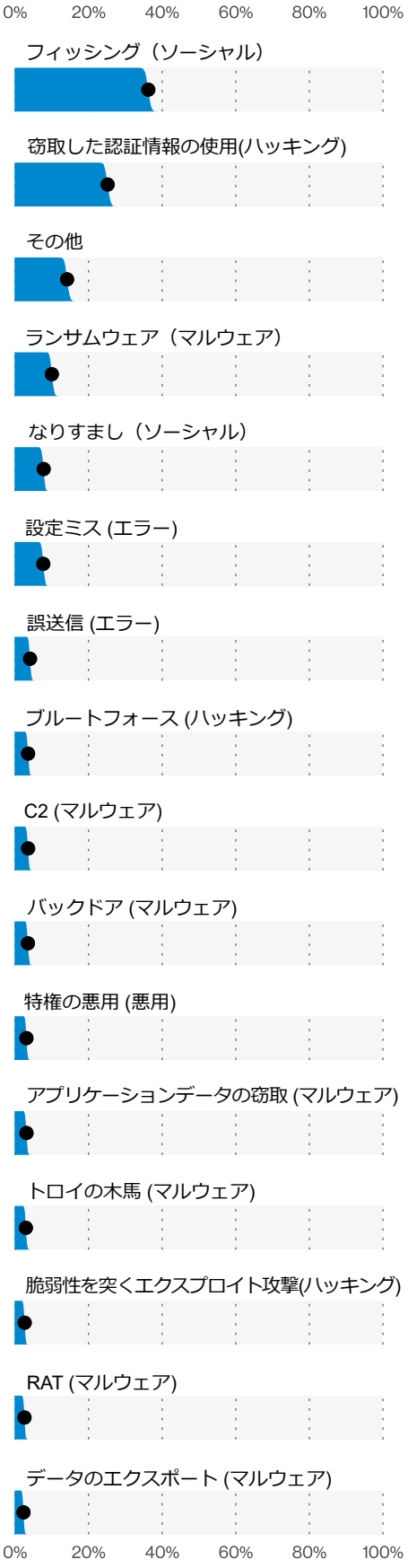


図20. データ漏洩/侵害での上位の攻撃の種類（n=4,073）

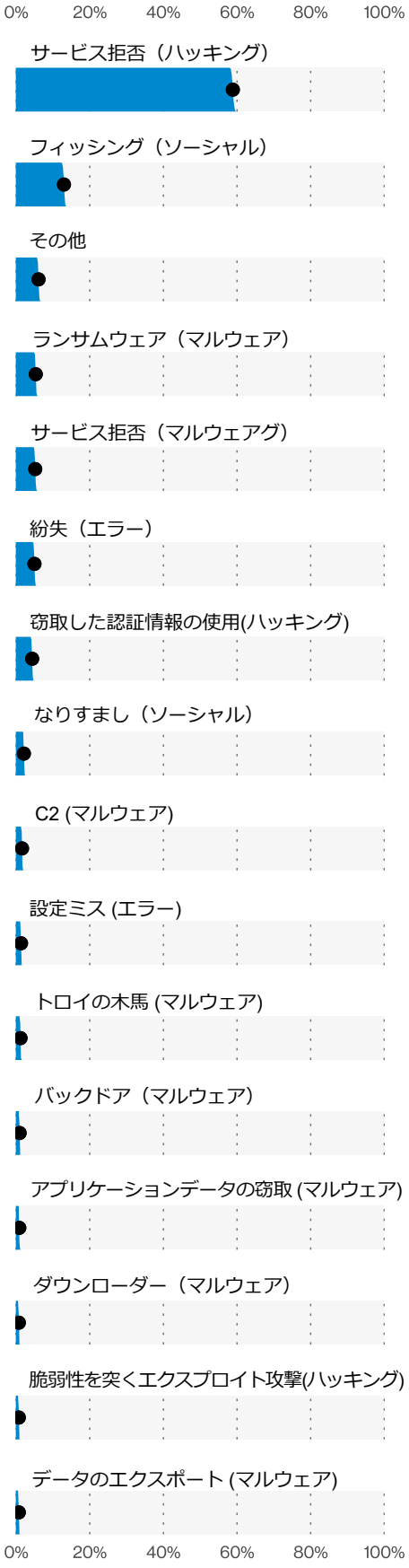


図 21. インシデントでの上位の攻撃の種類（n=24,362）

17 「口にしたくない問題」とは、もちろんウイルスのことですね。

18 https://enterprise.verizon.com/resources/articles/analyzing-covid-19-data-breach-landscape/

図22は、その記事で取り上げた「攻撃」が、昨年の報告書と比較してどのように変化したかを示しています。DBIRチームでは、増加する可能性のある攻撃として、フィッシング、窃取した認証情報の使用、ランサムウェア、各種エラーを取り上げました。

2020年という予想外の年であっても、変わらないと確信できることがあります。フィッシングは、過去2年間、データ漏洩/侵害の攻撃で上位を占めています。しかし、その栄光に甘んじることなく、検疫を利用してその頻度を高め、データ漏洩/侵害の36%を占めるようになりました（昨年の25%から増加）。この増加は、世界中で自宅待機命令が発令された際に、まずフィッシングや新型コロナウィルス感染症関連のフィッシングの疑似餌に殺到したことを考えると、我々の予想と一致します。

フィッシングは、これまでと同様に、データ漏洩/侵害で窃取された認証情報の使用と密接に関連しています。確かに、リモートワーカーの増加により、ここでも増加が予想されました。しかし、報告されたデータ漏洩/侵害の件数は25%程度にとどまっており、これは依然として重要な数字です。

攻撃の種類に関して今年大きく変わったのは、ランサムウェアが大活躍し、データ漏洩/侵害の件数において3位を獲得したことです（10%に出現し、昨年の2倍以上の頻度となりました）。すでに説明したことでもありますが、これは労働形態の変化というよりも、被害者を「名指しで辱める」という攻撃者の戦術の変化と関係しているのかもしれません。

このような攻撃者は、まずデータを暗号化して流出させ、被害者が身代金を支払わない場合には、そのデータを公開すると脅すことができます。このようなデータ漏洩/侵害の二重恐喝が攻撃者の行動規範で認められているかどうかはわかりませんが、そもそも行動規範があるという事実はありません。

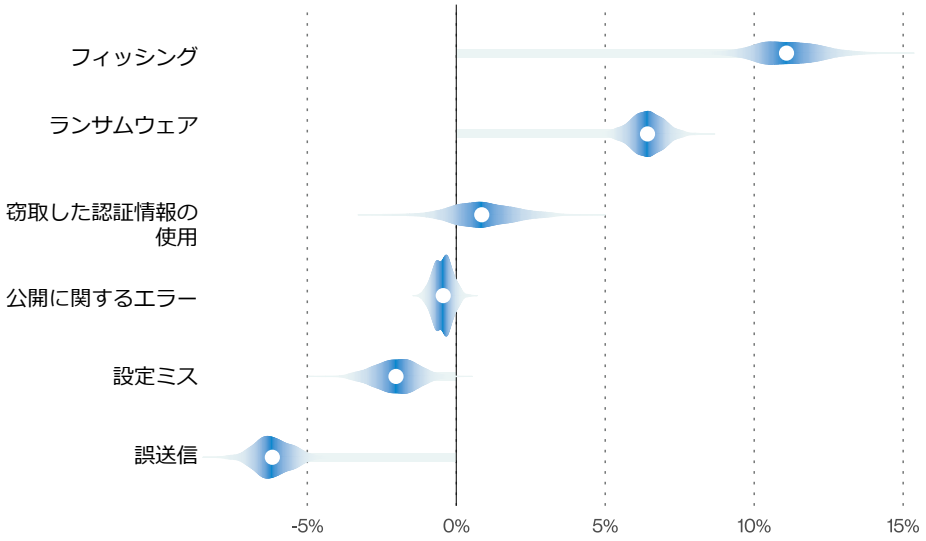


図 22. 新型コロナウィルス感染症に関連する攻撃の種類の変化

このパズルの最後のピースは「エラー」関係のもので、増加するものと考えていましたが、実際には今年度は22%から17%に減少しました。これは、3年間続いていた横ばいまたは増加の傾向を解消するものです。確かに絶対数としては、エラーによるデータ漏洩/侵害の件数は883件から905件に増加しています。しかし、ソーシャルエンジニアリングによる情報漏洩が急増したため、データセットに占めるエラーの割合は減少しました。

もちろん、DBIRチーム内では、この誤算を密かに非難し合っています。しかし、相対的に見ても絶対的に見ても、これは重要な値です。図23が示すようにマルウェア関連のデータ漏洩/侵害と同程度のものであり、皆さんの会社の制御システムに関する定義戦略の中心に据えるべきものです。

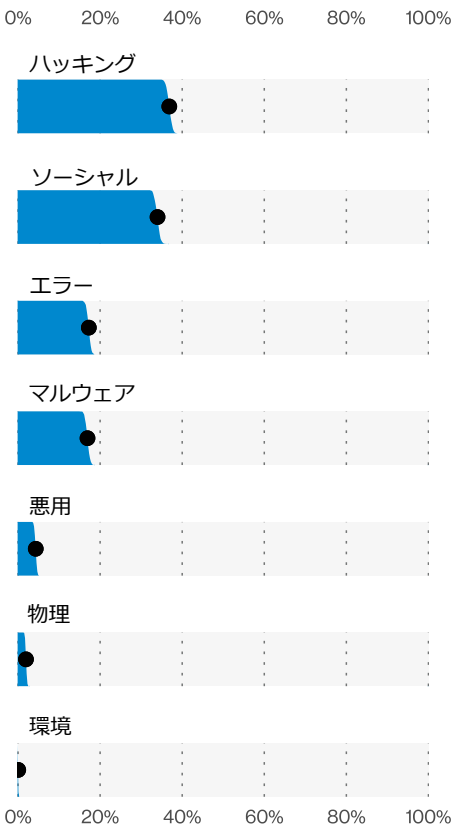


図23. データ漏洩/侵害での攻撃（n=5,257）

攻撃には結果が伴う[19]

ここ数年で収集し始めたデータポイントは攻撃の結果に関するもので、特に現在進行中の攻撃チェーンの研究を補完するものとして考えると、興味深い洞察が得られます。たとえば、攻撃者は、盗んだ認証情報の使用やフィッシング行為を行って攻撃対象とする組織に侵入した後、目的のデータを窃取するためにマルウェアを展開することがあります。

図24のヒートマップは、最も頻度の高い結果が上位の「攻撃」カテゴリーとどのように関連しているかを示しています。

ここで注目すべき点は、これらの調査結果が、私たちが分析したインシデントの一部に存在する攻撃チェーンの情報とどの程度一致しているかです。攻撃が「侵入」に集中している場合、図25に示すように、チェーンチャートの最初の攻撃の上位に近くなり、「データの抜き取り」は最後の攻撃と相関関係があります。「悪用」による攻撃は、データ漏洩/侵害された資産への正当なアクセスを前提としたり、必要としたりすることが多いため、「データの抜き取り」に集中するという点で異なります。マルウェアに関しては、最近の変異種であるスイスアーミーナイフマルウェアの亜種のような動作を考えると、ケーキを残しながらも食べるという二つの事を実現させているように見えます[20]。

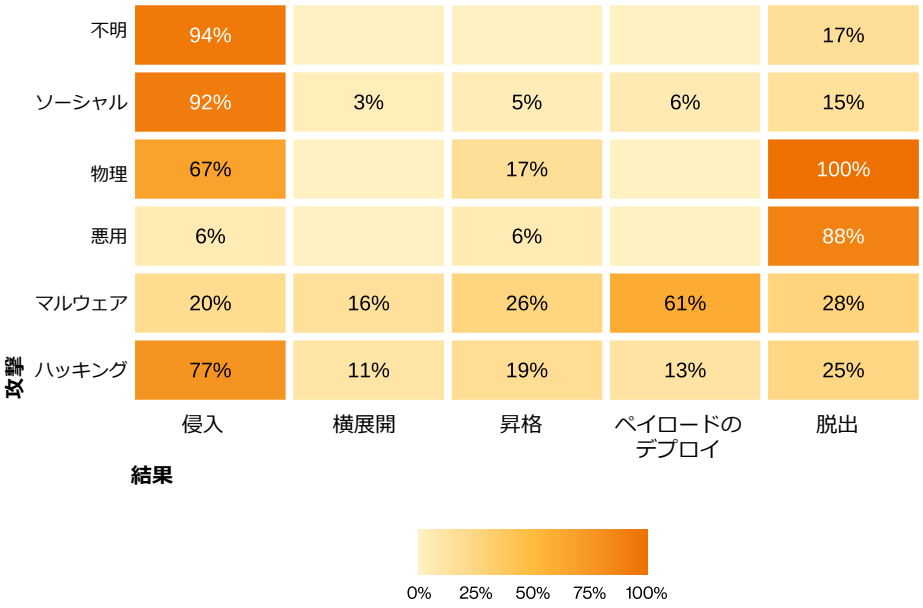


図24. データ漏洩/侵害をもたらす攻撃の結果

19 世の中のお母さんたちの言う通りです。
20 ケーキならいいのですが。

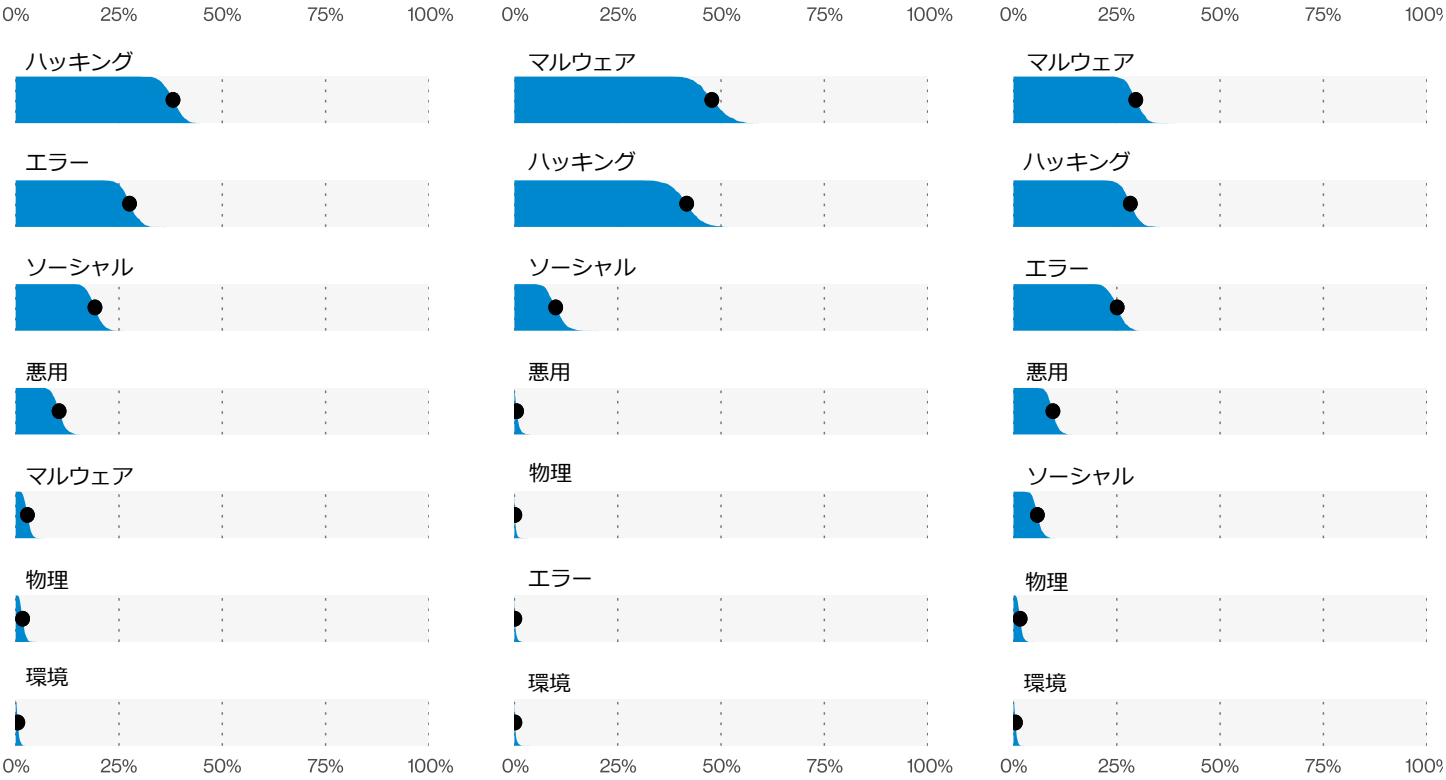


図 25. データ漏洩/侵害の開始、中間、終了時のアクション

共有アクセスはダブルアクセス

今年のもう1つの注目すべき変化は、ハッキングの攻撃パスとして「デスクトップの共有」の順位が2位に上がったことです。図26が示すように、攻撃パスとしてはWebアプリケーションの影に完全に隠れていますが、5%のしきい値に達しているため、それらの認証セキュリティに注意することをお勧めします。特筆すべきは、この攻撃パスに含まれるハッキングの89%に、ある種の認証情報の悪用（窃取した認証情報の使用やブルートフォース）が関わっていることです。

図26. データ漏洩/侵害の上位のハッキング経路（n=1,610）

資産

図27と図28を見て、まだ2020年は来てなかったのではないかと思ったとしても仕方ないでしょう。インシデントに関係するWebアプリケーションやメールサービスの普及により、サーバーは依然として資産の中で優位を占めています。また、ソーシャルエンジニアリングによる攻撃が人々（今ではユーザーデバイスを超えている）を危険にさらすようになると、詐欺やスパイ活動に使用されるマルウェアを配信するフィッシングメールやWebサイトが支配的になることが予想されます。

しかし、データ漏洩/侵害に関わる資産を確認してください。デジタルトランスフォーメーションの炎がゆっくりと燃え上がり、目に見える大きな火炎となった世界の影響を垣間見ることができます。図29によると、最もデータ漏洩/侵害された資産としての個人とユーザーデバイスの間には大きな隔たりがあり、ユーザーデバイスの減少は過去2年間と比較して統計的に確認できます。

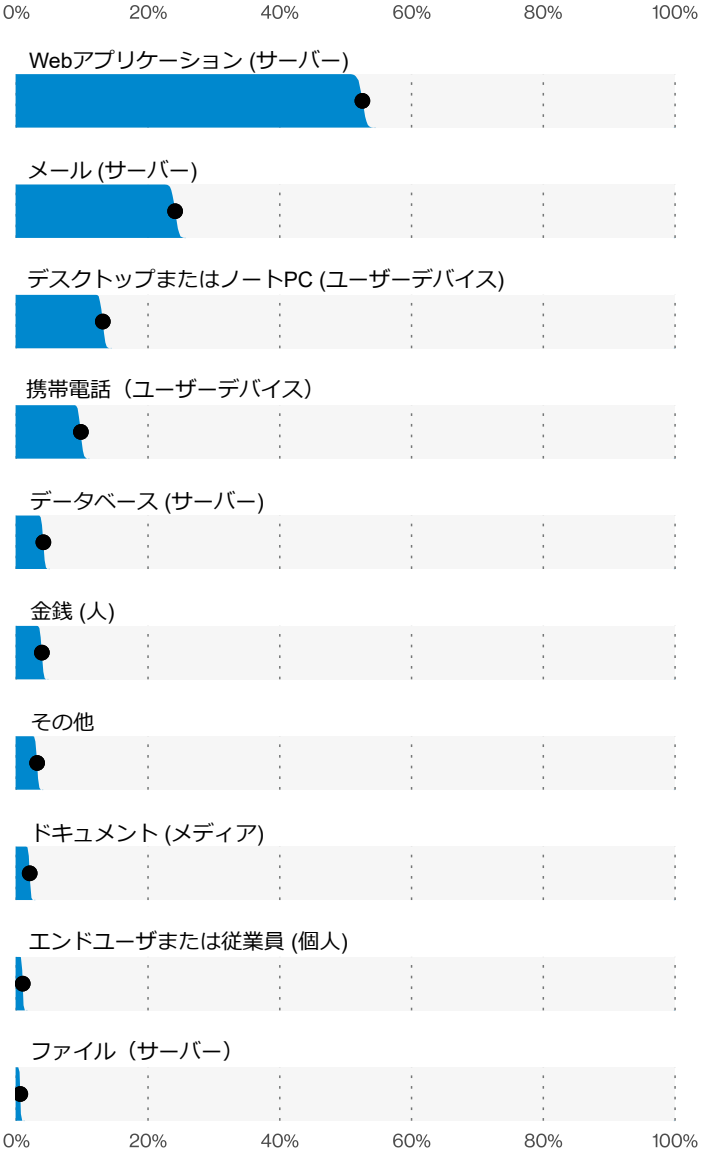


図28. インシデントの上位の資産の種類（n=9,188）

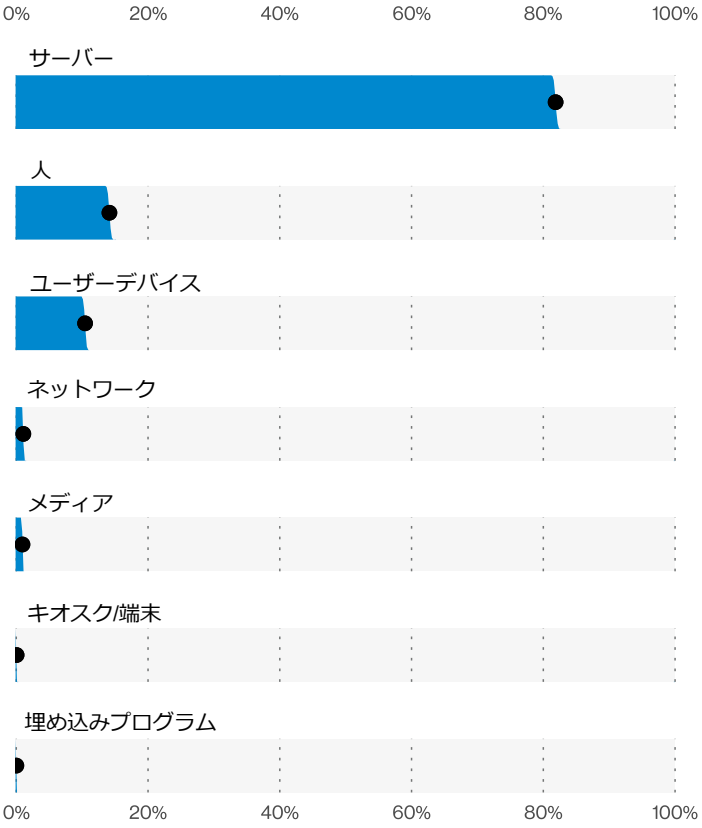


図 27. インシデントの資産（n=27,634）

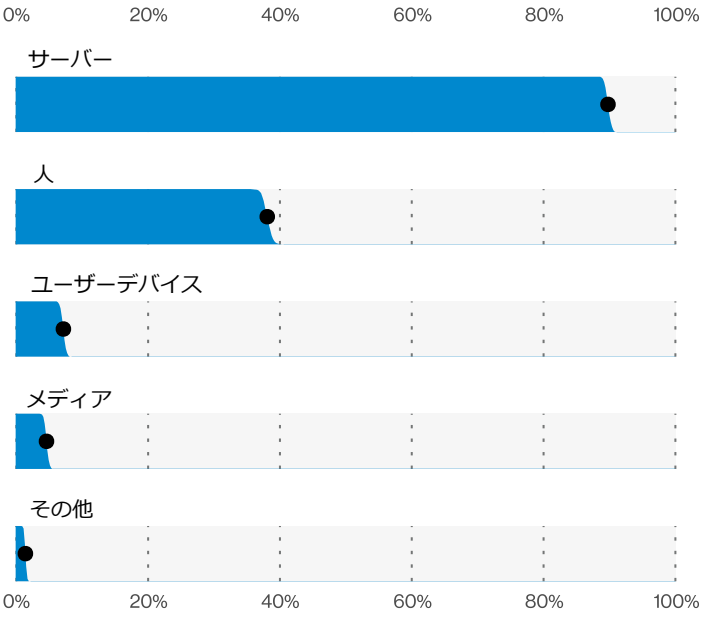


図29. データ漏洩/侵害の上位の資産（n=4,717）

この結果は、データ漏洩/侵害の攻撃パスがソーシャルアプリケーションやWebアプリケーションに移行していること、そしてそれらの手口が、認証情報を収集してクラウドベースのメールシステムに利用するなど、サーバーへの依存が高くなっていることを考えると、納得がいきます。

これに関連して、今年度はインシデントとデータ漏洩/侵害の両方において、外部のクラウド資産がオンプレミスの資産よりも多く見られたという結果も、驚くほどのことではなさそうです。次世代のAI[21]クラウドセキュリティ製品のマーケティングパンフレットにそのことを記載する前に、クラウド資産の数の10倍もの不明（資産の場所に関する情報が得られない、極めて明白なインシデント）がありました。これは、もし何が起こったのかを詳しく知っていれば、方向転換をすることができたでしょう。それでも、無作為に選んだ組織のサンプルでは、Web上に存在する組織の17%がインターネットを介したクラウド資産を保有していました[22]。もし現時点で明かになっていないのであれば、クラウド資産はセキュリティテーブルの中に含まれ、予算を与える価値があることになります[23]。

インターネット上に存在する組織を無作為に選んだ場合でも、それらの組織がインターネットを介して接続する資産は中央値で17個あります（図30）。図31は、これらの組織の脆弱性の程度を示しています。ほとんどの組織には脆弱性が全くありませんでした。また新しい脆弱性のほうがより一般的であると思われるかもしれません[24]。しかし実際には、昨年見たように、古い脆弱性のほうが多くなっています[25]。

Alexaの上位100万ドメインのようなものから選択するのではなく、世界中の数百万の企業のデータベースからランダムにサンプリングしました。100万社のうち、（ドメイン名が組織につながるような）Web上の存在はわずか1.4%でした。平均的なセキュリティ意識の高い組織は、平均的な企業とはかなり異なる可能性があることを忘れがちです。

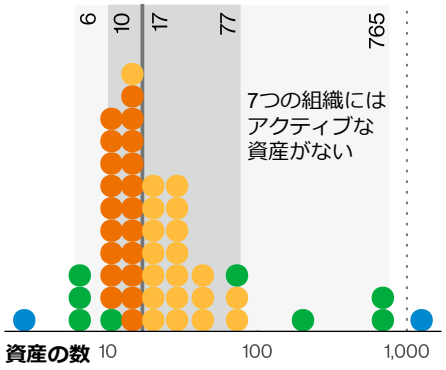


図30. 無作為に選んだ組織におけるインターネット関連の資産の数（n=85）
1=組織の2%

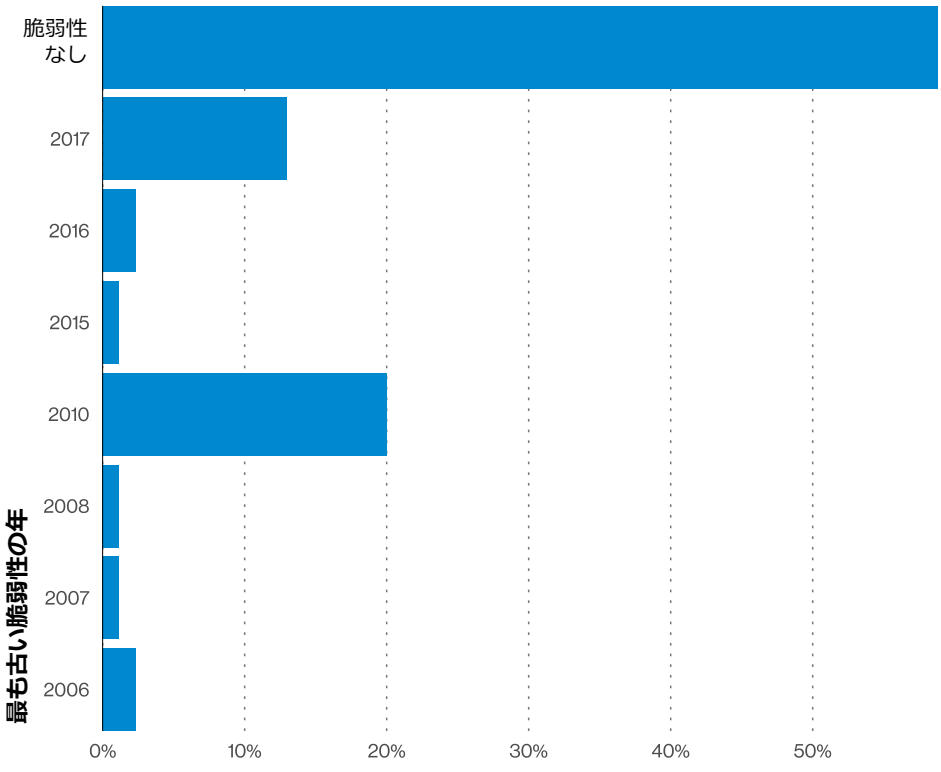


図31. 組織の最も古いインターネット関連の脆弱性（n=85）

21 「インテリジェンス」ではなく「人工」を強調しています。
22 「無作為に選んだ組織」の意味については、サイドバーを参照してください。
23 ひどい「絵に描いた餅」のジョークはカットしました。ご安心ください。
24 ほら、パッチがあるためです。
25 ただ「団塊の世代の脆弱性」とは言わないでくださいね、喧嘩になりますから。芝生から出て行けと言われるかもしれません。

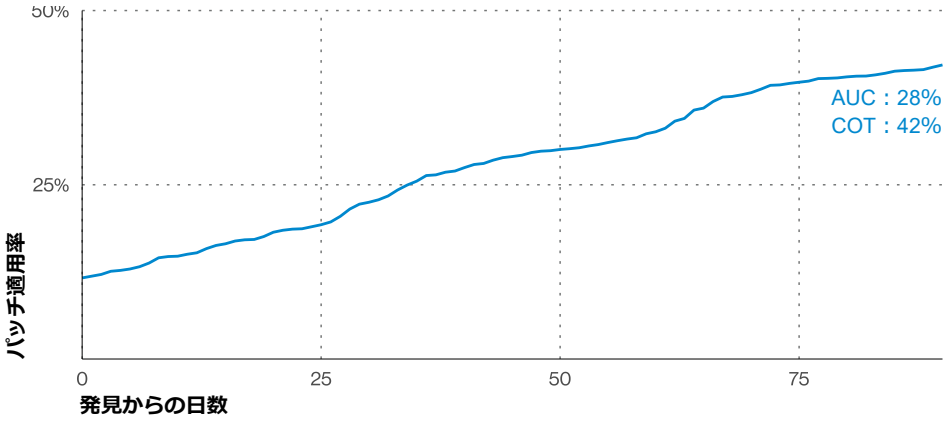


図33. 脆弱性スキャンデータにおけるパッチ適用状況（n=110）

この古い脆弱性こそが、攻撃者が悪用し続けているものなのです。図32は、攻撃者が一括して悪用しようとした脆弱性が発見された年をハニーポットの視点から見たものです。もし元NBCのキャスターでジャーナリストのトム・ブロコウ（Tom Brokaw）がこの報告書を作成していたら、これらの脆弱性を「最も偉大な脆弱性」と呼ぶでしょう。エターナルブルーは人気の高いエクスプロイトですが、これは、攻撃者が脆弱性を狙う理由に、発見されてからの時間はあまり関係ないことを示しています。むしろ、脆弱性を悪用することで攻撃者にどのような能力がもたらされるか、また、現在利用されているエクスプロイトやペイロードの堅牢性のほうが問題のように思えます[26]。

では、適度に、きちんとした、セキュリティ意識の高い組織はどうすればいいのでしょうか？図33によると、今年度の組織でのパッチの適用度は、決して良いものではありませんでした。素晴らしいものではありませんでしたが[27]、パッチの適用が芳しくなかった理由として、いくつか仮説が考えられます。

どの組織にとっても理想的なのは、セキュリティを向上させるためではなく、組織の生産性を向上させるために脆弱性の優先順位を上げることで、難しいパッチではなく適用が簡単なパッチを当てることです。パッチを適用しなければならない場合、そのたびにキーボードを置いてゲームコントローラーを手にするまでの時間が長くなることを意味します[28]。セキュリティの向上に寄与しない脆弱性へのパッチ適用を避けることができれば、セキュリティを維持しつつ、作業量を大幅に減らすことができます（従業員やサービスプロバイダーが燃え尽きることも少なくなります）。

このセクションの冒頭の図28では、携帯電話がリストアップされています。昨年と同様、この結果はやや拍子抜けするもので、大半は単に携帯電話を紛失しただけの話です。しかし、これで携帯電話に関する調査が終わったわけではありません。図34には、悪意のあるURLとAPK[29]に関するモバイルデータもあります。要するに、大きな組織でなくても、メンバーの誰かが悪意のあるURLを受け取ったり、悪意のあるAPKをインストールしたりする可能性は十分にあるということです[30]。

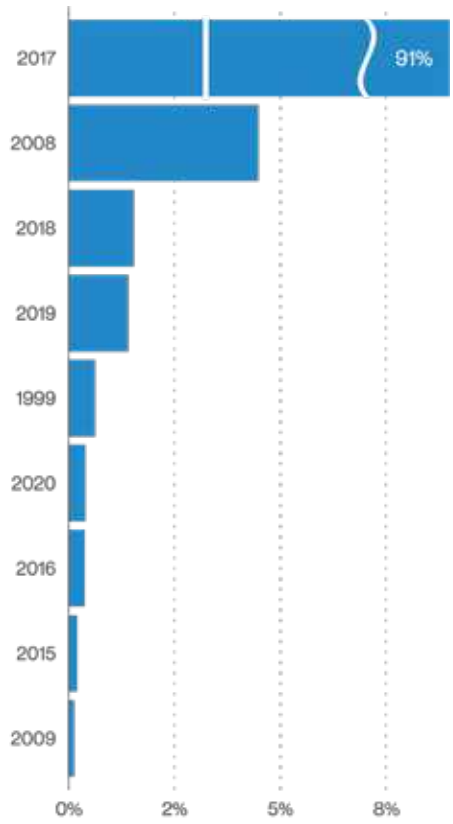


図32. 年別のハニーポットデータの脆弱性の割合（n=42,532,746）
エターナルブルーはこのうち37,217,565件。2017年はこれがなければ3%で2位にランクされていたでしょう。

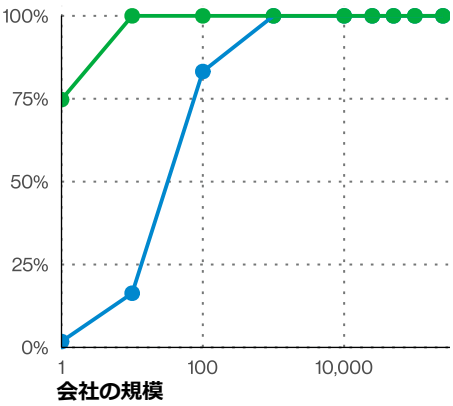


図34. 組織の規模に応じて、社内の誰かが悪意のあるURLを受信したり、悪意のあるAPKをインストールしたりする確率（n=5,440,000）

26 このセクションを書いている間にも、Microsoft Exchangeのリモートコード実行脆弱性（CVE-2021-26855）が活発かつ大規模に悪用されています。これは、インターネット上で高まる悪用のバックグラウンドノイズの一部にもなる要素をすべて備えています。

27 2017年度データ漏洩/侵害調査報告書、図56。

28 または子供、またはランニングシューズ、またはあなたを正気に保つ何か他のもの。

29 Androidアプリ。

30 よくご存知の方は、「資産」のセクションに情報技術（IT）と運用技術（OT）の資産に関する記述がないことにお気づきかもしれません。それは、私たちのデータセットにもほとんど含まれていなかったからです。このようなOTでのデータ漏洩/侵害はどこかにあるとは聞いていますが、我々のデータセットにはありません。

属性

属性とは影響を受ける資産のConfidentiality（機密性）、Integrity（完全性）、Availability（可用性）（「CIA[31]トライアド」と呼ばれる）の侵害のことです。データの機密性への攻撃が確認されたデータ漏洩/侵害であっても、フィッシングで人の行動を変容させる完全性に関するインシデントであっても、資産に対する攻撃はCIA侵害となります。まず、機密性と最も頻繁に侵害されるデータの種類について説明します。

過去のDBIRでも指摘してきたように、認証情報は依然として最も狙われているデータの1つです（図35）。次に、個人情報が挙げられます。個人情報には、社会保障番号、保険関連情報、氏名、住所などの収益化しやすいデータが含まれていることを考えると、攻撃者がこうしたデータに狙いを定めるのも不思議ではありません。個人情報は、転売の価値があることは言うまでもなく、将来的には金融詐欺にも役立ちます。

また、データ漏洩/侵害をするのは攻撃者だけではありません。残念ながら、自社の従業員がミスを犯し、問題につながる可能性も否定できません。しかし、これらのミスは、認証情報に絡む可能性は低く、個人情報などのデータに関わる可能性が高いようです（図36）。

過去のDBIRでも指摘してきたように、認証情報は依然として最も狙われているデータの1つです。

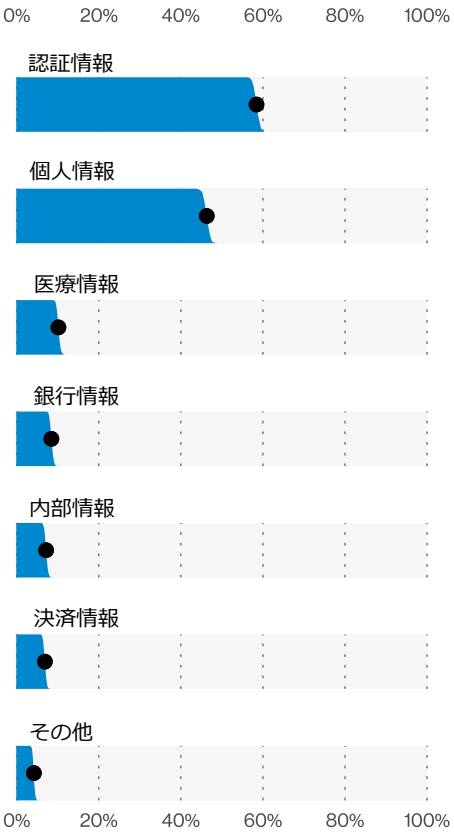


図35. データ漏洩/侵害での上位のデータの種類（n=4,552）

図36. エラーによるデータ漏洩/侵害での上位のデータの種類（n=839）

31 エイリアン情報を含んだXファイルをダウンロードできるようにしたCIAではなく、別のもの。

完全性の侵害（図37）については、通常、ソーシャル攻撃またはマルウェア攻撃の結果として起こります。ソーシャル攻撃としては、フィッシングやなりすましによるものが、標的となる被害者の行動を変えてしまいます。場合によっては、なりすましによって不正な取引が開始され、想定していないところにお金が流れてしまうこともあります。今年度のデータセットでは、フィッシングとなりすましの攻撃が蔓延しており（データ漏洩/侵害の43%）、「行動の変容」が完全性の侵害の中で1位にランクインしているのは当然のことです。

しかし、マルウェアによる攻撃も忘れてはなりません。ソフトウェアのインストールが2位になったのは、「システム侵入」パターンにマルウェアのコンポーネントを含むケースが多かったためです。ほとんどの場合、マルウェアはシステムにアクセスした後に攻撃者によって直接インストールされますが、通常は、盗まれた認証情報の使用やブルートフォースなどのハッキングが行われた後にインストールされます。

最後に、可用性に関する侵害について説明します（図38）。最も多いのは「難読化」で、これはランサムウェアがインストールされ、暗号化が開始された場合に発生します。2番目に多い侵害は「紛失」で、資産の紛失や盗難が原因で、データにアクセスできなくなります。

図37. データ漏洩/侵害での完全性の種類（n=2,762）

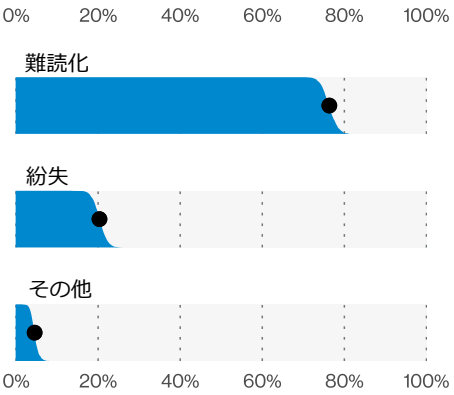


図38. データ漏洩/侵害での可用性の種類（n=541）

タイムライン

今年度は、どのような種類のデータ漏洩/侵害が発見まで最も時間がかかるかを見てみることにしました（図39）。これまで発見に時間がかかったのは、内部の犯行による「特権の悪用」でした。しかし、最新のデータを見てみると（主に新しいパターンによって得られた知見による）、「特権の悪用」と「システム侵入」の違いはごくわずかであることがわかりました。どちらも、発見までに時間がかかるデータ漏洩/侵害に属していました。

逆に、最も早く発見されるデータ漏洩/侵害は、何かが間違っていることがすぐに明らかになるようなものです。たとえば、従業員が侵入の証拠を見つけた「資産の盗難」や、失敗を犯した従業員が沈んだ気持ちになり、早く収束させたいと思って報告した「エラー」などです。これらはいずれも社内で発見する方法です。もしこの種のデータ漏洩/侵害を簡単かつ迅速に従業員が報告できるプロセスをまだ導入していないのであれば、検討すべきでしょう。従業員を早期警戒システムとして育成することは、大きな投資効果が期待できます。

また、対局的な発見方法として、身代金請求書を画面に表示する形で攻撃者から「通知」される場合があります。

最後に、どのようなデータが最も早くデータ漏洩/侵害されるのか分析したところ、認証情報であることが判明しました。これは特にフィッシングのケースに該当します。通常、盗まれた被害者の認証情報は、標的にした被害者の組織にさらにアクセスできるようにするために使用されます。

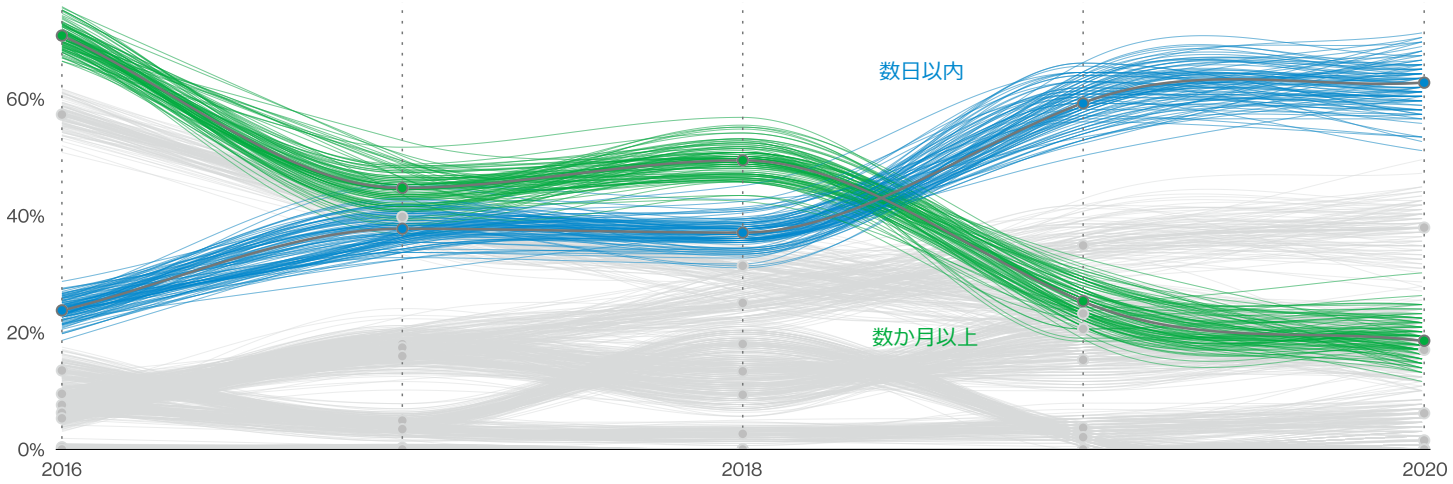


図39. データ漏洩/侵害における時間経過に伴う発見

影響

人手が多ければ作業が楽になる

攻撃者は、データ漏洩/侵害やインシデントの被害者に降りかかる不利益から多大な利益を得続けています。この利益自体も確かに興味深いものですが[32]、本当に関心があるのは、被害者側のほうで被害金額がどれほど嵩むかということです。図40は、FBIのインターネット犯罪苦情センター（Internet Criminal Complaint Center：IC3）に報告された調整後の損失額に基づいて、インシデントの種類による損失額の範囲を示しています[33]。この図では、各ドットはインシデントの半分を表しています。IC3のデータによると、第一に、攻撃がビジネスメール詐欺（BEC）、コンピュータデータの漏洩/侵害（CDB）、ランサムウェア攻撃のいずれであっても、インシデントの大部分では実際には金銭的損失には至らなかったという事実があります（それぞれ42%、76%、90%）。

損失が発生したとしても、それは一過性のものであり、すべてのインシデントに当てはまる性質のものではありませんでした。ビジネス成立のルールに従うと、攻撃者は市場が負担できる金額を請求すると考えられます。小規模な組織であれば、たいてい少額の請求です。しかし、大規模な組織の場合、損失ははるかに大きくなります。報告された損害をもたらしたデータ漏洩/侵害を調査したところ、BECの95%は250ドル～985,000ドルの範囲にあり、中央値は30,000ドルでした。これはかなり大きな範囲だと思います。しかし、CDBの場合は、95%が148ドル～160万ドルで、中央値が30,000ドルと、さらに範囲が広くなっています。最後に、ランサムウェアの場合、損失額の中央値は11,150ドルで、95%の損失額の範囲は70ドル～120万ドルとなっています。

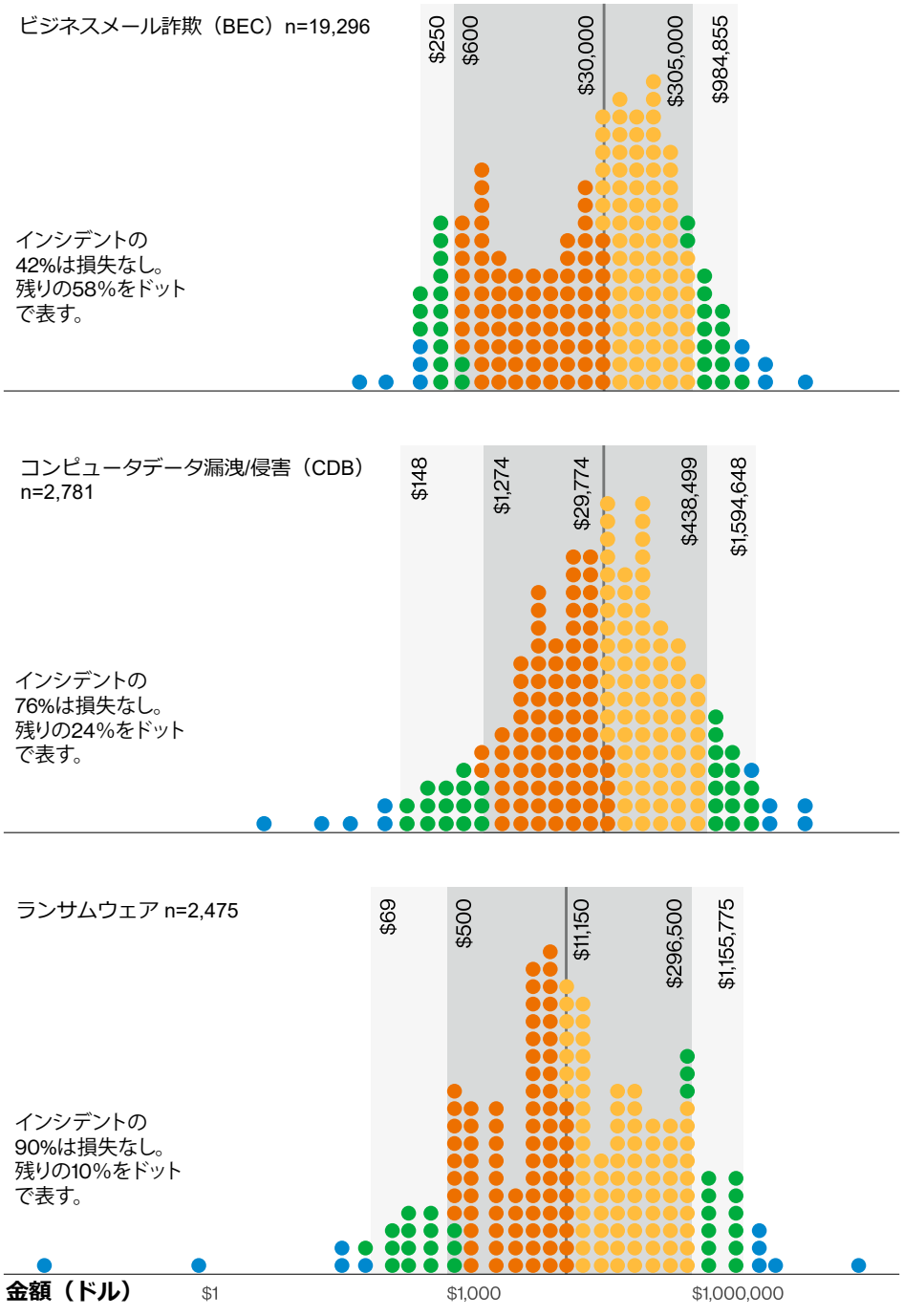


図40. インシデントの種類別の損失
1ドット=インシデントの0.5%

32 異なるタイプの攻撃の収益性を攻撃者の視点から分析することは魅力的ですが、それを行うのに必要なデータがあるとは思えないだけでなく、この分析が防御者よりも攻撃者に利益をもたらすかどうかもわかりません。

33 https://www.ic3.gov

これを少し違う形で見てみましょう。下半分（先ほどの中央値以下）だけに注目すると、CDBはランサムウェアよりも大きな損失を伴うことが多くなっています。この結果は、ランサムウェアのインシデントのうちの90%が損失を被らなかったことも合わせて、組織が身代金を支払わなくなったことを物語っているのかもしれません。また、この損失データには組織だけでなく個人も含まれていることも、数字が小さくなっている理由の1つです。残念ながら、組織と個人を区別できるほどの詳しいデータはありません。また、実際は膨大であった身代金を過少に報告するようなバイアスがかかっている可能性もあります。しかし、組織が身代金の要求を無視しているのであれば、支払額の範囲が低いことが、2019年後半に目撃された「名指しと恥さらし」ランサムウェア攻撃を行う攻撃者が台頭してきたことのもう1つの要因となった可能性があります。

このような状況を楽観的に見ると、資金を他の環境へ移すことを無効にできる可能性があるということです。IC3のRecovery Asset Team（RAT）は、被害者が失った資金を凍結して回収できるように支援することもあります。図41では、IC3のRATがBECに対処し、送信先の銀行と連携をとった結果、米国で発生したビジネスメール詐欺のうち半数は99%の資金が回収または凍結されたのに対し、全く回収されなかったのはわずか11%でした。もし、あなたの組織でインシデントが発生した場合は、国の法執行機関の地方支局に連絡し、支援を求めることを強くお勧めします。あるいは、データ漏洩/侵害が発生する前に、この機関のことをよく調べておくことをお勧めします。

もちろん、データ漏洩/侵害によって発生するコストは、直接的な損失だけではありません。攻撃者による被害とは別に、デジタルフォレンジック＆インシデントレスポンス（DFIR）や弁護士の費用がかかります。図42は、サイバー保険[34]の請求に基づいて、これらの分野で何が期待できるかを示しています。各ドットはインシデントの2%を表しています。ご覧の通り、インシデントの50%はフォレンジック調査の費用が発生していません。フォレンジック調査の費用が発生した場合でも、95%が2,400ドル～336,500ドルの範囲に収まっています。法務関係のコストが発生しなかったケースは36%と、フォレンジック調査よりもやや少なめでした。残りの64%は、95%が800ドル～54,000ドルの範囲でした。

なお、保険のデータには多少の偏りがあります。たとえば、訴訟費用や違約金は保険でカバーされない場合があります。また、全体の費用に含まれない控除免責金額が追加されることもあります。もちろん、口に出したくないような重要問題に取り組む際[35]、会社の評判失墜を保険がカバーしてくれるとは考えにくいです。そして、情報開示の要件、データ漏洩/侵害の規模、その他契約書などの細則に隠されていることなど、いくつかの要因によって、その損害は相当なものに上る可能性があります。

データ漏洩/侵害直後の数日間における株価への影響については、2.53%（Rosati, Cummins, Gogolin, van der Werff, & Lynn, 2017）、5%（Cambell, Gordon, Loeb, & Zhou, 2003）、2.1%（Cavusoglu, Mishra, & Raghunathan, 2004）、1%（Goel & Shawky, 2009）など、研究によって結論は大きく異なります。これらの研究結果は参考になりますが、長期的に何が起こるのかについてはあまり明らかになっていません。図43は、この問題を多少明らかにできるかもしれません。

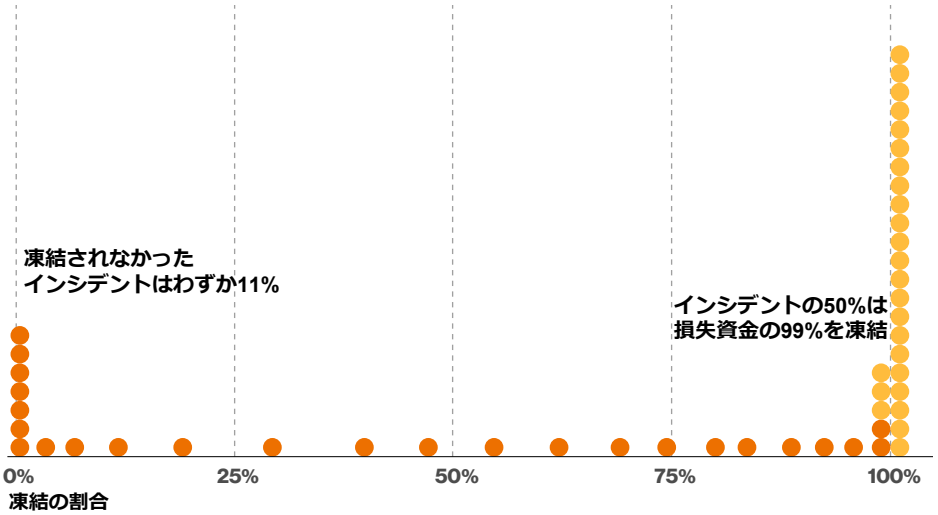


図 41. 回復のために凍結された損失の割合（n=1,086）
1ドット=インシデントの2% 。

34 ベライゾンでは、別料金にて「サイバー」を「セキュリティ」に置き換えたバージョンのDBIRを提供します。詳細は、お近くのベライゾンの営業担当にお問い合わせください。

35 また別の「口に出したくない重要問題」です。

comparitech.comが収集したデータによると[36]、被害に遭った企業では、6か月後のNASDAQ（米国株式市場）の株価は約5%下回っていますが、95%の企業を見ると、その株価は 48%下回っていたり、39%上回っていたりします。これらの組織の将来（データ漏洩/侵害後から2年後）を見ると、株価の下降傾向は続いており、おそらくデータ漏洩/侵害は実際には原因ではなく、症状であることが示唆されています[37]。

「データ漏洩/侵害のコストは全体でどのくらいになるのか」という疑問に答えるため、有能なデータオタクのように、今年度のデータセットに含まれるコスト情報をもとに、ブートストラップサンプリングを用いて1,000件のモンテカルロシミュレーションを行ってみました。シミュレーションされたデータ漏洩/侵害のうち14%は影響がありませんでした。影響があった86%の結果を表1に示します。これらの数字をどのように活用するかは、もちろん読者の皆様次第です。中央値である21,659ドルのコストを想定して計画を立てることもできますが、データ漏洩/侵害による影響の80%に相当する2,038ドル～194,035ドルを想定して計画を立てるほうが良いかもしれません。さらに言えば、最も一般的な95%の影響である826ドル～653,587ドルに備えることもできます。これに約5%の組織評価の下落（図43より）を加えれば、計画を立てることができる具体的な数字が見えてくるかもしれません。

データ漏洩/侵害の割合	下位	上位
中央値	$21,659	
80%	$2,038	$194,035
95%	$826	$653,587

表1. シミュレーションによるデータ漏洩/侵害コスト

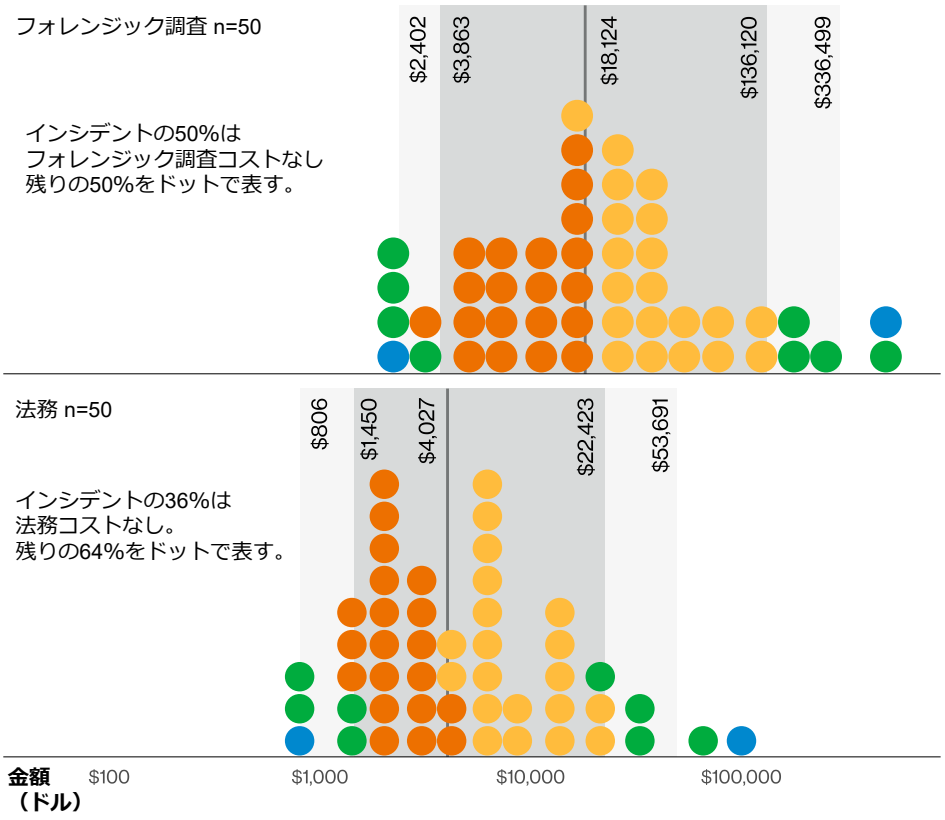


図42. インシデントの種類別コスト
1ドット=インシデントの2%

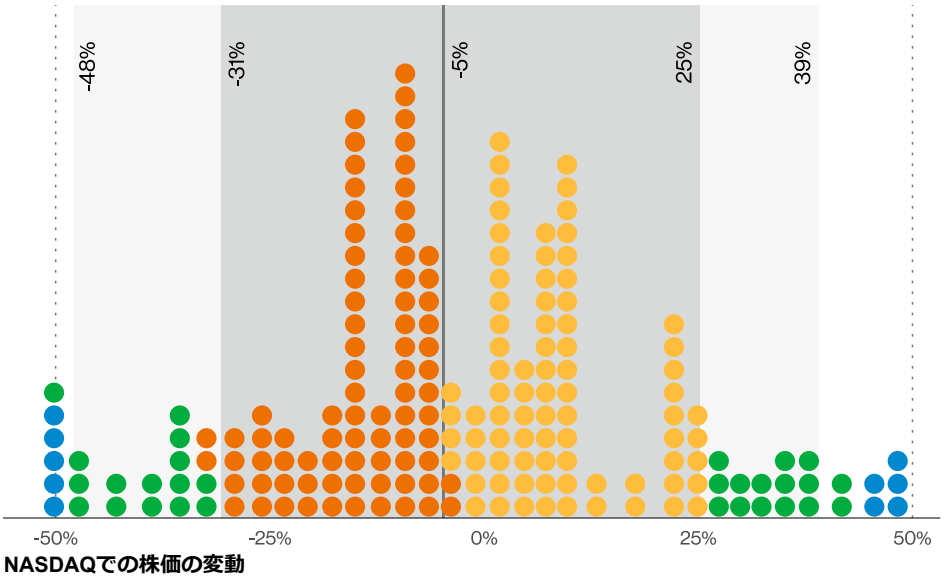


図43. 被害に遭った企業の6か月後の株価の変動（n=39）
1ドット=インシデントの0.5% 。

36 正確には、Paul Bischoff（@pabischoff）氏のブログ記事を参照：https://www.comparitech.com/blog/information-security/data-breach-share-price-analysis/
37 Dr.Frank N. Furterが賛同してうなずいています。

FBIについて

ハーバート・ステープルトン

FBIサイバー担当副アシスタント ディレクター

過去10年間でサイバー攻撃は飛躍的に増加しており、国家やサイバー犯罪者は、攻撃の規模、範囲、洗練度を高めています。このような複雑で機敏に変化する環境に対処するには、1つの政府機関、企業、技術、データソースだけでは対応できず、より包括的な対応が必要とされます。重要なインフラを保護し、攻撃者にリスクとその報いを与えるためには、公的機関や民間企業の能力を組み合わせたアーキテクチャを活用しなければなりません。

FBIは、サイバー攻撃についてできるだけ早く情報を共有し、一般市民に注意を喚起して備えてもらうよう努めています。またFBIは、法執行機関および米国諜報コミュニティの一員としての独自の権限を活用することで、政府がサイバー攻撃者に対抗できるようにし、また一般市民がセキュリティ態勢を強化できるよにし、皆さんの不可欠なパートナーと認められるよう努力しています。私たちは、独自の権限、世界最高水準の能力、永続的なパートナーシップ、そして存在感により、サイバー攻撃の発信元を特定する過程で、捜査、情報収集、被害者との対話を行うことができます。サイバー攻撃の発信元を明らかにすることで、米国政府は攻撃者にリスクとその報いを与え、民間企業を含むパートナーとの活動に優先順位をつけることができます。サイバー[サイバー犯罪との戦い]は究極のチームスポーツであり、私たち全員があらゆる手段を駆使してサイバー攻撃に対処することに取り組む必要があります。

FBIにとって最も重要であり、基本的なサイバー戦略の重要な要素は、対処に役立つ関連性の高い情報を政府のパートナー、国際社会、民間企業、そして一般市民と共有する能力です。しかし、サイバー攻撃の全体像を把握するためには、パートナーや民間企業、被害者から寄せられる情報にも依存しています。インターネット犯罪苦情センター（IC3）は、インターネットを利用した犯罪行為の疑いに関する情報をFBIに提供するための信頼性の高い便利なツールとしての役割を果たすとともに、法執行機関や民間企業との効果的なパートナーシップを構築しています。IC3に提供された情報はさらに詳しく分析され、捜査の手がかりとなったり、新たなサイバー攻撃が発見されたりします。IC3のデータ分析から得られた情報は、PSAやアラート、DBIRなどのレポートを通じて、一般市民や民間企業に公開しています。

2021年度のDBIRでは、FBIのIC3は、特にビジネスメール詐欺/メール詐欺（BEC/EAC）、およびIC3に報告されたその他のデータ漏洩/侵害インシデントに関するデータの供給に注力しました。近年、FBIのIC3では、BEC/EACやデータ漏洩/侵害事件は、企業や民間企業が被害者となる傾向が強く、一個人が標的にされるケースは少ないと考えています。IC3では、サイバー犯罪者がどのように進化しているかを理解するために、一般の人々が中心的な役割を果たしていると認識しています。市民がサイバー攻撃に関連する苦情を提出することで、FBIによる苦情の対処や、発展途上にあるサイバー攻撃の傾向に関する情報特定を支援することになるのです。

03

インシデントの分類パターン

インシデントの分類パターン：イントロダクション

時代は変わってきている

2014年を覚えていますか？アップタウンはファンキー（マーク・ロンソンのヒット曲「アップタウン・ファンク」に引っ掛けて）で、ファレル・ウィリアムスはハッピー（ファレル・ウィリアムスは「ハッピー」で大ヒットを飛ばしました）で、問題を抱えていても、それを振り払うことができました。DBIRがインシデントの分類パターンを初めて導入したのは2014年のことで、非常に頻繁に発生するVERIS（Vocabulary for Event Recording and Incident Sharing）の攻撃者、攻撃、資産、属性の複雑な組み合わせを表す便利なカテゴリーとして導入しました。その後、脅威の状況は少しずつ変化しているため、今年はDBIRのパターンを一新することにしました。

ご想像のとおり、この決断はDBIR作成チームにとって非常に難しいものでしたが、「ニューコーク」や「クリスタルペプシ」の発売など、大きく大胆で新鮮なビジネスの動きによって示されたリーダーシップから、チームは強さと勇気を得ることができました。

この新しいパターンで、今年分析されたデータ漏洩/侵害の99.3%、分析されたインシデントの99.6%を説明することができます。また、過去に発生した品質に関連したデータ漏洩/侵害の95.8%、品質に関連したインシデントの99.7%を説明することができます[38]。

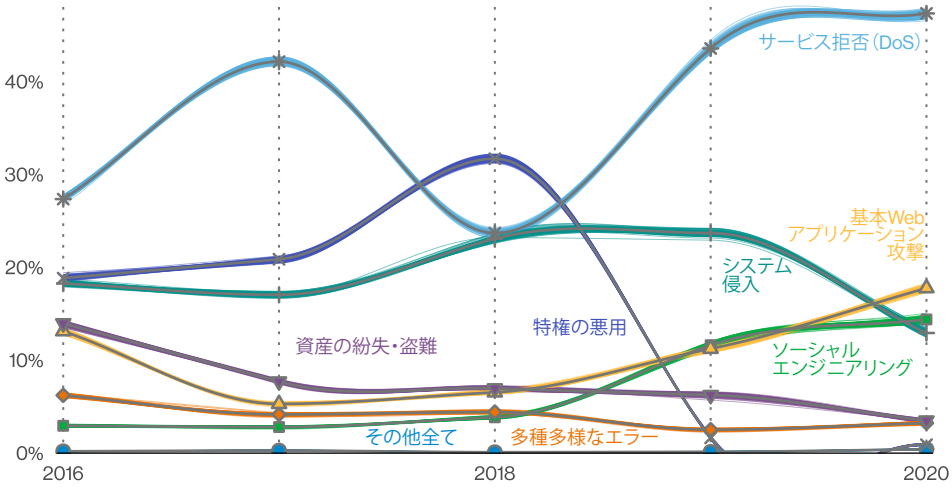


図44. インシデントパターンの経時的変化

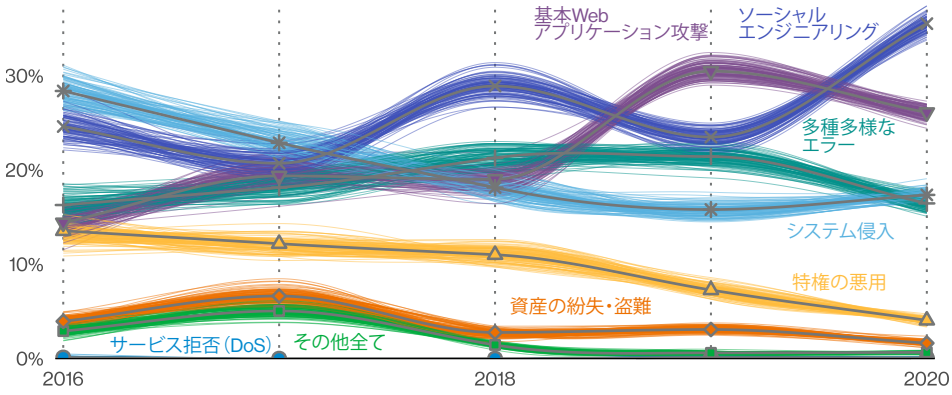


図 45. データ漏洩/侵害パターンの経時的変化

38 最後になりましたが、重要なのは、接触した細菌の99.9%を滅菌できることです（実際はそうはいきませんが）。

もちろん、すべてが変わったわけではありません。「サービス拒否（DoS）」、「基本Webアプリケーション攻撃[39]」、「資産の紛失・盗難」、「多種多様なエラー」、「特権の悪用」、「その他全て」などのパターンは、引き続き今年の調査でも採用されています。一方、「ペイメントカードスキミング」、「クライムウェア」、「サイバースパイ活動」、「POSへの侵入」などのパターンは廃止され[40]、代わりに「ソーシャルエンジニアリング」と「システム侵入」が追加されています。

パターン名に変更がないからといって、中身が同じというわけではありません。例えば、この2021年版の「多種多様なエラー」に割り当てられているものは、2014年版の「多種多様なエラー」に含まれていたものとは限りません。

当初のパターンは、階層的なクラスタリング手法に基づいており、そこからインシデントをパターンに割り当てるための単純なルールを作成することができました。これは非常に規範的なプロセスであり、当時はうまく機能していましたが、ひずみが生じ始めていました[41]。

今度の新しいパターンは、優れた機械学習型のクラスタリング[42]プロセスに基づいています。この決定は様々な意味で賭けでしたが、チームはこのプロセスによるデータを信頼すると約束し、それが功を奏しました。新しいパターンは、明らかに以前の規範的なパターンと同じような位置にありますが、古いパターンでは扱いにくかった複雑なインタラクションルールもうまく捉えています。

図46と図47は、インシデントとデータ漏洩/侵害が新旧のパターン間でどのように推移したかを示しています。まず、説明しやすい変化があります。「資産の紛失・盗難」は、ほとんどが「資産の紛失・盗難」のパターンに属しています。「多種多様なエラー」、「特権の悪用」、「基本Webアプリケーション攻撃」、「サービス拒否（DoS）」についても同様です。まず変わったのは「ペイメントカードスキミング」で、これは完全に「その他全て」のパターンに入りました。もともと現在の「システム侵入」のパターンと類似点があり、その点においてWebアプリケーションとは関係のないペイメントカードの侵害はこのパターンに入れられていました。カードスキミングはシステム侵入とはまったく性質が異なると思われ、明らかに「その他全て」に属するものです。

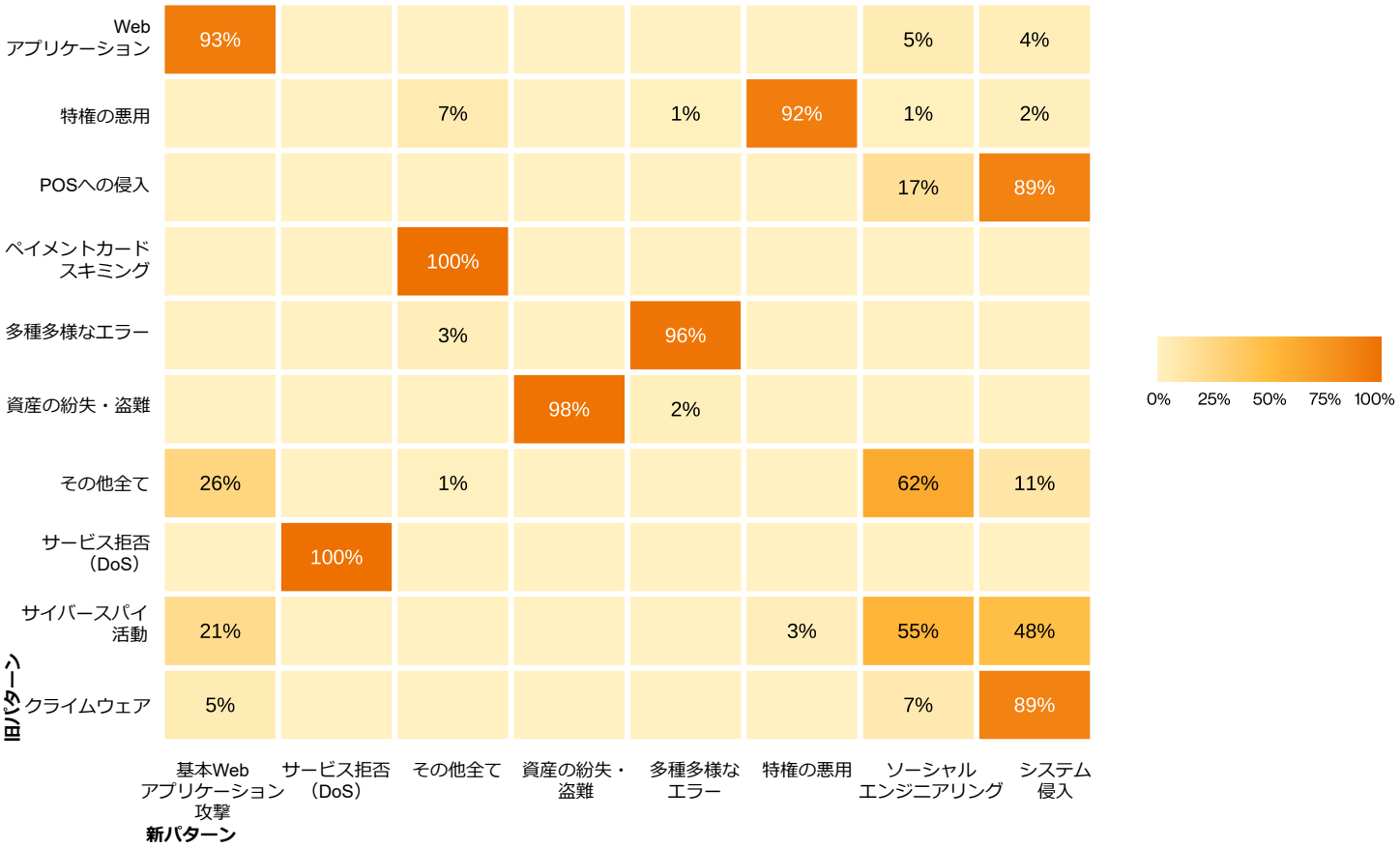


図46. インシデントの新旧パターンの対応関係

39 科学的に厳密なフォーカステストによるリブランディングを経て、一時的に「以前はWebアプリケーションとして知られていたパターン」となりましたが、ベライゾンのブランディング＆コミュニケーション部門からは、それもできないと言われてしまいました。ブランドのマークまで決定し、準備をすべて整えていたのに、愕然としました。

40 最も価値のあるパターン

41 義理の家族と過ごす3連休のようなものです。

42 次のコーナーでは必要以上に詳しくお話します。

さらに興味深い変化は、「PoSへの侵入」、「クライムウェア」、「サイバースパイ活動」、「その他全て」などのパターンです。これらは現在、データ漏洩/侵害の特徴によって定義されています。ソーシャルエンジニアリングが重要な要素だった場合は、新しいソーシャルエンジニアリングパターンに移行します。最初の侵入ポイントがWebアプリケーションであった単純な攻撃の場合、基本Webアプリケーション攻撃に当てはまります。または、もっと手の込んだシステム侵入の場合（攻撃者が気づかれないようにアクセスしてきて、さまざまな場所に攻撃を試すなど）、システム侵入は、Journeyの古い歌のように、両手を広げてこれらの事件を歓迎するのを待っています。このような大きな変更は計画されたものではありませんでした（率直に言って、データが教えてくれることに関しては、DBIRの内容は関係ありません）。しかし、パターンの焦点を変えたことで、これらのパターンのいずれかが業種の上位に現れたときに、より良いガイダンスを提供できるようになりました。「サイバースパイ活動」や「クライムウェア」は、ほとんどの場合、インシデントの複雑さが異なることを示唆していますが、対策する上では、脅威の攻撃者が楽な政府の仕事をしていようが、自由市場に熱狂的な起業家であろうが関係ありません。

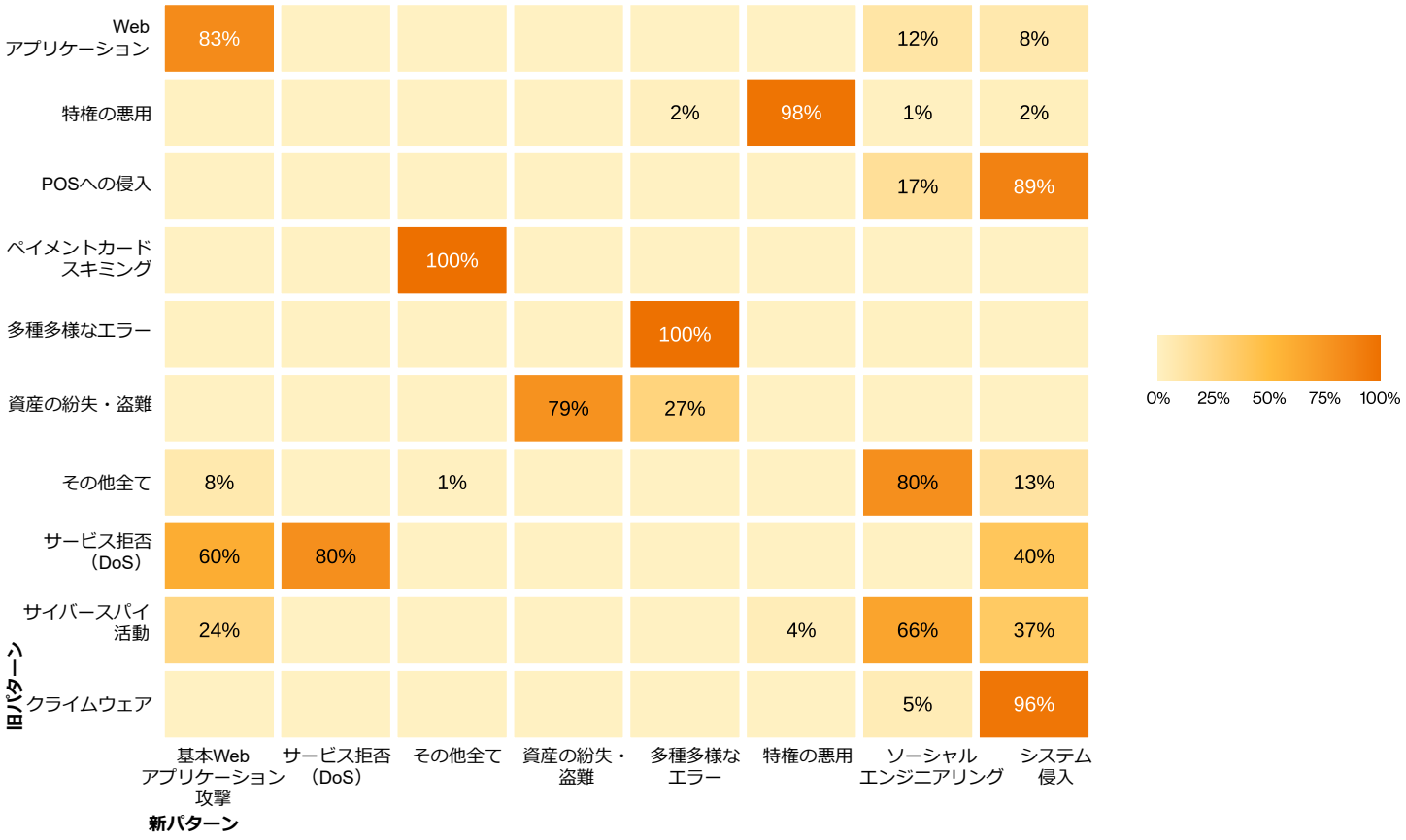


図47. データ漏洩/侵害の新旧パターンの対応関係

このような方法です

新しいパターンの考案は、表面的になぞったものではありません。以前から作業を進めていたものです。DBIRのデータを仕分けるのは、それほど簡単なことではありません。まず、データセットには2,600近い列があり、ほぼ確実に過剰適合の状態になります。2番目に、データのほとんどが絶対的でも連続的でもなく、論理的なものであるため、有効なアプローチが限られます。3番目に、データセットには80万行以上が含まれており、これも有効なアプローチを制限しています。4番目に[43]、クラスタ間で不均衡があることは十分考えられます。インシデントやデータ漏洩/侵害の数が他よりもはるかに少ないクラスタもあるでしょう。5番目に、結果がある程度説明可能である必要がありました。大規模な機械学習の試みでは、常に楽しい命題です。6番目に[44]、どのようなアプローチをとるにしても、データを後から分類するためのルールを作る必要がありました。毎年のようにデータを再クラスタリングするべきではないからです。最後に、精緻なインシデントのニュアンスを把握するために、1つのインシデントを2つ以上のパターンに分類できるようにすることです。これらの要素に加え、正しい情報を得ることの重要性から、DBIRチームはゆっくりと着実に作業を進めてきました。

うまくいった点を紹介する前に、うまくいかなかった点を先に説明します。チームはまず、2014年のパターンのオリジナル手法に似た階層型クラスタリングを行いました。残念ながら、これはあまりにもバランスが悪く、大きな傾向ではなく、小さく類似性の高いものを見つけてしまいました。木を見て森を見ないようなものです。K-meansクラスタリングが理想的ですが、総当たりでの比較が必要なため、データのサイズを考えると、メモリを消費しすぎてしまいます。我々のニーズに十分な数の特徴を使用することで、主成分分析が不利になることはありませんでした。潜在的ディリクレ配分法（Latent Dirichlet Allocation）では若干改善されましたが、まだ十分ではありません。ラッソ回帰（Lasso Regression）とリッジ回帰（Ridge Regression）では、うまく収束しませんでした。アソシエーションルールは、クラスタをうまく区別できず、予測因子とペアにする必要がありました。人工ニューラルネットワーク（ANN）は、予測はできてもクラスタリングはできませんでした[45]。ガウス有限混合モデルによるクラスタリングも試してみましたが、階層型クラスタリングとは逆の問題がありました。森を見て木を見ずといったように[46]。

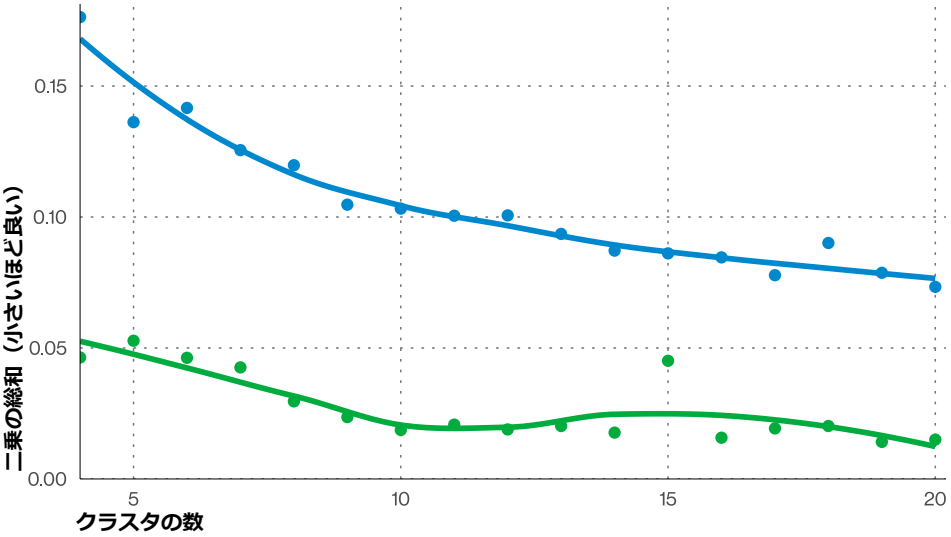


図48. クラスタ数によるモデル評価

最終的に採用したのは球形k-meansの手法でした。球形k-meansは、k-meansのクラスタリングの利点（新しいデータを分類する能力、大小両方のクラスタを見つける能力、過剰適合せずに高次元を処理する能力、論理的なデータを処理する能力、説明可能な能力）を提供する一方で、チームが扱う膨大なデータセットを詰まらせることはありませんでした。通常のk-meansは、データセットのすべての行の間の距離を、列の数の次元空間で計算します。そして、決められた数のクラスタの中心をランダムに作成し、最も近い中心にポイントを割り当てます。その後、各クラスタの中心を再計算し、クラスタのメンバーシップに大きな変化がなくなるまで、この2つのステップを繰り返します。このような距離計算には、多くの時間とメモリが必要です。球形k-Meansでは、余弦距離を計算し、その特別な構造を利用して、完全なオブジェクト間距離行列を計算しないようにすることで、これを改善しています[47]。

43 このリストは3項目しかないと思っていましたが、大変なことになりました。
44 もう1つ？わかりました。大変でした。
45 クラスタリングのためのANN、特に自己組織化マップも試しましたが、これもうまくいきませんでした。
46 初デートや家族の集まり、スーパーボウル®パーティで、好きなだけこの文章を声に出して読んでもかまいません。
47 http://www.stat.cmu.edu/~rnugent/PCMI2016/papers/SphericalKMeans.pdf

これらの新しいパターンは、明確な枠組みを与えてくれます。これによって、私たちは脅威の状況を説明することができ、またこの報告書をお読みいただく方は、組織内の関係者にそれを伝えることができるのです。

それでも、このアプローチがうまくいくと確信するまでには、10個のハイパーパラメータのバリエーションが必要でしたし、モデルを最終的に決定するためには、2021年のDBIRデータに基づいてさらに6つのクラスタバージョンを作成する必要がありました。クラスタ化の対象としたのは、主にVERISの4A（Action：攻撃、Actor：攻撃者、Asset：資産、Attribute：属性）、被害者、対象者、タイムライン、発見方法を扱った517個の列です。

古いインシデントよりも最近のインシデントを優先させるために、過去数年間のデータだけを使用しようとしましたが、最終的には指数関数的な重み付け関数を使用することにしました。Lloyd-[48]Forgy[49]様式の固定小数点アルゴリズムにKernighan-Lin連鎖による局所的な改善を加えたものを使用しました[50、51]。パターンの重なりを求めていましたが、球形k-Meansのファジネスパラメータでは結果が悪かったため、代わりにハードパーティションに設定し、クラスタリング後に、2番目に近いクラスタがメインクラスタとほぼ同じであれば、インシデントを複数のクラスタに含めるようにしました。その結果、新しいパターンがいくつかできました。

これまでの経験から、インシデントデータとデータ漏洩/侵害データは大きく異なることがわかっています。インシデントのサブセットであるデータ漏洩/侵害は、チームの分析ではインシデントよりも何倍も重要です[52]。インシデントとデータ漏洩/侵害の両方がパターンに反映されるように、クラスタリングを2回（それぞれ1回ずつ）実行しました。最適な数のクラスタを選ぶために、いくつかの異なる数のクラスタについて、二乗和（クラスタリングの成功度を示す指標）を計算しました。

次に、線の「折れ」付近で発生するパターンを手作業で調べました（インシデントの場合は5つ程度、データ漏洩/侵害の場合は8つ程度。図48を参照）。最終的には、8個のデータ漏洩/侵害と10個のインシデントのクラスタに落ち着きました。クラスタリングの後、クラスタを調査し、いくつかをグループ化し（「システム侵入」に5つ、「特権の悪用」と「多種多様なエラー」に3つ、「基本Webアプリケーション攻撃」、「ソーシャルエンジニアリング」、「資産の紛失・盗難」に2つ、「サービス拒否（DoS）」に1つ）、名前を付け、新しいパターンとしました[53]。

表2は、これらの作業の結果得られたものです。何も変わっていない箇所もあれば、すべてが変わった箇所もあります。しかし、何よりも重要な点は、これらの新しいパターンは明確な枠組みであり、これによって、私たちは脅威の状況を説明することができ、またこの報告書をお読みいただく方は、組織内の関係者にそれを伝えることができるということです。

ソーシャルエンジニアリング	人を心理的に危険にさらし、行動を起こしたり、機密を破ったりするように人の行動を変化させること。
基本Webアプリケーション攻撃	最初のWebアプリケーション攻撃の後、少数のステップ/追加攻撃を伴う単純なWebアプリケーション攻撃。
システム侵入	システム侵入は、ランサムウェアの展開など、目的達成のためにマルウェアやハッキングを利用する複雑な攻撃。
多種多様なエラー	意図しない行為により、情報資産のセキュリティ属性が直接攻撃されたインシデント。デバイスの紛失はこれには含まれず、盗難に分類。
特権の悪用	正当な特権が許可されていない方法でまたは悪意を持って使用されることで主に引き起こされるインシデント。
資産の紛失・盗難	置き忘れや悪意の有無にかかわらず、情報資産が消失したインシデント。
サービス拒否（DoS）	ネットワークやシステムの可用性を低下させることを目的とした攻撃。ネットワーク層とアプリケーション層の両方への攻撃を含む。
その他全て	この最後の「パターン」は、実際にはパターンではなく、むしろ、他のパターンの秩序ある範囲に収まらないすべてのインシデントが対象[54]。

表2. 新しいインシデント分類パターン

48 Lloyd, Stuart P.（1982）

49 Forgy, Edward W.（1965）

50 Dhillon, Guan and Kogan（2002）

51 これで理解できましたか？正直に言うと、我々はこれらの論文を読んでいません。ただ、ソフトウェアのオプションを選んだだけです。

52 「データインシデント調査報告書」ではなく、「データ漏洩/侵害調査報告書」です。

53 賢明な読者は、私たちが古いパターンを積極的に保持しようとしなかったことに気づくかもしれません。古いパターンがこれだけ多く残っているということは、2014年のパターンの妥当性を証明しています。

54 万が一のために、もう持っていない電子機器のケーブルをすべてとっておく箱のようなものです。

サービス拒否（DoS）

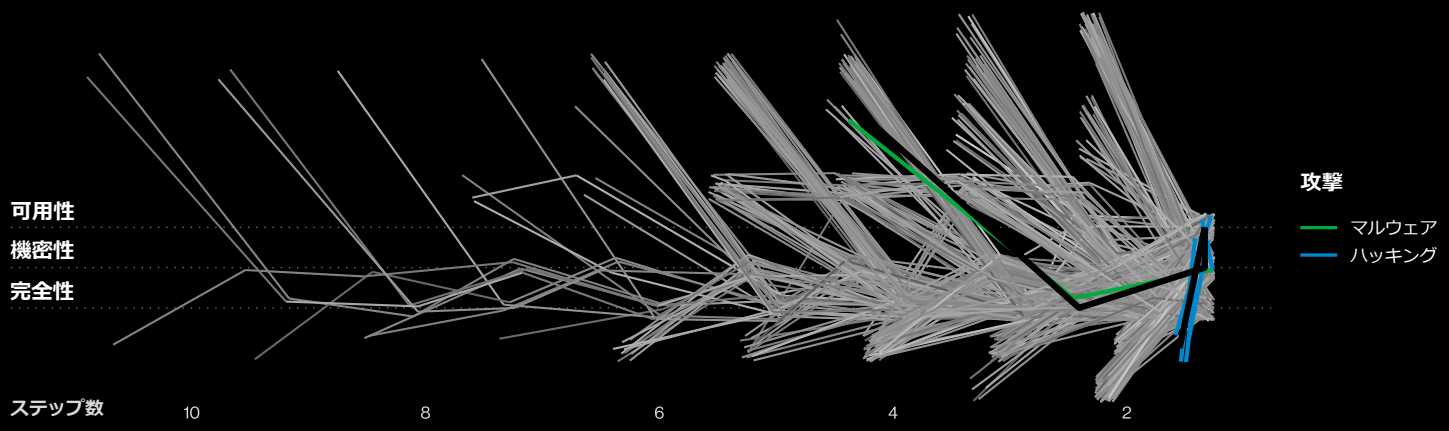


図49. サービス拒否（DoS）インシデントパス（n=5）

サマリー

「サービス拒否（DoS）」パターンは、ネットワークやシステムの可用性を低下させることを目的とした攻撃で構成されています。このパターンには、ネットワーク層とアプリケーション層の両方の攻撃が含まれており、インシデント全体で最も一般的なパターンです。しかし、このパターンは効果的に緩和するのが最も簡単な脅威の1つであることが多いため、多く発生しても気にする必要はありません。

頻度	インシデント14,335件、確認されたデータ暴露4件

サービス拒否（DoS）[55] は、実際に対処可能な情報セキュリティ脅威の1つです。これは、最新の脅威に直面し、どうすれば止められるのか分からず落ち込んでいるときに、自分を奮い立たせるために何かをするものです。確かに、図50にあるように、この脅威は小さいものではありません。実際、これはすべてのインシデントで最もよく見られるパターンです。

しかし、図51を見ると、ビット/秒（bps）の中央値である1.3Gbpsは、ご家庭のインターネット接続よりもほんの少し多いだけかもしれないことに気づくでしょう。インシデントの95%は、13Mbpsから99Gbpsの間で発生しており、容易に軽減できる範囲です。ぜひ、DoS緩和サービスに申し込んで、お目当てのお菓子をゲットしてください。

55 「Denial (The Nile) isn't just a river in Egypt（否定はエジプトの川ではない）」という言い回しがあるように、否定ばかりしていてはいけませんね。

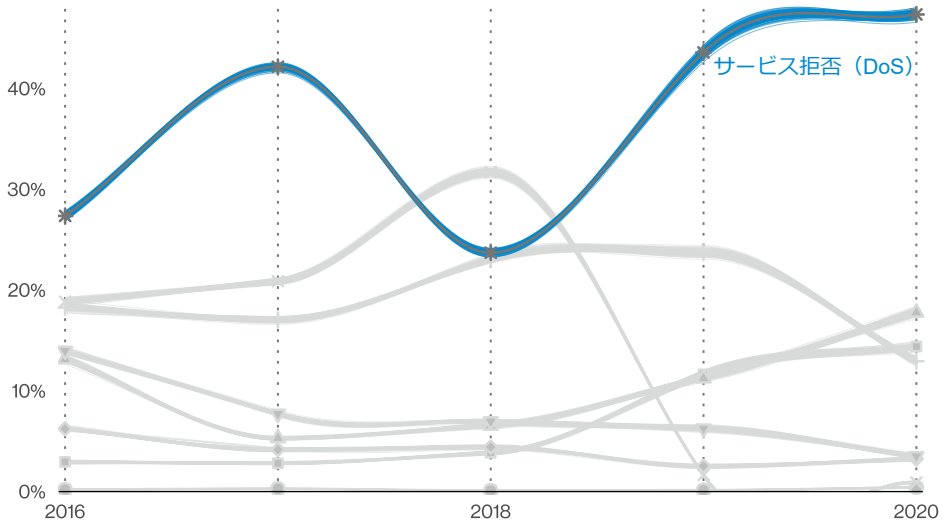


図50. インシデントパターンの経時的変化

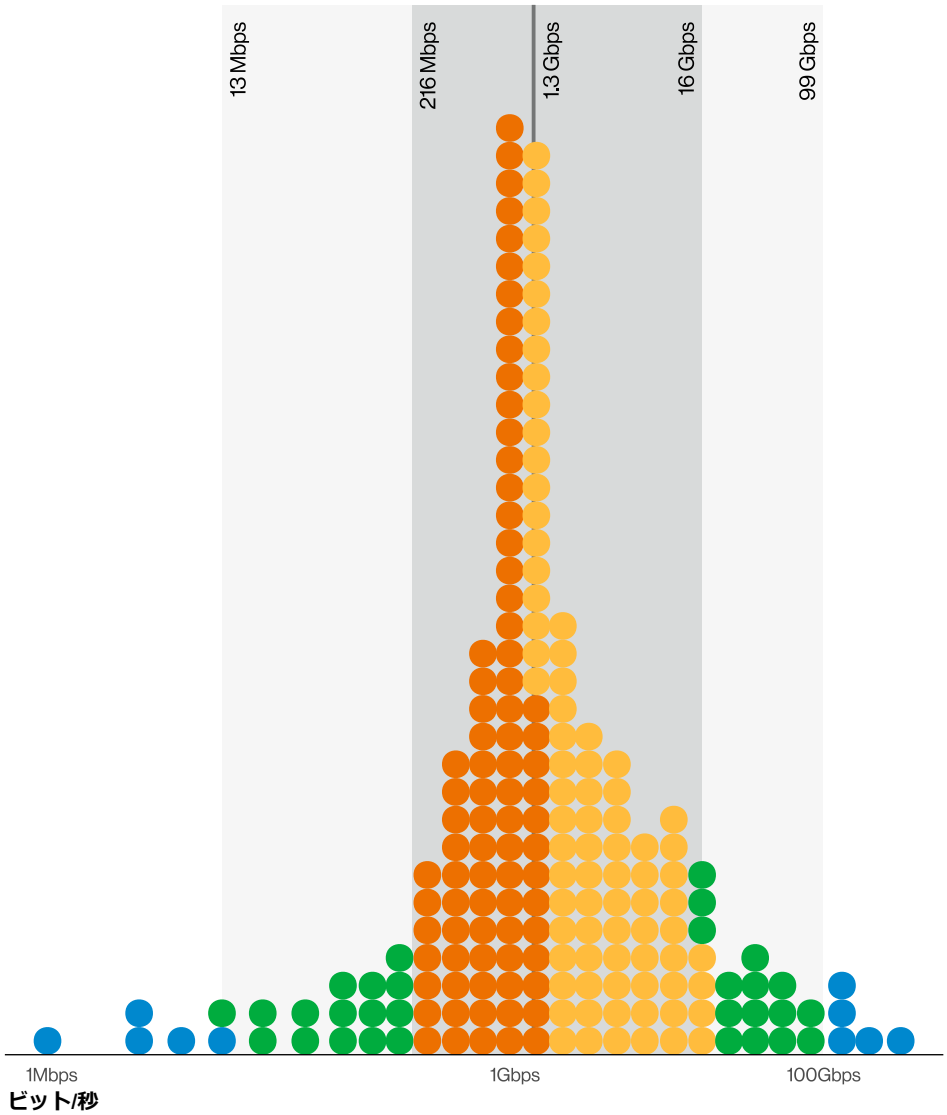


図51. DDoSインシデントにおける1秒あたりのビット数（n=11,306）
1ドット=組織の0.5%

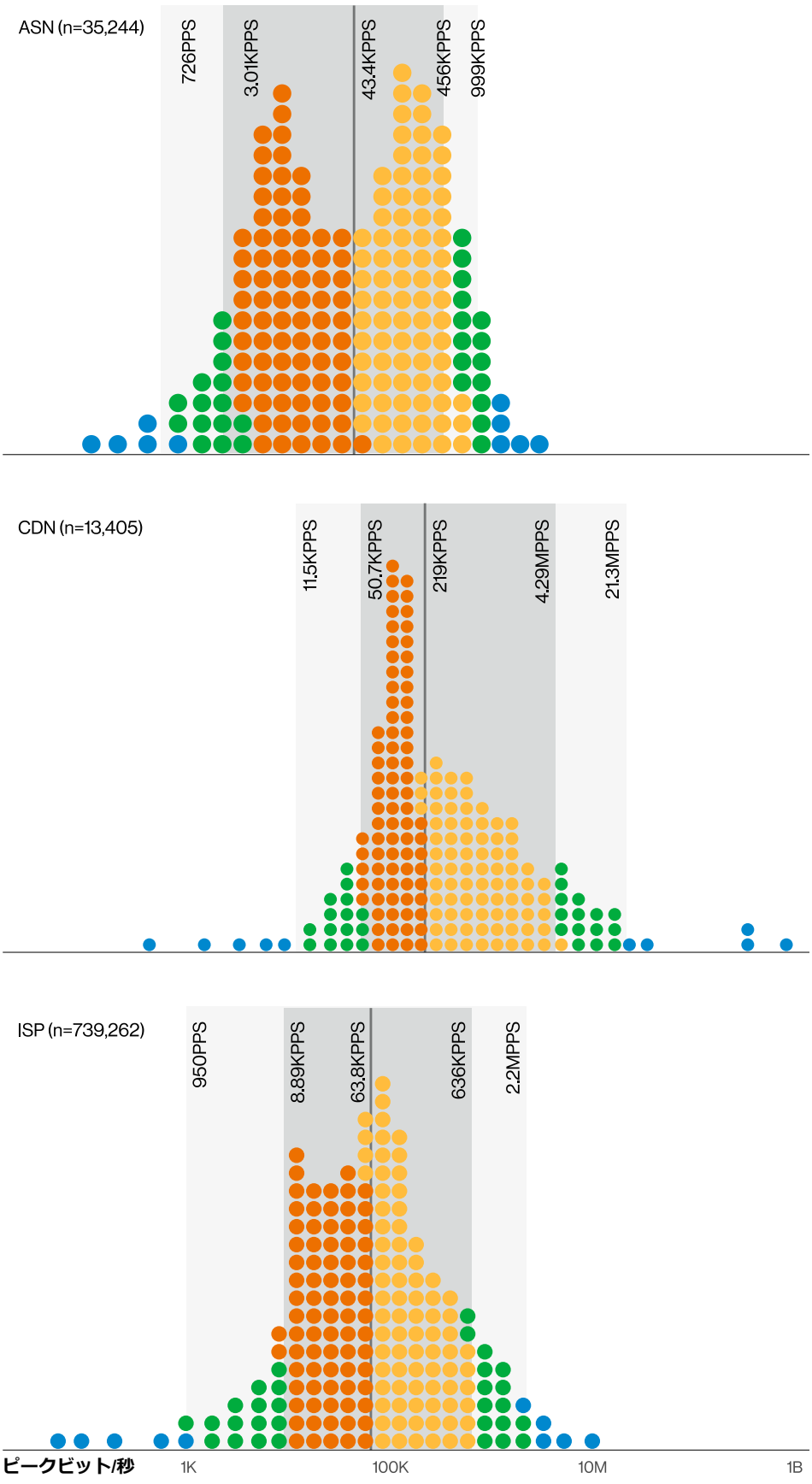


図52. さまざまなDoSの攻撃箇所におけるPPSのピーク
1ドット=組織の0.5%

DDoS攻撃がそれほど脅威ではない理由の1つは、これらの平均[56]パケットがあなたに届くまでに、多くのインターネットを経由しなければならないことです。図52は、DDoS攻撃が、スタート地点のインターネットサービスプロバイダ（ISP）から、中間地点の自立システム番号（ASN）、そしてユーザのサイトの直前にあるコンテンツ配信ネットワーク（CDN）に至るまで、様々な場所でどの程度ブロックされているかを示しています。これらすべてが、攻撃を軽減する役割を担っています。

図53は、いくつかの異なるタイプの攻撃について簡単に説明しています。DoS攻撃には、直接攻撃（攻撃者やボットネットから直接パケットが送られてくる）と、間接攻撃（攻撃者は脆弱なサービスにパケットを送信し、そのサービスが被害者にパケットを転送する）があります。また、リソースの枯渇を目的としたもの（メモリや処理に異常な負荷を与えるパケットを送信する）や、大量のパケットを送信するものなどがあります。図から分かるように、攻撃の種類によって大きな違いはありません（率直に言えば、1つのDDoS攻撃[57]で複数の攻撃が可能です）。

PPS（パケット/秒）とBPS（ビット/秒）の間を少しずつ行き来しています。主に入手可能なデータに基づいてこのような操作をしていますが、もし今、読者の中にそのことで夜も眠れない方がいるのであれば、その不安を解消したいと思います[58]。任意のパケットタイプ（いくつかあります）に対して、パケットに期待できるバイト数には一定の範囲があります。このことは、図54に示した直線的な性質を見ればわかります。このように、BPSであってもPPSであっても、結論は同じです。

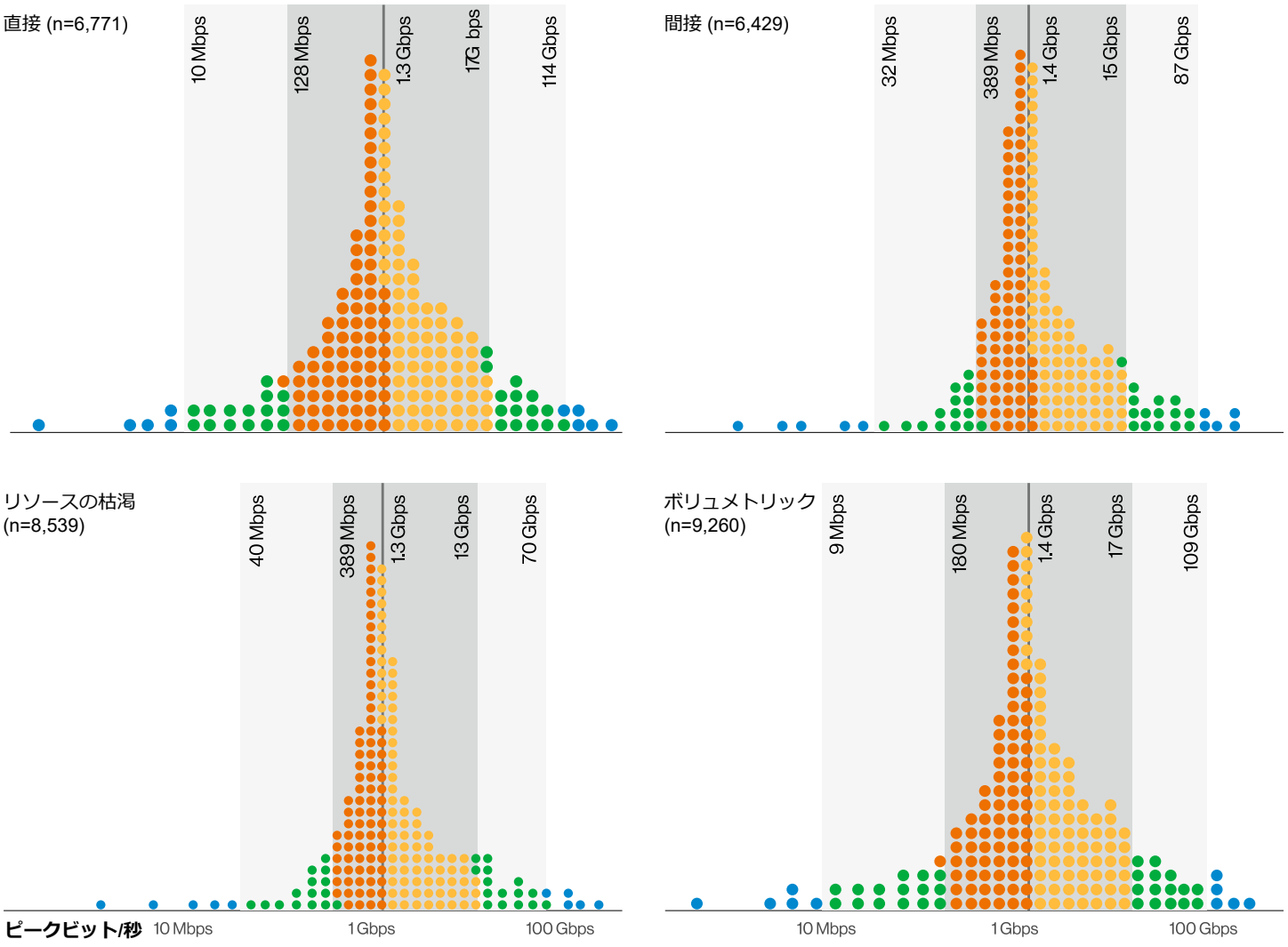


図53. さまざまなDoSタイプにおけるピークBPS

56 平均的な平均ではなく、悪意のある平均。

57 実際のところ、DDoS攻撃とは何なのでしょうか。最初のパケットで始まり、最後のパケットで終わるのでしょうか？どうやってわかるのでしょうか？同時に別のボットネットからの攻撃だったらどうでしょう？また、数秒間停止した後、再び開始された場合は？あるいは...あるいは....DBIRの脚注はいつからWikipediaのディスカッションページになったのでしょうか？

58 比喩的にも、文字通りにも。

図54. DoSの1件あたりのPPSとBPSの関係

図55では、1秒あたりのDDoSパケット数の均等性を知ることができます。これを見ると、大多数の組織では、データがかなりとがっていることがわかります。図 56 は、450,000 件の DDoS 攻撃で鍛えられた回帰型ニューラルネットワーク（RNN）の予測値です。このネットワークは、平均的なDDoS攻撃のタイミングを予測しますが、DDoS攻撃が平均的でない場合は予測に失敗します。だから次のDDoSを予測することに時間を費やす必要はありません。予測できないわけですから。サービスに対処を任して、休憩していればよいのです。

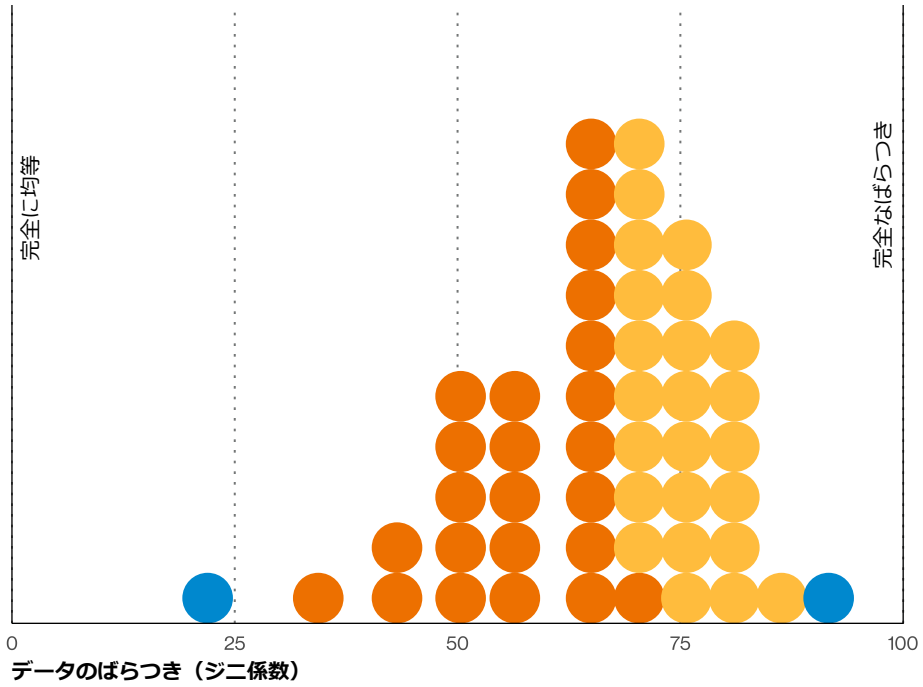


図55. 組織別のDDoS PPSのばらつき（n=54）
1ドット=組織の2%

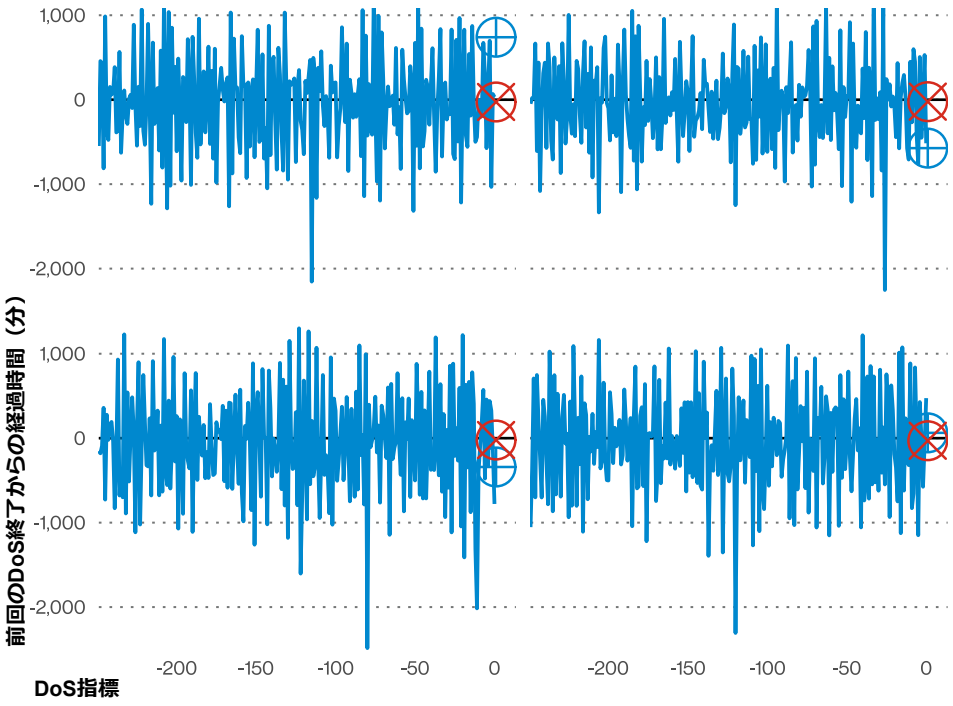


図 56. 次のDDoSを予測するように訓練されたRNNの予測値

資産の紛失・盗難

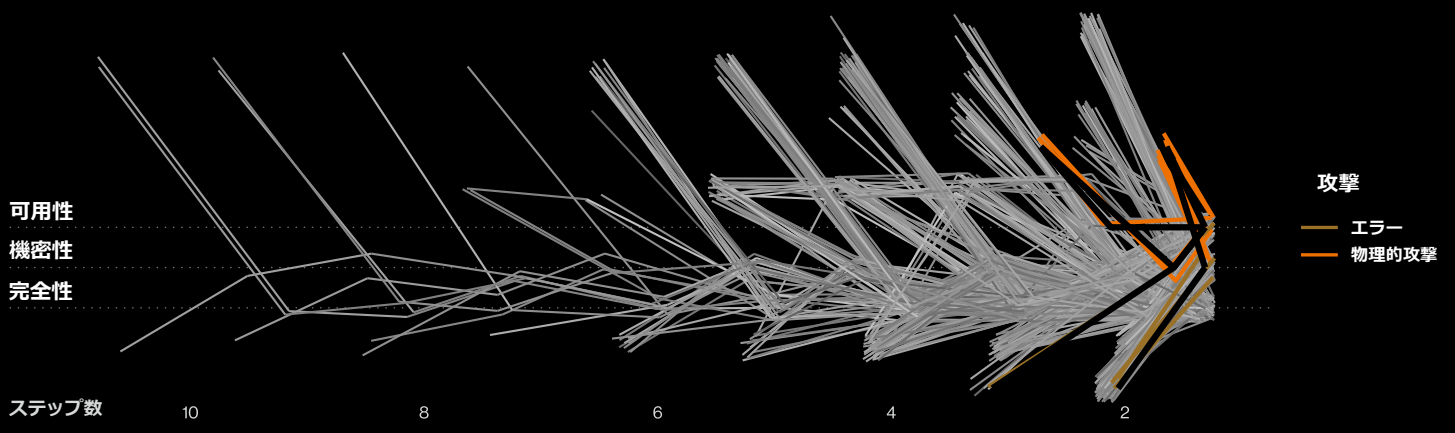


図 57. 資産の紛失・盗難のインシデントパス（n=13）

サマリー

デバイスの紛失や盗難は後を絶たず、このパターンがすぐに変わることはないでしょう。攻撃者が内部（紛失）であっても外部（盗難）であっても、これらのデバイス上のデータを保護するためのコントロールに変わりはありません。

頻度	インシデント1,295件、確認されたデータ暴露84件
攻撃者	外部（87%）、内部（17%）、複数の関係者（5%）、パートナー（1%）（漏洩/侵害）
攻撃者の動機	金銭目的(100%)（漏洩/侵害）
攻撃を受けたデータ	個人情報（80%）、医療情報（43%）、銀行情報（9%）、その他（7%）（漏洩/侵害）

ポケットやバッグの中の携帯電話に手を伸ばしたときに、携帯電話がなくなっていることに気づく、そんな沈んだ気持ちを誰もが経験していることでしょう。慌てて家中を探し回ったり、クッションをひっくり返したり、近くにいる人に電話をかけてもらったりした結果、最初から持っていたことがわかった、というのは私たちだけでしょうか。

いずれにしても、何千もの個人情報や仕事関連のファイルが入った小さなデバイスを置き忘れることに対するこの根源的な恐怖は、このパターンのデータ漏洩/侵害やインシデントに共通するテーマの1つです。パソコン、書類、USB機器、携帯電話などが、誤って、あるいはそれ以外の理由で消えてしまうことがあります。今年取り上げた多くのパターンやインシデントと同様に、コロナ厄災が世界中に広がっていく過程で人々がどのように仕事の習慣を進化させてきたかという2020年のこの特殊な状況を念頭に置いてください。

何千もの個人的なファイルや仕事関連のファイルが入っている小さなデバイスを置き忘れることに対するこの根源的な恐怖は、このパターンの侵害やインシデントの共通テーマの1つです。

特に、どこで、どのように仕事をするかということが資産の紛失・盗難に関わっています。また、ここでの調査結果は、必ずしも代表的な年のもとは言えないため、すこし割り引いて考える必要があるかもしれません。それでは、データを見てみましょう。

恒常的な盗難とエラー

この1年でさまざまなことが変化しましたが、このパターンでは大きく変わらないものもあります。その1つは、インシデントにおいて「エラー」が「盗難」を上回っていることです。DBIRのデータでは、例年と同様に、社内のユーザが誤って資産を紛失して報告するエラーの方が、資産が盗まれたと報告する人よりも圧倒的に多くなっています。しかし、組織にとって問題となるのは、どちらもほとんど同じです。そのデバイスに何のデータが入っていたのか、どのように保護されていたのか、どのように対処するのかを知る必要があります。どちらにしてもデバイスをリモートワイプしなければならないので、このようなケースで区別を付けることはほとんど無意味なことです。

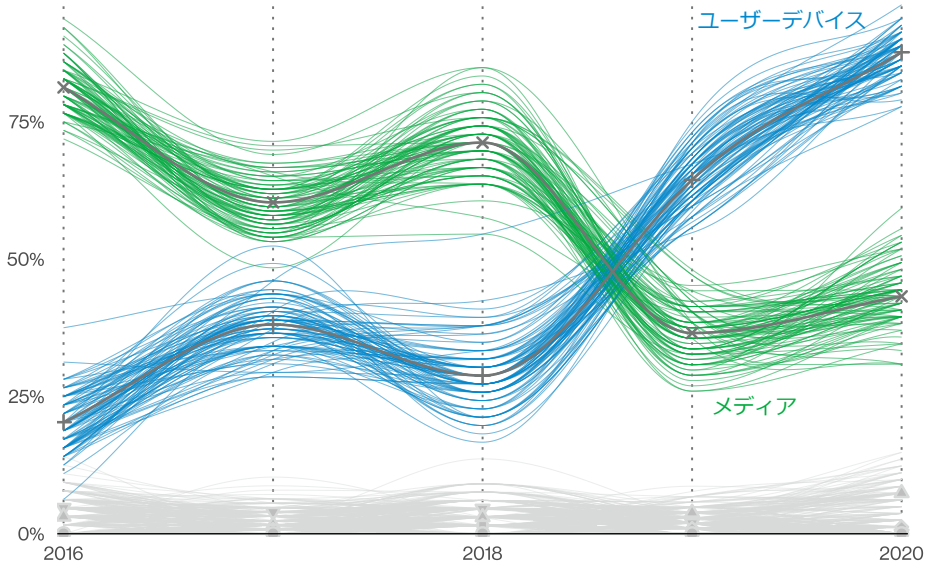


図58. 資産の紛失・盗難によるデータ漏洩/侵害における資産の経時的変化

データ漏洩/侵害の原因は紙かシリコンか？

ここ数年の傾向として、紛失・盗難によるデータ漏洩/侵害の主な原因が、書類などの紙媒体を含んだメディアから携帯電話などのユーザーデバイスへと移行していることが挙げられます。デジタルトランスフォーメーションがいつ起こったかを示すバロメーターが必要だとしたら、おそらく2019年にさかのぼるでしょう。この年、DBIRのデータセットで史上初めて、ユーザーデバイスがドキュメントよりも頻繁に盗難・紛失に遭ったのです。今年は、データ開示で判明しているデータ漏洩/侵害された資産の約43%が紙媒体で、残りはデスクトップとラップトップでした（図58）。侵害が確認されたかどうかわからないインシデントでは、携帯電話の紛失・盗難が最も多くなっています。ギャンブル好きというわけではありませんが、もしこの傾向が続くかどうかにお金を賭けるとしたら、おそらく「続く」に賭けるでしょう。というのも、多くの新しい組織、学校、企業がリモートワークに素早く移行しなければならなかったからです。

既知のデータ漏洩/侵害の大半で失われたデータの種類は、個人データであり、次いで医療データとなっていますが、これはさほど驚くべきことではありません。プライバシー侵害の情報開示（医療、その他）に関する法律の多さを考えれば、このようなデータがDBIRに出てくるのも無理はありません。最後に、資産の紛失や盗難を発見については（図59）、次世代AIではなく、従業員自身による発見が一番多くなっています。資産の紛失や盗難があった場合、簡単に組織に報告できる手段を従業員に提供するようにしましょう。例えば、携帯電話を紛失しても、電話番号があれば電話をかければ… いや、かけられませんね。とにかく報告が早ければ早いほど、組織はより良い対応ができます。「後悔先に立たず」です。

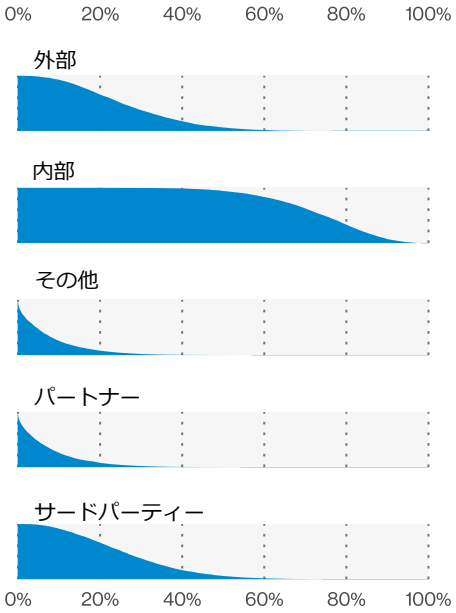


図59. 資産の紛失・盗難によるデータ漏洩/侵害における発見方法（n=9）

多種多様なエラー

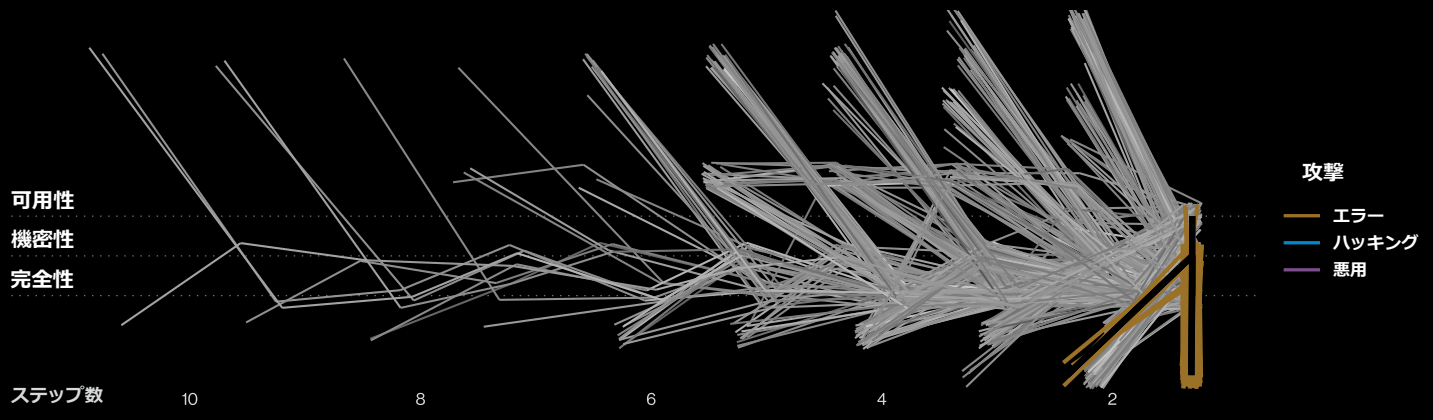


図 **60.** 多種多様なエラーのインシデントパス（n=126）

サマリー

エラーとは意図しない行動のことで、通常は内部の攻撃者が行うものですが、パートナーの攻撃者によるエラーも発生します。セキュリティ研究者によって発見されるデータベース資産の誤設定は、ますます大きな問題となっています。また、従業員が誤った宛先にデータを送信することも引き続き重要な問題です。

頻度	インシデント919件、確認されたデータ暴露896件
攻撃者	内部（99%）、パートナー（1%）、複数の関係者（1%）（漏洩/侵害）
侵害されたデータ	個人情報（79%）、医療情報（17%）, その他（13%）、銀行情報（13%）, 認証情報（13%）（漏洩/侵害）

「多種多様なエラー」パターンは、昔からの馴染みのある敵と言えます。このパターンは最初から含まれていて、エラーの内容も一定しています。このパターンについては何を言えばよいのか難しいところです。人間は、しばしば大きなミスを犯します。このパターンの攻撃者は、内部および／またはパートナーのみで構成されています。

内部の攻撃者の内訳を図61に示しますが、システム管理者と開発者については比較的直感的に理解できます。どちらも、通常、自分たちが保守しているシステムのデータに特権的にアクセスできるためです。しかし、「多くを与えられた者は、多くを期待される」という格言がここでも確実に当てはまります。システム管理者や開発者がミスを犯した場合、その範囲は平均的なエンドユーザのミスよりもはるかに大きな意味を持つことが多いのです。

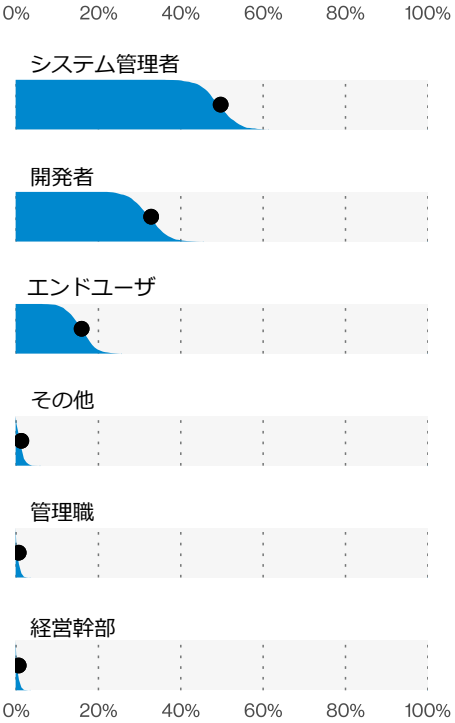


図 61. 多種多様なエラーのデータ漏洩/侵害における内部攻撃者の種類（n=157）

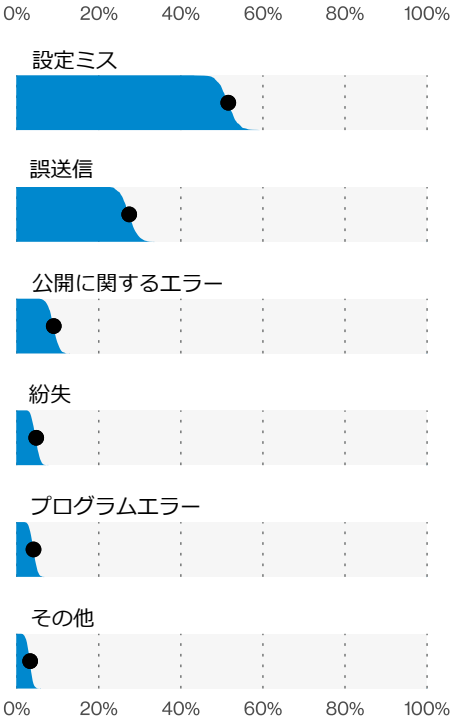


図62. 多種多様なエラーのデータ漏洩/侵害における上位エラーの種類（n=609）

図 63. 多種多様なエラーのデータ漏洩/侵害における発見方法の種類（n=110）

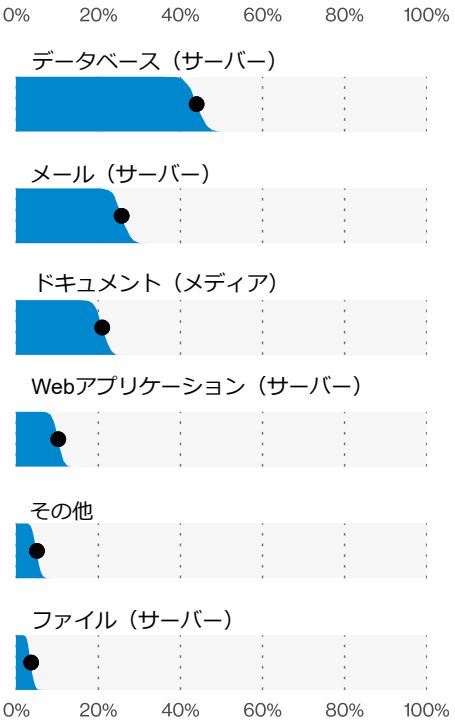


図64. 多種多様なエラーのデータ漏洩/侵害における上位の資産の種類（n=635）

残念なことに、誤送信は依然としてデータセットの中で健在であり、これらのデータ漏洩/侵害の多くは電子データのみ（例：誤った配信リストへのメール送信）ですが、紙の文書によるものもかなりあります。

ワインとチーズの組み合わせはありませんが、攻撃者と攻撃の組み合わせを見ていきましょう。システム管理者および開発者と「設定ミス」のさまざまな種類の組み合わせを考えると（図62）、この組み合わせが組織のデータ、あるいは顧客や従業員のデータの機密性に大打撃を与える可能性があることが想像できます。

もう1つの組み合わせは、データストア（リレーショナルデータベースやドキュメントデータベース、クラウドベースのファイルストレージなど）が管理されずにインターネット上に置かれており、それを検索するセキュリティ研究者との組み合わせがよく見られます（図63）。このような好ましくない組み合わせは、ここ数年増加傾向にあります。

残念なことに、誤送信はデータセットの中で健在であり、これらのデータ漏洩/侵害の多くは電子データのみ（例：誤った配信リストへのメール送信）ですが、紙の文書によるものもかなりあります（図64）。これらは、大量の一斉郵送が顧客層への情報伝達手段として好まれている業界で特に多く見られます。例えば、封筒の宛先が中身と合わなくなってしまうというものです。これらの事象の多くは、封入プロセスのさまざまな時点で基本的なサンプルチェックを行うことで回避できるものです。それにもかかわらず、このような現象が定期的に発生していますが、請求書についてはほとんど発生していません（請求書はいつも予定通りに届いていたようです）。

これらのケースで開示されてしまうデータの種類としては個人情報が最も多く、群を抜いています。

エラー行為に関わる資産は、前述の設定ミスのあるデータベースから、紙媒体の書類やユーザのデバイスまで、多岐にわたります（図64）。このうち一定の部分は資産の損失によるものですが、データへの不正アクセスが確認できないようにデバイスが設定されている場合は、データ漏洩/侵害ではなくインシデントとみなされます。

これらのケースで開示されてしまうデータの種類としては個人情報が最も多く、群を抜いています（図65）。医療データもこのような形で漏洩されますが、それほど多くはありません。その他のデータタイプにおける漏洩件数は非常に少ないです。

図66の素晴らしい発見のタイムラインを見てみてください。数時間から数日の間に発見されたすべてのデータ漏洩/侵害が、どのように折り重なっているかわかりますか？きっとこれは、探索コントロールが成功した物語なのでしょう。実際には、人々は通常、自分がミスったとすぐに気づくからかもしれません。しかし、万が一気づかなかったとしても、インターネット上で専用の検索エンジンを使ってミスを探している熱心なセキュリティ研究者の軍団がいるという安全策があるのです。

図65. 多種多様なエラーのデータ漏洩/侵害における上位データの種類（n=839）

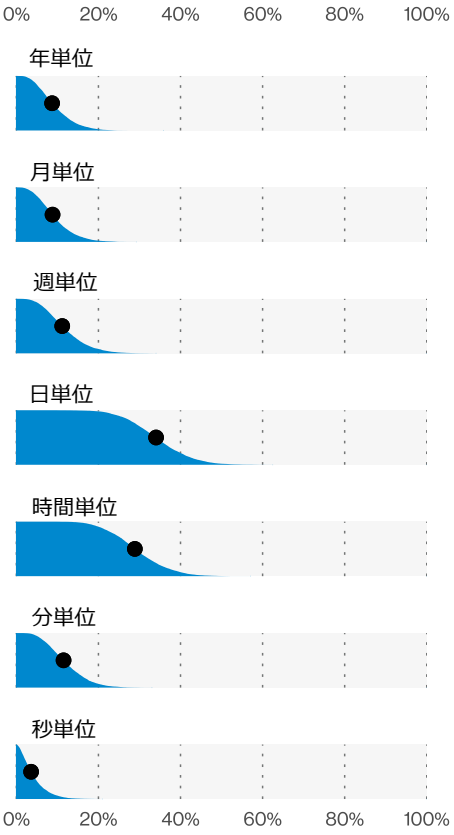


図66. 多種多様なエラーのデータ漏洩/侵害における発見のタイムライン（n=39）

特権の悪用

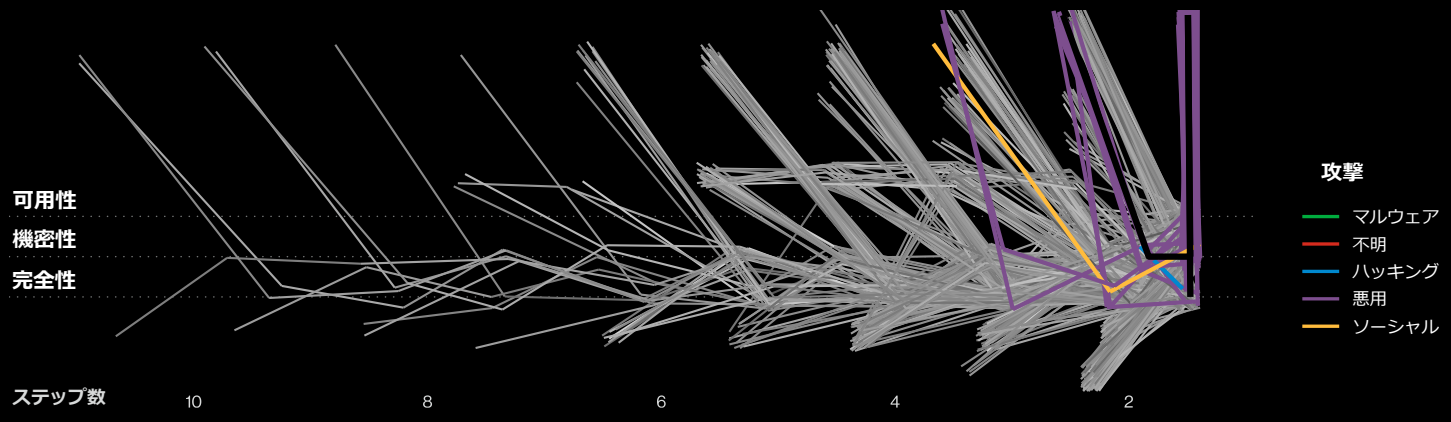


図 67. 特権の悪用のインシデントパス（n=51）

サマリー

このパターンでは、特権を不正に使用するタイプが最も多く、犯行の大半は金銭的な動機によるものでした。盗まれたデータの種類は個人情報が最も多く、やや意外なことに、リモートワーカーの増加は特権の悪用に目立つほどの影響を与えていないようでした。

頻度	インシデント265件、確認されたデータ暴露222件
攻撃者	内部（99%）、複数の関係者（9%）、外部（8%）、パートナー（2%）（漏洩/侵害）
攻撃者の動機	金銭目的（64%）、愉快犯（17%）、怨恨（14%）、スパイ活動（9%）、自己都合（3%）、イデオロギー（1%）（漏洩/侵害）
侵害されたデータ	個人情報（64%）、その他（35%）、医療情報（27%、 内部情報（19%）（漏洩/侵害）

このパターンは、信頼を寄せている人から裏切られるという不快なものです。特権の悪用とは、同僚が（さまざまな理由で）自分のアクセス権を奪い、そのアクセス権を使って権限のないデータを盗み取ったり、絶対にすべきでない方法で使用したりすることです。

これが悪意のある内部攻撃者のパターンであり、「シンデレラ物語」で言えば、純粋無垢な「多種多様なエラー」パターンの邪悪な義姉妹というところでしょうか。「多種多様なエラー」はちょっと不器用なところがありますが、「特権の悪用」はシンデレラが舞踏会に参加できないように、次から次へ雑用を押し付けてきます。

さて、この比喩はここで終わりにして、先へ進みましょう。サマリーの一覧表を見ると、不正使用があった場合、ほとんどのケースでデータ漏洩/侵害が確認されています。これらのほとんどは内部の関係者（ときにはパートナー）によるものですが、このパターンでは、複数のタイプの関係者が協調している証拠が頻繁に見られます。

内部犯行者の多くは、窃取したデータから現金を得ようとする欲に駆られています。ウケ狙いでやる人、または雇い主に恨みをもってやる人もいますが多くありません。そして最後に、競合するビジネスを始めるため、または次の雇用主に利益をもたらすためにやっている人たちもいました。ただし最後の3つは全体のごく一部であり、やはりここで注目すべきは、信頼できるアクセス権が付与されているかどうかにかかわらず、ほとんどが金銭的な動機を持っているということです。

犯行者の行動様式

「特権の悪用」パターンで最も多いのは特権の不正使用です(図68)。次に多いのは「データの誤操作」でした。なお、「その他」は、残りの種類を足したものです。これらの攻撃パスの大半は、ネットワークを利用した、資産への何らかのアクセスとされています。パンデミックの影響でリモートワークが増えていることから、自宅で不正使用を行う者がかなり増えると予想されました。しかし、リモートアクセスによる不正行為の増加は見られませんでした。これは、ケースを分析する際に詳しい内容がデータに含まれていなかったか、あるいは組織がこのアクセス経路を検出して報告することができなかっただけかもしれません。

これらのケースではさまざまな種類のデータが盗まれました。図69に示すように、個人情報が最も多く、その他にも医療情報、内部情報、銀行情報、さらには機密情報なども盗まれています。通常、どの種類のデータが盗まれるかは、個人がアクセスできるデータの種類によって決まります。

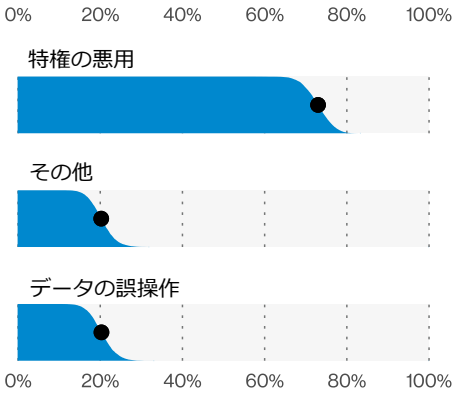


図68. 特権の悪用によるデータ漏洩/侵害における上位の悪用の種類（n=175）

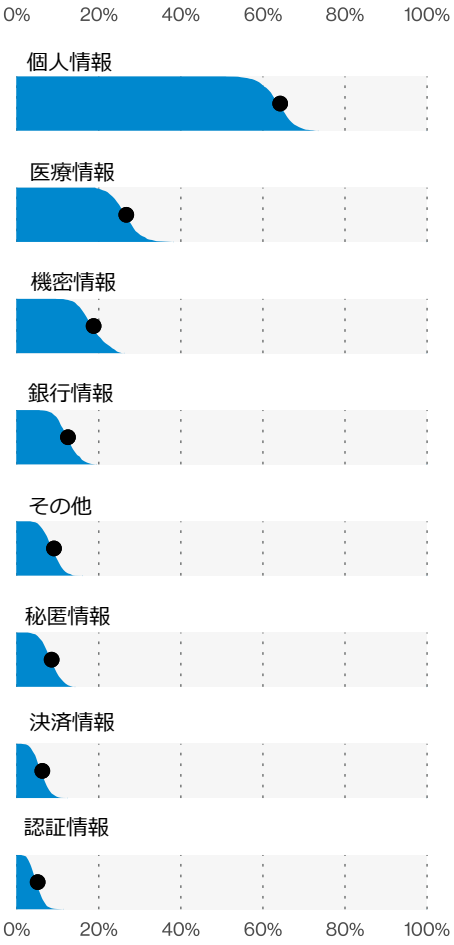


図69. 特権の悪用によるデータ漏洩/侵害における上位のデータの種類（n=176）

すべての検出

「タイムライン」のセクションで述べたように、不正使用によるデータ漏洩/侵害は検出が困難な場合があります。このパターンの検出のタイムラインをデータセット全体と比較すると、この点がよくわかります。特権の悪用のケースは、特権の悪用以外のケースよりも検出に数年かかるケースが多いのです（図70および71）。

今年の不正使用のケースでは、最も長い3つのタイムライン（数週間、数ヶ月、数年）がそれぞれ同程度であることがわかります。実際には、ほとんどの組織は、外部から侵入しようとする者を発見することを主眼に置いて管理を行っています。しかし、医療機関のように極めて機密性の高いデータを持ち、報告が義務づけられているなどの規制要件がある組織では、このような特権の悪用を迅速に発見できる探査コントロールの必要性が示されています。それが実施され、テストされるまでは、これまでの方法で盗みを続ける人がいるでしょう。

図70. 特権の悪用における発見のタイムライン（n=22）

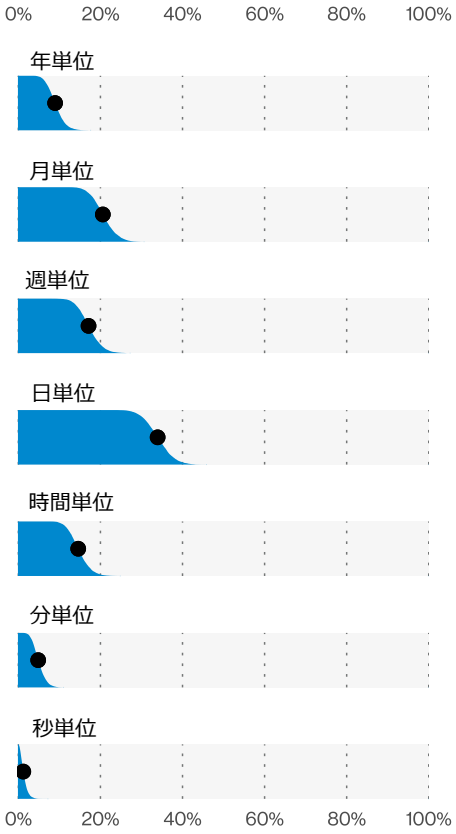


図71. 2021年のデータ漏洩/侵害における発見のタイムライン（n=195）

ソーシャルエンジニアリング

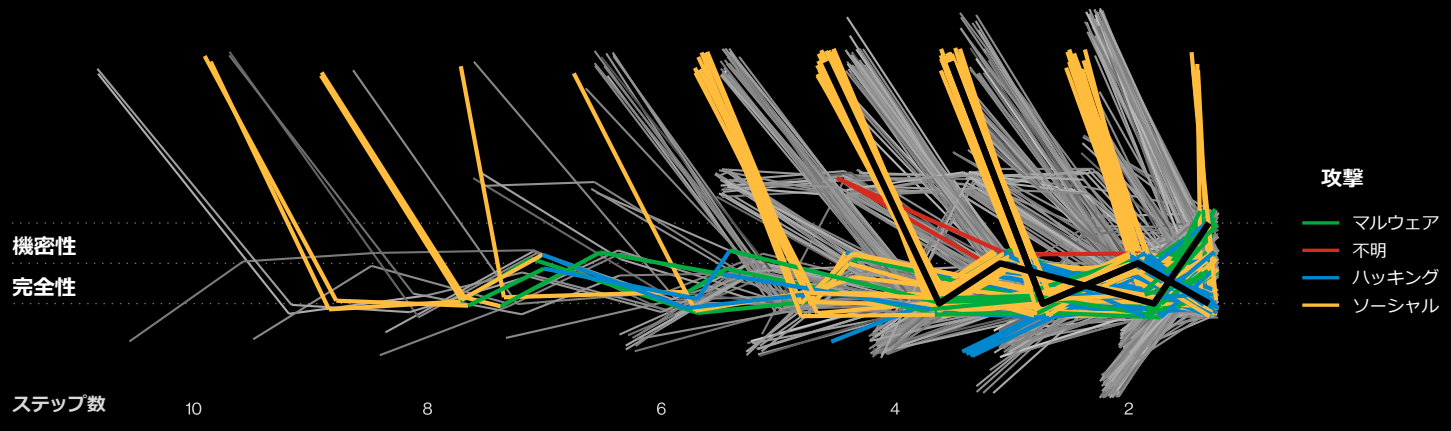


図 72. ソーシャルエンジニアリングのインシデントパス（n=103）

サマリー

このデータ漏洩/侵害パターンの大部分を占めるのはフィッシングであり、クラウド型のメールサーバーが標的になっています。2番目に多い形態は、ビジネスメール詐欺（BEC）です。この攻撃シナリオは、急速に増えている「詐称」を反映しており、ソーシャルエンジニアリングのインシデントは昨年の15倍になっています。さらに、ソーシャルエンジニアリング攻撃では、認証情報が奪われる機会も多くなっています。このパターンでは、盗まれた認証情報がハッキングとマルウェアの両方の攻撃で使用されました。

頻度	インシデント3,841件、確認されたデータ暴露1,767件
攻撃者	外部（100%）（漏洩/侵害）
攻撃者の動機	金銭目的（95%）、スパイ活動（6%）（漏洩/侵害）
侵害されたデータ	認証情報（85%）、個人情報（17%）、その他（9%）、医療情報（4%）（漏洩/侵害）

子供たちといっしょに長い時間過ごしたことのある人は、ソーシャルエンジニアリングをよく知っています。子供たちが親や兄弟を説得して自分たちのやり方で物事を進めようとするのを見るのは、とても楽しいものですが、これがまさにソーシャルエンジニアリングです。彼らを責めるわけではありません。誰もが人よりも先に行こうとするものです。しかし、攻撃者が3歳であろうと30歳であろうと、必要とする理由をうまく説明してきたからというだけで、自分が持っていたものは渡したくありません。

2017年以降、ソーシャルエンジニアリングによるデータ漏洩/侵害は全体的に増加傾向にあり、昨年から急増していることは間違いありません。ここ数年は、クラウド型メールサーバーへの攻撃の増加と相関しているようです。ただし、なぜ電子メールが攻撃者にとって魅力的なのかは判明できていません[59]。もしかしたら、メールアドレスそのもののためかもしれませんし、メールアドレスに含まれる内部情報のためかもしれません。また、認証情報や個人情報などの収益化が可能な情報のためかもしれません。あるいは、単にサーバーを再利用して、より悪質なメールを送信したいと考えているのかもしれません。わからないときは認めたほうがいいこともあります。

おそらく、すべてのソーシャルエンジニアリングのインシデントにソーシャルを利用した攻撃があっても驚くことではありませんが[60]、図72にあるように、マルウェアとハッキングも同様に増えてきています。

59 昔のDEFCONで生まれた格言のように、壇上の人（この場合は報告書の作成者）は、おそらく部屋の中で最も賢い人ではありません。もしかしたら、この場合、最も賢いのはあなたかもしれません。もしあなたが、攻撃者が侵害したメールアカウントで何をしているかを示すデータを持っているなら、我々に声をかけてください。

60 ほとんどがメールで配信されています。

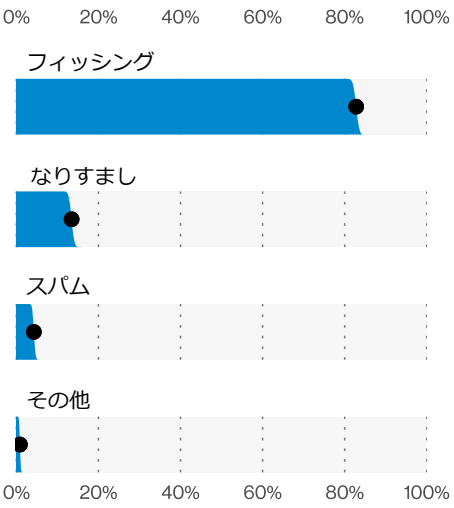


図73. ソーシャルエンジニアリングインシデントにおける上位のソーシャルの種類（n=3,810）

ソーシャルエンジニアリングによるデータ漏洩/侵害の多くは認証情報を盗みますが[61]、いったん認証情報を手に入れると、その盗み出した認証情報を有効に活用できます。これはまさにハッキング行為です。その一方で、フィッシングメールには、トロイの木馬やバックドアなどのマルウェアが添付されていることがあります（図74）。

例年と同様、ソーシャル攻撃は主にフィッシングですが、通常BECに関連する「なりすまし」[62]も目立っています。子供たちが親や兄弟を説得しようとする場面を思い出してください。これはその大人バージョンであり皆さんの所有物を狙って攻撃者が説得しようとしているのです。

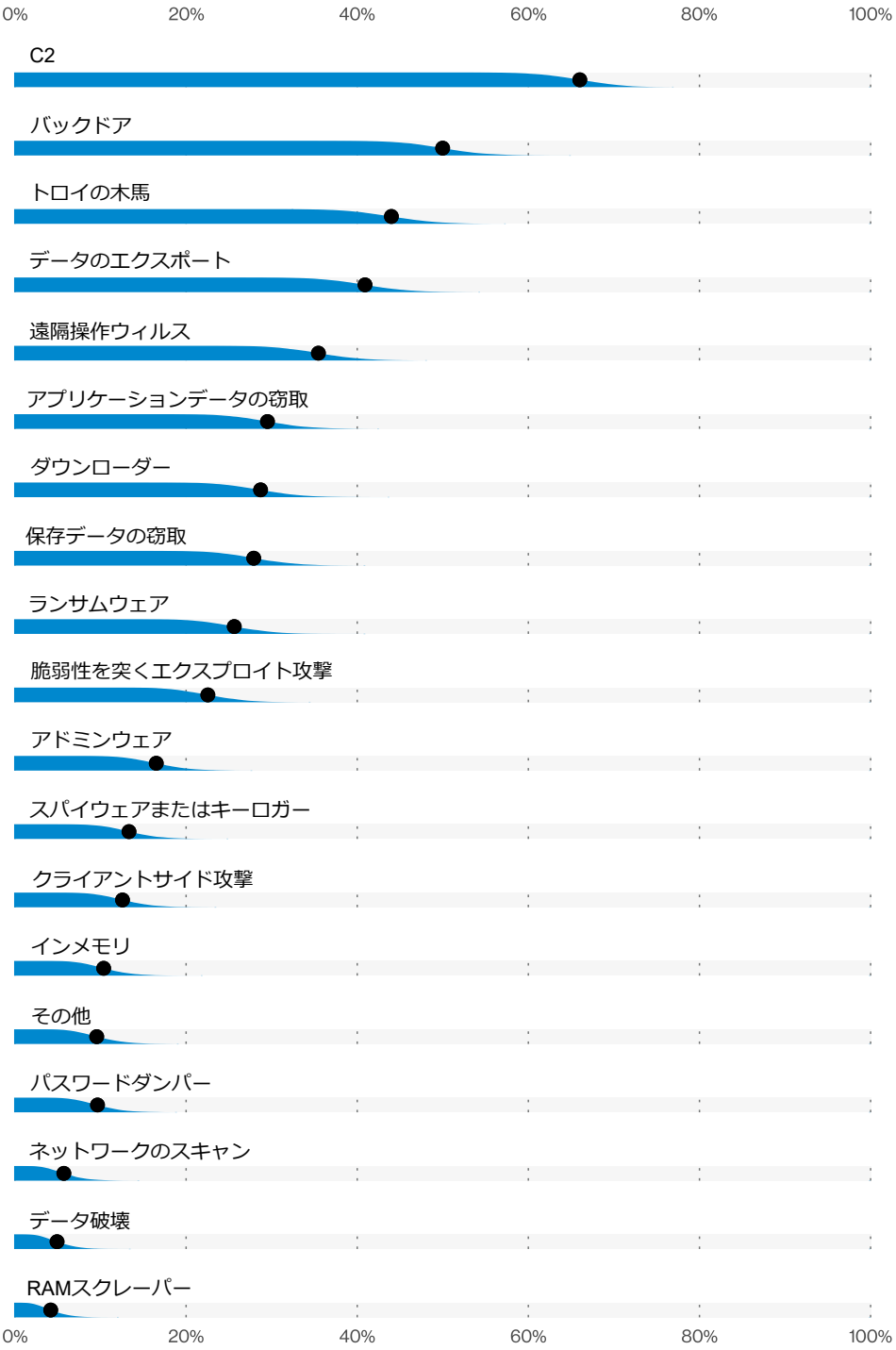


図74. ソーシャルエンジニアリングインシデントにおけるマルウェアの種類（n=130）

61 とはいえ、2番目に被害の多いデータの種類を見落とすわけにはいきません。それは個人情報です。誰かがあなたのメールを入手した場合、おそらく個人情報も入手していることは明白だからです。

62 面白いことに、BECはビジネス用のメールアドレスを侵害する必要はありません。Your.CEO@davesmailservice.comは、BDIRのデータセットに頻繁に登場します。

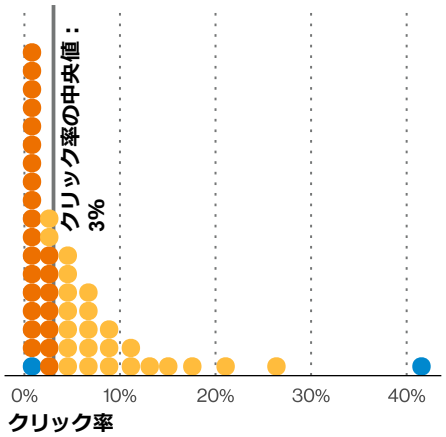


図75. 直近のフィッシングキャンペーンにおける組織のクリック率(n=18,177)
1ドット=組織の2%

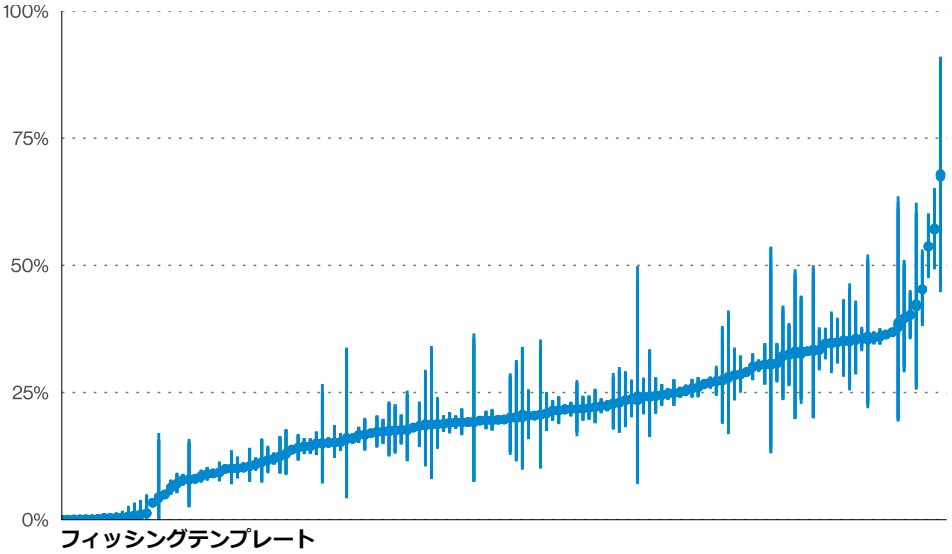


図76. さまざまなフィッシングシミュレーションテンプレートをクリックする可能性のある人の割合（n=1,186,766)。バーは私たちの自信を表します。バーが大きいほど自信がないことを意味します。

フィッシングに関する良いニュースは、フィッシングシミュレーションでのクリック率が中央値で3%にまで下がったことです。しかし、図75が示すように、「ほとんどの会社が3%前後」というわけでもありません。むしろ、クリック率がはるかに高い企業が大きな割合を占めているのです。

フィッシングメール自体がクリック率に大きく関係しています。150種類のフィッシングテンプレートを分析したところ[63]、予想されるクリック率が大きく異なることがわかりました。図76では、クリック率がほとんどないものから、半数以上の人がクリックすると予想されるものまであることがわかります。さらに、実際のフィッシングは、シミュレーションよりもさらに人を信じ込ませるだけの魅力があるかもしれません。1,148人のサンプルでは、本物とシミュレーションのフィッシングを受け取った人のうち、シミュレーションのフィッシングをクリックした人はいませんでしたが、本物のフィッシングメールをクリックした人が2.5%いました。最後に、フィッシングメールの量は一定せず、かなりばらつきがあります。図77に見られるように、メールによるマルウェアをずっと経験した組織はありません。一方、ほとんどの企業は、悪意のあるメールの量が極めて多い日を数日だけ経験していました。

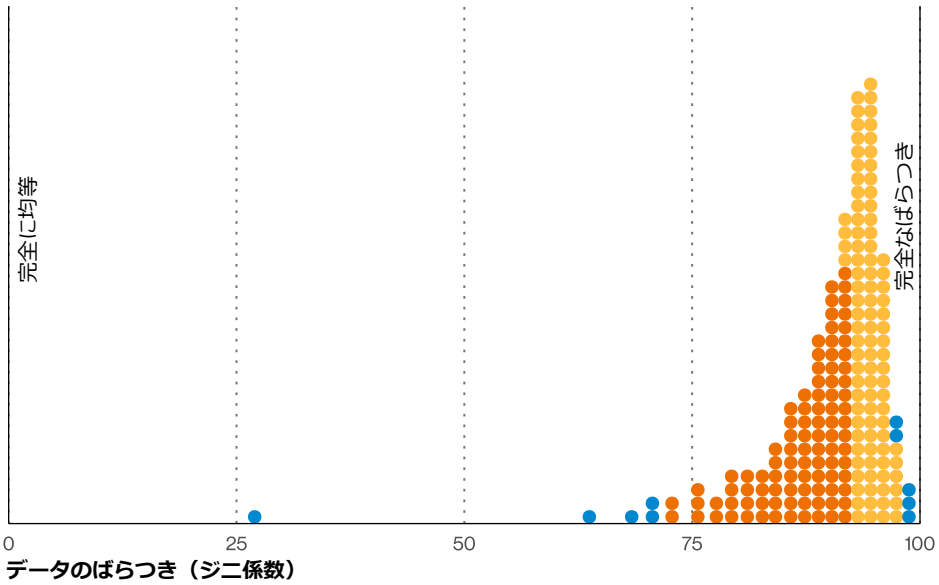


図77. 1日あたりのマルウェアフィッシングのばらつき（n=1,767）
1ドット=組織の2%

63 かなり漠然としています。「マルコフ連鎖モンテカルロ混合モデル」よりはマシだと思ったのですが、これはこれで怖いです(やってしまいましたが)。

エンジニアリングインシデント

図78は、もう1つの気になる統計を示しています。ソーシャルエンジニアリングのインシデントの大半は、外部から発見されています。図79の上位のインシデントのうち、社内で発見されたものは1つだけです（従業員による報告）。つまり、餌に釣られても、従業員は自分が釣られたことに気づかないということです。あるいは、自分が被害者になったかもしれないと、すぐに誰かに知らせる方法がないかのどちらかです。前者は対処が難しいですが、後者は簡単で、実装すべきです。よく知られているcert@yourorganizationhere.com（もちろん、監視されています）のメールのような基本的なもので、何か問題があることを警告することができます。

最後に、BECを見逃してはなりません。BECは、ソーシャル攻撃の中で2番目に多い形態であり、図80が示すように、その勢いは衰えていません。ソーシャルインシデントの中で、詐称は昨年の15倍にもなっています[64]。フィッシングやなりすましとともに、詐称はBECの勢いをさらに後押ししています。また、インシデントの種類によってはその影響を定量化することが難しい場合もありますが、BECの場合ははるかに簡単です[65]。「影響」のセクションで述べたように、金銭の獲得に成功したBECの58%のうち、損失の中央値は30,000ドルで、BECの95%は250ドルから984,855ドルの範囲にわたっています。1日の仕事としては悪くないです。

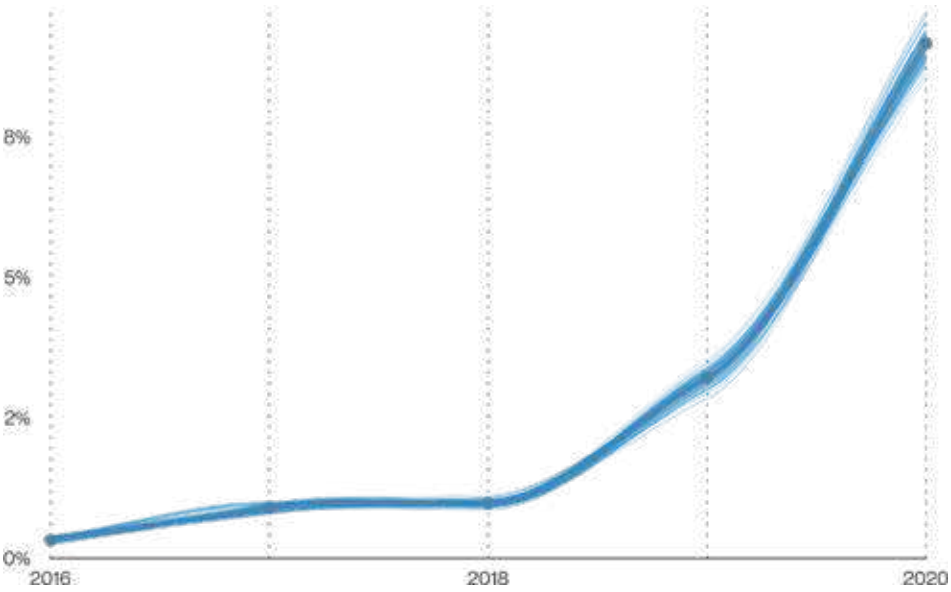


図80. 非DoSインシデントにおけるBECの経時変化

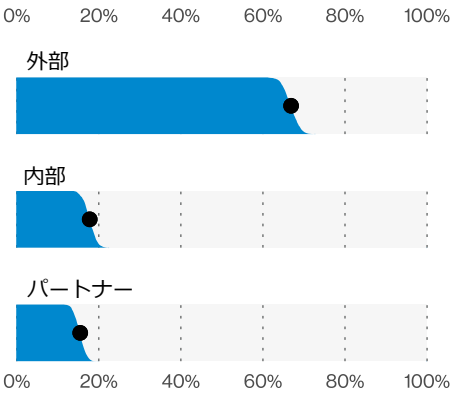


図78. ソーシャルエンジニアリングインシデントにおける発見方法（n=691）

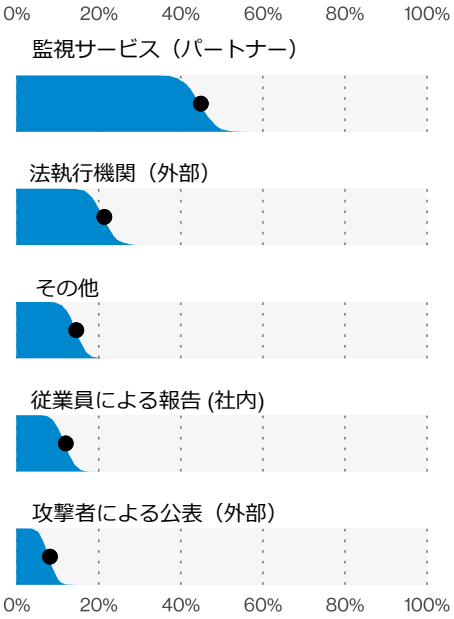


図 79. ソーシャルエンジニアリングインシデントにおける上位の外部からの発見方法の種類（n=234）

64 BECはメールアドレスを侵害することはないと述べましたが、侵害した場合、悪意のあるメールを送信するためにそのアドレスを使用することは、「詐称」による整合性の侵害とみなされます。

65 読者の中には、フィッシングに関するサイバー古謡をご存知の方がいらっしゃるかもしれません（2020年末からTikTokで世界的に大ヒットした「ウェラーマン（Wellerman）-シー・シャンティ」という19世紀の伝統的な船乗りの労働歌の替え歌）。「まもなくフィッシャーマンがやってきて、お楽しみの認証情報を持ってきてくれるだろう。いつか、ハッキングが終わったら、俺たちゃ暗号を持って、とんずらさ」

サイバーセキュリティ文化の構築

マーシャ・アルビスマン

Paranoids（ベライゾンメディアの情報セキュリティチーム）の行動エンジニアリングマネージャー

データ漏洩/侵害に関する話題は、企業が悪意のある攻撃者に侵入される「場合」から「時」へと変化しました。サイバー攻撃との戦いは、認証情報の盗難、ソーシャルエンジニアリング、人為的エラーなどの行為から守るために、組織がメンバーをどれだけ訓練し、適応させられるかに依存し続けています。

ベライゾンメディアでは、ほとんどのセキュリティ教育チームが提供しているシミュレーションやトレーニングは、実際の状況や、侵害につながる行動に対応しておらず、組織が受ける実際の攻撃を測定できていないと考えています。だからこそ、従来のセキュリティ啓発モデルから、行動科学を活用して、攻撃の経路を断つ行動につながる習慣を変えていくことが重要なのです。

HuangとPearlsonのサイバーセキュリティ文化モデル[66]では、サイバーセキュリティ行動は、リーダーシップ、グループ、および個人レベルで見える組織の価値観、態度、および信念によって推進されることを示唆しています。従業員がサイバーセキュリティをどのように優先し、解釈し、学び、実践するかに影響を与えることで、管理者は組織内にサイバーセキュリティ文化を創造することができます。

ベライゾンは、HuangとPearlsonのモデルと行動科学の手法[67]を組み合わせて、従業員のセキュリティ行動の改善を目的とした実験と意思決定を行うための3段階のアプローチ[68]を開発しました。このアプローチにより、2年間でパスワードマネージャーの導入率が3倍になり、従業員のフィッシングから受ける影響が半分になりました。これは、私たちのフィッシングシミュレーションプログラムと、セキュリティ運用チームが測定した実際に企業が受けた攻撃を関連付けて計算した結果です。

セキュリティ侵害につながる人的リスクを最小化するための特定のアプローチはありません。各企業は同じタイプの攻撃でも異なる種類のものを経験しており、それに応じて行動工学やサイバーセキュリティ教育プログラムをカスタマイズする必要があります。ベライゾンメディアのデータに基づく測定可能なアプローチは、カスタマイズされたプログラムを構築するための出発点として使用することができます。

66 https://scholarspace.manoa.hawaii.edu/bitstream/10125/60074/0634.pdf
67 テクニックの一覧は、次の脚注のケーススタディの用語辞典を参照。
68 https://cams.mit.edu/wp-content/uploads/Verizon-Media-CyberCulture-Paper.pdf

システム侵入

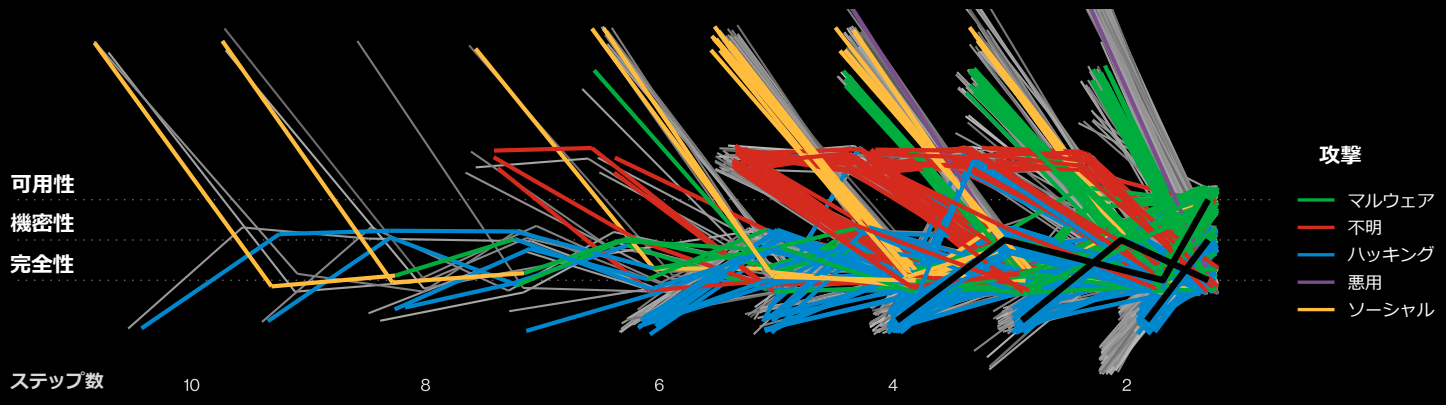


図81. システム侵入のインシデントパス（n=251）

サマリー

この新しいパターンは、より複雑な攻撃で構成されており、通常、多数のステップが含まれています。これらの攻撃の大部分はマルウェア（70%）が関与しており、通常はランサムウェアの種類に属するものですが、Webアプリケーションのペイメントカードのデータを狙うMagecartによる攻撃の種類もあります。また、ハッキング（40%）も多くの攻撃に含まれており、多くの場合、盗んだ認証情報の使用やブルートフォース攻撃が行われています。

頻度	インシデント3,710件、確認されたデータ暴露966件
攻撃者	外部（93%）、内部（8%）、複数の関係者（1%）（漏洩/侵害）
攻撃者の動機	金銭目的（95%）、スパイ活動（6%）（漏洩/侵害）
侵害されたデータ	個人情報（48%）、その他（35%）、認証情報（33%）、決済情報（24%）（漏洩/侵害）

これは「新しい」パターンの1つであるだけでなく、後述するように、話題に上がるほど興味深いものの1つです。このパターンは、より複雑な攻撃で構成されており、攻撃者が隠れた富を見つけるために環境内を移動する際に、複数の段階を踏んでいることがよくあります。

以前であれば、このセクションで取り上げるインシデントのいくつかは、「サイバースパイ活動」のパターンに分類されていたでしょう。このパターンでは、秘密を探ろうとする国家とその関連攻撃者のハチャメチャな活動のほとんどが取り上げられていました。また、「クライムウェア」のパターンや、最後は、クレジットカードを処理するサーバーを狙った、忘れられがちな「POSサーバー攻撃」などで見つかるものもあります。この新しい「システム侵入」パターンは、攻撃者の動機にかかわらず、より手の込んだ「人間が操作する」攻撃を（時にはわずかであっても）捕捉することを目的としています。それでは早速、その詳細をご紹介しましょう。

チェーン攻撃者

「訓練された」データサイエンティストを集めたDBIRチームでは、イベントチェーンが関わっていることを示す図81のような複雑なデータや詳細なグラフを提示されると、重要な発見になりそうなものを素早くトリアージします。「確かに色の数が多い」「線が長くなるに違いない」といったことを発見し、それらが本当に関連性があるのか、統計的に有意かどうかを確認します。今回のケースでは、線が長いことから、このパターンの攻撃の多くは、最終的に目的を達成するまで、攻撃者がさまざまな攻撃を行うことを示しています。データ漏洩/侵害とインシデントの両方に関わるステップの数が同じなのは、「ソーシャルエンジニアリング」のパターンくらいです。色彩から判断するに、このパターンでは、ほとんどがマルウェアのイベントで、多少ハッキングが見られ、その他の攻撃の種類がごくわずかに添えられているという組み合わせになっています。

図82では、マルウェアが70%以上、ハッキングが40%以上の割合で関与していることを示しています。最後に、非常に大まかに言えば、このパターンのインシデントの大部分は、金銭的な動機を持った外部の攻撃者によるものであることがわかります。このパターンは、調べれば調べるほど興味深いものです。

データを詳しく調べてみると、このパターンを構成する主な「要素」は3つあることがわかりました。1つ目はランサムウェアで、ランサムウェアのケースの99%がこの1つのパターンに当てはまります。2つ目はマルウェア全般、そして3つ目は、Magecart攻撃です。この攻撃では、データをエクスポートするスクリプトで Webアプリケーションを処理しながら侵害します。それでは詳しく見ていきましょう。

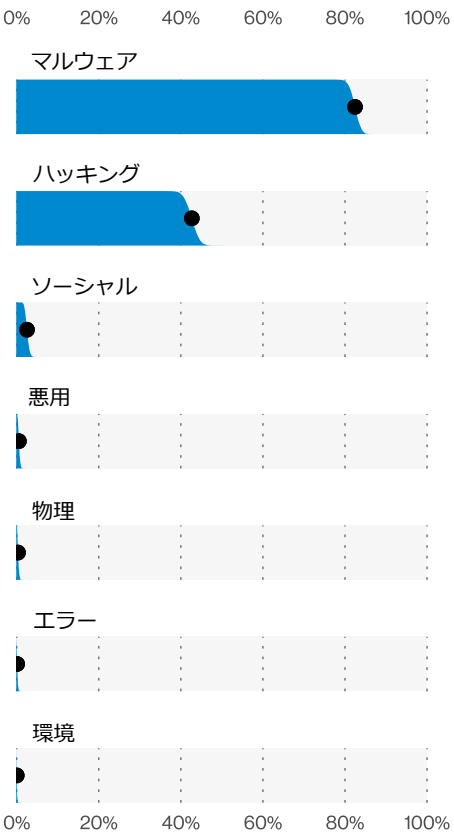


図 82. システム侵入のデータ漏洩/侵害における攻撃（n=966）

ランサムウェアについてまだ書くことがあるの？

あいにくランサムウェアはこの数年、常に書かなければならなかった項目であり、今後の報告書でもおそらく書き続けることになるでしょう。今年度も残念ながら、ランサムウェアの事例がまた増えてしまいました。ランサムウェアは2016年から増加傾向が続いており、現在ではインシデント全体の5%を占めています。新たに分かった事実として、現在、データ漏洩/侵害の全体の10%にランサムウェアが使用されています。これは、攻撃者が単にデータを暗号化するだけでなく、窃取したデータを公開するという新しい戦術を採用しているためです。これらの攻撃では、ランサムウェアがシステムに侵入する方法にいくつかのバリエーションがあり、攻撃者のそれぞれの強い好みによって攻撃パスはいくつかに分けられます。最初の攻撃パスは、窃取した認証情報の使用やブルートフォースによるものです。ランサムウェアのケースの60%は、直接インストールされるか、またはデスクトップ共有アプリを介してインストールされていることがわかっています。残りの攻撃パスとして、メール、ネットワーク伝播、他のマルウェアによるダウンロードがあります。最後の他のマルウェアによるダウンロードについては、昨年、7.8%の組織が既知のランサムウェアを1つ以上ダウンロードしようとしていたことがWebプロキシ検出のデータセットで判明しているため、驚くべきことではありません（図83）。この種のインシデントやデータ漏洩/侵害では、主にサーバーが標的となっていますが、これはデータの格納場所であることを考えると当然のことです。

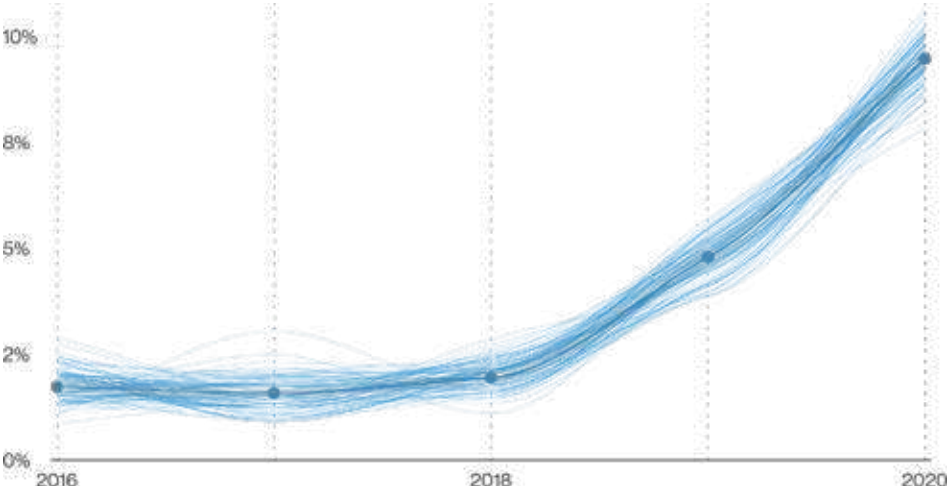


図83. 漏洩/侵害におけるランサムウェアの経時的変化

Magecart型攻撃

このパターンで見つかった2つ目の攻撃の種類は、ペイメントカードを処理するWebアプリケーションを狙うものでした。ここで「DBIRチームよ、Webアプリケーション攻撃に特化したパターンがあるのではないか」と突っ込まれる前に、このセクションで取り上げるインシデントは、いくつかの重要な要素に基づくそれらの攻撃とは若干異なることをあらかじめ述べておきます。一番大きな違いは、ペイメントカードのデータを窃取するためにマルウェアが使用されていることです。「システム侵入」のパターンでは、このパターンで標的となったWebサーバーのうち、60%がアプリケーションのデータを窃取するマルウェアをインストールしており、インシデントの65%でペイメントカードのデータが盗まれていたことがわかりました。この種の攻撃は、ビズ[69]で我々が、当初の標的に基づいて「Magecart型攻撃」と呼んできた攻撃の傾向を踏襲しています。この種の攻撃型に慣れていない方のために説明すると、攻撃者は何らかの脆弱性を悪用した後、盗んだ認証情報などを使ってクレジットカード情報を処理するEコマースサイトのコードにアクセスします。コードベースやサーバーへのアクセスを利用して、決済データを正しいエンドポイントだけでなく、自分たちのサーバーにも転送する追加コードを挿入することで、気づかれないように貴重なデータを吸い上げます。

マルウェアの30%は攻撃者が直接インストールしたもので、23%はメールで送られてきたもの、20%はWebアプリケーションから落とされたものでした。多くの人が驚くことではありませんが、マルウェアのこれら3つの主要な侵入経路をカバーする強固な防御策の重要性が浮き彫りになりました。

一般的なマルウェア

このパターンの最後の項目は、システム上で発見されたマルウェアの一般的な使用です。これらの状況の多くでは、そのマルウェアが将来的にさらなる損害を引き起こすために使用されたのか、それとも本来得意とすることを行わせるためにマルウェアが置かれたのか、必ずしもわからない場合があります[70]。ランサムウェアのケースを除外したところ、残ったマルウェアのケースの40%でC2/トロイの木馬/ダウンローダーが使用されていることがわかりました。また、マルウェアがどのようにしてシステムに侵入したかという点についても興味深い結果が出ています。マルウェアの30%は攻撃者が直接インストールしたもので、23%はメールで送られてきたもの、20%はWebアプリケーションから落とされたものでした。驚かない人も多いと思いますが、マルウェアのこれら3つの侵入経路に対応できる強固な防御策の重要性が浮き彫りになりました。

1日に発生したマルウェアの数を見ると、図84に示すように、大多数の組織ではこのデータには大きな変動があり、比較的静かな日もありますが、そうでない日もあります。

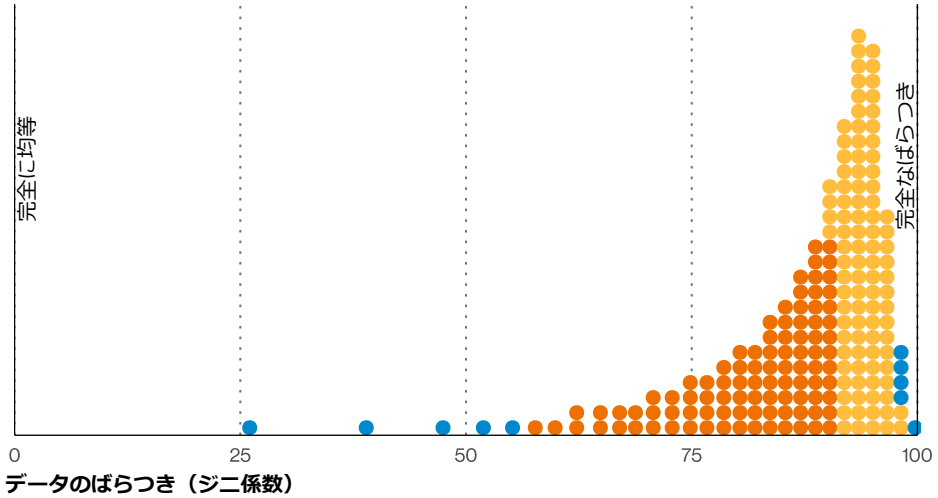


図 84. 1日あたりのマルウェアのばらつき（n=16,524）
1ドット=組織の0.5%

69 サイバービジネスのようなビジネスはありません。
70 マルウェアだって、最高の人生を送りたい。

これらのマルウェアイベントの重大性は必ずしも分かっていませんが、我々が調査したボットネットインシデントのデータによると、ボットネット感染の大半において侵害された認証情報は3つ以下であることが分かっています。つまり、環境内にマルウェアが存在していても、適切に掃除・処理されていれば、恐らくこの世の終わりということにはなりませんが、とにかく悪化させないことが一番です。

全体像が変わる

過去数回の報告書では、決済情報を狙った攻撃は減少してきていると言及してきました。引き続き、このパターンの傾向を確認しています。図85に示すように、純粋に決済情報を標的にする攻撃は少なくなり、被害組織の業務に影響を与えるあらゆるデータを広く標的にする傾向にあります。これにより、ランサムウェアのインシデントで組織が支払いを行う可能性が高まります。これまで何度も繰り返してきたように、ランサムウェアによる収益化が好まれるようになってきており、標的にされるデータもそれに合わせて変化していきます。このパターンで発生する攻撃は、我々が追跡しているすべての業界に何らかの影響を与えており、つまり攻撃者が利益を得るために張る網の広さを示しています。

純粋に決済情報を標的にする攻撃は少なくなり、被害組織の業務に影響を与えるあらゆるデータを広く標的にする傾向にあります。これにより、ランサムウェアのインシデントで組織が支払いを行う可能性が高まります。

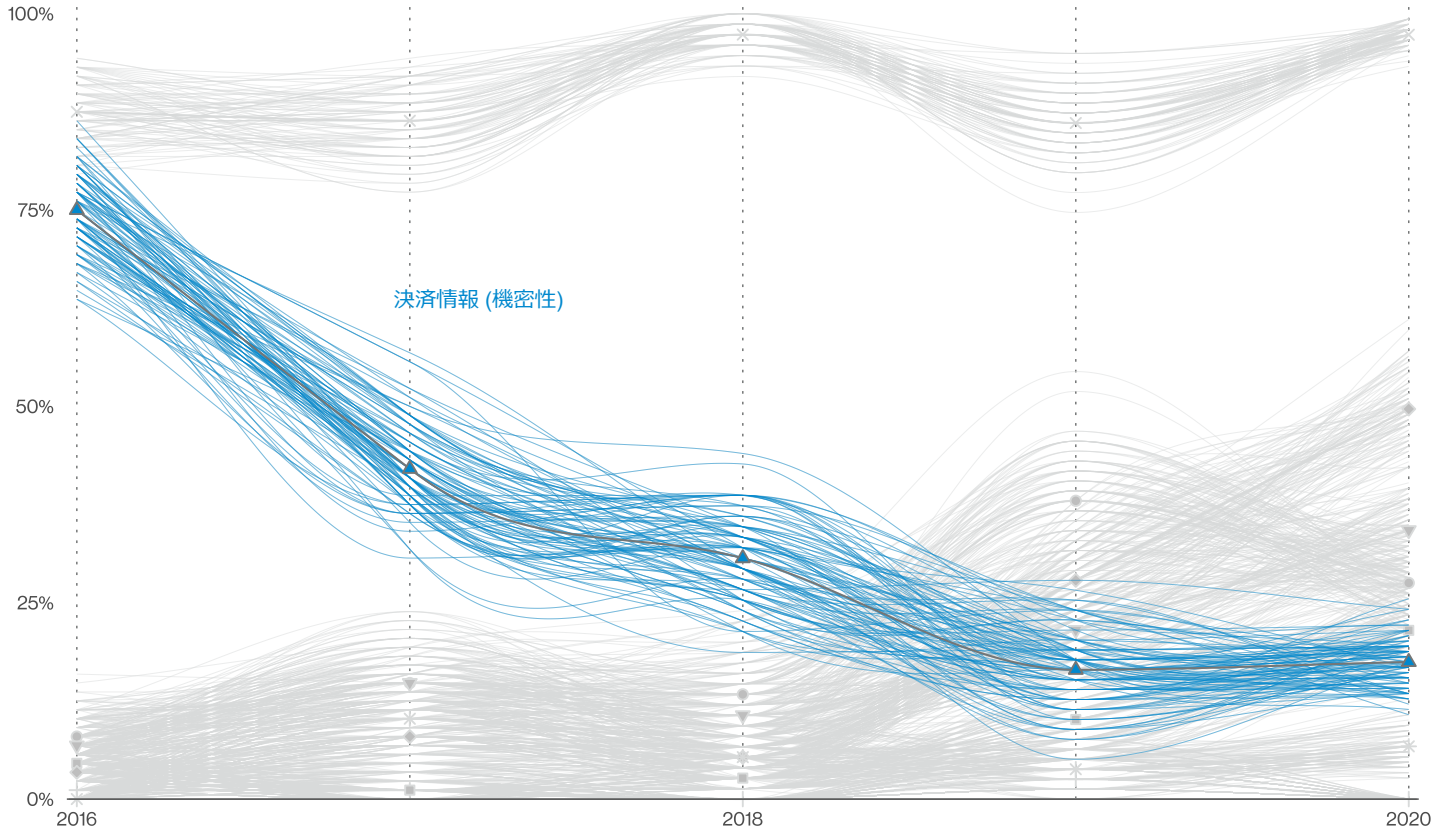


図85. データ漏洩/侵害における属性の種類の経時的変化

基本Web アプリケーション攻撃

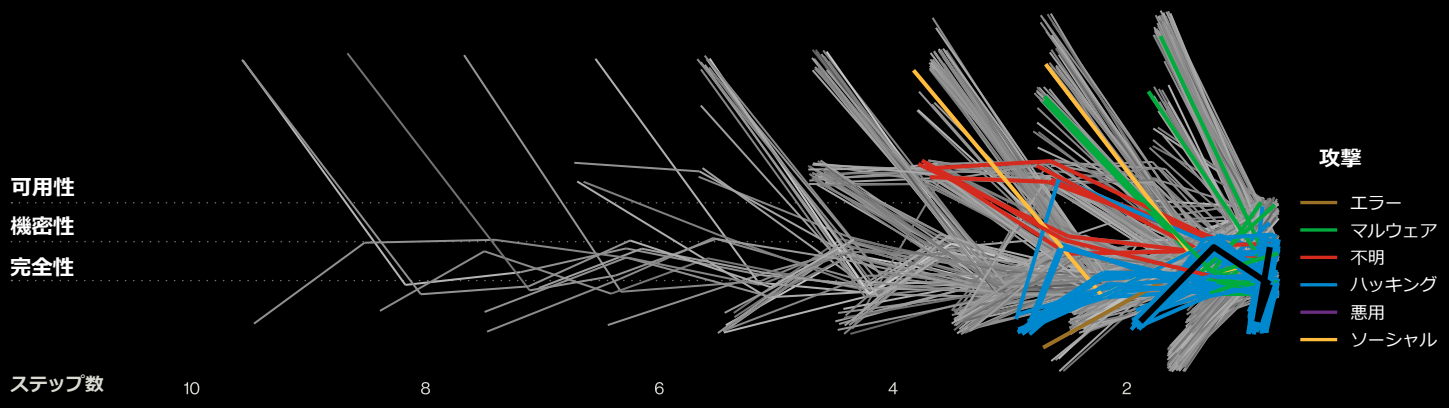


図86. 基本Webアプリケーション攻撃のインシデントパス（n=130）

サマリー

基本Webアプリケーション攻撃では、最初にWebアプリケーションを侵害した後に、いくつかのステップや追加の攻撃が行われます。これらの攻撃は直接的な目的に特化しておりますが、その範囲はメールやWebアプリケーションのデータへのアクセスから、マルウェアの配布や改ざん、将来のDDoS攻撃のためにWebアプリケーションを再利用することまで多岐にわたります。

頻度	インシデント4,862件、確認されたデータ暴露1,384件
攻撃者	外部（100%）、内部（1%）、複数の関係者（1%）（漏洩/侵害）
攻撃者の動機	金銭目的（89%）、スパイ活動（7%）、怨恨（2%）、愉快犯（1%）（漏洩/侵害）
侵害されたデータ	認証情報（80%）、個人情報（53%）、その他（ 25%）、内部情報（12%）（漏洩/侵害）

Basic Web Application Attacks：基本Webアプリケーション攻撃（BWAA）は、信頼のおける「Webアプリケーション」パターンを新たに改良したものです（BWAHA（「泣き叫ぶ」という意味のスラング）にしたかったのですが、Hを当てはめることができませんでした）。この名前が口語的であることは承知の上ですが、オープンWebやWebに隣接するインターフェイスを標的とした、短くて要点を突いた攻撃の性質をよりよく表しています（息が爽やかになり、歯も白くなります）。名前のもう1つの選択肢も、ほぼ同じ長さでした。単純Web攻撃グループ（Simple Web Attack Group：SWAG）と言うのですが、この方が良かったかもしれません。なぜなら、これらの攻撃は、低空飛行で簡単に手に入る小物を探しているからです。

このパターンに含まれる資産は、図88によると圧倒的に「サーバーのハッキング」が多いのですが、ここにはいくつかの異なるサブパターンが含まれており、それらはすべて説明しやすく、視覚化しやすいものになっています。

最初のサブパターンは、図86に示されているように、実際のWebアプリケーションやメールサーバーを攻撃するために、盗んだ認証情報の使用やブルートフォースをWebアプリケーション経由で行います。侵害されたメールサーバーのほぼすべて（96%）がクラウドベースであり、その結果、個人情報、内部情報、医療情報が漏洩しました。

図 87. 基本Webアプリケーション攻撃でのデータ漏洩/侵害で使われた攻撃（n=1,384）

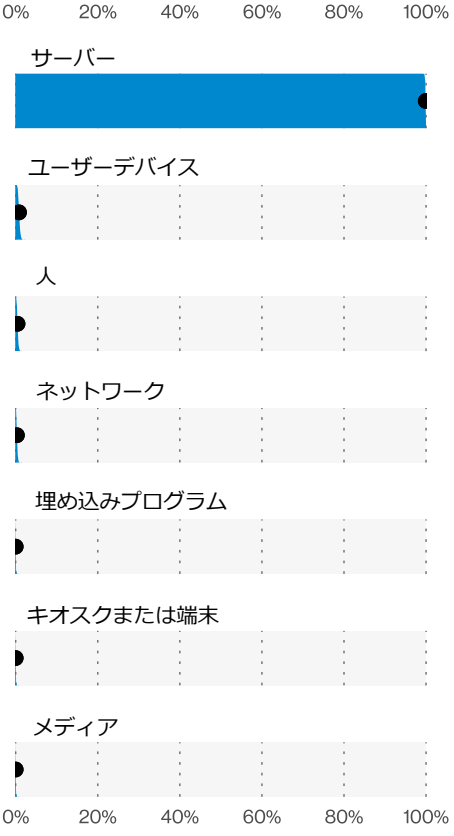


図 88. 基本Webアプリケーション攻撃でのデータ漏洩/侵害の標的となった資産（n=1,369）

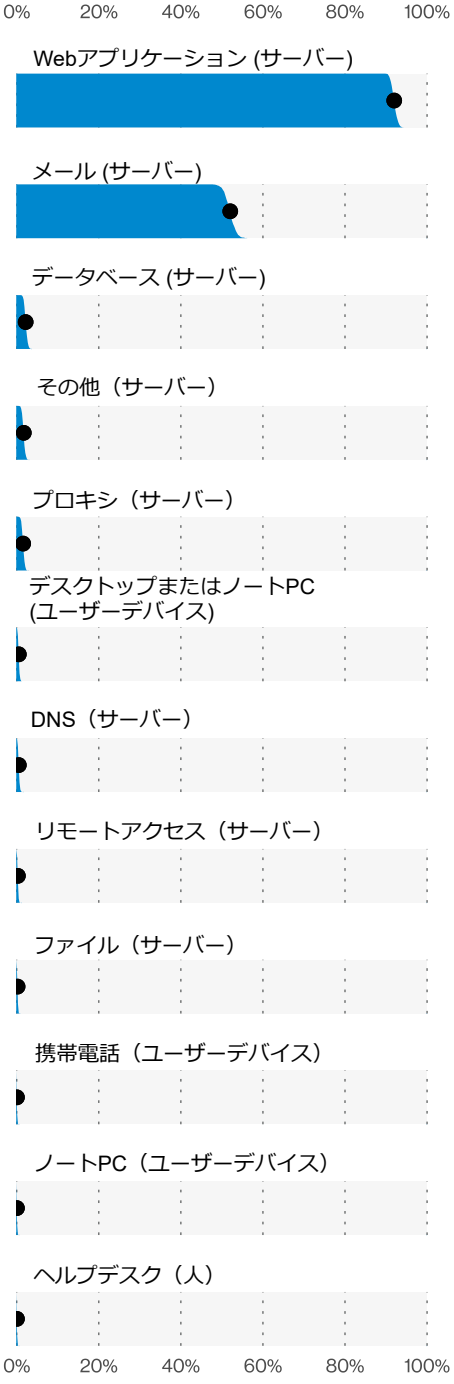


図 89. 基本Webアプリケーション攻撃でのデータ漏洩/侵害の標的となった資産の種類（n=1,324）

これらのブルートフォースの試みは、すべて同時に起こるわけでもなく、予測可能な規則性があるわけでもありません。

賢明な読者の皆様は、盗まれた認証情報を使用することがこのBWAAの主要な特徴であるとすれば、ソーシャルエンジニアリングやシステム侵入など、他の攻撃者が好んで使用する手法と何が違うのか、と指摘されることでしょう。よい質問です。このパターンでの認証情報の不正使用は、被害者が認識している限りでは、どんなソーシャルエンジニアリング攻撃よりも先に発生していることがわかりました。これは、認証情報が別の場所で実際に侵害され、さらに不幸なことに被害を受けたシステム上で目立った変化がない状態だったため、被害者がそれに気づかなかったか、あるいはクレデンシャルスタッフィング攻撃の被害者であったことを意味しています。

今回のデータセットで分析したSIEMデータによると、ブルートフォース攻撃とクレデンシャルスタッフィング攻撃は非常に多く発生しています。図90が示すように、監視している組織の23%にこれらの種類の攻撃に関連したセキュリティイベントが発生しており、そのうち95%に637回～33億回（！）もの試行が行われていることがわかりました。これは額面としては非常に大きな数字ですが、世の中には脆弱なサービスを探す自動化ボットやワームが大量に存在することを考えると、当然のことのように感じられます。

しかし、他のパターンをご覧になっている方はお気付きかもしれませんが、これらのブルートフォースの試みは、すべてが同時に起こるわけでもなく、予測可能な規則性があるわけでもありません。図91を見ると、今回調査した組織では、これらの攻撃が非常に不均等な間隔で発生していることがわかります。起こりうる認証情報のダンピングに対応するための投資は、1ヶ月に1回程度の頻度で行えばよいという単純なものではないようです。

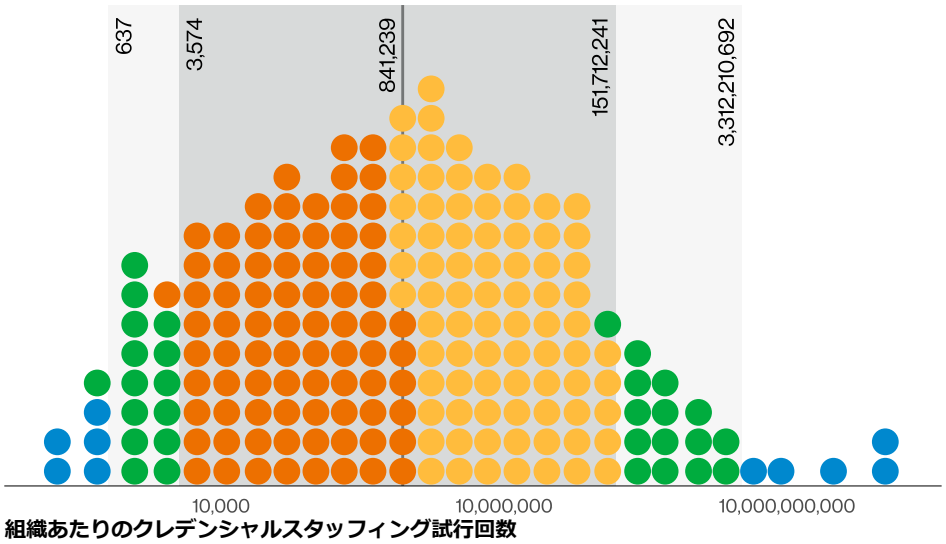


図90. 組織あたりのクレデンシャルスタッフィングの試行件数（n=821）
1ドット= 組織の0.5%

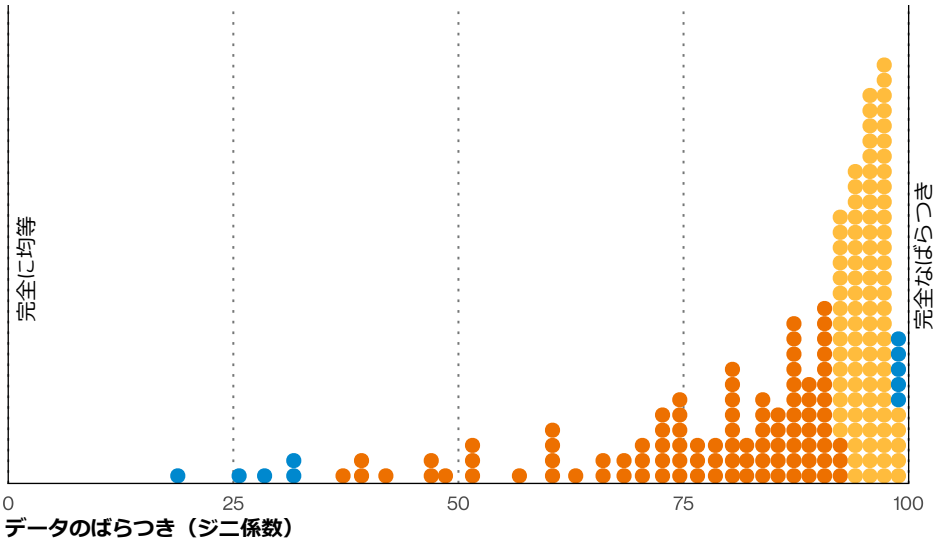


図 91. 1日あたりのログイン試行のばらつき（n=328）
1ドット= 組織の0.5%

もう1つのサブパターンは、Webアプリケーションの脆弱性を悪用するものです。これらは、図92が示すように、認証情報関連のものほど多くはありませんが、重要なものです。脆弱性の利用は、同系のパターンである「システム侵入」の領域でもありますが、このBWAAでは、Webアプリケーションだけに焦点を当てているわけではありません。最初のWebアプリケーション侵害の後も、さらに少数のステップや攻撃を加えられているのです。

このようなインシデントでは、攻撃者は、マルウェアの配布や改ざん[71]のためにWebアプリケーションを再利用したり、将来的なDDoS攻撃のためにマルウェアをインストールして、一日の仕事を終えます。言うまでもなく、ここでの動機の多く、正確には78%の動機が「二次的なもの」です。攻撃が「タダの不動産」を目の前に、不正な領域を拡大しないわけがありません。図93は、インシデントにおけるこの分布を示していますが、「改ざん」のように、完全に侵害が行われたことの確認が取れないケースもよくあります。

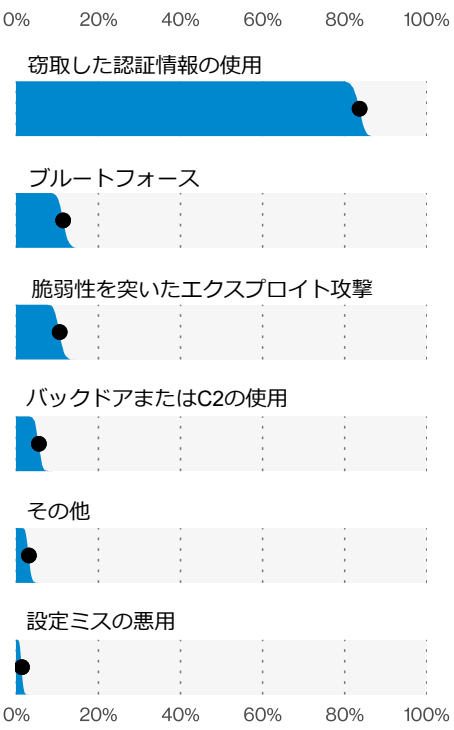


図92. 基本Webアプリケーション攻撃のインシデントにおける上位のハッキングの種類（n=947）

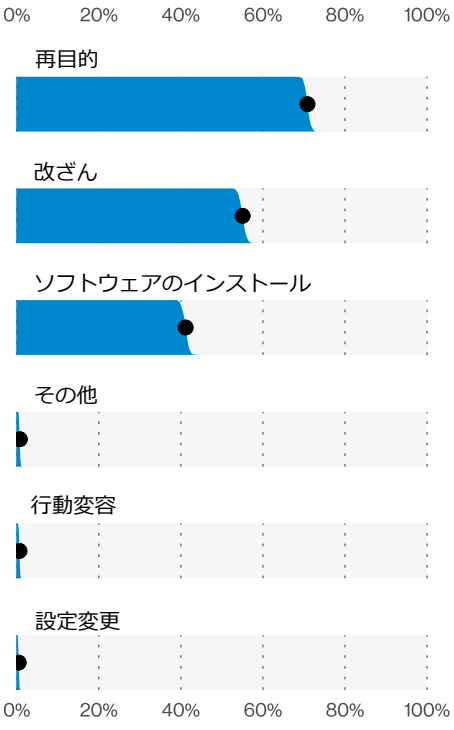


図93. 基本Webアプリケーション攻撃でのデータ漏洩/侵害における上位の完全性の種類（n=3,653）

71 今が1990年代なら!GeocitiesのDBIRウェブリングに参加しよう!

その他全て

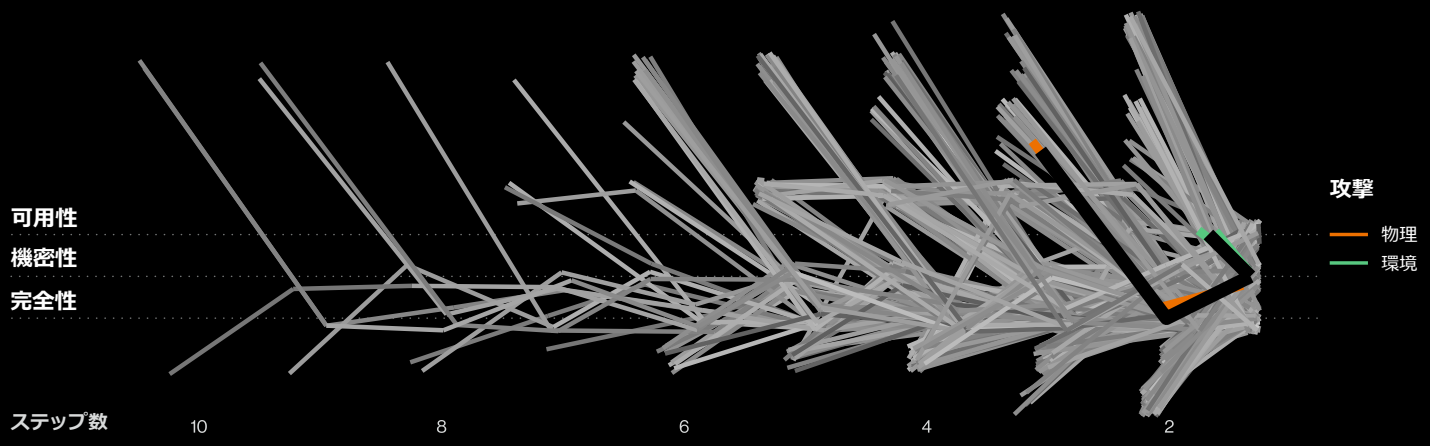


図 94. その他全てのインシデントパス（n=3）

サマリー

このパターンは再調整され、現在は主に「物理的な改ざん」のケースで構成されており、さらに環境が要因となった3つのケースが新しく追加されています。今年度、このパターンはどの業界でもこれといって目立つものはなく、「ソーシャルエンジニアリング」が天文学的に台頭する前に占めていた「他のどこにも当てはまらない残り物」という地位に追いやられています。

頻度	インシデント129件、確認されたデータ暴露38件
攻撃者	外部（95%）、内部（5%）（漏洩/侵害）
攻撃者の動機	金銭目的（100%）（漏洩/侵害）
侵害されたデータ	決済情報（61%～96%）（漏洩/侵害）

フェアウェイプロット（図94）は、「その他全て」パターンに含まれる2種類の主なインシデントをよく表しています。昨年、このパターンは非常に人気があり、いくつかの業界で上位3つのパターンに含まれていたことを覚えている方もいらっしゃるかと思います。他のパターンに当てはまらないインシデントで一杯になってしまったために、明らかに再調整する必要があったのです。

データを精査し、再調整を完了した今でも（詳しくは「パターンの紹介」セクションを参照）、「その他全て」パターンに当てはまるインシデントやデータ漏洩/侵害がまだいくつかあります。それは、物理的な改ざんのケース（ATMやガソリンポンプのスキミングなど）や、非常に珍しいことにかけては並ぶものがない「環境」に関わるケースです。まさに今年度、環境に関連する攻撃の3件のケースがデータセットに入りました。

ついにこれらのケースについて語れるようになったことについて、我々VERISのマニアックな精神を誇りに思います。「環境関連のデータ漏洩/侵害について質問してください」という車のステッカーを作ることも考えましたが、このステッカー自体は環境に良くありません。

以前は、「ペイメントカードスキミング」だけのパターンがありましたが、ここ数年、データセットの中で劇的に減少しています。今年度は、これまで以上に急激な減少が見られました。本報告書のデータセットに含まれるスキミングインシデント（すべてデータ漏洩/侵害が確認された）は、わずか20件でした。この減少は、少なくとも部分的には新型コロナウィルス感染症の影響を受けた渡航制限によるものだと考えています。

例年、特に一般公開しているデータセット（VCDB）[72]では、海外のスキミンググループが米国に来て、自分たちが選んだインフラ（ATMを好む者もいれば、ガソリン給油機を重視する者もいる）にスキミング装置を設置している証拠が見られました。実際、犯人たちが盗んだデータを持って帰国するまでの主要なルートをたどることができました。2020年3月から始まった渡航制限により、このような集中的な攻撃を行う自由度は著しく低下しています。この種の攻撃が国家レベルで追跡されなくなった可能性もありますが、世界の大半の国にとって非常に困難な年であった中、少なくとも1つの前向きな結果が得られたと考えたいと思います。

次に、環境関連のデータ漏洩/侵害について説明します。前述のとおり、これに関するデータ漏洩/侵害は3件と非常に少数です。しかし、これらは別々の独立した事件です。火災、ハリケーン、竜巻が原因で発生したものがあります（表3）。この3つのケースでは、自然の力に遭遇したことで、紙の書類が風に吹き飛ばされました（「オズの魔法使い」のように）。これらのケースで攻撃者となったのは、不可抗力である外部の力と考えられます。DBIRチームは、自然がデータ漏洩/侵害の舞台から退き、いつもどおり出番の予定された攻撃者の記録に喪失が発生することを願っています。

漏洩/侵害件数	環境の種類
1	火災
1	ハリケーン
1	竜巻

表3. 環境によるデータ漏洩/侵害

72 https://github.com/vz-risk/VCDB

04

業種別のハイライト

各業種の概要

今年度は、29,207件のインシデントを調査した結果、5,258件のデータ漏洩/侵害を確認しました（表4）。今回も、これらのインシデントやデータ漏洩/侵害を各業種に分けて、攻撃対象や脅威の観点から、すべての業種が同じ状況にはないことを説明します。特定の業種が受ける攻撃の種類は、その業種がどのようなインフラに依存しているか、どのようなデータを扱っているか、そして人々（顧客、従業員、その他すべての人）がどのようにその業界と関わっているかに大きく関係しています。

ビジネスモデルがモバイル機器に特化しており、顧客が携帯電話のアプリを利用するような大企業とインターネットに接続していないがPOSベンダーを利用してシステムを管理しているような小規模な個人商店とでは、リスクが異なります。インフラ、そして逆に言えば攻撃対象がリスクを大きく左右します。

このことを念頭に置きつつ、読者の皆様には、各業種で報告されているデータ漏洩/侵害やインシデントの数に基づいて、その業種のセキュリティ態勢（またはその欠如）を推測しないよう注意していただきたいと思います。これらの数字は、データ漏洩/侵害の報告に関する法律やパートナーの知名度など、いくつかの要因に大きく影響されます。そのため、いくつかの業種では報告件数が非常に少なく、サンプルも少ないこともあり、その少ない数から得られる統計値の信頼性も低くなることをご承知ください。

例年どおり、BDIRチームは業種別のデータ漏洩/侵害やインシデントをパターン、アクション、資産に分類したヒートマップを作成しました（それぞれ図95と図96）。これらの図は、我々が収集したデータに含まれる「だから何なのか」という疑問に答えるものであり、業種に応じて、どのような攻撃パターンに遭遇する可能性が高いかを示すものとして有用です。また、各業種別のCISコントロールと組み合わせることで、どのようにリスクを軽減するのが最善かを判断するための指針にもなります。

インシデント	合計	小規模（1～1,000人）	大規模（1,000人以上）	不明	漏洩/侵害	合計	小規模（(1-1,000人）	大規模（1,000人以上）	不明
合計	29,207	1,037	819	27,351		5,258	263	307	4,688
宿泊および飲食業（NAICS 72)	69	4	7	58		40	4	7	29
官公庁（NAICS 56)	353	8	10	335		19	6	7	6
農業（NAICS 11)	31	1	0	30		16	1	0	15
建設業（NAICS 23)	57	3	3	51		30	3	2	25
教育サービス業（NAICS 61)	1,332	22	19	1,291		344	17	13	314
芸術、娯楽、およびレクリエーション業（NAICS 71）	7,065	6	1	7,058		109	6	1	102
金融および保険業（NAICS 52)	721	32	34	655		467	26	14	427
医療および社会福祉業（NAICS 62)	655	45	31	579		472	32	19	421
情報産業（NAICS 51)	2,935	44	27	2,864		381	35	21	325
管理（NAICS 55)	8	0	0	8		1	0	0	1
製造業（NAICS 31-33)	585	20	35	530		270	13	27	230
鉱業、採石業、石油・ガス採掘業（NAICS 21）	498	3	5	490		335	2	3	330
その他のサービス業（NAICS 81）	194	3	2	189		67	3	0	64
専門的・科学的・技術的サービス業（NAICS 54）	1,892	793	516	583		630	76	121	433
公務（NAICS 92）	3,236	22	65	3,149		885	13	30	842
不動産業（NAICS 53）	100	5	3	92		44	5	3	36
小売業（NAICS 44-45）	725	12	27	686		165	10	19	136
卸売業（NAICS 42)	80	4	10	66		28	4	7	17
運輸および倉庫業（NAICS 48-49)	212	4	17	191		67	3	8	56
公益事業（NAICS 22)	48	1	2	45		20	1	2	17
不明	8,411	5	5	8,401		868	3	3	862
合計	29,207	1,037	819	27,351		5,258	263	307	4,688

表4. 被害者の業種および規模別のセキュリティインシデントおよびデータ漏洩/侵害の件数

データ漏洩/侵害

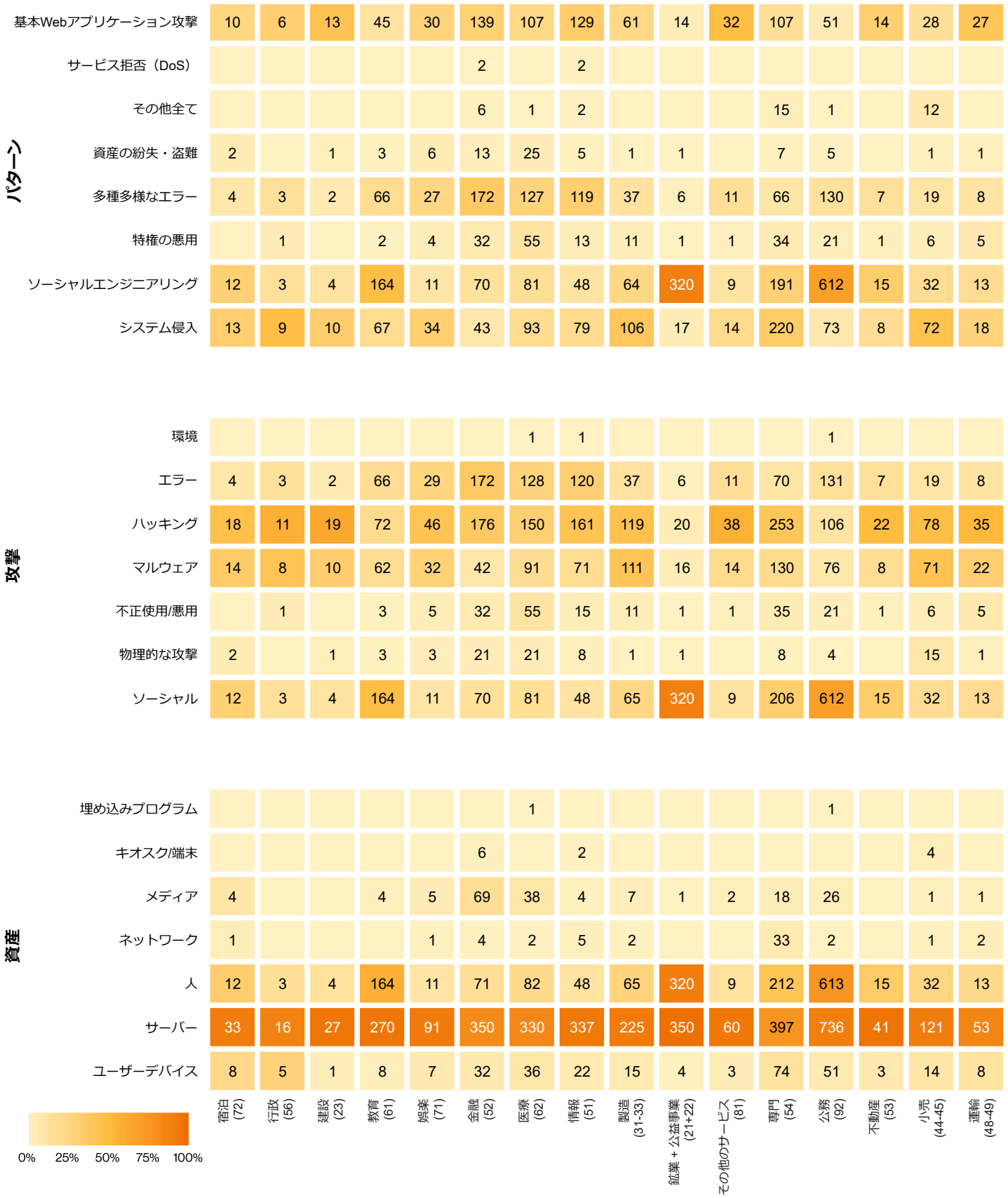


図 95. 業種別のデータ漏洩/侵害

インシデント

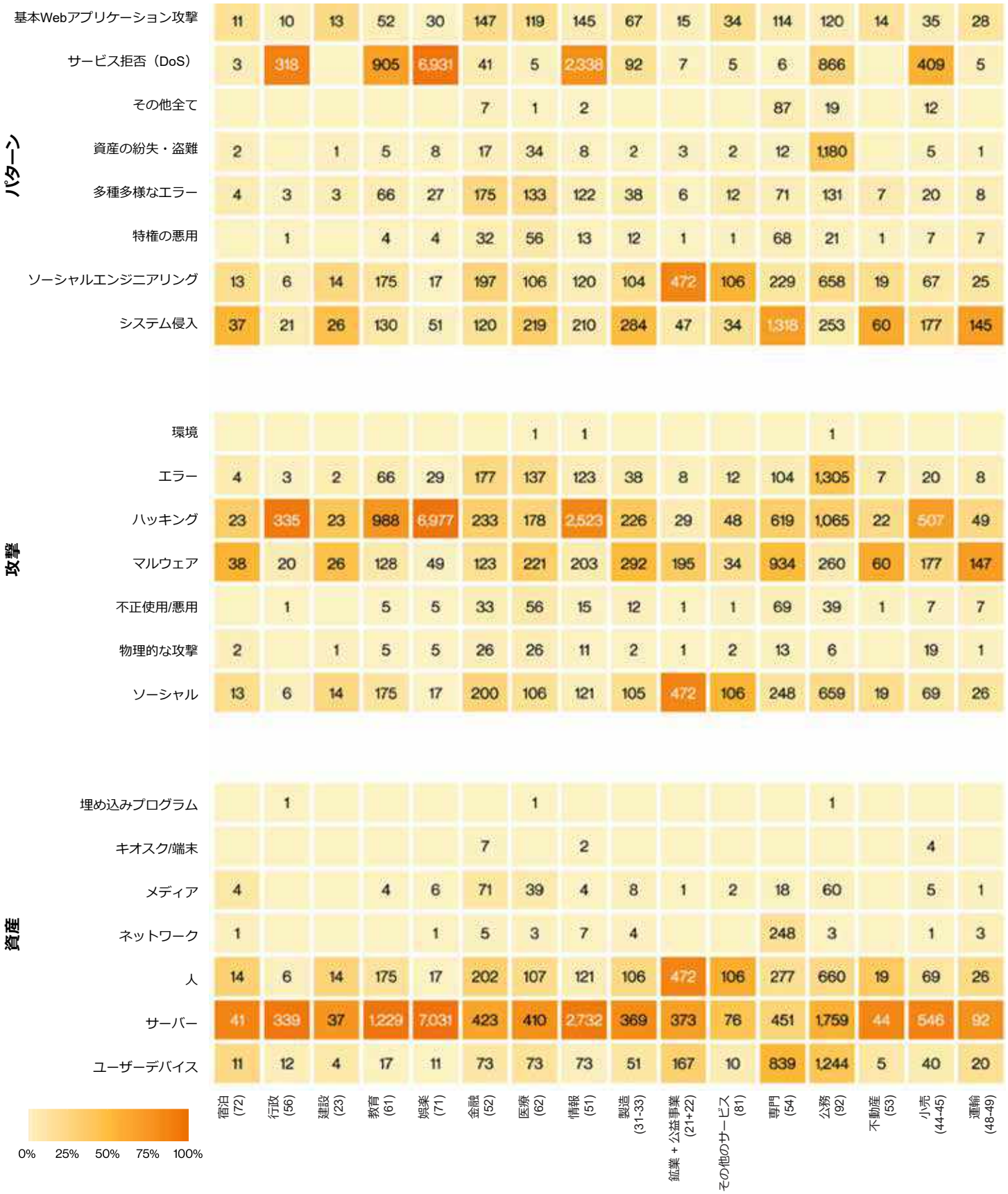


図96. 業種別のインシデント

サンプル数の少ない業種については、実際の値が含まれる可能性のある範囲を提示します。これにより、信頼区間を維持しつつ、十分な数のサンプルがあった場合の実際の数値のイメージを提供することができます。例えば、「宿泊業界では、92%の攻撃が金銭目的の動機によるものであった」ではなく、「金銭目的の動機による攻撃は86～100%であった」と示しています。本報告書で使用されている統計の信頼度の背景について詳しくは、「方法論」のセクションをご覧ください。

なお、今年度は一部の業種のセクションが例年よりも内容が少なくなっています。これは、新しいパターンでの詳細な分析に目を向けてもらいたいからです。ご自分の業種の状況をまず知りたい場合は[73]、各業種のセクションの「サマリー」カラムにある一覧表で上位のパターンを確認し、各パターンのそれぞれのセクションをじっくり読まれることをお勧めします。

また、各業界のセクションでは、読みやすいように、「実装グループ1」（IG1）のどのCISコントロールを優先すべきかを説明していますので、すぐにセキュリティ対策の戦略を練りたい方にはお勧めです。

本報告書で使用されている統計の信頼度の背景について詳しくは、「方法論」のセクションをご覧ください。

73 あなたを責めることなどできません。我々も先にデザートを食べることがありますから。

宿泊および飲食サービス業 NAICS 72

サマリー

宿泊および飲食サービス業では、ハッキング、ソーシャルエンジニアリングおよびマルウェアによる攻撃がほぼ同じ頻度で発生しています。

頻度	インシデント69件、確認されたデータ暴露40件
上位3つのパターン	「システム侵入」、「ソーシャルエンジニアリング」、「基本Webアプリケーション攻撃」がデータ漏洩/侵害件数の85%を占めている
攻撃者	外部（90%）、内部（10%）（漏洩/侵害）
攻撃者の動機	金銭目的（86%～100%）、スパイ活動（0%～14%）（漏洩/侵害）
侵害されたデータ	個人情報（51%）、認証情報（49%）、決済情報（33%）、その他（15%）（漏洩/侵害）
IG1による優先保護対策	セキュリティ意識およびスキル向上トレーニングプログラムの実施（14）、アクセス制御管理（6）、企業資産およびソフトウェアのセキュアな設定（4）

宿泊および飲食業（NAICS 72）では、今年度は過去に比べてデータ漏洩/侵害件数が減少しました（昨年は92件）。これは、2020年の大半が世界的な危機状況に見舞われたため、旅行や外食が大幅に減少したことが原因と考えられます。その結果、取引件数が減少し、ひいてはデータ漏洩/侵害の件数も減少したと考えられます。とはいえ、40件のインシデントは、いくつかの結論を導き出すのに統計的に十分な数です。この業界で最も多く見られたパターンは、「システム侵入」、「ソーシャルエンジニアリング」、「基本Webアプリケーション攻撃」でしたが、これらを見分ける方法はほとんどありませんでした（図97）。

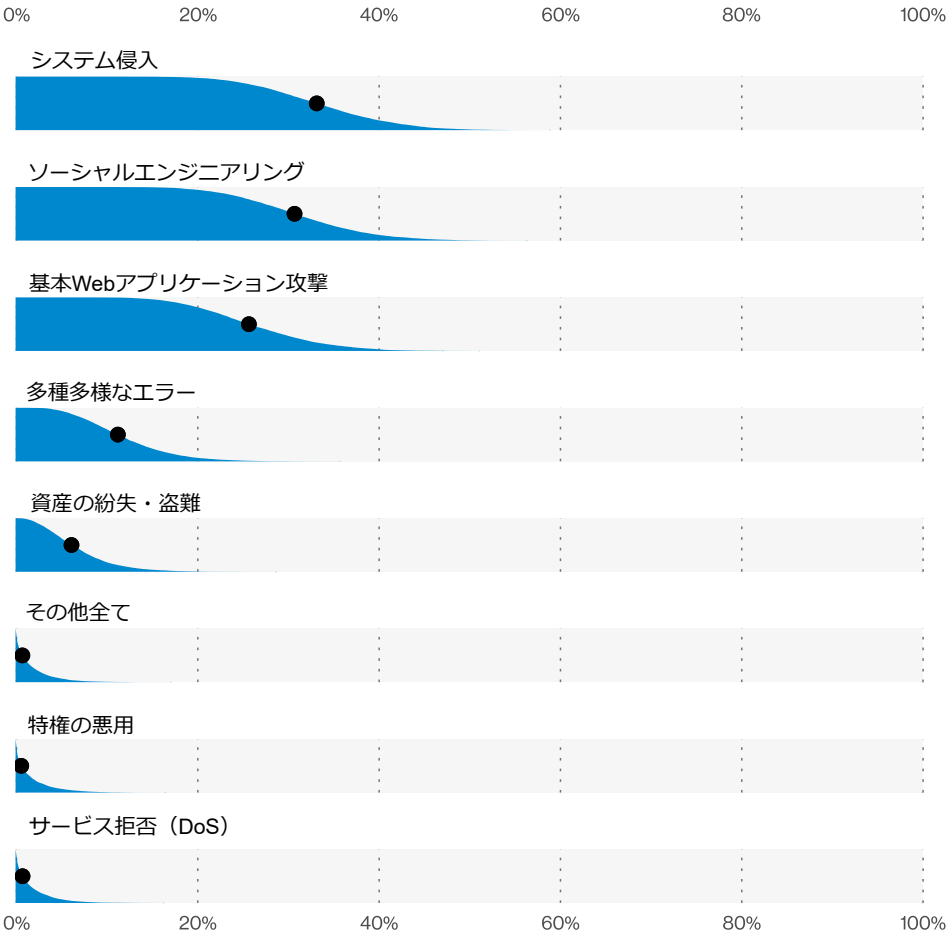


図 97. 宿泊および飲食サービス業のデータ漏洩/侵害のパターン（n=40）

本報告書の別の箇所で指摘しているように、特定の攻撃タイプがまとめられて「システム侵入」のパターンを形成しています。これには、以前は「クライムウェア」パターンに含まれていたマルウェア攻撃も含まれています。しかし、パターンが変わったとはいえ、図98に示すように、この業種で流行しているマルウェアは、バックドア、C2、トロイの木馬など、これまでも見られた種類のものです。

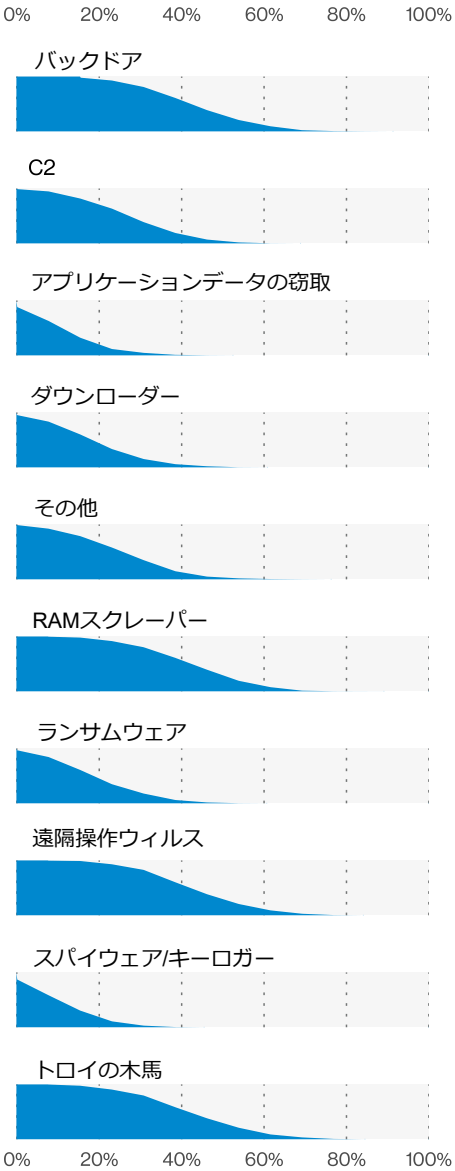


図 98. 宿泊および飲食サービス業のデータ漏洩/侵害における上位のマルウェアの種類（n=13）

この業種で見られるマルウェアでは、攻撃者による直接インストールが圧倒的に多い攻撃パスとなっています。

狙われたデータのタイプとしては、「認証情報」（49%）、「個人情報」（51%）、「決済情報」（33%）がいずれも同数かそれに近い数字となっており、これも前述の攻撃タイプから予想されるものです。最後に、サンプル数が非常に少ない（n=18）ことは認めざるを得ませんが、発見方法は（判明している場合）、39%～75%が第三者経由となっています（これも長年の傾向です）。通常、発見は法執行機関からの通知や共通購入先の監査によるものですが、場合によっては攻撃者自身の通知によるものもあります。組織外の誰かから通知が来るのを待たなければならない場合、データ漏洩/侵害の影響も当然大きくなるので、この業界における攻撃の発見方法に何らかの前向きな変化があることを期待したいところです。

芸術、娯楽、レクリエーション業 NAICS 71

サマリー

この業種では、窃取した認証情報の使用、フィッシング、ランサムウェアが引き続き大きな役割を果たしています。また、医療情報の漏洩も予想外に多く見られました。

頻度	インシデント7,065件、確認されたデータ暴露109件
上位3つのパターン	「システム侵入」、「基本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83%を占めている
攻撃者	外部（70%）、内部（31%）、複数の関係者（1%）（漏洩/侵害）
攻撃者の動機	金銭目的（100%）（漏洩/侵害）
侵害されたデータ	個人情報（83%）、認証情報（32%）、医療情報（26%）、その他（18%）（漏洩/侵害）
IG1による優先保護対策	セキュリティ意識およびスキル向上トレーニングプログラムの実施（14）、企業資産（1）およびソフトウェアの安全な設定（4）、アクセス制御管理（6）

今年度はエンターテイメントの消費のされ方が一時的に変化しましたが、攻撃者はこの業界で過去数年間使用し、成功を収めてきた攻撃の組み合わせをそのまま継続していました。すなわち、Webアプリケーションを標的とし、マルウェアを最大限に活用するというものです。そしてもちろん、時折起こる人間の失態が、人生を面白くしてくれるのです。

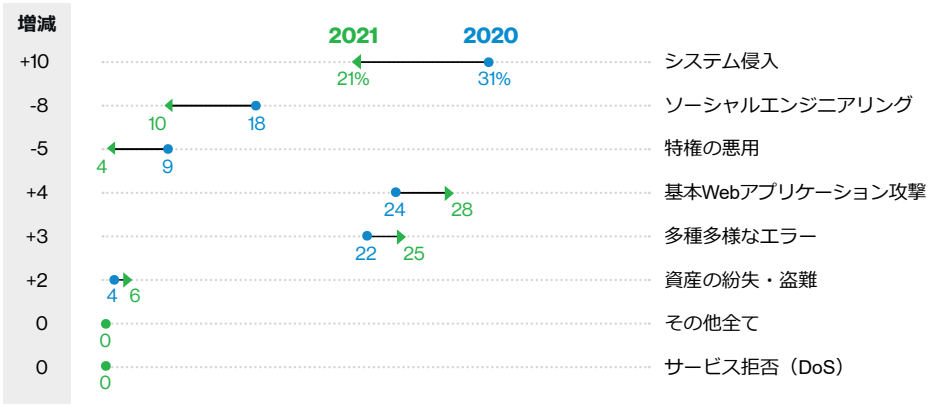


図 99. 芸術、娯楽、レクリエーション業のデータ漏洩/侵害におけるパターン

「システム侵入」、「Webアプリケーション」、「多種多様なエラー」がほぼ同率で上位にランクインしています。これらを合計すると、この業種におけるデータ漏洩/侵害の83%を占めます。これは、例年の傾向であり、昨年の報告書（図99）でも確認されています。この点を考慮すると、「窃取した認証情報の使用」、「ランサムウェア」、「フィッシング」、「設定ミス」などの行為がほとんどの侵害の原因となっていることは、当然のことと言えるでしょう（図100）。

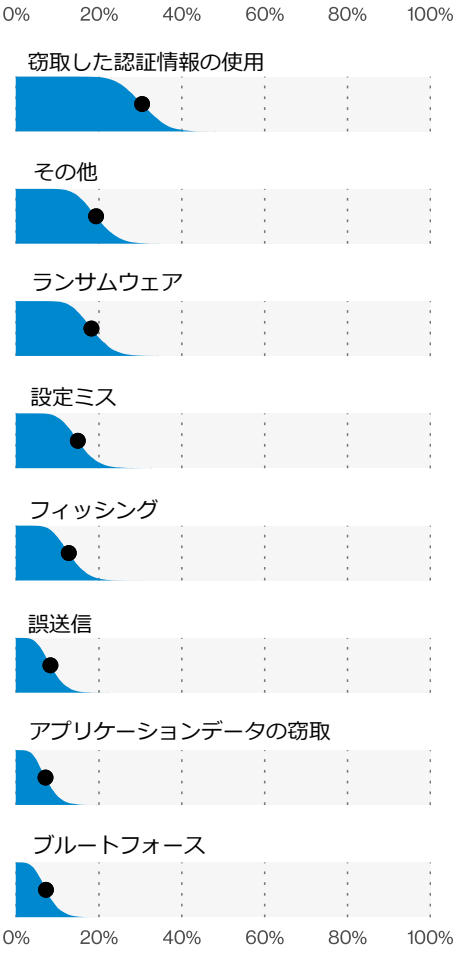


図100. 芸術、娯楽、レクリエーション業のデータ漏洩/侵害における上位の攻撃（n=90）

少し意外だったのは、医療情報のデータ漏洩/侵害が多かったことです。通常、医療記録の喪失は医療業界と関連していると考えられますが、データをもう少し詳しく調べてみると、個人健康情報（PHI）が、この業種に属するスポーツプログラムに関連していました。データが医療に関連するものであったことが不明瞭だったため、最悪のケース（個人情報ではなく医療情報の漏洩）が報告されたのかもしれません。しかし、これは重要な教訓です。自分の組織が医療分野ではないからといって、医療データを保有していない（あるいは適切に保護する義務がない）と思い込んではいけません。

インシデント面では、今年度もDDoS攻撃が非常に多く発生しました。これは、この業種に属するギャンブルWebサイトが原因である可能性があります。したがって、オンラインのギャンブルプラットフォームを運営している場合は、DDoS攻撃を想定しておくのが安全策です。

教育サービス業 NAICS 61

サマリー

教育分野では、「なりすまし」を利用したソーシャルエンジニアリング攻撃の割合が非常に高くなっています。これらの攻撃は、通常、不正な資金移動に誘導することを目的としています。「多種多様なエラー」と「システム侵入」も同様にまだ履修登録されており、対応に手一杯です。

頻度	インシデント1,332件、確認されたデータ暴露344件
上位3つのパターン	「ソーシャルエンジニアリング」、「多種多様なエラー」、「システム侵入」がデータ漏洩/侵害件数の86%を占めている
攻撃者	外部(80%)、内部(20%)、複数(1%)（漏洩/侵害）
攻撃者の動機	金銭目的（96%）、スパイ活動（3%）、愉快犯（1%）、自己都合（1%）、怨恨（1%）（漏洩/侵害）
侵害されたデータ	個人情報（61%）、認証情報（51%）、その他（12%）、医療（7%）（漏洩/侵害）
IG1による優先保護対策	セキュリティ意識およびスキル向上のためのトレーニング（14）、アクセス制御管理（6）、企業資産の安全な設定（1）およびソフトウェア（4）

新型コロナウィルス感染症パンデミックの影響で、授業はオンラインや教室での対面授業との併用で行わなければならず、場合によっては全く行わないこともあるなど、教育分野は確かに厳しい1年でした。これらの課題は、主に犯罪者にとってのチャンスです。この業界では、学校生活を送る人々のデータやシステムにアクセスしようとする金銭目的の動機を持つ者が攻撃を行っています。

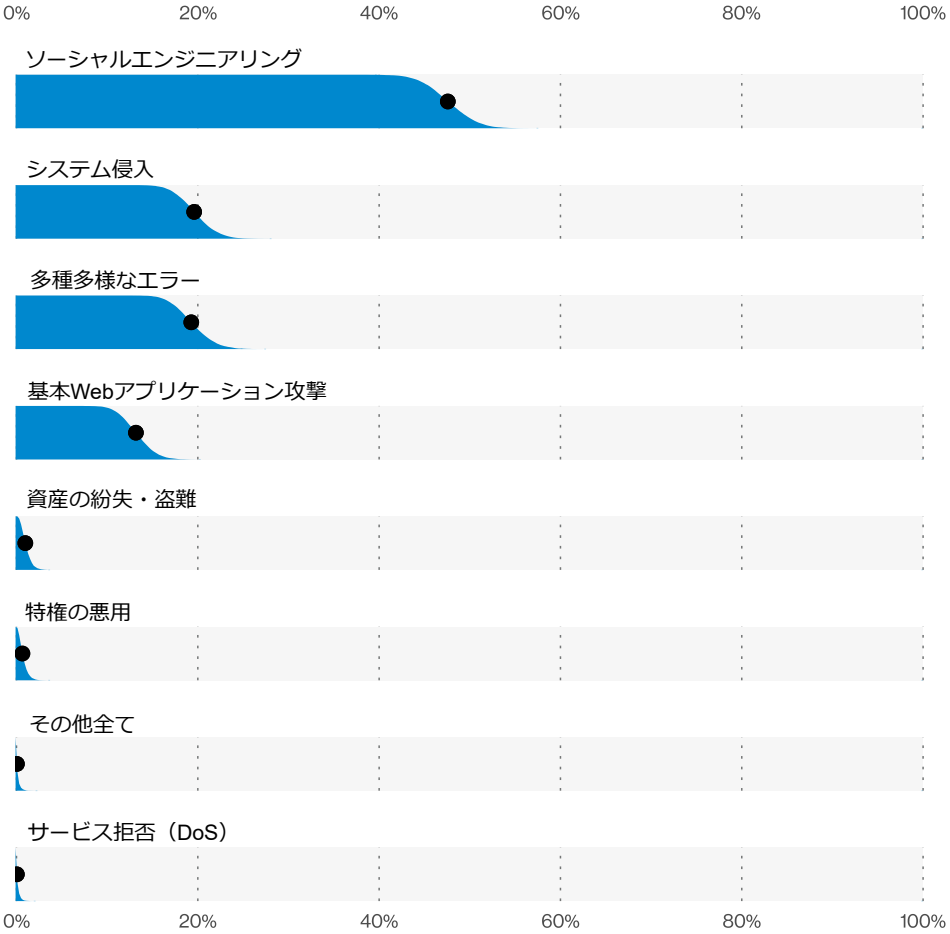


図101. 教育サービス業におけるデータ漏洩/侵害のパターン（n=344）

この業界で人気のあるパターンの1つがソーシャルエンジニアリングですが（図101）、これらのケースを見てみると、通常よりも多く「なりすまし」が発生していることがわかります。ソーシャルエンジニアリングの専門家は、シンプルなフィッシングメールを作成し、被害者が連絡してくるのを待つことがよくあります。教育サービス業界では、攻撃者たちはクリエイティブライティングの履修コースを思い出して、被害者が反応するような説得力のあるシナリオの作成に勤しんでいるようです（図102）。

攻撃者たちはその努力に見合った良い結果を得ているでしょうか？はい、「他人の資産の横領」コースでA評価の成績を上げています。自分の口座に振り込ませることに成功し続けていることを考えると、彼らは明らかに人を信じ込ませる作文を書く技術を習得しています。

電信送金やその他の支払いを行う担当者を対象に、この種の攻撃に対抗するための特別なトレーニングを実施すべきなのは当然のことです。また、新しい銀行口座への送金を防ぐための管理も必要です。

この業種のパターンでは、「多種多様なエラー」と「システム侵入」がほぼ同数で2位となりました。最も多いのは「設定ミス」です（アクセス制御を行わずに作成されたデータベースのほとんどは、世界中に公開されてしまっています。知識は無料に限りますからね）（図103)。

システム侵入のパターンには、ハッキングとマルウェアという2つの攻撃が見えます。クレデンシャル攻撃は最も一般的な出発点であり、認証情報は多くの場合、他のデータ漏洩/侵害の結果や認証情報の再利用によってもたらされます。攻撃者は、足場を固めると、マルウェアのインストールに移ります。ランサムウェアは人気の高いマルウェアで、暗号化を施す前にデータのコピーを取って、それを使って被害者を脅迫する犯行グループもあります。

ランサムウェアは人気の高いマルウェアで、暗号化を施す前にデータのコピーを取って、それを使って被害者を脅迫する犯行グループもあります。

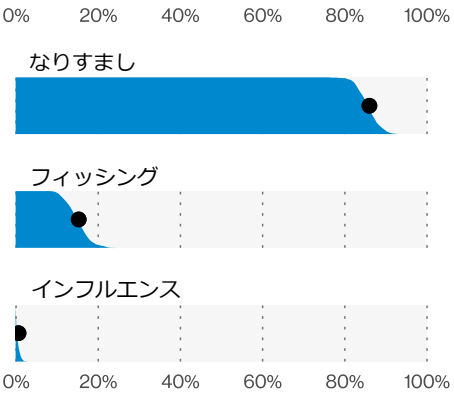


図102. 教育サービス業でのデータ漏洩/侵害におけるソーシャル攻撃の種類（n=164）

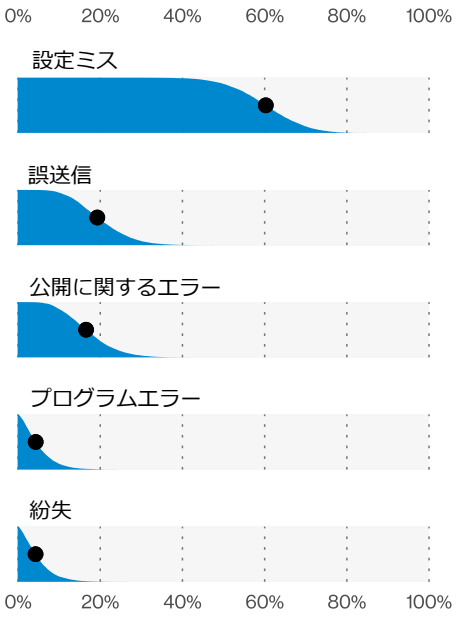


図 103. 教育サービス業でのデータ漏洩/侵害におけるエラーの種類（n=33）

金融および保険業 NAICS 52

サマリー

誤送信は金融業でのエラーの55%を占めています。金融業界は、外部の攻撃者からのクレデンシャル攻撃やランサムウェア攻撃に頻繁に直面しています。

頻度	インシデント721件、確認されたデータ暴露467件
上位3つのパターン	「多種多様なエラー」、「基本Webアプリケーション攻撃」、「ソーシャルエンジニアリング」がデータ漏洩/侵害件数の81%を占めている
攻撃者	外部（56%）、内部（44%）、複数の関係者（1%）、パートナー（1%）（漏洩/侵害）
攻撃者の動機	金銭目的（96%）、スパイ活動（3%）、怨恨（2%）、愉快犯（1%）、イデオロギー（1%）（漏洩/侵害）
侵害されたデータ	個人情報（83%）、銀行情報（33%）、認証情報（32%）、その他（21%）（漏洩/侵害）
IG1による優先保護対策	セキュリティ意識およびスキル向上トレーニングプログラムの実施（14）、企業資産およびソフトウェアのセキュアな設定（4）、アクセス制御管理（6）

金融サービス業界は、急激な落ち込みや目まぐるしい上昇、予期せぬ変動など、変化が激しいことで昔から知られています（Redditユーザの皆様、ありがとうございます）。この業界は、サイバーセキュリティに関しても、非常に多様な変化を遂げています。ここ数年で見られるようになったのは、内部の犯行者と付随する行動が、より有名で悪質な外部の攻撃者と同程度になってきていることです。

今年度は、この業種におけるデータ漏洩/侵害の44%が内部の犯行によるものでした（2017年以降、緩やかながらも着実に増加しています）（図104）。こうした犯行の大半は、例えばメールの宛先を間違えたりするなどの偶発的なものです。これはエラーによるデータ漏洩/侵害全体の実に55%（今年度の全データ漏洩/侵害の13%）を占めています。

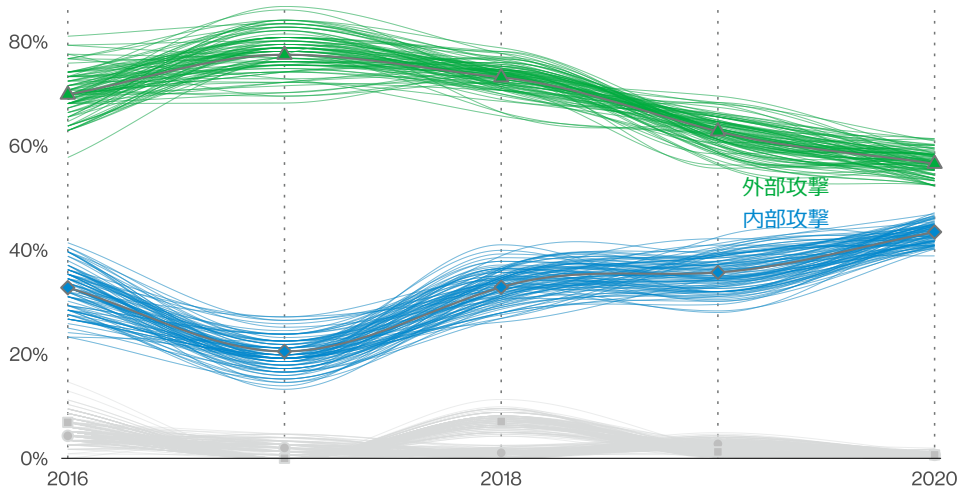


図 104. 金融および保険業でのデータ漏洩/侵害の経時的変化

悪意のある外部の攻撃者に目を向けると、金融業界では、他の業界で上位を占めるクレデンシャル攻撃、フィッシング、ランサムウェアの攻撃と同様の猛攻にさらされています。狙われたデータのタイプでは、個人情報が第1位で、次いで銀行情報、認証情報の順になっていますが、この業界の特徴を考えれば当然のことでしょう。

最後に、この業界では、データ漏洩/侵害の発見を外部に大きく依存する傾向が続いています。大体は、悪質な攻撃者が自らの存在を表明することや（インシデントの38%）、監視サービスからの通知（インシデントの36%）を受けて初めてデータ漏洩/侵害の事実を認識するのです。

医療および社会福祉業 NAICS 62

サマリー

過去数年間と同様に、基本的な人的ミスがこの業界を悩ませています。最も多いエラーは、電子文書であれ紙の文書であれ誤送信（36%）です。しかし、悪意ある内部の攻撃は、2年連続で上位3つのパターンから外れました。金銭目的を動機とする組織的な犯罪グループが引き続きこの分野を標的としており、ランサムウェアの展開が手口として人気を集めています。

頻度	インシデント655件、確認されたデータ暴露472件
上位3つのパターン	「多種多様なエラー」、「基本Webアプリケーション攻撃」、「システム侵入」がデータ漏洩/侵害件数の86%を占めている
攻撃者	外部（61%）、内部（39%）（漏洩/侵害）
攻撃者の動機	金銭目的（91%）、愉快犯（5%）、スパイ活動（4%）、怨恨（1%）（漏洩/侵害）
侵害されたデータ	個人情報（66%）、医療情報（55%）、認証情報（32%）、その他（20%）（漏洩/侵害）
IG1による優先保護対策	セキュリティ意識およびスキル向上トレーニングプログラムの実施（14）、企業資産およびソフトウェアのセキュアな設定（4）、アクセス制御管理（6）

2019年以降、医療業界でのデータ漏洩/侵害の実行犯は、内部の犯行者から主に外部の攻撃者へと変化しています。この傾向は、他の業界で見られる長期的な傾向とも一致しています。どの業界も自社の従業員が主要な攻撃者になることを望んでいないため、これは実際には良いニュースです。医療業界の上位のパターンの1つは引き続き「多種多様なエラー」となっており、中でも「誤送信」が最も多いのですが、少なくともエラーは悪意のあるものではありません（図105）。悪意のある内部犯行者によるデータ漏洩/侵害は、ここ数年、この業種の上位3つのパターンには現れていません。しかし、これはもはや発生していないことを意味するのか、それともまだ存在してはいるが（未確認生物のビッグフットのように）捕まえられていないだけなのか、それは時間が経ってみないとわかりません。

2年連続で、この業種では個人情報の漏洩が医療情報よりも多いことがわかりました。医療情報が最も多く保有されていると予想される業種であるにもかかわらず、この結果は奇妙に思えます。しかし、外部からの攻撃が増加していることから、データの窃取が場当たり的な性質のものであることが考えられます。例えば、医療データが厳重に管理されている場合、攻撃者がアクセスできるのは個人情報だけになるかもしれませんが、この情報は金融詐欺には有効です。簡単に言えば、攻撃者は手に入れられるものを手にして逃げるということです。

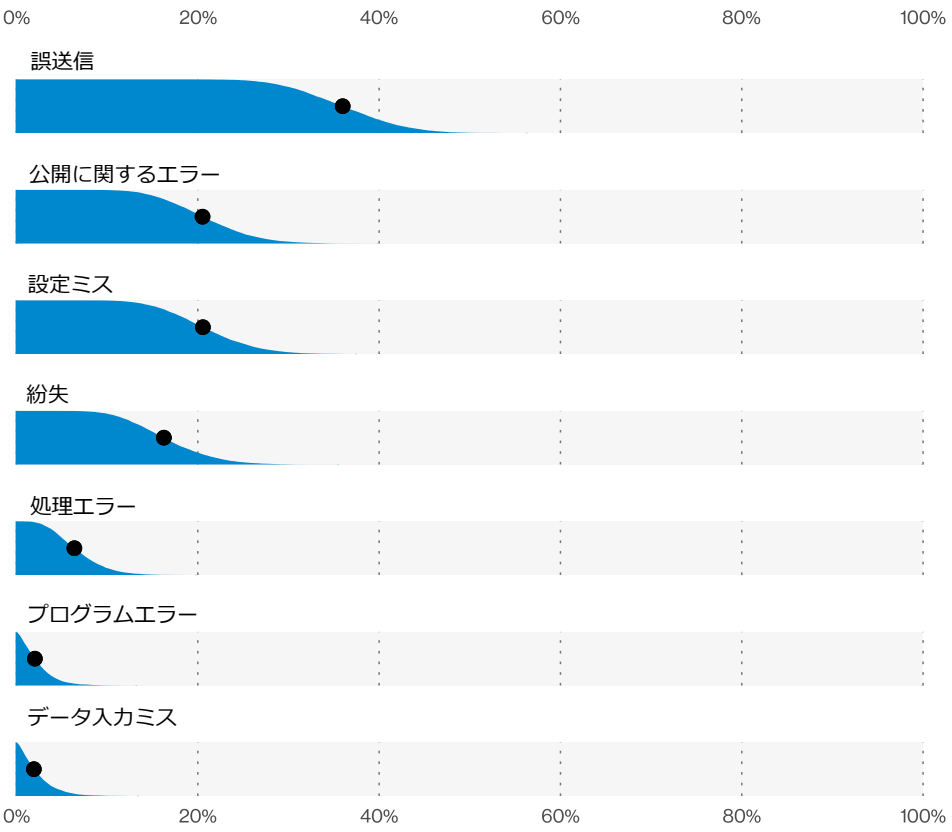


図 105. 医療および社会福祉業のデータ漏洩/侵害におけるエラーの種類（n=70）

情報産業 NAICS 51

サマリー

この業界は、認証情報を盗もうとするボットネットに悩まされています。エラーも非常に多く、中でも「設定ミス」が多く見られます。インシデントの観点からは、DoS攻撃が大部分を占めています。

頻度	インシデント2,935件の、確認されたデータ暴露381件
上位3つのパターン	「基本Webアプリケーション攻撃」、「多種多様なエラー」、「システム侵入」がデータ漏洩/侵害件数の83%を占めている
攻撃者	外部（66%）、内部（37%）、複数の関係者（4%）、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（9%）、怨恨（2%）、自己都合（1%）、愉快犯（1%）（漏洩/侵害）
侵害されたデータ	個人情報（70%）、認証情報（32%）、その他（27%）、内部情報（12%）（漏洩/侵害）
IG1による優先保護対策	セキュリティ意識およびスキル向上トレーニングプログラムの実施（14）、企業資産およびソフトウェアのセキュアな設定（4）、アクセス制御管理（6）

エラーや事故は、世界観次第で、複雑なシステムの自然現象と捉えることも、あるいは、堅牢でよく練られた組織の安全装置を克服したインターンの過失とすることもできます。いずれにしても、情報産業業界ではエラーは珍しいことではありません。「多種多様なエラー」は、「基本Webアプリケーション攻撃」や「システム侵入」と合わせて、この業界における攻撃の83%を占めています。

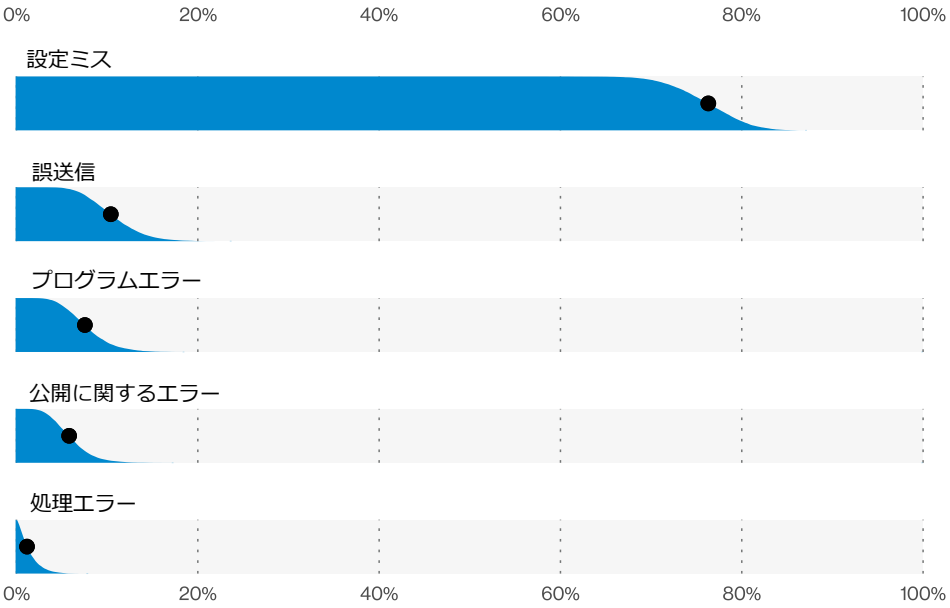


図106. 情報産業でのデータ漏洩/侵害におけるエラーの種類（n=111）

エラーの種類としては、「設定ミス」が全体の70%以上を占めています（図106）。これに続くのが、「誤送信」、「プログラミングエラー」、「公開に関するエラー」の3つです。このような組み合わせであれば、システムエンジニア（あるいは「年中無休のDevOpsスーパーエンジニア」とでも呼ぶ？）が重要な役割を果たしたことは、これらのエラーによるデータ漏洩/侵害の内部攻撃者に関しては、驚くべきことではありません。エラーによるデータ漏洩/侵害の全体的な割合はここ数年増加していませんが、この業界の組織が直面する永続的な問題であることに変わりはありません。

何か不愉快なことが起こったことを組織が発見したとき、外部の攻撃者は通常、それをニュースとして公表します（図107）。データ漏洩/侵害の50%は、悪質な攻撃者自身によって公表されていることがわかりました。これは、親切なようでいて、実はそうではありません。これは通常、身代金請求書で「今日は本当に大変な一日になりますよ」と丁寧な口調で告げたり、研究者や勧告者が監視するフォーラムで公然とデータを共有したり販売したりする場合に、当の攻撃者本人が告知します。セキュリティ研究者ほどうかと言えば、今回のデータ漏洩/侵害発見件数の30%はセキュリティ研究者によるものです。

インシデントだけを見てみると、この業界はDoS攻撃が多いことがわかります。これはコンピュータがネットワーク化されて以来、あるいは少なくともこの報告書の刊行が始まってからずっと続いている傾向です（図108）。インシデントのうち、DoSだけで観測されたハッキング行為の90%以上を占めており、残りはブルートフォースや窃取した認証情報の使用といった認証情報ベースの攻撃です。

ボットネット関連の攻撃を分析したところ、情報産業においてもう1つ興味深い結果が得られました。今年度は、情報産業の組織を標的にして認証情報を盗むボットネットによるデータ漏洩/侵害件数が、金融業界のものを上回ったのです（図109）。データはまさに新しく採掘された石油のようです。

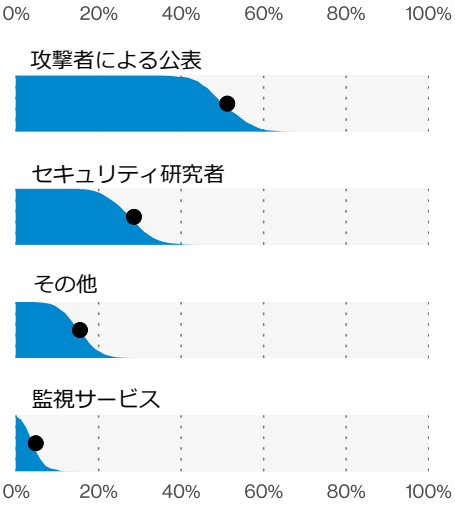


図107. 情報産業でのデータ漏洩/侵害における上位の発見方法の種類（n=84）

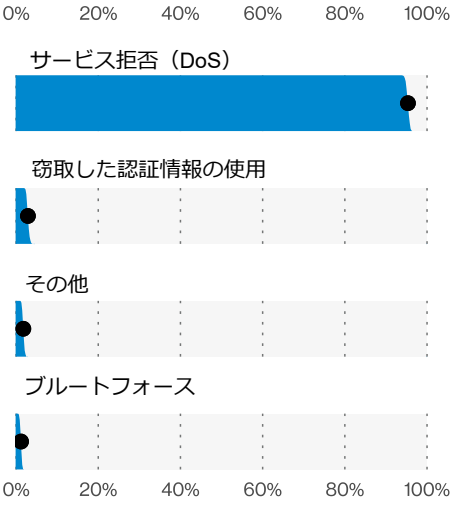


図108. 情報産業でのデータ漏洩/侵害における上位のハッキングの種類（n=2,452）

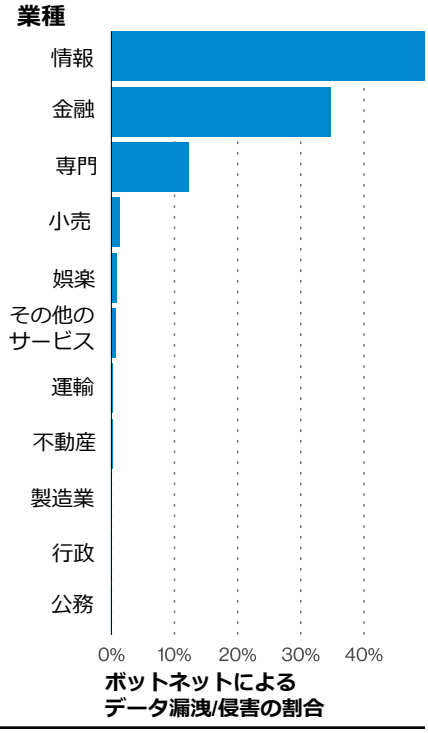


図 109. ボットネットによる攻撃を受けた業種（n=222,162）

製造業

NAICS 31-33

サマリー

この業界は、他の多くの業種と同様に、ソーシャルエンジニアリング攻撃に悩まされています。また、製造業ではランサムウェア関連のデータ漏洩/侵害が著しく増加しています。

頻度	インシデント585件、確認されたデータ暴露270件
上位3つのパターン	「システム侵入」、「ソーシャルエンジニアリング」、「基本Webアプリケーション攻撃」がデータ漏洩/侵害件数の82%を占めている
攻撃者	外部（82%）、内部（19%）、複数の関係者（1%）（漏洩/侵害）
攻撃者の動機	金銭目的（92%）、スパイ活動（6%）、自己都合（1%）、怨恨（1%）、二次的動機（1%）（漏洩/侵害）
侵害されたデータ	個人情報（66%）、認証情報（42%）、その他（36%）、決済情報（19%）（漏洩/侵害）
IG1による優先保護対策	セキュリティ意識およびスキル向上トレーニングプログラムの実施（14）、アクセス制御管理（6）、企業資産およびソフトウェアのセキュアな設定（4）

昨年、私たちは有機アーモンドミルクやトイレットペーパーの不足に直面し、工場や製造業のサプライチェーンに長く負担がかかっていることの本当の意味を改めて認識しました。2020年にパンデミックによる需要が発生したことで、製造業の一部の分野は、滅多に見ることのない困難な課題に直面したのです。それでも、製造業は、寛大さの欠片もない攻撃者たちに見過ごしてはもらえませんでした。

とはいえ、サイバー犯罪の観点から見れば、直面した課題は特別なものではありませんでした。実際、製造業は、漏洩/侵害データセット全体と同様に、システム侵入、ソーシャルエンジニアリング攻撃、基本Webアプリケーション攻撃という悪質な3つの攻撃を受けています。

データ漏洩/侵害

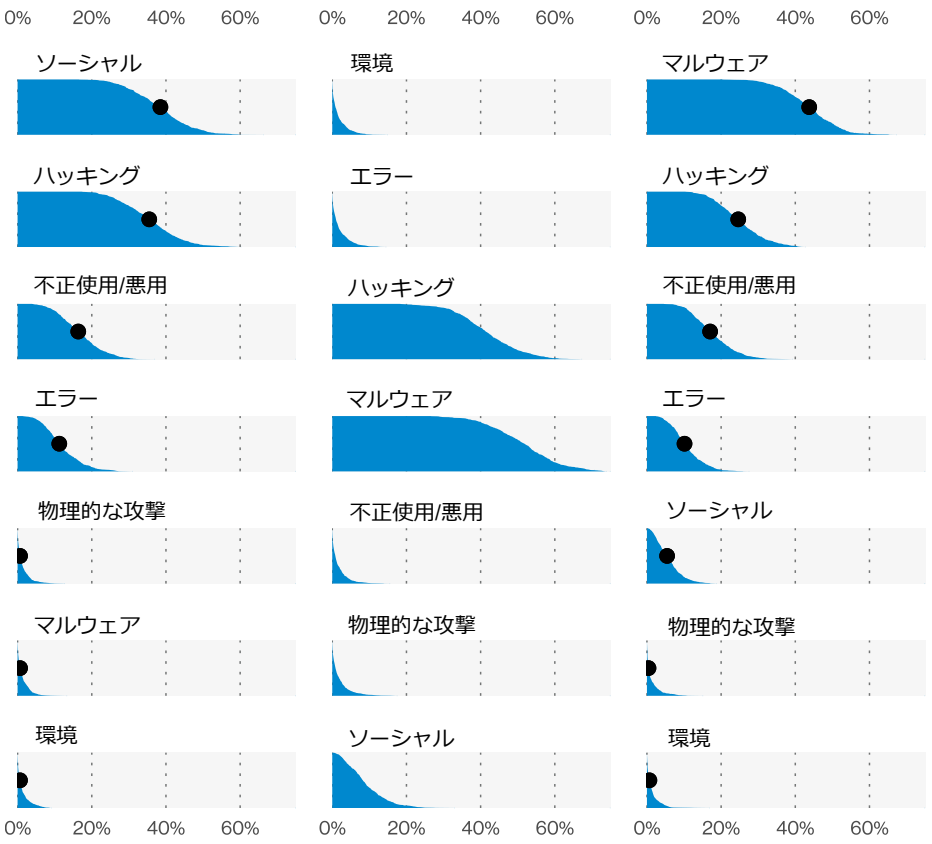


図110. 製造業のデータ漏洩/侵害の開始時、中間時、終了時の攻撃

このシナリオは図110にあるとおり、データ漏洩/侵害の各ステップで取られた上位の攻撃を示しています。攻撃者は、ソーシャルエンジニアリング攻撃（75.4%がフィッシング）またはハッキング攻撃（79.5%が窃取した認証情報の使用）を利用して最初の足場を確保する傾向にありました。そこからさらに認証情報を悪用したり、マルウェアをインストールしたりすることになります。

また、マルウェア関連のデータ漏洩/侵害では、ランサムウェアの役割が例年に比べて大幅に増加しています（61.2%）。これは、ランサムウェアを使用する攻撃者たちが「名指し非難」戦術を取り続けていることが原因と考えられます。このようなケースでは、データ漏洩/侵害されただけでなく、同時にデータにアクセスできなくなっていることが考えられます。

この業界で最も攻撃を受けたデータタイプは個人情報であり、これは自動化が進んだことと攻撃のしやすさに関連していると思われます。このデータタイプ（主に顧客のPIIから成る）は、認証情報を上回り、昨年の統計では同数であった関係が崩れました。これは、認証情報の漏洩は攻撃者が環境内を移動する際に自然に発生するため、多くの攻撃者たちが最終目的を達成していることを示唆しています。

また、ランサムウェア関連のマルウェアのインシデント数（前述のデータ漏洩/侵害とは異なる）も昨年より急増し、図111に示すように、DoSとフィッシングを抜いて最も多い攻撃の種類となっています。

「大規模工場と一人の"暗号化の達人"とでは、どちらが勝つか」と自問してみてください。驚くべき答えが待っているかもしれません。この業界の防衛戦略において、この点は間違いなく重点的に改善すべき分野です。

ランサムウェア関連のマルウェアのインシデント数（データ漏洩/侵害とは異なる）も昨年より急増し、DoSとフィッシングを抜いて最も多い攻撃の種類となっています。

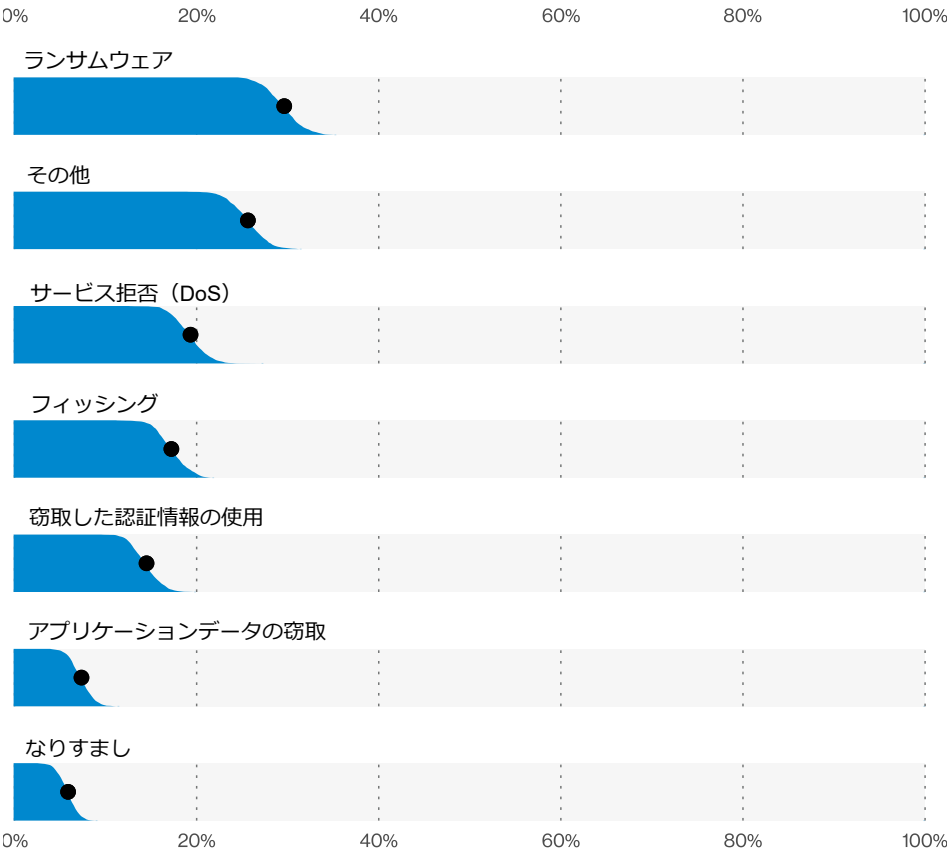


図111. 製造業のインシデントにおける上位の攻撃の種類（n=476）

鉱業、採石業、石油・ガス採掘および公益事業 NAICS 21+22

サマリー

これらの業界では、今年度、ソーシャルエンジニアリング攻撃を受けました。失われたデータの種類としては、認証情報、個人情報、内部情報が最も多くなっています。また、ランサムウェアもこれらの業界にとって大きな脅威となっています。

頻度	インシデント546件、確認されたデータ暴露355件
上位3つのパターン	「ソーシャルエンジニアリング」、「システム侵入」、「基本Webアプリケーション攻撃」がデータ漏洩/侵害件数の98%を占めている
攻撃者	外部（98%）、内部（2%）（漏洩/侵害）
攻撃者の動機	金銭目的（78%～100%）、スパイ活動（0%～33%）（漏洩/侵害）
侵害されたデータ	認証情報（94%）、個人情報（7%）、内部（3%）、その他（3%）（漏洩/侵害）
IG1による優先保護対策	セキュリティ意識およびスキル向上トレーニングプログラムの実施（14）、アクセス制御管理（6）、アカウント管理（5）

私たちの多くは、貴金属や鉱物を採掘する方法や、発電方法、PlayStation 5を起動するために必要な複雑なインフラを管理する方法について考える必要はありませんが、これらの業界の人々は、日常的にこれらのことを行わなければなりません。彼らは、雷雨、パイプの破損、リスなどのさまざまな環境上の脅威と戦わなければならないだけでなく、サイバー世界からの脅威にも直面しています。ここでは、現代のあらゆるモノをつなげるコネクテッドワールドを可能にしてきた産業が、そのコネクテッドワールドに噛みつかれようとしているわけです。では詳しく見ていきましょう。

これらの業界は、上位3つのパターンに関して、他の業界と大きな違いはありません。しかし、これらのパターンの内訳には違いがあります。これらの業界では、今年度はソーシャルエンジニアリングがデータ漏洩/侵害とインシデントの両方を支配しているようですが、一部の組織ではフィッシングキャンペーンが持続的に発生しています（図112）。この業種のデータ漏洩/侵害件数の86%はソーシャルエンジニアリングによるものであり、これにシステム侵入と基本Web アプリケーション攻撃が続きます。

次に多い攻撃タイプはランサムウェアで、この業界におけるソーシャルエンジニアリング以外の攻撃の44%を占めています。

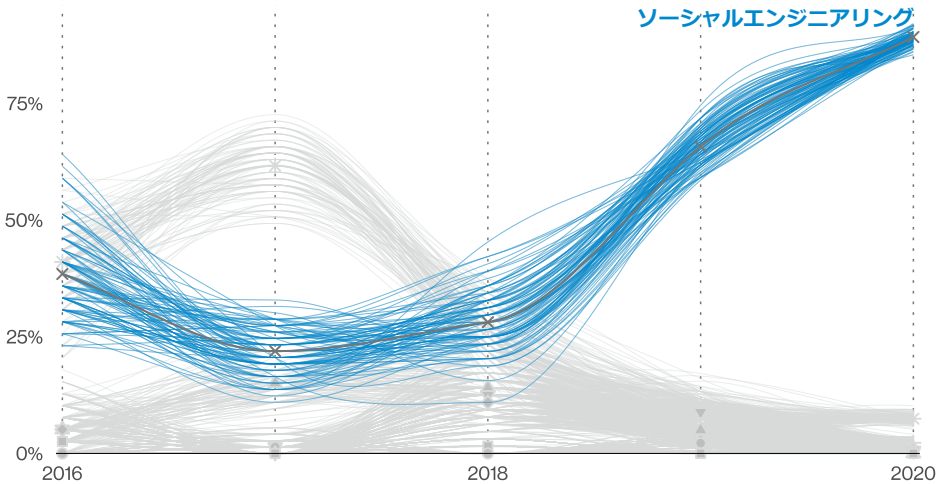


図 112. 鉱業、採石業、石油・ガス採掘および公益事業のインシデントのパターンの経時的変化

専門的・科学的・技術的サービス業 NAICS 54

サマリー

この業界では、「システム侵入」と「ソーシャルエンジニアリング」のパターンの組み合わせが大半を占めています。窃取した認証情報の使用は広く行われており、従業員はソーシャルエンジニアリングの手法に騙される傾向が顕著に見られます。

頻度	インシデント1,892件、確認されたデータ暴露630件
上位3つのパターン	「システム侵入」、「ソーシャルエンジニアリング」、「基本Webアプリケーション攻撃」がデータ漏洩/侵害件数の81%を占めている
攻撃者	外部（74%）、内部（26%）（漏洩/侵害）
攻撃者の動機	金銭（97%）、スパイ活動（2%）、怨恨（1%）（漏洩/侵害）
侵害されたデータ	認証情報（63%）、個人情報（49%）、その他（21%）、銀行（9%）（漏洩/侵害）
IG1による優先保護対策	セキュリティ意識およびスキル向上トレーニングプログラムの実施（14）、アクセス制御管理（6）、企業資産およびソフトウェアのセキュアな設定（4）

専門的なサービスを提供している企業であれば、NAICSコードが多種多様であり、攻撃対象の範囲が大きく異なることをご存知でしょう。共通しているのは、インターネットに接続されたインフラに依存していることと、そのアーキテクチャに内在するリスクです。「システム侵入」と「ソーシャルエンジニアリング」のパターンが上位を占めていることは、インフラの脆弱性だけでなく、これらの組織の従業員の脆弱性も示しています（図113）。

「システム侵入」パターンの背後にいる攻撃者は、標的にアクセスするために自由に使える強力なツールを持っています。これらのケースの中には、窃取した認証情報の使用や脆弱性の利用から始まり、最終的には被害者へのマルウェアの投下に至るまでの攻撃手段があります。多くの場合、そのマルウェアはランサムウェアであり、恐喝による要求や業務の中断につながります。ランサムウェアの増加については、以前のDBIRでも紹介しましたが、その傾向は衰える気配がありません。また、被害者に支払いを促すために、データのコピーを取るという手口も増えています（昨年度の報告書のデータ収集期間が終了した直後から見られるようになりました）。このように、データ漏洩/侵害が確認されたランサムウェアのケースでは、被害者のデータのコピーをインターネット上に公開するケースが増えています。

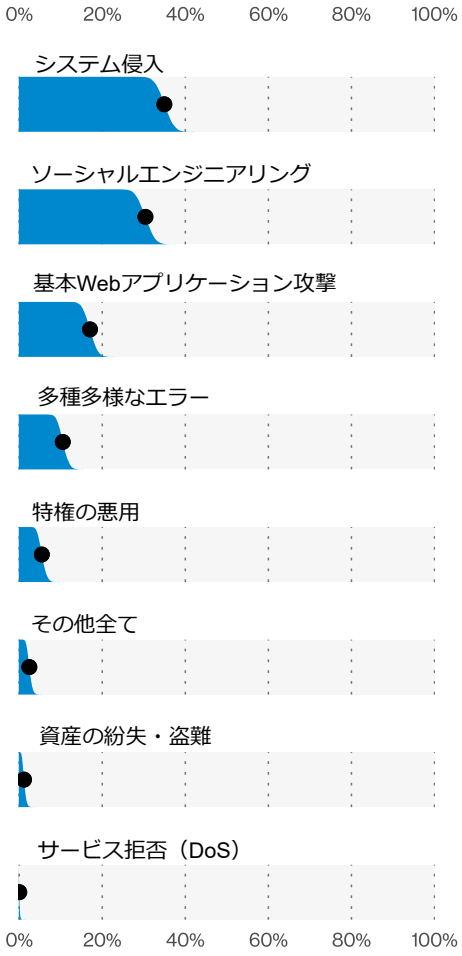


図 113. 専門的・科学的・技術的サービス業のデータ漏洩/侵害のパターン（n=630）

これを「ソーシャルエンジニアリング」のパターンと組み合わせると、インフラだけでなく、ソーシャルエンジニアリング攻撃の手口に耐えられる従業員の能力についても心配しなければなりません。攻撃としては「フィッシング」が最も多いが、メールによる「なりすまし」も多く見られました。（図114）。

架空のシナリオを使ったら、その後に続くのはたいてい金銭を得ようする攻撃です。これは不正取引としてデータに表示され、誰かがソーシャルエンジニアリング攻撃に引っかかったときの行動変容の完全性違反とともに表されます（図115）。

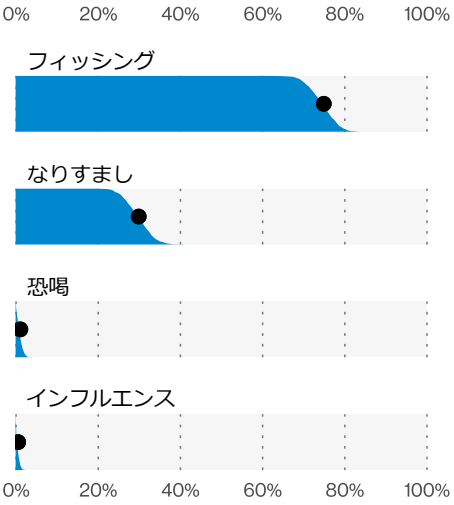


図114. 専門的・科学的・技術的サービス業のデータ漏洩/侵害におけるソーシャル攻撃の種類（n=191）

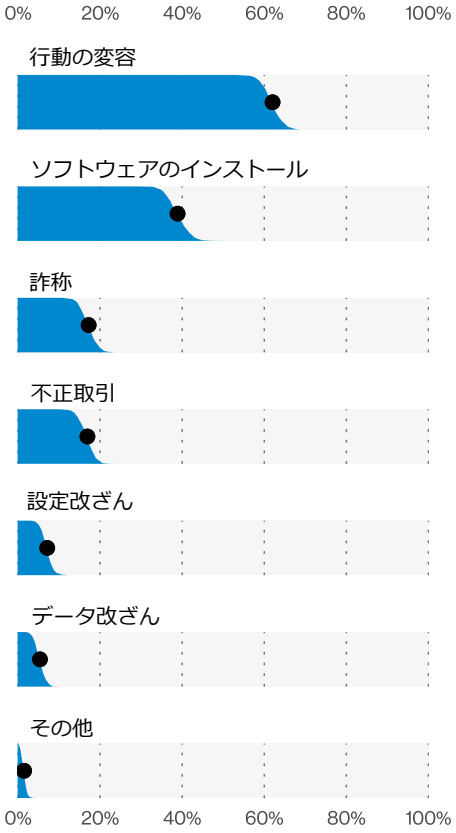


図115. 専門的・科学的・技術的サービス業のデータ漏洩/侵害における上位の完全性の種類（n=337）

ソーシャルエンジニアリング攻撃としては「フィッシング」が最も多いですが、メールによる「なりすまし」も多く見られました。

公務 NAICS 92

サマリー

この業界における最大の攻撃者は、何と言ってもソーシャルエンジニアです。信憑性のあるフィッシングメールを作成できる攻撃者は、この業界で驚異的な割合で認証情報を持ち逃げしています。

頻度	インシデント3,236件、確認されたデータ暴露885件
上位3つのパターン	「ソーシャルエンジニアリング」、「多種多様なエラー」、「システム侵入」がデータ漏洩/侵害件数の92%を占めている
攻撃者	外部（83%）、内部（17%）（漏洩/侵害）
攻撃者の動機	金銭目的（96%）、スパイ活動（4%）（漏洩/侵害）
侵害されたデータ	認証情報（80%）、個人情報（18%）、その他（6%）、医療（4%）（漏洩/侵害）
IG1による優先保護対策	セキュリティ意識およびスキル向上トレーニングプログラムの実施（14）、アクセス制御管理（6）、アカウント管理（5）

この業種では、「ソーシャルエンジニアリング」のパターンがデータ漏洩/侵害の69%以上を占めています（図116）。明らかに、この業種はフィッシング常習者お気に入りのハニーホールとなっています。ソーシャルエンジニアリング攻撃は、ほとんどがメールを使ったフィッシングでした（図117）。「なりすまし」はほとんど使われていません。普通のフィッシングで事足りているのですから、わざわざ新しいシナリオを作成する必要はないのでしょう。

図116. 公務のデータ漏洩/侵害のパターン（n=885）

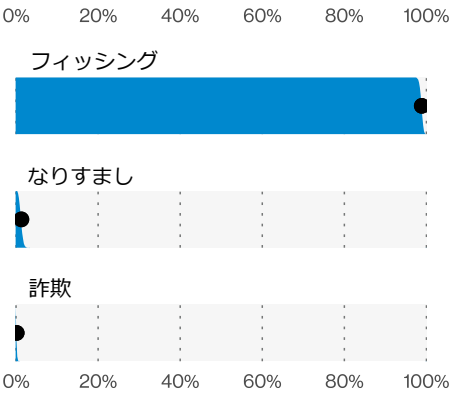


図117. 公務のデータ漏洩/侵害におけるソーシャルエンジニアリング攻撃の種類（n=611）

「多種多様なエラー」パターンは2位にランクしていますが、1位にかなり差をつけられており、「設定ミス」（セキュリティ研究者は通常発見しませんが、これが最も一般的な組み合わせであることは驚きでした）と「誤送信」で構成されています（図118）。確かに、政府機関は大量の郵便物を送ることが多く、誤った受信者に配信された資産として2番目に多かったのは紙の文書でしたが、1位は昔ながらの電子メールでした。

「システム侵入」は、ハッキングとマルウェアを組み合わせたパターンで、上位3つに入っています。このパターンでは、窃取した認証情報の使用、次にC2またはランサムウェアの機能を持つマルウェアの投下が最も一般的であることがわかりました。

最も頻繁に窃取される認証情報は、被害者のネットワークやシステム内で攻撃者の存在感を高めるために使用されます（図119）。この分野でデータ漏洩/侵害が確認されたデータタイプは、「個人情報」が「認証情報」に次いで多くなっています。

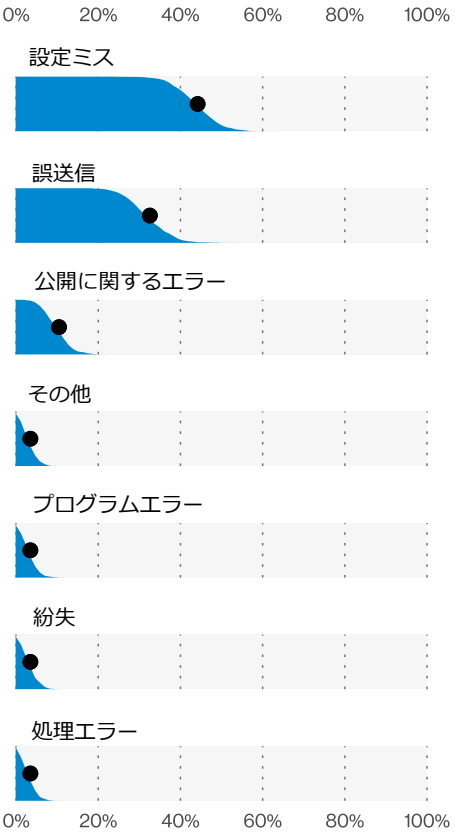


図118. 公務のデータ漏洩/侵害における上位のエラーの種類（n=86）

図119. 公務のデータ漏洩/侵害における上位のデータ種類（n=841）

小売業 NAICS 44-45

サマリー

小売業は、ペイメントカードと個人情報の両方を利用して現金を得ようとする金銭目的を動機とする犯罪者の標的であり続けています。ソーシャルエンジニアリング攻撃の手口としては「なりすまし」や「フィッシング」などがあり、前者では振り込め詐欺が行われることが多いです。

頻度	インシデント725件、確認されたデータ暴露165件
上位3つのパターン	「システム侵入」、「ソーシャルエンジニアリング」、「基本Webアプリケーション攻撃」がデータ漏洩/侵害件数の77%を占めている
攻撃者	外部（84%）、内部（17%）、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（99%）、スパイ活動（1%）（漏洩/侵害）
侵害されたデータ	決済情報（42%）、個人情報（41%）、認証情報（33%）、その他（16%）（漏洩/侵害）
IG1による優先保護対策	セキュリティ意識およびスキル向上トレーニングプログラムの実施（14）、企業資産およびソフトウェアのセキュアな設定（4）、アクセス制御管理（6）

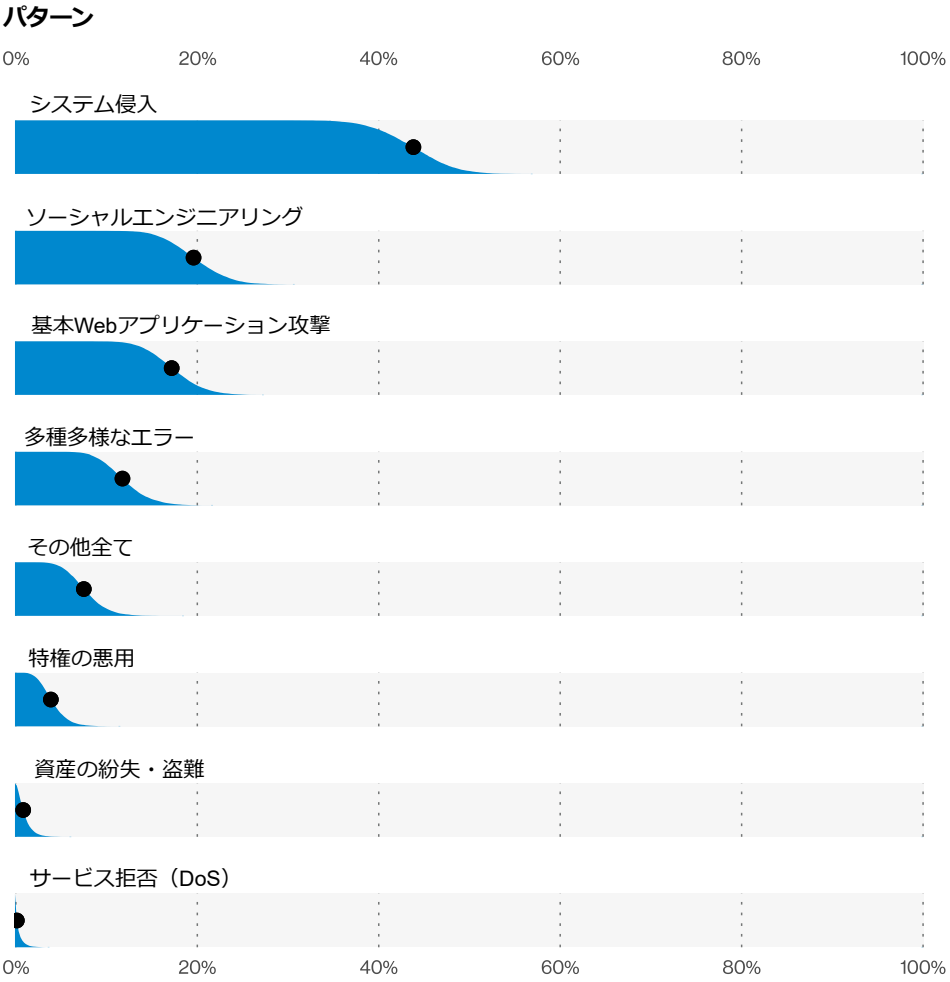


図120. 小売業のデータ漏洩/侵害のパターン（n=165）

サマリーの一覧表で最初に注目すべきは、インシデントの数と確認されたデータ暴露の数の差です。この主な原因は、この業界で大量のDoS攻撃（409件）が行われたことにあります。また、データ漏洩/侵害のパターンとしては「システム侵入」がトップでしたが（図120）、データ漏洩/侵害が確認できなかったインシデントでは2位でした（このパターンでは177件、そのうち69件でデータ漏洩/侵害が確認された）。

つまり、データ漏洩/侵害件数の少なさに惑わされることなく、この業種は依然として標的であるということです。

「システム侵入」のパターンが多く見られ、アプリケーションのデータを取得するために、「窃取した認証情報の使用」と「マルウェア」の投下を併用するのが一般的です。

前にも言いましたが、もう一度言います。みんな認証情報が大好きです。認証情報は、データタイプの中でもシュガーシロップをかけたドーナツのようなものです。

「なりすまし」（攻撃者が架空のシナリオを作成してターゲットをおびき寄せ、最終的には様々な形で送金させること）は、他の業界では通常見られないほど一般的になっています（図121）。誤解がないように、ここでもフィッシングの誘い文句は有効だということは言っておきます。従業員をターゲットにしてなりすましをするのは、犯罪者がお金を得るために懸命に働かなければならないことの表れなのか、それとも、従業員のふりをして詐欺を行うことのほうが単に簡単なだけなのか、判断は難しいです。

当然のことながら、侵害されたデータの上位には、ペイメントカード情報（金銭目的を動機とする犯罪者にとってこの業界が非常に魅力的である理由の大部分を占める）、個人情報（これも様々な金融詐欺に役立つ）、および認証情報が上がっています（図122）。

前にも言いましたが、もう一度言います。みんな認証情報が大好きです。認証情報は、データタイプの中でもシュガーシロップをかけたドーナツのようなものです。

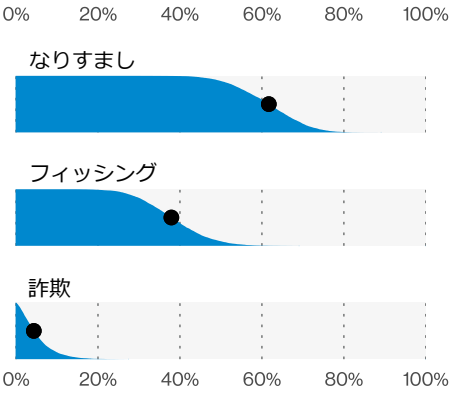


図121. 小売業でのデータ漏洩/侵害におけるソーシャルエンジニアリング攻撃の種類（n=32）

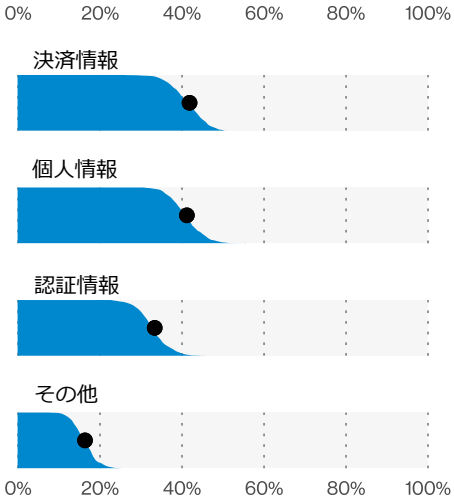


図122. 小売業でのデータ漏洩/侵害における上位のデータ種類（n=153）

05 中小企業

中小企業のデータ漏洩/侵害が増加

小規模（従業員数1,000人未満）

頻度	インシデント1,037件、確認されたデータ暴露263件
上位3つのパターン	「システム侵入」、「多種多様なエラー」、「基本Webアプリケーション攻撃」がデータ漏洩/侵害件数の80%を占めている
攻撃者	外部（57%）、内部（44%）、複数の関係者（1%）、パートナー（0%）（漏洩/侵害）
攻撃者の動機	金銭目的（93%）、スパイ活動（3%）、愉快犯（2%）、怨恨（1%）、その他（1%）（漏洩/侵害）
侵害されたデータ	認証情報（44%）、個人情報（39%）、その他（34%）、医療情報（17%）（漏洩/侵害）

1つのサイズでほぼすべてに対応

今年度のデータを組織の規模別に分析していて最初に気づいたのは、データ漏洩/侵害件数に関して中小企業と大企業の差が、かなり小さくなっていることです。昨年度は、小規模な組織でのデータ漏洩/侵害の発生件数は、大規模な組織の半分にも満たなかったのです。多くの政党とは異なり、今年度は、大規模組織で307件、小規模組織で263件のデータ漏洩/侵害が発生しており、両者の差はそれほど大きくありません。

もう1つの興味深い発見は、組織の規模にかかわらず、上位のパターンが同じだったことです。組織の規模の観点から比較をし始めてから初めて、この2つのグループのデータはかなり似たような結果になりました。少なくともパターン的には、どちらかを見れば分かる状況と言えそうです。

昨年、小規模な組織が大きく悩まされたのは、「Webアプリケーション」、「その他全て」、「多種多様なエラー」でした。今年は、「その他全て」のパターンを再調整し、残りの攻撃の大部分を占めるハッキングやマルウェアが「システム侵入」のパターンに該当することから、小規模の組織でもパターンの変更がかなりの部分を占めるようになりました。一方、大規模組織では、実際にかなりの変化がありました。昨年のトップ3は、「その他全て」、「クライムウェア」、「特権の悪用」でした。パターンの再調整により、「クライムウェア」タイプのイベントのほとんどが「システム侵入」と「基本Webアプリケーション攻撃」に入れられましたが、「特権の悪用」パターンには大きな変化は見られませんでした。つまり、会社のデータを悪用する内部犯行が減少したことを示しています。

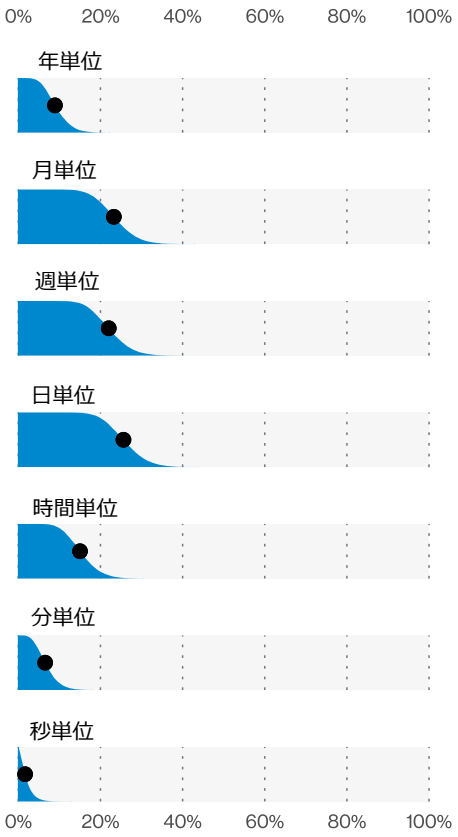


図123. 中小企業でのデータ漏洩/侵害における発見のタイムライン（n=83）

大企業（従業員数1,000人以上）

頻度	インシデント819件、確認されたデータ暴露307件
上位3つのパターン	「システム侵入」、「多種多様な エラー」、「基本Webアプリケーション攻撃」がデータ漏洩/侵害件数の74%を占めている
攻撃者	外部（64%）、内部（36%）、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（87%）、愉快犯（7%）、スパイ活動（5%）、自己都合（2%））、怨恨（2%）、二次的動機（1%）（漏洩/侵害）
侵害されたデータ	認証情報（42%）、個人情報（38%）、その他（34%）、内部情報（17%）（漏洩/侵害）

2つの組織規模の間でパターンがほぼ一致したことについて、これが両者にとってどのような意味を持つのかを少し説明します。まず、どちらも金銭目的を動機とする組織犯罪者に狙われています。プロの犯罪者は金銭を動機とする傾向があるので、皆さんにとってこれは新しい情報ではありません（そのはずです）。さらに言えば、アマチュアの犯罪者もきっとそのほとんどが金銭目的でしょう。賭けてもよいです（皆さんには分からないように賭けますが）。

よく見られる「システム侵入」と「基本Webアプリケーション攻撃」のパターンについては、単純なものから複雑なものまで多種多様な攻撃があり、Webインフラに狙いを絞ったものが多いです。窃取した認証情報を使ってマルウェアをインストールするというハッキング攻撃は、これらの攻撃者が手引きにする攻略ガイドとなっています。最近では、システムに侵入してからランサムウェアを展開するケースが増えています。時にはデータのコピーを取った後で、被害者にビットコインをかき集めて差し出すように要求することもあります。

発見のタイムラインに目を向けると、組織の規模によって違いが見られます（それぞれ図123と図124）。昨年度の報告書では、小規模な組織は大規模な組織よりも迅速に侵害を発見している点で優れているようだと報告しました。

今年度のデータによると、大規模な組織では半数以上（55%）のケースで「数日以内」に侵害を発見するようになったのに対し、小規模な組織では47%とあまり積極的ではないことがわかりました。

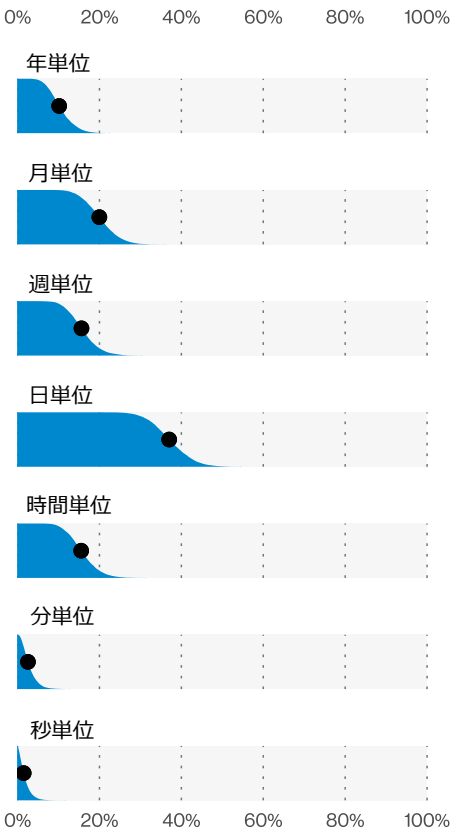


図124. 中小企業でのデータ漏洩/侵害における発見のタイムライン（n=92）

06

地域別の分析

地域について

昨年度、初めて地域別にインシデントを分析し、マクロリージョンの観点から発表しました。今年度は、サイバー犯罪についてよりグローバルな視点を読者に提供するために、再び（可能な限り）世界の様々な地域を訪れました。予想されるように、データの提供者の存在、地域の情報開示規制、私たち自身のケースロードなどのいくつかの要因に基づいて、強弱の違いはあるにせよ特定の地域に焦点を当てています。

あなたは以下に挙げられていない地域に住んでいたり、働いていたりしますか？あなたが拠点としている地域にもっと焦点を当てるべきだとお考えですか？そのような場合は、DBIRのデータ提供者になることをベライゾンまでご連絡ください。または、あなたの地域や業界の他の組織にもデータの提供を呼びかけてください。そうすれば、私たちは毎年、調査対象地域をさらに充実させていくことができます。お住まいの地域がこの報告書に掲載されていない場合、必ずしもその地域の情報が全くないということではなく、単にその地域でのインシデントの数が統計的に十分でないことを意味していることにご留意ください[74]。

本報告書の世界の地域は、国のスーパーリージョンとサブリージョンを組み合わせた国連のM49規格に基づいて定義されています。これにより、調査地域は以下のように分けられます。

アジア太平洋地域（APAC）：南アジア（034）、東南アジア（143）、中央アジア（143）、東アジア（030）、そして最後にオセアニア（009）を含むアジア太平洋地域

ヨーロッパ、中東、アフリカ地域（EMEA）：北アフリカ（002）、ヨーロッパと北アジア（150）、西アジア（145）を含むヨーロッパ、中東、アフリカ地域

北アメリカ（NA）：主に米国とカナダにおけるデータ漏洩/侵害が含まれる北米地域（021）

74 英語の表現でよく使われる「メッセンジャーを責めても仕方がない」です。つまりこの報告書がルールを作っているわけではないので、すべて答えられるわけではありません。（秘密結社イルミナティと銀河系宇宙人、あるいはそのような類が作ってます）。

アジア太平洋地域（APAC）

サマリー

アジア太平洋地域で最も多いデータ漏洩/侵害は、金銭目的の動機を持つ攻撃者が従業員をフィッシングして認証情報を窃取し、その認証情報を使ってメールアカウントやWebアプリケーションサーバーにアクセスすることで発生しました。

頻度	インシデント5,255件、確認されたデータ暴露1,495件
上位3つのパターン	「ソーシャルエンジニアリング」、「基本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/侵害件数の98%を占めている
攻撃者	外部（95%）、内部（6%）（漏洩/侵害）
攻撃者の動機	金銭目的（96%）、スパイ活動（3%）、愉快犯（1%）（漏洩/侵害）
侵害されたデータ	認証情報（96%）、個人情報（3%）、その他（2%）、機密情報（1%）（漏洩/侵害）

アジア太平洋地域は、地球上の広大な部分を占めており、多くの国、言語、多様な文化が存在するとともに、猛毒の爬虫類も多く生息しています。この多様性に伴い、APAC地域では、昨年1年間に比較的幅広い業種においてデータ漏洩/侵害が発生しました。想定される主要な業種はすべて、ある程度の被害に遭っています。金融サービス、医療サービス、小売業、製造業、教育サービスなど、すべての業種が含まれています。実際、昨年度初めて、アジア太平洋地域のデータ漏洩/侵害件数が他の地域を上回りました。

今年度、特に顕著な数字を記録したのは、NAICS 21の鉱業、採石業、石油・ガスの採掘業です（図125）。これは、この業種の組織が巧妙なソーシャルエンジニアリング攻撃の餌食になったことが原因です。

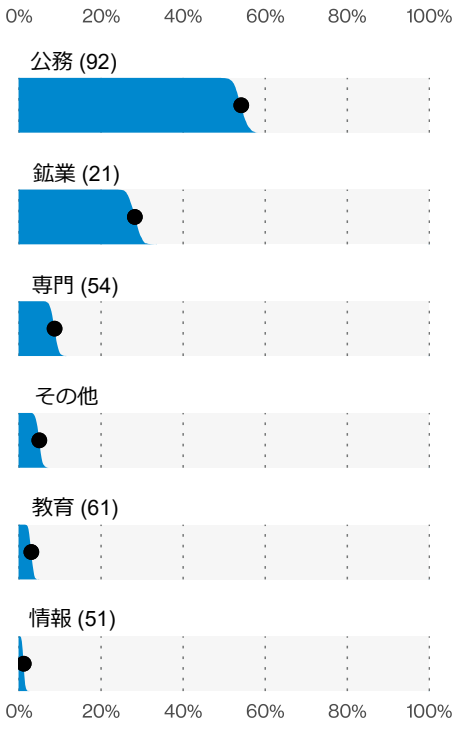


図125. アジア太平洋地域におけるデータ漏洩/侵害の上位の業種（n=1,130）

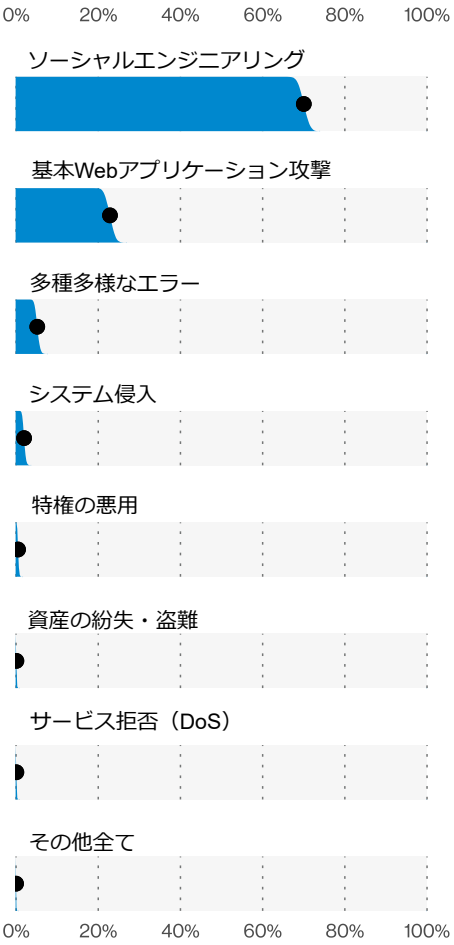


図126. アジア太平洋地域におけるデータ漏洩/侵害のパターン（n=1,495）

図126に示すように、アジア太平洋地域の攻撃の70%には、フィッシングなどのソーシャルエンジニアリングの要素が含まれています。これらの攻撃で盗取されたのは、ほとんどが認証情報（98%）でした。これらの認証情報は、ソーシャルエンジニアリング攻撃をエスカレートまたは横展開するために使用されるか、あるいは組織が運用するWebアプリケーションに侵入するために使用されました（23%）。

この報告書の他のセクションをご覧になった方は、この時点である疑問をお持ちかもしれません。誰がこれらの犯罪を実行したのか？暗い部屋でパーカーを着ていたのだろうか？なぜこの地域ではランサムウェアが見られないのか？おっしゃる通りです。私たちが知る限り、これらの犯罪はほとんどが金銭目的の動機を持った組織犯罪者によるものです。私たちはこのトピックに関して裏付けに乏しいデータしか持っていませんが、パーカーと暗い部屋がある程度関与していることは確かだと思います。しかし、最後の、そして最も興味深い質問である「ランサムウェアはどこにあるのか」に関して、アジア太平洋地域のランサムウェアはマルウェアの種類で10位であり、他の地域で見られるものとはかなり対照的です。しかし、これは、この種のマルウェアが実際に少ないのではなく、本報告書のデータ提供者とその取扱い件数の副産物であることは間違いありません。アジア太平洋地域では、他の地域と同様、「止まれ、あり金とデータを全部置いて行け」という攻撃が盛んに行われていると思われます。

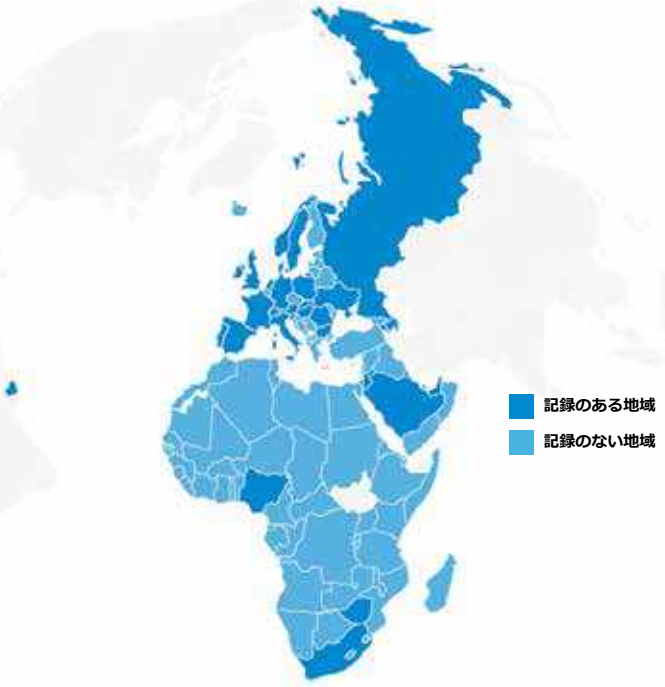
欧州・中東・アフリカ地域（EMEA）

サマリー

欧州・中東・アフリカ地域は、引き続き「基本Webアプリケーション攻撃」、「システム侵入」、「ソーシャルエンジニアリング」に悩まされています。

頻度	インシデント5,379件、確認されたデータ暴露293件
上位3つのパターン	「基本Webアプリケーション攻撃」、「システム侵入」、「ソーシャルエンジニアリング」がデータ漏洩/侵害件数の83%を占めている
攻撃者	外部（83%）、内部（18%）（漏洩/侵害）
攻撃者の動機	金銭目的（89%）、スパイ活動（8%）、愉快犯（1%）、怨恨（1%）（漏洩/侵害）
侵害されたデータ	認証情報（70%）、内部情報（52%）、個人情報（22%）、その他（16%）（漏洩/侵害）

この地域では、2年連続で「基本Webアプリケーション攻撃」が最も多く見られ、データ漏洩/侵害件数の約54%を占めています。



EMEAは、欧州・中東・アフリカ地域を指します。この地域では、2年連続で「基本Webアプリケーション攻撃」パターンが最もよく見られ、データ漏洩/侵害件数の約54%を占めています。

これらの攻撃は、アプリケーション自体の格納データを取得することが目的の場合もありますが、他の形態の悪事を働くための単なる手段である場合もあります。

この地域では、「システム侵入」、「ソーシャルエンジニアリング」、「多種多様なエラー」の3つのパターンが拮抗して2位を占めています（図127）。欧州・中東・アフリカ地域で最も多くデータ漏洩/侵害されているデータタイプは認証情報であり、これが各パターンの位置を説明するのに役立ちます。多くの場合、窃取された認証情報が使用されたことは分かっていますが、最初にどのようにして入手したかについては必ずしも明らかにされていません。しかし、攻撃者が認証情報を入手する際には、多くの場合、フィッシングという形のソーシャルエンジニアリングが用いられていることがわかっています。

最初に手に入れた方法にかかわらず、窃取した認証情報を使用することは、攻撃者が組織に侵入するための主要な手段であり、多くの場合、Webアプリケーションを介して行われます。

最後に、EMEAの攻撃者の17%は内部の人間（多くはシステム管理者）であり、上位4つのパターンに「多種多様なエラー」が含まれているのはそのためです。大半（67%）のケースは、意図しない「設定ミス」によるものです。

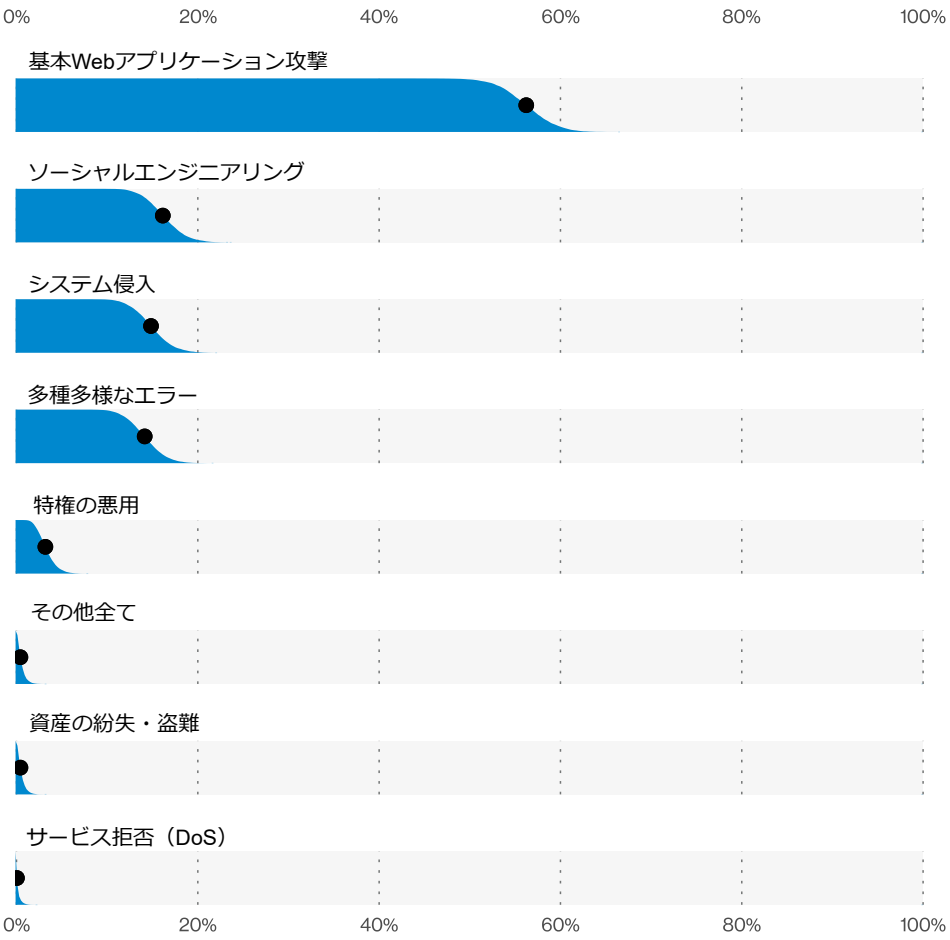


図127. 欧州・中東・アフリカ地域におけるデータ漏洩/侵害のパターン（n=293）

北アメリカ（NA）

サマリー

北アメリカの組織は、金銭や簡単に収益化できるデータを求める金銭的動機を持った攻撃者の標的になり続けています。ソーシャルエンジニアリング、ハッキング、マルウェアは、引き続きこれらの攻撃者が好んで利用するツールとなっています。

頻度	インシデント13,256件、確認されたデータ暴露1,080件
上位3つのパターン	「ソーシャルエンジニアリング」、「システム侵入」、「基本Webアプリケーション攻撃」がデータ漏洩/侵害件数の92%を占めている
攻撃者	外部（82%）、内部（19%）、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（96%）、スパイ活動（3%）、怨恨（2%）、愉快犯（1%）（漏洩/侵害）
侵害されたデータ	認証情報（58%）、個人情報（34%）、その他（27%）、内部情報（11%）（漏洩/侵害）

北アメリカのインシデントおよびデータ漏洩/侵害に関するデータを見る際には、示された数字に対する規制環境の影響を認識することが重要です 。

この地域のデータ漏洩/侵害の開示に関する法律は広く普及しており、その結果、サイバー犯罪に対する可視性は、このような法律がない地域よりも高くなっています。医療サービスや公務は規制の厳しい業界であるため、これらの業界での普及率が高くなっています。前述の法律に加えて、この地域には他の地域よりも多くのデータ提供者がいることを念頭に置く必要があります。

北アメリカのデータに関しては、2つのはっきりとした競争があるようです（図128）。1つ目は、「ソーシャルエンジニアリング」と「システム侵入」が拮抗していることです（それぞれ約35%）。もう1つは、「基本Webアプリケーション攻撃」と「多種多様なエラー」の間で、どちらの攻撃が小さいかを競っていることです。これらのグループの間では、信頼区間が大きく重なっているため、どちらが勝っているかを明確にすることは非常に困難です。したがって、これらのパターンの統計を見るときは、実際には2組のパートナーが一緒に踊っているということを念頭に置いてください。

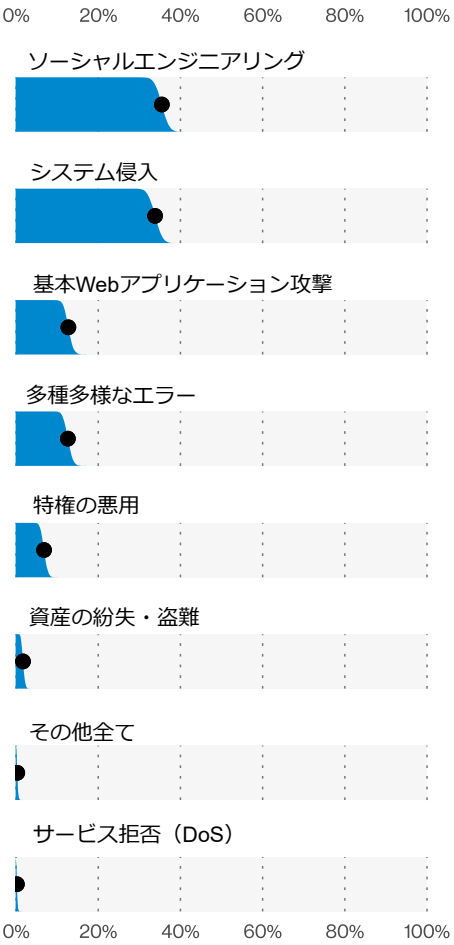


図128. 北アメリカにおけるデータ漏洩/侵害のパターン（n=1,080）

新しい「ソーシャルエンジニアリング」パターンは、主に「なりすまし」と「フィッシング」の攻撃で構成されています（図129）。通常は、念入りなシナリオを作成して行うフィッシングよりも、シンプルなタイプのフィッシングが多く見られます。一般的に、犯罪者は効率的に行動する傾向があり、基本的なことで成功を収めることが多いのですが、なぜ必要以上に手間をかけるのでしょうか？考えられる答えの1つは、「なりすまし」攻撃者の最終的な目標が、通常のフィッシング攻撃者のそれとは異なるということです。「なりすまし」攻撃は、手っ取り早く金銭に近づくための試みであることが多く、最も一般的な目的は、被害者に影響を与えて送金させることです（もちろん偽装して）。このような架空のシナリオは攻撃者によって多少異なりますが、例えば、銀行情報のすり替えや、架空の請求書の支払いなどがあります。一方、フィッシング攻撃者は、現金ではなくデータを目的としている場合があり、最終的な目的は、フィッシングで窃取したデータ（認証情報）を収益化すること、または組織への足掛かりを得ることのいずれかです。「システム侵入」パターン（これも新しい）では、多くの場合、ハッキングとマルウェアを組み合わせた攻撃が行われています。一般的には、窃取した認証情報を使ってアクセスし、その後、攻撃者が組織内での目的を達成するためにマルウェアを投下します。北アメリカでは、これはランサムウェアの展開を意味します。昨年度の報告書でも述べたように、ランサムウェアのグループは、暗号化を開始する前に、被害者に対抗する手段としてデータのコピーを取得します。これを始めたのはMazeグループで、彼らが成功を収めると、他のグループもこの流れに乗りました。現在では、ランサムウェアのグループの多くが、このようなデータダンプをホストするためのインフラを独自に開発しており、それが一般的なものとなっています。

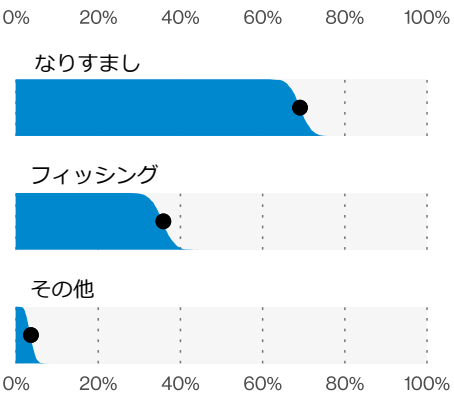


図129. 北アメリカにおけるデータ漏洩/侵害のソーシャルエンジニアリング攻撃の種類（n=385）

これらのソーシャルおよびマルウェア攻撃には、CIAの3要素のうちの「完全性」の違反を引き起こすという共通の特徴があります。ソーシャル攻撃では、ソーシャルエンジニアリング攻撃の影響を受けた被害者の行動の変化を表す「行動変容」が見られます。成功している「なりすまし」攻撃に関しては、被害者に送金させることができると、「不正取引」の「完全性」属性が現れます。マルウェアは、もちろん、違反行為としてのソフトウェアのインストールにつながります。また、詐称は、フィッシング攻撃者のPhredとなりすましのPattiのもう1つの副次的効果であり、両者とも（他の多くの人と同様に）他人のふりをして、組織内でより多くの被害者（フォロアーとでも言いましょうか）を得ようとしています。

フィッシング攻撃が広く行われていることを考えると、ここで認証情報が頻繁に登場します（図130）。個人情報も主要な標的となります。社会保障番号や保険番号などのデータ要素に加えて、犯罪者がさらなる金融詐欺を行うためのその他の情報が含まれているためです。

発見のタイムラインを見ると、かなりの割合で1日以内に発見されていることがわかります（それぞれ図131と図132）。しかし、これらのケースの半分以上は、攻撃者がデータ漏洩/侵害を公表することで発見されています。これは、ランサムウェアが発見される典型的な方法で、身代金の請求書が画面上に表示されたときに発見されます。この公表が行われるのは、暗号化が開始された直後と考えられます。私たちは、内部の検知管理者がデータ漏洩/侵害の大半を発見する責任があると考えています。しかし、少なくとも身代金の請求書が表示された時点で、組織は侵入を阻止し、ネットワークから犯人を追い出すことができます。

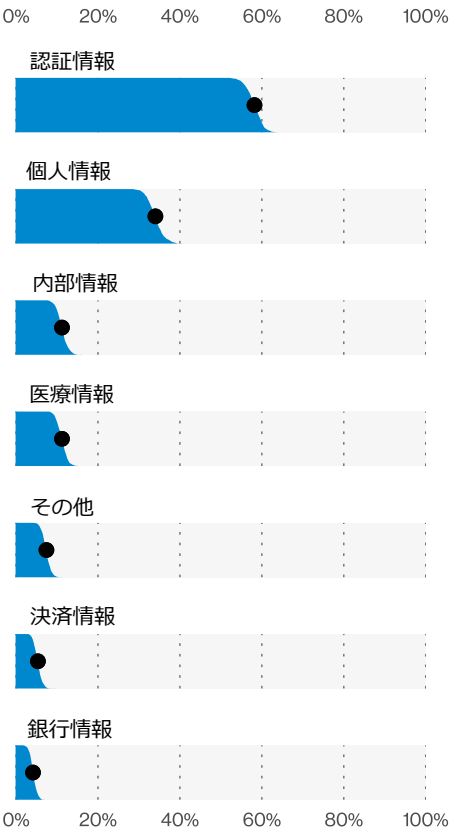


図130. 北アメリカにおけるデータ漏洩/侵害の上位のデータの種類（n=579）

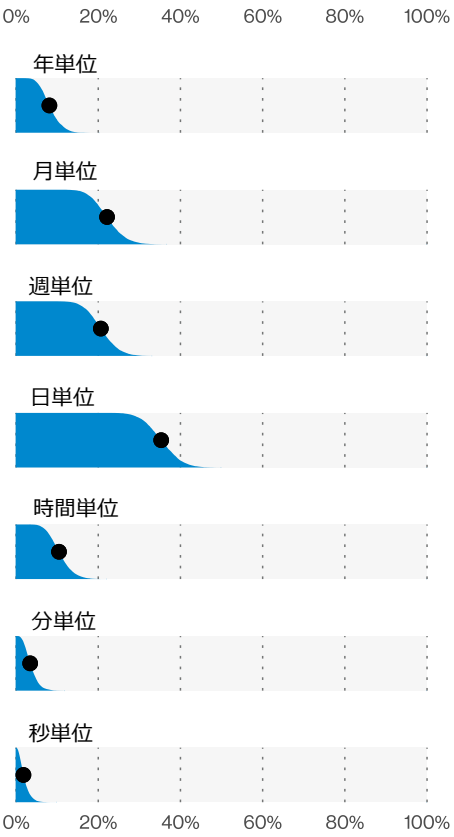


図131. 北アメリカにおけるデータ漏洩/侵害の発見のタイムライン（n=128）

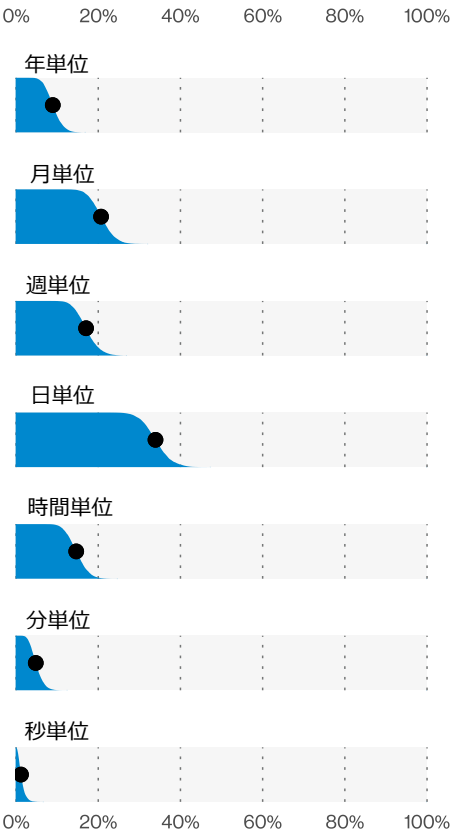


図132. データ漏洩/侵害の発見のタイムライン（n=195）

07 まとめ

これで第14回目のデータ漏洩/侵害調査報告は終了です。

自分自身を、そしてお互いを褒めてあげてください。いや、大きな大きな、バーチャルハグがいいかもしれません[75]。すべてうまく行くでしょう。読者の皆さん、今回も私たちと一緒に時間を過ごしてくださり、ありがとうございました。報告書の情報が皆様のお役に立てれば幸いです。また、内容が皆様にとって有益で、かつ理解しやすいものであることを願います。今年度の報告書でも何度か触れましたが、次のカーブを曲がった先に何が待っているのかを見通すことは必ずしも容易ではありません。しかし、1つだけ分かっていることは、理性を保ち、思いやりと気遣いを持って[76]、そして何よりもお互いに協力し合えば、それがどんなものであっても私たちは対処できるということです。

もちろん、毎年この報告書を完成させるために、時間、専門知識、そして最も重要なデータを惜しみなく提供してくださる協力者の方々に感謝せずに、この報告を締めくくることはできません。DBIRチームを代表して、皆様に感謝いたします。読者の皆様におかれましては、ご質問、ご意見、ご感想などがございましたら、お気軽にご連絡ください。来年の15号で、また皆様にお会いできることを楽しみにしています。安全に、そして幸せにお過ごしください。

75 腕がものすごく長くて距離を保てる人はリアルハグでも良いです。
76 脆弱性研究者のダン・カミンスキーのように。

年間総括[77]

1月

2019年、2020年ともにVerizon Threat Research Advisory Centerの情報収集は、中国を拠点とする攻撃者menuPassによるクラウド環境を標的としたサイバースパイ活動から始まりました。継続化する脅威の中には、リモートアクセスに対する攻撃がありました。シトリックス製品の新たな脆弱性を狙った攻撃や、Pulse Secure、FortiOS、Palo AltoのVPNサーバーに対する継続的なパスワードスプレー攻撃などです。ロンドンの金融サービス企業であるTravelex社は、大晦日にSodinokibiランサムウェアに感染しましたが、これはPulse Secure VPNサーバーへのパッチ適用を怠ったことが原因であるとする情報もあります。米国沿岸警備隊は、Ryukの感染により港湾施設が30時間にわたって閉鎖されたことを発表しました。2020年の最初のゼロデイ攻撃は、JScriptにおけるInternet ExplorerのUse After Free脆弱性CVE-2020-0674を悪用したものでした。Qihoo 360は、DarkHotel攻撃者による、エクスプロイトのカクテルを利用した水飲み場型攻撃を報告しました。CVE-2020-0674（Internet ExplorerのJScript）とCVE-2019-17026（Firefox）とCVE-2017-11882（Office Equationエディタ）です。

2月

オーストラリアのサイバーセキュリティセンターは、オーストラリアの輸送・物流会社であるThe Toll Groupが攻撃されたことを受けて、「Mailto」や「Netwalker」と呼ばれるランサムウェアに関する勧告を発表しました。パッチチューズデーに、マイクロソフト社は、CVE-2020-0674に対するパッチを含む99のパッチをリリースしました。また、Microsoft Exchangeの脆弱性、CVE-2020-0688に対するパッチも公開されました。VTRACは、2週間以内に、Exchange Serverの脆弱性を狙った大量のスキャンと悪用に関する情報を収集しました。Cybersecurity and Infrastructure Security Agency（CISA）は、天然ガスのパイプライン施設に対するRyukランサムウェアの攻撃に関する情報を警告として発表しました。産業用制御システム（ICS）のセキュリティ企業であるDragos社は、1月の米国沿岸警備隊の報告書へのリンクを含む評価を公開しました。Google社は、Chromeブラウザの新バージョンをリリースした5日後に、野放状態で悪用されていた型混乱の脆弱性（CVE-2020-6418）を緩和するための別のバージョンをリリースしました。

3月

西部劇（映画のジャンル）のファンは、夕食時に「チャックワゴンの三角ベルを鳴らす」ことに気づくことでしょう。新型コロナウィルス感染症は、サイバー犯罪者にも同じ効果をもたらし始めました。おそらく最もすぐに役立つコレクションは、RiskIQの「COVID-19 Daily Update」レポートとドメインのウォッチリストまたはブロックリストです。PrevailionとProofpointは、新型コロナウィルス感染症を餌にしたTA505攻撃に関する情報を作成しました。1月末までに、マイクロソフトは、Windows 7の新しい脆弱性を悪用した限定的な標的型攻撃について顧客に警告していました。Windows 10には脆弱性はありませんでした。CVE-2020-1020は、Adobe Type Manager Libraryのセキュリティ欠陥でした。FIN7は、Trustwave社の顧客を対象に、50米ドルのギフトカードを餌とした悪意のあるUSBドライブを配布しました。

4月

BAHは、GRU（ロシアの軍事情報機関）による200件以上のサイバー作戦の再評価を発表し、それらがロシアの戦略的ドクトリンに準拠しており、ある程度予測可能であると結論付けました。Recorded Futureは、MITREのATT&CKを活用して、2019年に最も一般的なサイバー攻撃者のTTPを調査したレポートを発表しました。Malwarebytes社は、『APTs and COVID-19: How advanced persistent threats use the coronavirus as a lure』を刊行しました。新型コロナウィルス感染症パンデミック時のサイバーセキュリティに関するリソースとしては、BBCのサイバーセキュリティ特派員であるJoe Tidy氏の検索可能な「Coronavirus Phishing Scams」コレクションと、National Cyber Security Allianceの「COVID-19 Security Resource Library」の2つがありました。マイクロソフト社がパッチを当てた113の脆弱性のうち、3つが野放し状態で悪用されていました。CVE-2020-1020とCVE-2020-0938に対するパッチは、「Adobe Type Manager Libraryのパッチが適用されていない脆弱性を利用した、限定的な標的型Windows 7ベースの攻撃」を緩和しました。3番目の奇襲攻撃は、Windowsカーネルの特権昇格の脆弱性CVE-2020-1027を悪用したものでした。しかし、マイクロソフト社は、4月の終わりまでに、オートデスクのDLLの脆弱性（CVE-2020-7085）に対するアドバイザリを臨時でリリースしました。

77 VTRACのDavid M. Kennedy氏のご協力に感謝します。

5月

オラクル社は、WebLogicサーバーが4月のクリティカルパッチアップデートに含まれていたCVE-2020-2883のパッチを適用されることなく野放しで悪用されてたいたことを報告しました。F-Secure社は、Amazon Web ServicesやGCPなどのデータセンターやクラウド環境で頻繁に使用されている構成管理ツールである SaltStackのSalt管理フレームワークに、2つの深刻な脆弱性があることを発表しました。CISAは、「Top 10 Routinely Exploited Vulnerabilities」を発表しました。 ESET社は、韓国と台湾のゲーム会社に対するWinntiの攻撃についての情報を発表しました。台湾の法務省は、両国の石油精製所に対するランサムウェア攻撃にWinntiが関与していると考えています。Broadcom/Symantec Intelligence社は、Greenbugによる南アジアの通信会社への攻撃を取り上げました。Cisco社は、同社のバックエンドサーバ6台が、SaltStackの脆弱性CVE-2020-11651およびCVE-2020-11652を悪用したハッカーによって侵害されたことを公表しました。オーストラリアの物流大手であるToll Groupは、3ヶ月間で2回目のランサムウェア攻撃を受けました。Trustwave社は、英国のテクノロジー企業が中国の銀行から義務付けられている納税ソフトウェアにバックドアを仕込んだ「GoldenSpy」に関するレポートを配信しました。

6月

Cycldekという知名度の低い中国の攻撃者が「USBCulprit」というマルウェアを展開しました。カスペルスキー社は、このマルウェアがインターネットから隔離されたシステムに拡散し、そこからデータを盗み出すことを目的としていると評価しています。6月にパッチが適用された150以上の脆弱性のうち、パッチリリース前に悪用されていたものはありませんでした。オーストラリアのモリソン首相は、政府や企業を含むオーストラリアの組織が、現在、外国の洗練された「国家支援」の攻撃者から標的にされていると述べました。「Evil Corp」と呼ばれるこのAPT級のサイバー犯罪者は、比較的新しいランサムウェア「WastedLocker」で「大物狩り」を始めました。NCC GroupとSymantec社は、Evil Corpの新しいキャンペーンに関する情報を独自に発表しました。

7月

F5 BIG-IP装置を導入している企業は、2つの新しい脆弱性を利用した攻撃の危険にさらされており、U.S. Cyber Command社は「直ちに修正する」よう呼びかけています。エクスプロイトコードはITWでした。BIG-IPのハニーポットが攻撃され、マルウェアがインストールされました。FortiGuard社、Palo Alto社、Deep Instinct社は、ホンダとエネル社のシステムを停止させたランサムウェア「EKANS（SNAKE）」に関する情報を報告しました。シトリックス社は、Citrix ADC、Gateway、SD-WANに新たに存在する11の脆弱性に対するセキュリティ速報とパッチを公開しました。VTRACは、3日以内に、ハニーポットでシトリックスの脆弱性が検出され、その後、暗号通貨のマイニングソフトウェアをインストールしようとする不正行為が行われたという報告を収集しました。英国、米国、カナダは共同で、APT29（Cozy Bear）（ロシア）が新型コロナウィルス感染症ワクチンの研究機関を標的にしていると報告しました。Sansec社は、Lazarus GroupがMagecartによるペイメントカードのスキミングを利用して米国およびEUの電子商取引業者を攻撃していることを報告しました。McAfee社とSentinelOne社は、それぞれLazarusによる異なるキャンペーンを報告しています。

8月

Cisco社のファイアウォールやマネージドサービスプロバイダーとその顧客が使用している管理ツール「TeamViewer」に関するセキュリティ勧告を収集しました。銀行業務用トロイの木馬の新しい亜種であるIcedID、Dridex、Emotetを広めるキャンペーンに関する情報を収集しました。MITREが「2020 CWE Top 25 Most Dangerous Software Weaknesses」を発表しました。米国の3機関が、新たに有名になった北朝鮮の攻撃者BeagleBoyのこと、およびこの攻撃者がATMの「ジャックポット」攻撃に使用するマルウェアについて共同レポートを発表しました。F-Secure社は、北朝鮮の脅威が仮想通貨組織を標的にしていることを報告しています。

9月

Group-IBは、2015年以降、Magecartペイメントカードのスキミングキャンペーンを行っている攻撃者UltraRankを報告しました。SWIFTとBAE Systemsは、『Follow the Money』というそのタイトルにふさわしいサイバー犯罪経済に関するレポートを発表しました。CISAは、イランの脅威活動をカバーする2つの製品を発表しました。SenseCyによると、イラン人が利用するいくつかの脆弱性は、ランサムウェアの利用者にも好まれているとのことです。Intel 471は、Lazarusがターゲットへの初期アクセスにロシアのクライムウェアを使用していると評価しています。Microsoft Securityは、いわゆる「ZeroLogon」の脆弱性（CVE-2020-1472）のパッチが適用されていないシステムを悪用した野放しの攻撃を報告しています。

10月

オーストラリアのサイバーセキュリティセンター（ACSC）は、オーストラリアの組織に影響を及ぼす「継続的かつ広範な」Emotetキャンペーンに関する勧告を発表しました。VTRACは、Netlogon/ZeroLogon（CVE-2020-1472）の悪用に関する脅威情報を引き続き収集しています。CISAとマイクロソフト社は、MuddyWaterやTA505といったAPT級の攻撃者によるNetlogon/ZeroLogonの悪用を確認しています。ClearSky Securityによると、イランのAPT攻撃者「MuddyWater」は、イスラエルの組織を標的にしています。Telsy社は、MuddyWaterが、イタリアの航空宇宙およびアビオニクス分野の専門家を標的とした別のキャンペーンの背後にいるとしています。Google社は、過去最大級の2.54TbpsのDDoS攻撃を軽減したと発表しました。米国のバーベキューレストランチェーン「Dickey's」は、2019年7月から2020年8月にかけてPOS攻撃を受けました。

11月

VTRACは、8つの新しい脆弱性について、リスクに関連する情報を収集しました。そのうち3つはすでに悪用されており、残りは攻撃が成功したという報告もなくエクスプロイトコードが野放し状態になっています。11月のパッチチューズデーには、マイクロソフト社のパッチが114件、アドビ社の製品アップデートが2件、SAP社のセキュリティノートが12件（ホットニュースが6件）、Chromeブラウザのアップデートが4件、インテル社のセキュリティアドバイザリが40件リリースしました。マイクロソフト社の脆弱性1件、Chromeブラウザの脆弱性5件については、すでにエクスプロイトコードが野放しにされています。Bitdefenderは、東南アジアの政府を攻撃する中国のAPTのレポートを発表しました。LazarusとKimsukyによる攻撃は、それぞれESETとEAST Securityによって報告されました。Egregorランサムウェアは、Mazeランサムウェアの後継としての地位を確立しつつあります。オーストラリアのサイバーセキュリティセンターは、リモートアクセス用トロイの木馬「SDBBot」とランサムウェア「Clop」を使用したTA505攻撃について、医療分野に注意を喚起しました。

12月

Malwarebytes社とCERT-Bund社は、Gootkitバンキング・トロイの木馬とREvil（Sodinokibi）ランサムウェアを使ってドイツのユーザを狙っていたキャンペーンについて警告しました。SolarWinds Orionのアップデートプロセスを悪用した画期的な攻撃は、おそらく最もコストのかかるサイバー攻撃としてWannaCryを凌駕するでしょう。第一段階のSunburstマルウェアにさらされた18,000人のSolarWindsの顧客に対し、攻撃者の優先ターゲットの中に含まれていたかどうかを調べるために、脅威調査を行うことになりました。マイクロソフト社では、「ピンポイントで標的とされ、洗練された追加の手段で侵害された」40以上の顧客を特定しました。SolarWindsのネットワーク内には、少なくとも2人の異なる攻撃者がいたと考えられます。一人はFireEye社が発見したAPT級の攻撃者で、あまり洗練されていないもう一人のほうは、SUPERNOVAのバックドアを広めていました。APT攻撃者のほうは、極めて少ない数の被害者を優先に置き、Teardropドロッパー・トロイの木馬を使ってCobalt Strike Beaconを配信する攻撃を強化していました。優先されたこれらの被害者の数はおそらく数百人程度で、Sunburstのネットワークを利用したコマンド＆コントロールやマルウェアの配布を解明することで特定されます。

08
付録

付録A：方法論

読者の皆様が本報告書を高く評価してくださっている理由のひとつは、データの収集、分析、発表の際に採用している厳密さと誠実さです。

読者の皆様がこのようなことに関心を持ち、鋭い目で情報を吟味してくださることが、我々の誠実さを保つことにつながります。私たちの方法を詳しく説明することは、その正直さの重要な部分を占めています。

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。verizon.com/business/resources/reports/dbir/2021/report-corrections/

次に、私たちは自分たちの作業をチェックしています。DBIRで挙げた数値の根拠となるデータをGitHubリポジトリで見ることがで きますが[78]、昨年と同様にファクトチェックレポートも公開しています。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[79]。

最後に、フランソワ・ジャコブが「デイサイエンス（昼間の科学）」と「ナイトサイエンス（夜の科学）」について説明しています[80]。デイサイエンスは仮説に基づく作業（仮説検証）ですが、ナイトサイエンスは創造的な探求（探索的分析）です。DBIRはまさにナイトサイエンスです。Yanaiらが述べているように、デイサイエンスに焦点を当てすぎると、データの中に潜む殺し屋を見逃してしまうことがあるのです[81]。私たちは、完璧ではないかもしれませんが、入手可能な最善の真実[82]（後述するバイアスの影響を受けた上で、所定の信頼レベルに到達している真実）を提供していると信じています。

しかし、因果関係を証明することは、現在の科学の制御された実験に任せるのが最善です。私たちにできるのは相関関係だけです。相関関係は因果関係ではありませんが、ある程度の関連性があり、役に立つことが多いのです。

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。ベライゾン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。

DBIRのプロセス

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はVocabulary for Event Recording and Incident Sharing（イベント記録とインシデント共有のための言語）を略したもので、無料で利用でき、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ベライゾンが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。

一部のソーススプレッドシートは、一貫した変換を行うために、自動マッピングによってベライゾンの標準スプレッドシートのフォーマットに変換されています。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、区分が欠けている場合は追加し、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2ヶ月間、毎晩実行され、データが収集および分析されます。

78 https://github.com/vz-risk/dbir/tree/gh-pages

79 テスト方法について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

80 ヤコブF.の『The Statue Within:An Autobiography』（CSHL Press; 1995）の下地になっているのはItai Yanai, Martin Lercher らによる『Selective attention in hypothesis-driven data analysis』（bioRxiv 2020.07.30.228916）

81 本当なのです。データを印刷して、仮設検証している人はその殺し屋を見落としてしまうのです。

82 エリック・ブラックの『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』（とても良い本です。お薦めします）。

インシデントデータ

私たち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、私たち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。

今年度も信頼区間を利用して、小さなサンプルでも分析できるようにしました。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. 少量のサンプルでは、値がある範囲にあることや、値が互いに大きい/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、ベライゾン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、次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、2019年11月1日から2020年10月31日まで）である必要があります。本報告書の分析対象は主に2020年の事例ですが、全期間のデータがあらゆる箇所で参照されており、特に傾向を表すグラフで使用されています。また、組織属性の損失に結び付けることのできない個人に影響を及ぼすインシデントおよびデータ漏洩/侵害については、これを除外しました。例えば、ご友人の私用ノートPCが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。

データ漏洩/侵害

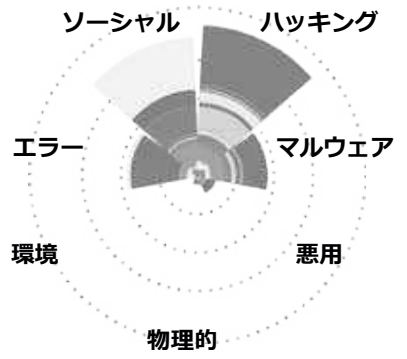


図133. 攻撃別の各貢献度

データ漏洩/侵害

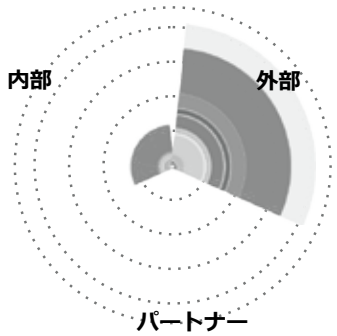


図134. 攻撃者別の各貢献度

データ漏洩/侵害

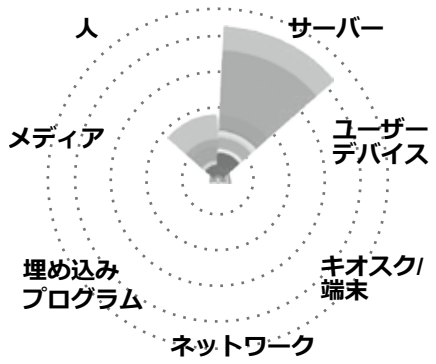


図135. 資産別の各貢献度

データ漏洩/侵害

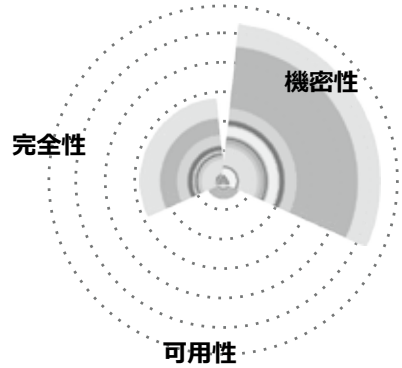


図136. 属性別の各貢献度

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（私たち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、そのため私たちでも把握していないデータ漏洩/侵害も数多くあります。したがって、全世界で発生するデータ漏洩/侵害（私たちの調査対象母集団です）を全て把握できる調査を私たち、または他の誰かが毎年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[83]。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±0.6%[84]、データ漏洩/侵害では±1.5%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。ベライゾンでは、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。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、私たち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。

図133～136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、バイアスが大きくな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

83 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

84 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またはマルコフ連鎖モンテカルロ法によって決定された95%信頼区間です。詳しくは、ModernDiveの第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.htm

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、その軸に沿って小規模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貢献しているのが見て取れます。

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。ベライゾンでは、データセット全体を探索的分析（ナイトサイエンス）に使用しているため、特定の仮説検証（デイサイエンス）は行いません。Earth-616や多元宇宙の他の地球のデータ漏洩/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これが最善の方法であると考えています。

上述のように、私たち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）。

データのサブセット

私たち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、分析の一環として私たち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。

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には分析を必要とするにもかかわらず「インシデント」または「データ漏洩/侵害」という私たちの通常のカテゴリー に当てはまらなかった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。ベライゾン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全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。

付録B：CISコントロール

1	企業資産のインベントリと管理
2	ソフトウェア資産のインベントリと管理
3	データ保護
4	企業資産とソフトウェアのセキュアな設定
5	アカウント管理
6	アクセス制御管理
7	継続的な脆弱性管理
8	監査ログ管理
9	電子メールとWebブラウザの保護
10	マルウェア対策
11	データ復旧能力
12	ネットワークインフラ管理
13	ネットワークの監視と防御
14	セキュリティの意識向上とスキルのトレーニング
15	サービスプロバイダーの管理
16	アプリケーションソフトウェアセキュリティ
17	インシデントレスポンス管理
18	侵入テスト

この重要で有益なセクションを忘れてはいません。安心してください。

心配ご無用です。監査人、CISO、統制フリークの皆様からのご要望にお応えして、コミュニティが作成したCIS Controlsを使用してマッピングを更新します[85]。ご存知でない方もいらっしゃるかもしれませんが、CISコントロールは、今年度のDBIRのパターンと同様に、8回目のメジャーアップデートを行い、創造的に「CIS Controls v8」と名付けられました。幸いなことに、VERISにマッピングされたCISコントロールを「バージョン8にしておけばよかった」ということはありません。

CISコントロールは、コミュニティによって構築、維持、サポートされている一連のベストプラクティスであり、攻撃者の行動に基づいて組織が防御の優先順位を決めることを目的としています。いわゆる「攻撃から防御を学ぶ」アプローチのベストプラクティスです。DBIRは、マクロレベルでの攻撃者の知識を得るための1つのリソースに過ぎません。それにもかかわらず、私たちは幸運なことに、彼らのコミュニティプロセスにフィードバックを提供し、意見を提案する立場にありました。NISTのサイバーセキュリティフレームワーク（CSF）の戦略的ロードマップを取締役会レベルで発表する場合でも、新しいセキュリティプログラムの取り組みに対する個別の資金要求を守る場合でも、私たちの目標は、DBIRの調査結果とデータを、皆さんの会社の取り組みに簡単に結び付けられるようにすることです。貴重な時間を割いて協力してくださった方々の努力により、ベストプラクティスが進化していく様子を目の当たりにし、我々は感激しています。ここでは、何が変わったのかをご紹介します。

- クラウドやモバイルなどのテクノロジーの導入
- 「ボーダーレス」なネットワークと、ネットワーク/システム管理者間の緊密な連携を考慮して、コントロールをアクティビティ別に編成し、コントロールの数を20から18に削減

85 https://www.cisecurity.org/controls/

- データ保護の重要性を示すため、コントロールの順序を変更（従来は13、現在は3）
- 組織がクラウドサービスをどのように管理すべきかを示す「サービスプロバイダー管理」コントロールを追加

CISコミュニティがバージョン7から継続することを決定した、より有用なコンポーネントの1つに、実装グループ（IG）があります。IGは、組織がリソース、リスク、その他の要因に基づいて、コントロールの実施にさらに優先順位をつけるのに役立ちます。これは、すべての組織がセキュリティを必要としている一方で、医療用医薬品の国際的なリーダーである巨大なUmbrella社は、ラクーンシティの研究施設を保護するために、地元のペットホテルよりも大規模で異なるセットを必要としているという考え方です。IGは互いに重なり合い、実装グループ1はコントロールの一部（約36%）が実装される出発点となり、その後、153のセーフガードすべてが実装される実装グループ3へと発展していきます。

図137は、マッピングをより詳細に分解し、パターン間の関係と各実施グループのCISコントロールとの重なりを示しています。

報告書では、各業界の「最強保護の実装グループ1コントロール」が追加されていることに気づかれたと思います。コントロールのパターン、実装グループ、セキュリティ機能へのマッピングを組み合わせて使用することで、規模や予算にかかわらず、すべての組織が導入を検討すべきコントロールの中核となるセットが見つかりました。

コントロール4：企業資産とソフトウェアのセキュアな設定

このコントロールは、名前が長ったらしいだけはありません。安全なソリューションを後から付け加えるのではなく、最初から設計することに重点を置いたセーフガードを含みます。このコントロールでは、設定ミスなどのエラーベースの違反や、ポータブルデバイスのリモートワイプ機能を強制することによる資産の損失を減らすことに大きな効果があります。

コントロール5：アカウント管理

このコントロールは、技術的にはバージョン8の新しいコントロールですが、保護機能は、「境界保護」や「アカウントの監視と制御」など、いくつかの以前のコントロールに見られた以前のアカウント管理の実践を一元化したものであるため、非常に馴染みやすいものとなっています。このコントロールは、組織がアカウントへのアクセスを管理することを目的としており、ブルートフォース攻撃やクレデンシャルスタッフィング攻撃に対して有効です。

コントロール 6:アクセス制御管理

このコントロールは、コントロール5の従兄弟にあたります。単純にユーザーアカウントを監視し、そのアカウントへのアクセスを管理するのではなく、権利と権限を管理し、最後に環境の主要なコンポーネントに多要素認証を実施します。これは、「窃取した認証情報の使用」に対して有効な手段となります。

コントロール14：セキュリティ意識向上とスキルのトレーニング

このコントールは古典的なものであるため、多くの説明は必要なさそうです。エラーやソーシャルエンジニアリングが広く普及していることを考えると、認知的な危険性に満ちた世界に対応するチームをサポートするためには、意識向上と技術トレーニングにお金をかけることが賢明であることは明らかです。

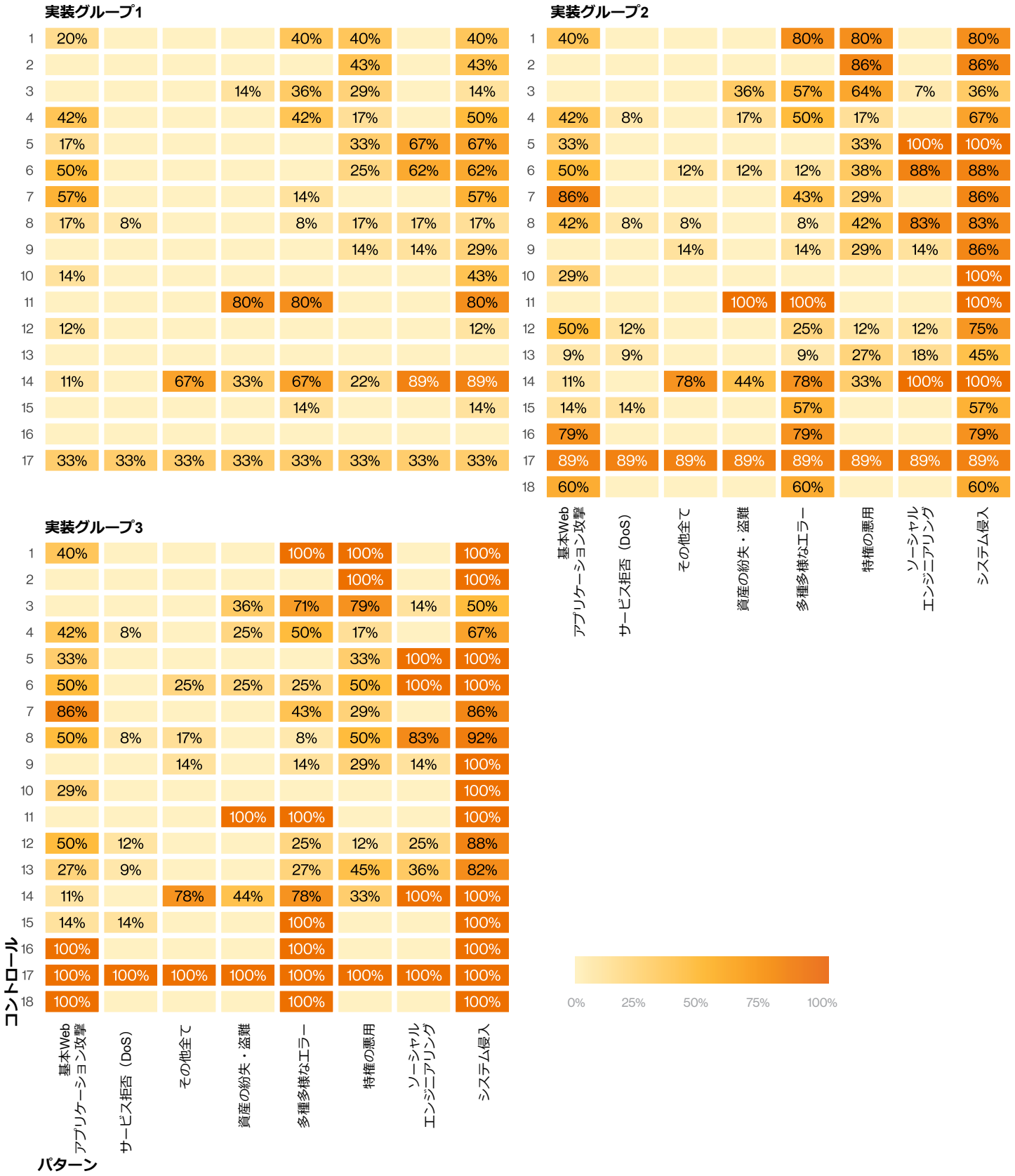


図137. CISとパターンのマッピング

付録C: 米国シークレットサービス

デビッド・スミス
担当特別捜査官
犯罪捜査部
米国シークレットサービス

バーナード・ウィルソン
ネットワーク侵入対応
プログラムマネージャー
犯罪捜査部
米国シークレットサービス

世界的なパンデミックの中での金融インフラの保護

2020年は「新型コロナウィルス感染症」と呼ばれる世界的なパンデミックが発生した年として記憶され、その短期的・長期的な影響が懸念されています。パンデミックは、ロックダウンとリモートワークへの急速な移行に始まり、経済の減速とそれに伴う救援活動へと続きました。このパンデミックは生活のあらゆる面に影響を及ぼし、特にサイバー犯罪を助長するものでした。

わずか数週間のうちに、組織は可能な限りリモートワークに移行しなければなりませんでした。大幅に拡大したリモートワークへの依存により、基盤となるインターネットや情報技術のインフラの弱点に関連した攻撃の数と深刻さが急増しました。これにより、多くの組織で事業継続計画（BCP）のテレワーク部分に関連するインシデントが増加しました。BCPは一般的に、組織のネットワーク上で利用可能なサービスへのリモートアクセス、内部コミュニケーションのための電子メールトラフィックの急増、企業のビデオおよびオーディオコミュニケーションへの依存度の増加に関する規定を含みます。このような変化に伴い、一般的な通信手段を悪用したマルウェアやソーシャルエンジニアリングによる攻撃が増加しました。

多要素認証や仮想プライベートネットワーク（VPN）の導入を怠った組織は、パンデミックの際に標的となった被害者の大きな割合を占めました。アクセスに対するゼロトラストモデルは、将来的な理想ではなく、すぐに基本的なセキュリティ要件となったのです。PIV（Personal Identity Verification）、FIDO（Fast Identity Online）などのソリューションによる否認防止機能は、ゼロトラストアーキテクチャに不可欠なものとなりました。適切なネットワークセグメンテーション、横方向への移動の防止、最小特権、「Never Trust, Always Verify（決して信用せず、常に検証する）」などのセキュリティ体制と原則は、ネットワーク環境における不正な存在を防止または不正から回復するための組織の能力を示す強力な指標であることが証明されています。

2020年、パンデミックのさなか、サイバー攻撃者は、医療・公衆衛生分野を含む米国の被害者に対するマルウェア攻撃を増加させました。米国シークレットサービスは、小額のものから数億円の身代金を要求するものまで、ランサムウェアの攻撃件数が著しく増加したことを指摘しています。ほとんどの組織は、これらの攻撃を軽減するための適切なデータバックアップソリューションを持っていましたが、サイバー攻撃者は、機密データの流出に焦点を移しました。これらのサイバー攻撃者は、組織化された犯罪グループであることが多く、追加の身代金を支払わないとデータを公開すると脅すことで、窃盗を収益化しようとしました。このような収益化には暗号通貨が用いられ、収益の行き先を不明瞭にして、法執行機関が犯罪の責任者を特定して逮捕するのを妨げようとしています。

シークレットサービスをはじめとする法執行機関は、パンデミック対策のための詐欺行為を防止・抑止することに注力し、特に州に割り当てられた失業給付プログラムのための連邦資金に焦点を絞りました。

シークレットサービスの主な任務の1つは、米国の金融インフラを保護することです。今回のパンデミックでは、連邦政府が前例のない対応を迫られました。連邦議員は、パンデミックの経済的影響に対処するため、2.6兆ドルの納税者の資金を放出することを承認しました。連邦政府の資金が公開されたことで、パンデミック救済プログラムを悪用しようとする組織的な犯罪グループや個人の注目を集めました。その結果、シークレットサービスをはじめとする法執行機関は、パンデミック対策の詐欺行為を防止・抑止することに注力し、特に州に割り当てられた失業給付プログラムのための連邦資金に焦点を絞りました。この努力により、15億ドル以上が犯罪者の手に渡るのを防ぐことができ、被災地への支援を目的とした数億ドルが州や受給者に確実に返還されました。

しかし、このような努力にもかかわらず、犯罪者はパンデミック救済資金をさまざまなプログラムから流用しようと試み続け、その中には企業を支援するための6,973億ドルの融資も含まれていました。シークレットサービスとそのパートナーである法執行機関は、これらの犯罪を防止・軽減し、最終的には責任者を見つけて逮捕するための取り組みを拡大してきました。

2020年は、組織化されたサイバー犯罪集団がもたらす永続的な脅威が改めて示された年でした。病院のランサムウェア攻撃、流出した顧客データの販売、ATMのキャッシュアウト攻撃、パンデミックの救援金の窃盗など、犯罪の内容が何であれ、組織的な犯罪が蔓延していることは共通しています。犯罪者は、不正な利益を得るという共通の関心事に基づいて、公式または非公式に組織化され、時には国家に支援された悪意ある攻撃者と提携することもあります。サイバー攻撃者は、新たな機会に基づいて活動を素早く変化させ、利用可能なあらゆる戦術、技術、手順を用いて資金を盗み、ロンダリングを行います。組織犯罪を解体し、サイバー攻撃者を逮捕するためには、国内外の法執行機関が協力してサイバー犯罪グループとそのスキームに立ち向かうことが重要です。

シークレットサービスは、このような継続的な犯罪の変化に対応するため、連邦、州、地方、外国の法執行機関、検察、民間企業、学界が連携した「サイバー詐欺対策本部（CFTF）」のネットワークを運営しています。シークレットサービスのCFTFでは、サイバー犯罪を軽減するための重要なツールである信頼関係と情報共有を促進するために、アウトリーチ活動が中核となっています。犯罪者を逮捕することはシークレットサービスの究極の目標であり、今後もそうあり続けるでしょうが、米国の金融インフラを守るためには、予防と軽減も同様に重要です。

付録D:協力企業

A

Akamai Technologies

Ankura

Apura Cybersecurity Intelligence

Arics Cooper

Atos（Paladion)

AttackIQ

B

Bad Packets

BeyondTrust

Bit Discovery

Bit-x-bit

BitSight

BlackBerry Cylance

C

Center for Internet Security

CERT European Union

CERT National Insider Threat Center

CERT Polska

Chubb

Cisco Talos Incident Response

Coalition

Computer Incident Response Center Luxembourg（CIRCL)

CrowdStrike

Cybersecurity and Infrastructure Security Agency（CISA)

Cybir（formerly DFDR Forensics)

D

Dell

Digital Shadows

Dragos, Inc

E

Edgescan

Elevate Security

Emergence Insurance

EUROCONTROL

F

Farsight Security

F-Secure

G

Global Resilience Federation

Government of Telangana, ITE&C Dept.

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

Grey Noise

H

Hasso-Plattner Institut

Homeland Security Solutions B. V（HLSS)

I

ICSA Labs

J

JPCERT/CC

K

KnowBe4

L

Lares Consulting

Legal Services - ISAO

LMG Security

M

Malicious Streams

Maritime Transportation System ISAC（MTS-ISAC)

Micro Focus

Mishcon de Reya

mnemonic

N

National Cybersecurity & Communications Integration Center（NCCIC)

NetDiligence®

NETSCOUT

P

ParaFlare Pty Ltd

Proofpoint

PSafe

Q

Qualys

R

Rapid7

Recorded Future

S

S21sec

SecurityTrails

Shadowserver Foundation

Shodan

SISAP - Sistemas Aplicativos

Swisscom

T

Tetra Defense

V

VERIS Community Database

Verizon Cyber Risk Programs

Verizon DDoS Shield

Verizon Digital Media Services

Verizon Managed Security Services - Analytics（MSS-A)

Verizon Network Operations and Engineering

Verizon Professional Services

Vestige Digital Investigations

VMRay

Verizon Threat Research Advisory Center（VTRAC)

W

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）

か

カスペルスキー

さ

サイバーセキュリティ マレーシア（通信マルチメディア省（KKMM）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

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）


ankura
COLLABORATION DRIVES RESULTS

Akamai

CROWDSTRIKE

emergence

apura

Malicious Streams


CERT-EU

Mishcon de Reya

VICTORIA
Australia

LMG
SECURITY

digital shadows_

GREYNOISE

AricsCooper

CHUBB

kaspersky

ICSA labs

edgescan

bit-x-bit

IRISS

F-Secure

CyberSecurity
MALAYSIA

KnowBe4

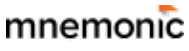
EUROCONTROL

ATTACKIQ

NASK
CERT.PL

DELL Technologies

CIRCL
Computer Incident
Response Center
Luxembourg

HOMELAND
SECURITY
SOLUTIONS BV

mnemonic

BeyondTrust

FORSIGHT
SECURITY

MICRO
FOCUS

JPCERT CC®

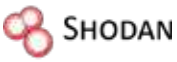
Coalition

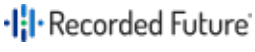

BIT
DISCOVERY

Check Point

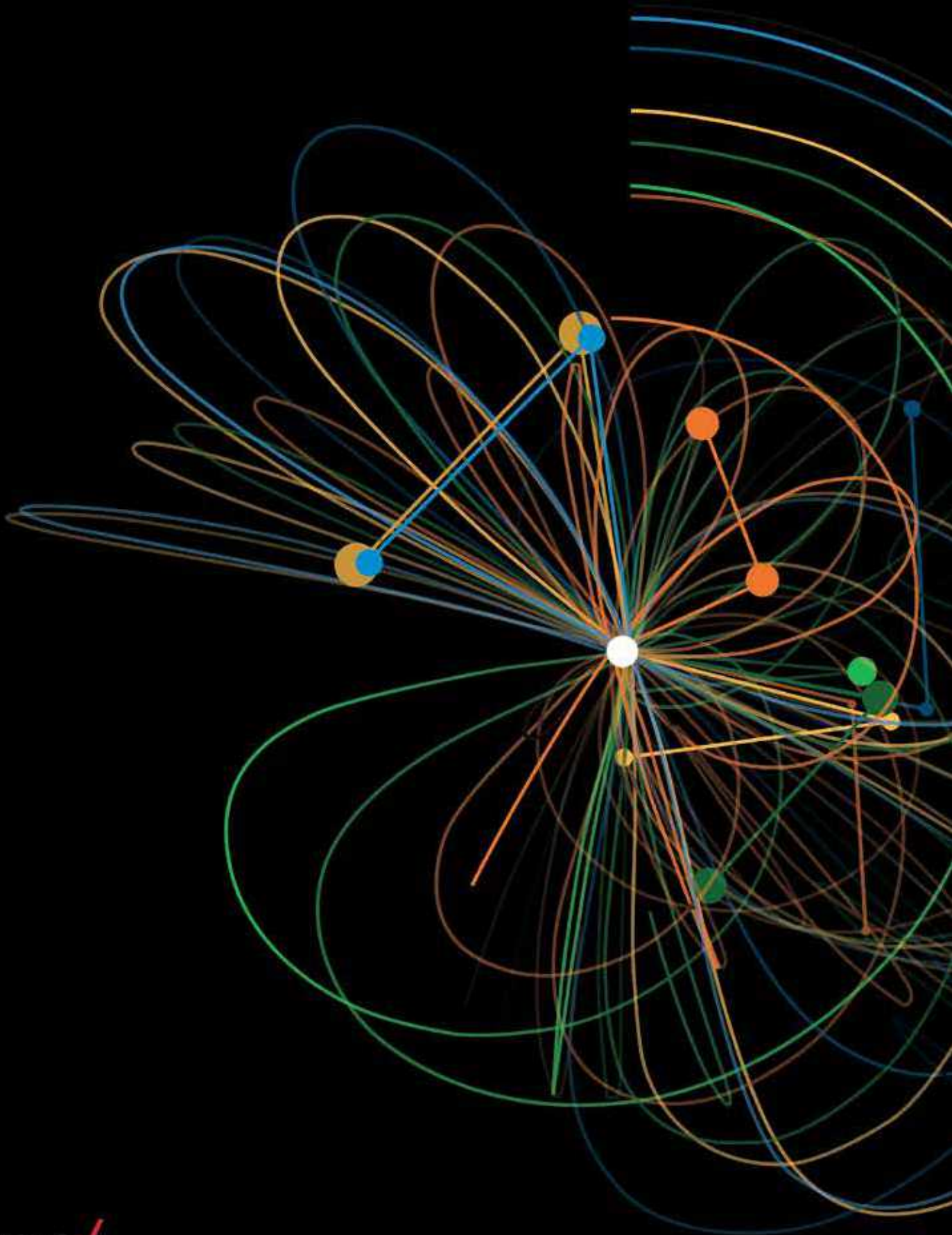
HPI
Hasso
Plattner
Institut
Digital Engineering · Universität Potsdam

CYBIR





Verizon Threat
Research Advisory
Center (VTRAC)



verizon