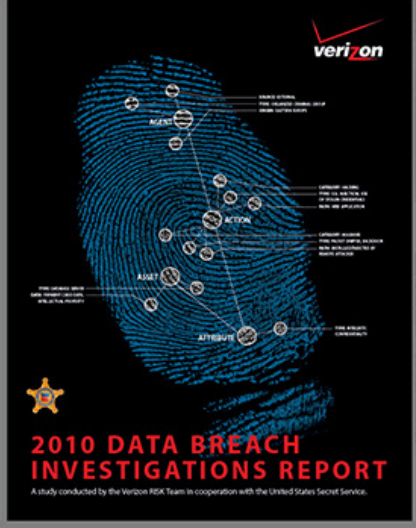
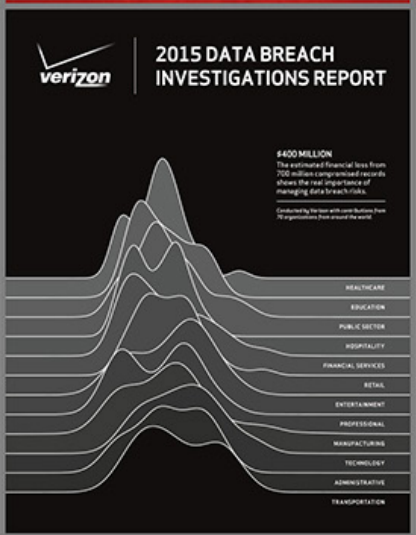
DBIR

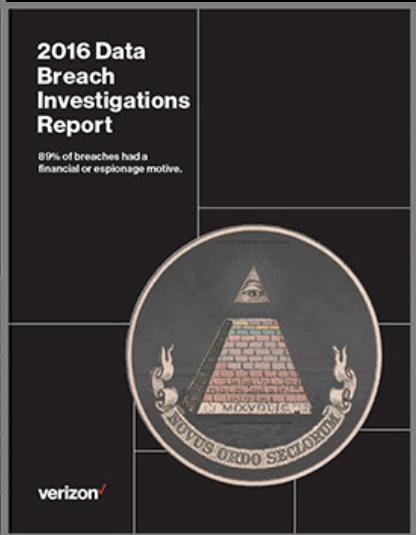
データ漏洩/侵害調査報告書



表紙について

長年にわたる読者の方は覚えていらっしゃるかもしれませんが、2008年の報告書の表紙はサーバールームにひっそりと置かれた椅子の写真でした。あの写真には多くの組織において、正しくその資産とデータを守っていないという事実を表現する意図がありました。2022年の表紙は、懐かしさとともに多くの組織は依然としてその人とシステムに注意を払うことに苦労しているという意図を込めて、2008年の報告書に立ち返ってみました。重ねた時間軸とドット模様は、15年の報告書の歩みの中でグローバルでの情報提供にご参加くださった組織の数を表しています（年毎に分かれています）。





目次

本書の凡例と定義

2022年度データ漏洩/侵害調査報告書（DBIR）へようこそ。初めての方は最初にこのセクションをお読みいただくことをお勧めします（何度も読んだという方は「はじめに」にお進みいただいて構いません）。私たちはこの報告書の作成に長い間取り組んできて、使われている言葉が少々難解であることも理解しています。しかし命名規則、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（Threat action）：資産に影響を及ぼすために使用された手口（行為）。VERISでは、マルウェア、ハッキング、ソーシャルエンジニアリング、不正使用/悪用、物理的攻撃、エラー、環境という7つの主要攻撃カテゴリーを使用します。大まかな例としては、サーバーのハッキング、マルウェアのインストール、ソーシャルエンジニアリング攻撃によって人の行動に影響を及ぼすことなどが挙げられます

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

詳細情報はこちらをご覧ください。

- **github.com/vz-risk/dbir/tree/gh-pages/2022** – 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、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。

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。

斜めの棒グラフは、毎号のDBIRの読者にはおなじみのものです。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）。

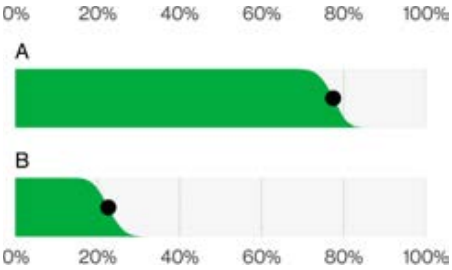


図1. 棒グラフの傾きの例（n=205）

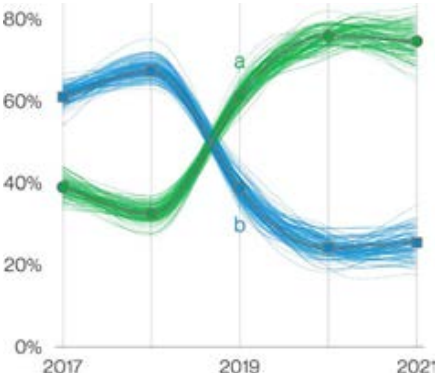


図2. スパゲッティチャートの例

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。

ピクトグラムプロットは、比較的新しいグラフで、斜めの棒グラフと同様の方法で不確実性を捉えようとするものですが、より単一の割合に適しています。

この複雑なデータセットの参照が、例年よりもさらにスムーズになることを願っています。

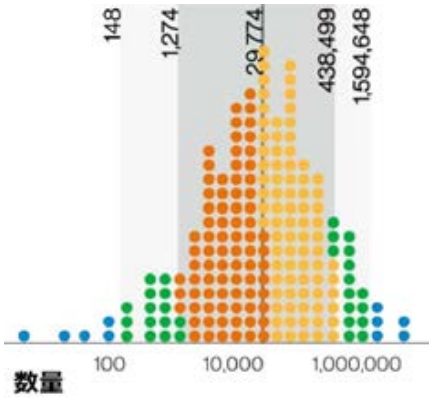


図3. ドットプロットの例（n=672）。各ドットは組織の0.5%を表す。オレンジ：80%の下半分。黄色：80%の上半分。緑色：80%-95%。青：異常値。組織の95%：148 - 1,594,648。80%：1,274 - 438,499。中央値：29,774（対数スケール）。

図4. ピクトグラムプロットの例（n=4,110）。それぞれの人型は40のデータ漏洩/侵害

注意：この注意書きはいつも「方法論の」セクションに記載しているものですが（この種の情報はそこに属するため）、本報告書をそこまで読み進めない人のために、ここでも言及することにしました。毎年、DBIRの対象となるインシデントのタイムラインは、ある暦年の11月1日から翌暦年の10月31日までです。したがって、このレポートに記載されているインシデントは、2020年11月1日から2021年10月31日の間に発生したものです。2021年のケースロードは、2022年の報告書の主な分析対象ですが、特にトレンドグラフでは全範囲のデータを参照しています。後者の日付からこの報告書が発行されるまでの期間は、世界中の80以上の協力者からデータを入手し、そのデータを匿名化して集約し、データセットを分析し、最後にグラフを作成して報告書を執筆することに費やされています。ローマは一日にして成らず、DBIRもまた然りです。

ご質問、ご意見

皆様のご意見をぜひお聞かせください。dbir@verizon.com、LinkedIn、Tweeter: @VerizonBusiness with #dbir

データにご不明な点がありましたら Tweet @VZDBIR!

はじめに

ベライゾンの15回目のデータ漏洩/侵害調査報告書へようこそ。この報告書の発行を開始してから15年も経ったとは、本当に信じがたいことです。人間の成長になぞらえると、歯の矯正が終わり、ようやく運転免許が取れるようになり、皮肉を言い過ぎたり、おそらく野蛮な感じになったり、さらに皆様に感謝もされなくなった報告書ということになるのかもしれません。しかし、私たちはそんなことは気にしません。ただ、「ありがとうございます！」と言いたいわけです。この業界をより良くするために、データ、洞察力、豊富な経験を惜しみなく提供してくださる協力者の方々に感謝します。また、読者の皆様には、この長く壮大な旅にお付き合いいただき、さらに大きな感謝をしております。このレポートを作成するために懸命に働けるのは、読者の皆様がいるからです。そして何よりも、私たちが実質的に仕事をしなくて済むようにしていただき、本当にありがとうございます。

この数年間は、私たち全員にとって圧倒的なものでした。驚きの限界に達したと思った瞬間、世界はまた新たなカーブを私たちに投げてきました。正直なところ、サスカッチ（Bigfootとも呼ばれ、北米の森林にいるとされる未確認生物）が知事に選ばれても、エリア51がベッド＆ブレックファストをオープンしても、ランサムウェアがまた増えても、私たちスタッフは瞬き一つしないほどです。ネタバレになりますが、そのうちの1つは実際に起こりました。（おめでとう、スクワッチ！（サスカッチに由来するプロバスケットボールチーム、シアトルスーパーソニックスのマスコット）がんばったね）。

この一年は、いろいろな意味で特別な年でしたが、サイバー犯罪の不透明な世界に関しては、確実に記憶に残る年でした。よく知られた重要インフラへの攻撃から大規模なサプライチェーンの侵害まで、金銭的動機に基づく犯罪者や極悪非道な国家主体の攻撃者が、この12ヶ月間にこれほどまでに大暴れしたことは、かつてないほどです。本レポートでは、例年通り、企業に対するこれらの攻撃やその他の一般的な行動について、データから読み取れることを検証していきます。また、DBIRの第15版にちなんで、時折、過去のレポートにおけるコメントや図表を参照し、業界としての進歩や、脅威の状況、攻撃者が利用する技術がどのように変化してきたかを確認したいと思います。今年、DBIRチームは23,896件のセキュリティインシデントを分析し、5,212件のデータ漏洩/侵害を確認しました。

それを踏まえて、2018年版DBIRの「はじめに」を再確認してみましょう。「DBIRは、セキュリティ実務者が、サイバー犯罪に関して企業によく降りかかるものについて、データに基づく現実的な見解を探す場所を提供するために作成されました。何が起きているのか、そして自分たちを守るために何ができるのかを知る必要があるからこそ、10年以上経った今でもDBIRは重要な存在であり続けているのです。私たちは、過去数年間と同様に、このレポートとそこに含まれる情報が、攻撃者があなたの業界の組織に対してどのような手口を使う可能性があるかについてのあなたの認識を高め、必要なセキュリティ対策の支援を経営陣に促すツールとして、また、従業員にセキュリティの重要性と彼らの支援方法を説明する方法として、利用できることを望んでいます」。

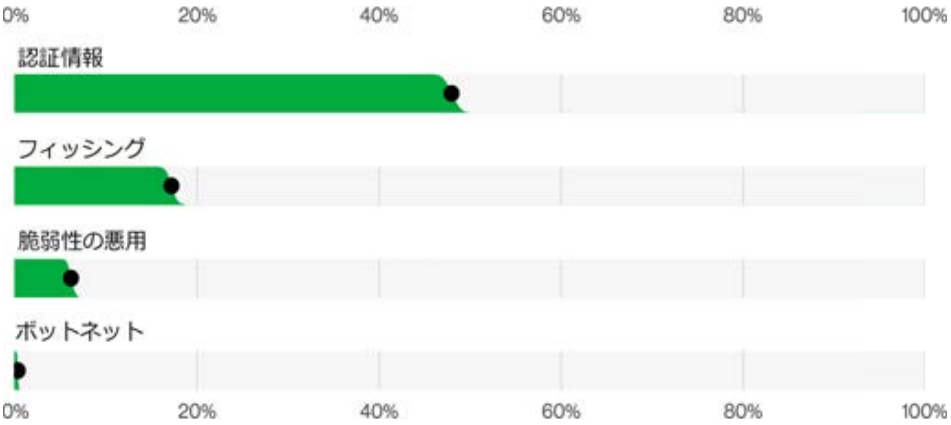
私たちのこの主張は、一貫して変わっていません。私たちは、皆様がこのレポートを楽しむだけでなく、この中に役立つ情報を見つけてくれること期待しているのです。改めましてありがとうございます。

DBIRの執筆陣（DBIR チーム）

Gabriel Bassett、C. David Hylender、Philippe Langlois、Alex Pinto、 Suzanne Widup

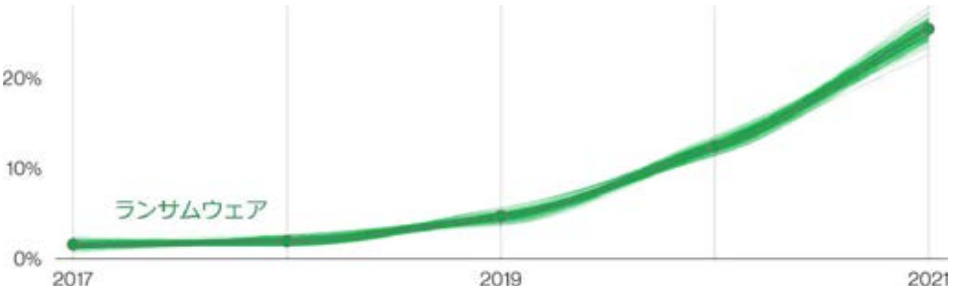
Verizon Threat Research Advisory Center（VTRAC）のDave Kennedyに対し、本報告書への継続的支援と毎年の貢献、およびVerizon Sheriff Teamの貴重な支援に対し、心より感謝いたします。

主な調査結果



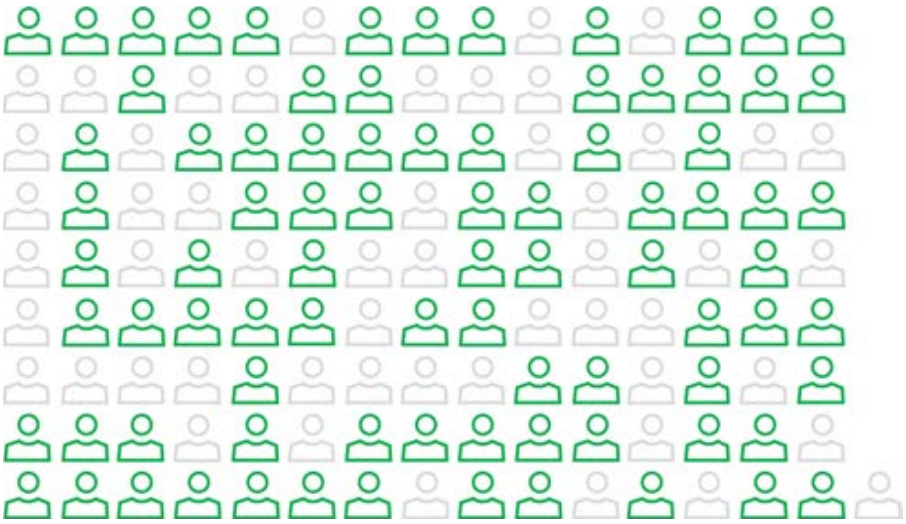
企業の資産につながる主な経路として、「認証情報」、「フィッシング」、「脆弱性の悪用」、「ボットネット」の4つがあります。これらはいずれも、DBIRで取り上げたあらゆる領域に蔓延しており、それぞれに対処する計画を策定しない限り組織は安全ではいられません。

図5. エラーや誤使用ではないデータ漏洩/侵害の種類（n＝4,250）



今年、ランサムウェアは約13%増加し、過去5年間の合計と同程度の増加率を示しており、増加傾向が続いています（今年度は全体の25%）。忘れてはならないのは、ランサムウェアの核心は、組織内のネットワークアクセスを収益化するモデルであるということです。上記の4つの主要経路をブロックすることで、ランサムウェアがネットワーク侵入に最もよく利用する経路をブロックすることができます。

図6. データ侵害におけるランサムウェアの割合の経時的変化



2021年度の報告書では、1つの主要なサプライチェーンにおけるデータ漏洩/侵害の影響が、いかに広範囲に及ぶかを説明しました。今年度のシステム侵入インシデントの62%は、サプライチェーンが原因でした。金銭の取得を動機とする攻撃者とは異なり、国家の支援を受けた攻撃者は、データの漏洩/侵害にはまったく手を染めず、単にネットワークアクセスだけを利用することを選択することがあります。

図7. システム侵入インシデントにおけるパートナー攻撃の割合（n＝3.403）
それぞれの人型は25インシデント

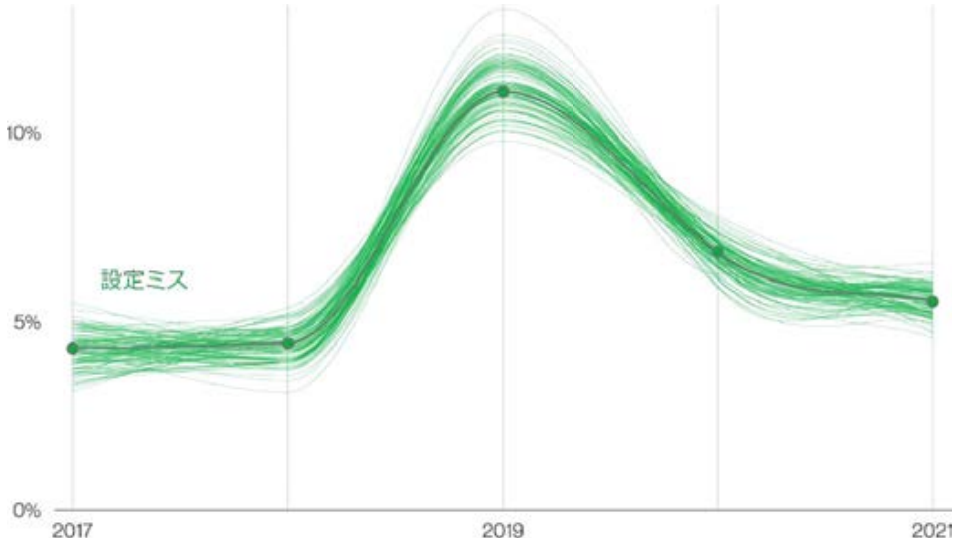


図8. 設定ミスによるデータ漏洩/侵害の経時的変化

「エラー」パターンは引き続き大きな割合の傾向にあり、漏洩/侵害の13%の原因となっています。これにはクラウドストレージの設定ミスが大きく影響しています。このパターンは2年連続でやや横ばいになっていますが、従業員によるエラーは無視できません。

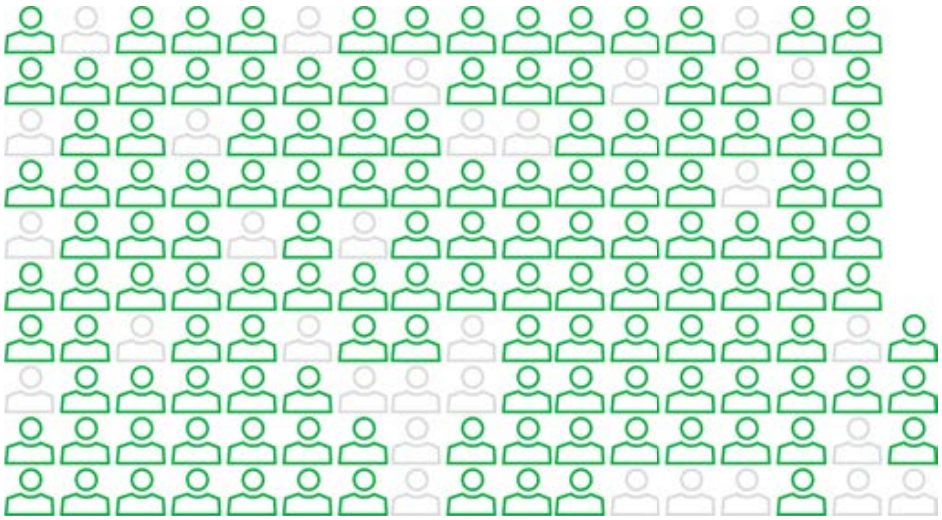
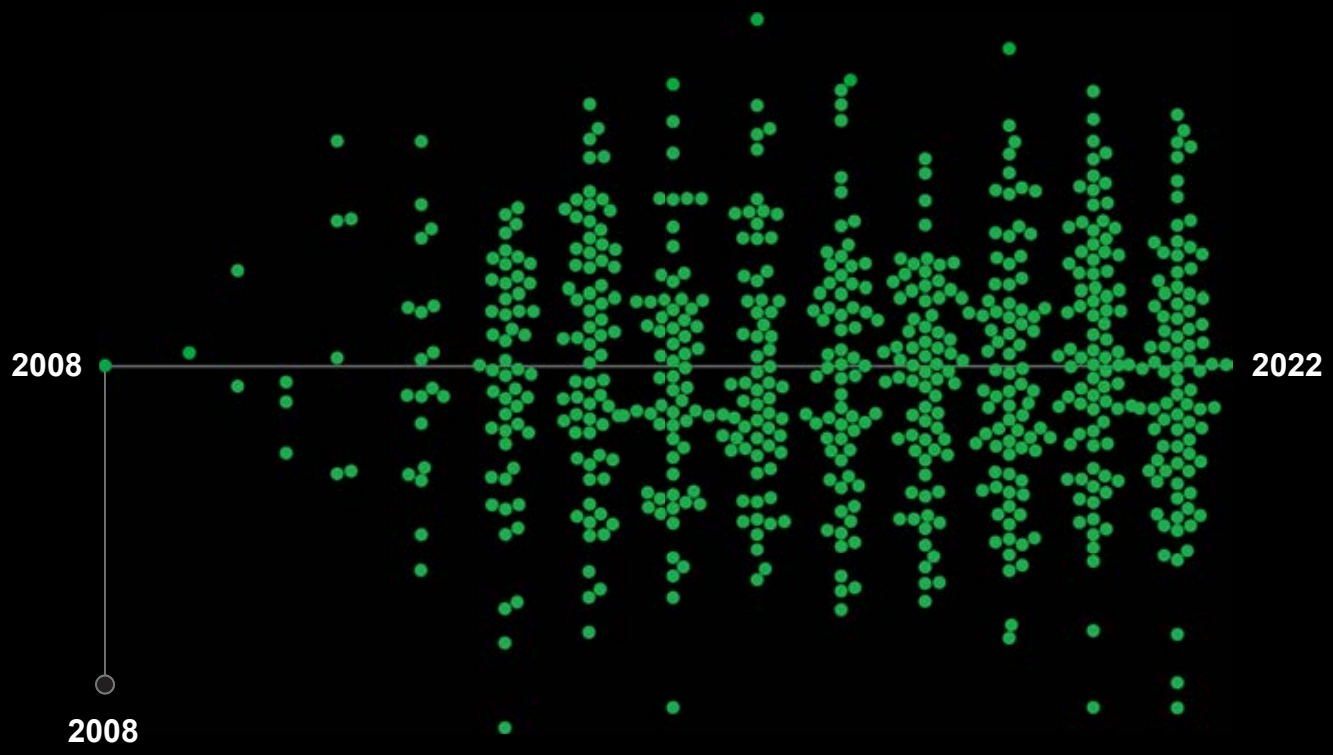


図9. データ漏洩/侵害における人的要因（n＝4,110）
それぞれの人型は25のデータ漏洩/侵害

人的要素は、今回の調査でもデータ漏洩/害を引き起こす要因となっています。今年度の漏洩/侵害のうち82%は人的要因が関与しています。盗まれた認証情報の悪用、フィッシング、不正使用、あるいは単なるエラーにかかわらず、インシデントにおいてもデータ漏洩/侵害においても同様に、人的要素が依然と大きな部分を占めています。

2
結果と分析



結果と分析：概要

DBIRの15周年記念同窓会へようこそ。名札を手に、懐かしい顔ぶれを見つけて、2008年当時を思い出してください。さて、この15年間で私たちはどのように変化したのか、皆様にご報告しましょう。

1枚の写真も百聞に如かずですが、図もまた然りです。DBIRに掲載されているグラフは、データの主要なストーリーと主要な制約の両方を伝えるために何度も繰り返された結果であり、これは厄介な命題です[1]。DBIRのデータセットは、様々なフォーマットで提供され、多くの異なるニュアンスや偏りを持つ協力者たちから寄せられたものです。DBIRチームは、これらのデータがデータ漏洩/侵害やインシデントの世界の「純粋なサンプル」ではないことを理解しています（そんなものは存在しないのですから）。それでも、意味のある分析を抽出することは可能です。

最初のDBIRで使用した図10のようなチャートは、すでにお馴染みかもしれません。これらの棒グラフは、小さい集合を簡単に比較できる優れた手段ですが、そのパーセンテージに重要な情報が隠されてしまうこともあります。そこで、データの曖昧さや不確実性のレベルについて、読者の皆様に正確にお伝えするために、時間をかけて、図11のような斜めの棒グラフに移行してきました。これを使って、データに対する信頼性に基づいて、「もの」の比較とそれらの値の範囲の両方を把握することができます。また、同じ考え方を折れ線グラフにも適用し、平均に基づく単線として傾向を表現する代わりに、信頼区間内の線の集合をプロットしています。これの優れた点は、「物事は変化する」という核となるメッセージを伝えるだけでなく、「このような変化の可能性もある」という誠実な図解を提供することができる点です。

このデータ漏洩/侵害の旅を15年続けた後、私たちは、途中で遭遇したすべての締め切り、失敗したカバーのアイデア、激論について回想していることに気づきました。しかし、私たちの旅の本当の宝物は、名声でも、メガヨットでも、本の取引でも、データ漏洩/侵害の分析ですらなく、長年にわたって築き上げた友人たちなのかもしれません。当初、このレポートはベライゾンのデータのみに基づいていましたが、その後、世界中の87のパートナーや協力者が加わり、このレポートが実現しました。皆様のおかげで、合計914,547件以上のインシデント、234,638件の漏洩/侵害、8.9TBを超えるサイバーセキュリティデータを収集して分析し、読者に最高の分析結果をお届けすることができたのです。本当に、私たちは巨人の肩の上に立っているのです。それでは、分析結果をご覧ください。

1 ロックで厄介なのは韻を踏んでいるだけではありません。

攻撃者 – 相手にしたくない友達

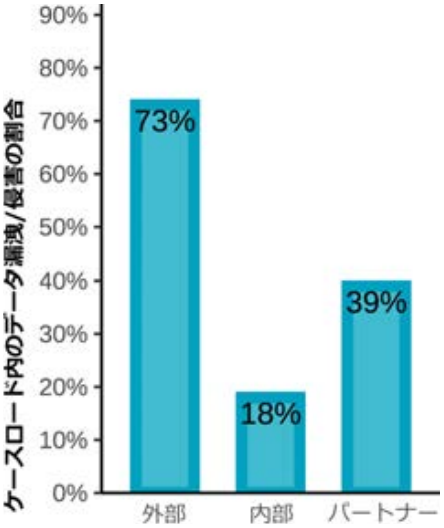


図10. データ漏洩/侵害の発生源（2008年DBIR、図3）

図11. データ漏洩/侵害の攻撃者（n=5,146）

調査結果によると、データ漏洩/侵害の原因は、他のどの原因よりも外部からの攻撃である可能性が非常に高いことがわかりました。4件の事例のうち3件近くが、被害組織の外部からの攻撃を示す証拠を見つけています。企業規模が大きくなるにつれてリスクが高まることを明らかにした他の調査結果と同様に、調査員が扱ったデータ漏洩/侵害の39%にビジネスパートナーが関与していました。内部を発生源とする侵害は最も少ない件数（18%）で、4対1の割合で外部の発生源によるものを上回っています。

内部関係者によるデータ漏洩/侵害が比較的少ないことは、一部の人にとって驚くべきことかもしれません。内部関係者によるインシデントは、他の原因によるインシデントよりも数が多いと広く信じられており、一般的に報告されています。しかし、私たちのケースロードでは、データ漏洩につながるインシデントについては、そうではないことが示されています。もちろん、この結果は、内部関係者がその活動を秘密にしておくことに長けているという事実に照らして考慮されるべきです。（2008年 DBIR）

2008年に初めてこのレポートを発行して以来、変わっていないことがあります（最初のiPhoneが発売されたのはそのわずか1年前です）。携帯型の不思議な機械がまだそれほど普及していなかった2008年の頃のサイバー[2]セキュリティの世界では、外部からのインシデントよりも内部のインシデントのほうが多いと信じられており、少なくとも「セキュリティインシデントの大部分については間違いない」と考えられていました。時間の浪費と白髪の増加、そして全体として情報セキュリティの肩の力が抜けたこの15年間のおかげ（?）で、今振り返ると、図11が示すように、データ漏洩/侵害の80%は組織の外部の者によって引き起こされており、攻撃者は内部よりも外部の方が圧倒的に多いと自信を持って言うことができます。

2 今年のDBIRに掲載された145もの「サイバー」関連資料をすべて見つけることができますか？まあ無理でしょうね...。

内部の犯行によるデータ漏洩/侵害の中央値（漏洩したレコード件数で測定）は、外部の犯行によるものを10倍以上上回りました。同様に、パートナーが関与するインシデントは、外部ソースによるインシデントよりもかなり数が大きくなる傾向があります。これは、特権を持つ関係者は、外部の人間よりも組織に大きなダメージを与えることができるという原則を裏付けています。（2008年DBIR）

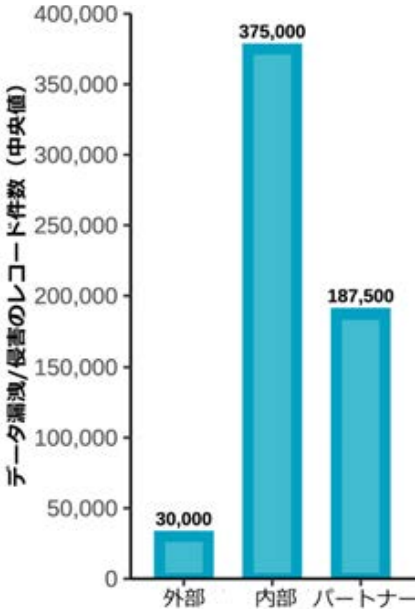


図12. データ漏洩/侵害のレコード件数の中央値（2008年 DBIR図5）

2008年のレポートでは、データ漏洩/侵害のレコード件数が指標として選ばれていました。しかし、21世紀に入ってからは、影響の大きさを表す通貨が主流となっています。レコード件数は依然として注目されていますが、一般的には過去数年間と同じレベルの重要性で見られているわけではありません。しかし、内部要因のデータ漏洩/侵害の中央値は、2008年は37万5,000件でしたが、今年は、図13が示すように8万件に留まっています。レコード件数が減少しているように見えますが、このレポートでも業界全体でも、さまざまな変化が起きていることを念頭に置くことが重要です。したがって、レコード件数の変化は、攻撃者がデータを現金化する方法が増えたことを反映している可能性があります。

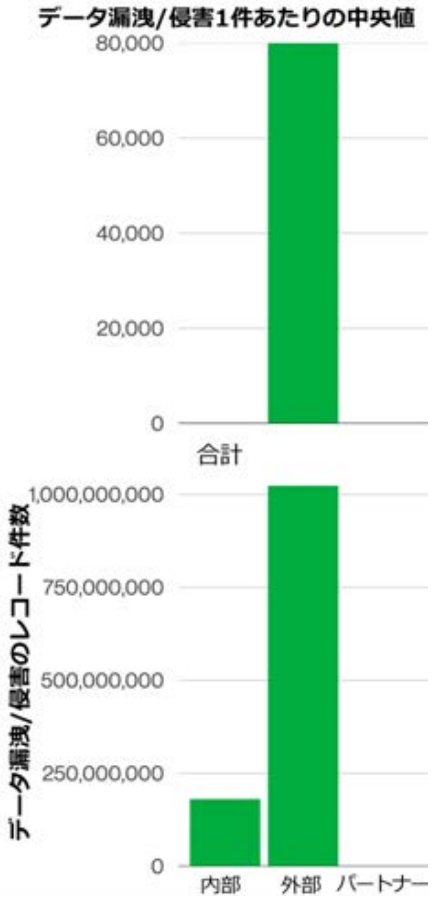


図13. 攻撃者別のデータ漏洩/侵害の件数（n=54）

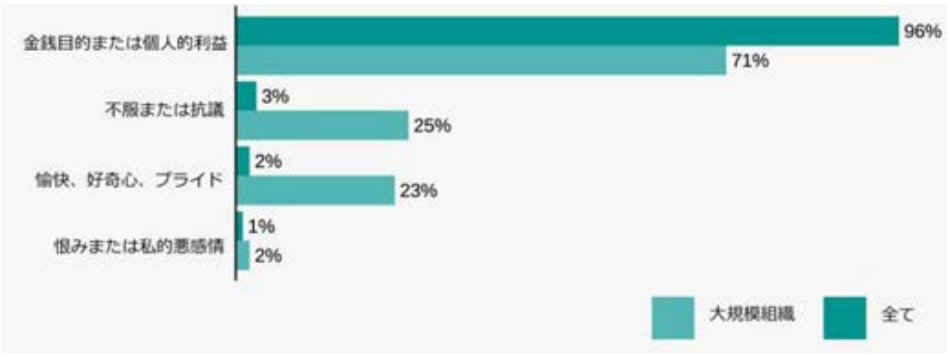


図14. 外部のデータ漏洩/侵害の動機（外部内の漏洩/侵害の割合別）
（2012年 DBIR図15）

結論：ほとんどのデータ窃盗犯は、現金に換えられる情報を意図的に盗もうとするプロの犯罪者です。古くから言われているようなことです。

しかし、これがすべてではありませんし、最も重要なことでもありません。2011年に見られた最も大きな変化は、世界中の大規模な組織に対する「ハッキング」の台頭です。2011年に防御の網をかいくぐった活動家グループに結びつけられた事例の頻度は、それまでのすべての年を合わせた頻度を上回りました（2015年DBIR）。

動機は、ほとんどの場合、当初のDBIRの分析テーマではありませんでした（ただし、2008 年には標的型攻撃と日和見的攻撃という文脈での考察はありました）。2010年には、「今日のサイバー犯罪者は、知識やスリルを求める趣味人ではなく、オンライン犯罪で得られる不正な利益によって動機づけられている」という見解があります。今日のDBIRの読者にとっては当たり前のことかもしれませんが、当時は「家に引きこもってこのサイトをハッキングし、兄弟たちに自慢してやろう」というようなステレオタイプな行動が、データ漏洩/侵害の一定割合を占めていると多くの人が考えていたことを忘れてはいけません。いずれにせよ、不正な経済活動や個人的な恨み、あるいは不注意によるトラブルがどの程度あるのかを定量的に把握するには、攻撃者の動機を理解することが重要です。

追跡を始めた2015年以降、金銭取得を目的とする動機がトップになっています。しかし、同年は、ハッキング（特に情報漏洩）の台頭が多くの攻撃を占めました。スパイ活動関連の攻撃はレーダーにひっかかることすらありませんでしたが、7年後の世界は大きく変わっています。スパイ活動は何年もの間2位の座を占め、ハッキングはほとんどの場合、単に後回しにされているのです。しかし、次に進む前に、スパイ活動がここ数年で増加しているのはほぼ間違いないものの、2015年に全く登場しなかったのは、当時の私たちの協力者と一般的なケースの量による可能性がかなり高いことを指摘しておきます。

図15. 外部攻撃者の動機（組織規模別）

攻撃

「攻撃」セクションは、セキュリティインシデントやデータ漏洩/侵害がどのように展開されたかを示します。ハリウッドのアクション映画のようなものですが、予算は控えめで、爆発やカーチェイスはありません。しかし、華々しい演出がないにもかかわらず、こうした侵害につながる行動は、犠牲者に明確な影響を及ぼします。DBIRでは、攻撃をバラエティ（攻撃の種類）と経路（攻撃を起こした手段）に分けて議論しています。図16から図19は、インシデントと侵害に関連する攻撃の種類と経路を示しています。

図16. インシデントの上位の攻撃の経路（n=18,419）

図17.インシデントの上位の攻撃の種類（n=18,511）

攻撃のカテゴリー

ハッキング：論理的なセキュリティ機構を回避したり妨害したりすることで、承認なしに（または承認を越えて）意図的に情報資産にアクセスしたり危害を加えたりしようとする行為。

マルウェア：所有者の同意なしにデバイスの状態や機能を変更する、デバイス上で実行される悪意のあるソフトウェア、スクリプト、またはコード。

エラー：誤って、または不注意に行われた（または行われずに放置された）もの。

ソーシャル：情報資産の人的要素（ユーザ）を利用するために、偽装、操作、脅迫などを用いること。

悪用：委託された組織のリソース又は特権を、意図されたものとは異なる目的または方法で使用すること。

物理的：接近、所有、または力を伴う意図的な脅威。

環境：地震や洪水などの自然現象だけでなく、資産が置かれている身近な環境またはインフラに関連する危険も含む。

注意：バックドアが攻撃者に直接アクセスポイントを提供するのに対し、C2はマルウェアが利用する間接的な接続です。「バックドアまたはC2」には、バックドアとマルウェアのみが提供するC2の両方が含まれ、「バックドア」にはマルウェアが提供するバックドアとハッキングが提供するバックドアの両方が含まれます。どちらも他方のサブセットの関係ではないため、両方とも残しています。読者としては、攻撃者が確立したリモートアクセスが重要であり、その永続的なアクセスを作り出す方法が数多く存在することがおわかりいただけるはずです。

図18. データ漏洩/侵害の上位の攻撃の経路（n=3,279）

図19. データ漏洩/侵害の上位の攻撃の種類（n=3,875）

インシデント全体の46%を占める「サービス拒否（DoS）」攻撃が明らかにトップであり、次いでマルウェアの種類である「バックドアまたはC2」が17%を占めています。しかし、それ以上に興味深いのは、今年の上位の攻撃経路には「パートナー」と「ソフトウェアアップデート」が含まれていることです。初めて挙げられたソフトウェアアップデートについては、後のセクションで詳しく説明します。Webアプリケーションが1位の侵入経路であり、当然のことながら、多数のDoS攻撃に関連しています。この組み合わせは、窃取した認証情報の使用（一般に何らかのWebアプリケーションを標的としている）と共に、過去数年間に観察されたものと一致しています。

データ漏洩/侵害の種類を見ると、上位の種類は入れ替わりがやや激しく、「窃取した認証情報の使用」、「ランサムウェア」、「フィッシング」がすべて上位5位に入っています。また、「その他」のカテゴリーは、今年も上位3位以内にこっそりランクインしています。これは、データセットが多種多様であることが主な原因です。つまり、トップ10には入っていないけれども、注目すべきさまざまなものがあるのです。また、逆に言えば、データ漏洩/侵害の種類の73%が上位10種類の中に含まれているということもできます。攻撃が180種類以上あることを考えると、これはそれほど驚くことではありません。「パレートの法則」はどうでしょうか[4]。

攻撃経路という点では、インターネット上に企業の存在を示す主な方法が、企業が悪者にさらされる主な方法であるという考え方によく合致しています。Webアプリケーションと電子メールは、データ漏洩/侵害の上位2つの経路です。これに続くのが不注意で、誤配信や設定ミスなどのエラーに関連するものです。その次に続くものとして、RDP（Remote Desktop Protocol）などを取り込むデスクトップ共有ソフトウェアや、インターネット経由で他のコンピューターへのリモートアクセスを可能にするサードパーティソフトウェアがあります。残念ながら、認証情報を入力するだけでインターネット経由で資産に直接アクセスできるのであれば、犯罪者も同じことができます。

4 「ピーターの法則」は全く別のものなので、それと混同しないように。

2008年当時を振り返って

DBIRは、発行開始以来、劇的に成長し、進化してきましたが、中核となる統計情報の多くが変わらないことは、非常に興味深いことだと考えています。2008年の図20を見ると、その数字が現在と非常によく似ていることがわかります。ハッキングが引き続き主要な行動であり、マルコード（マルウェア）がそれに続いています。2008年の調査報告書では、「エラー」は2つの方法で記録されています。データ漏洩/侵害の直接の原因となったエラー（暗い色のバー）と間接的に寄与したエラー（明るい色のバー）です。現在では、この内訳は使用していませんが（いくつかの理由があり、そのうちの1つは、ほとんどすべてのデータ漏洩/侵害において、エラーが果たす役割は少なくとも小さいと言えるため）、データ漏洩/侵害全体の14%を「エラー」が占めています。しかし、そこから先は、やや乖離が生じます。これは、特に「ソーシャル」と「エラー」に関して言えることですが、DBIRの調査データが、最初の年は500件だったものが、今年は5,000件を超えるまでに拡大し、規模もソースの多様性も年々大きくなっていることを念頭に入れておいてください。

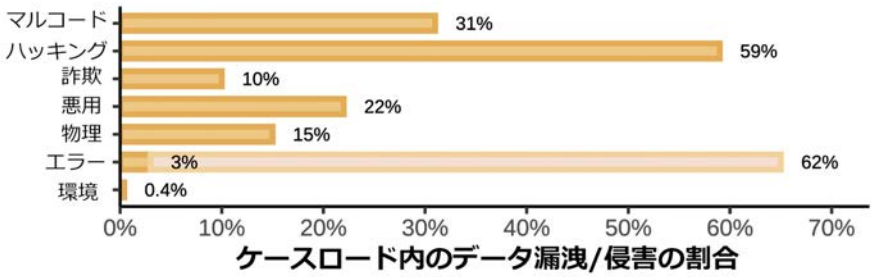


図20. 脅威のカテゴリー（2008年 DBIR 図9）
暗い色 = 直接的要因、 明るい色 = 間接的要因

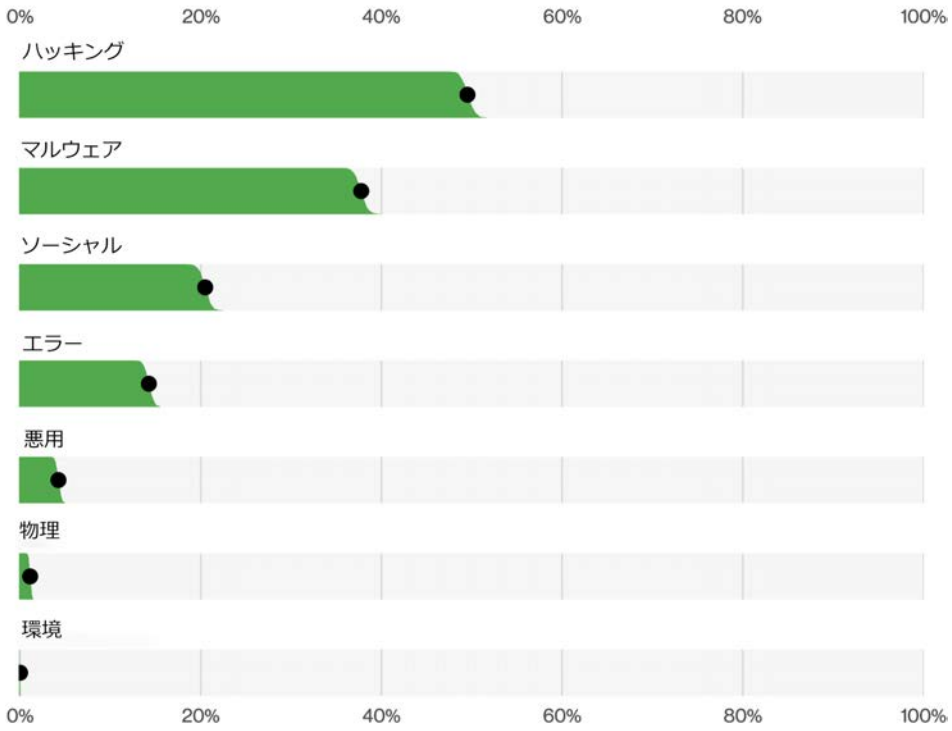


図21. データ漏洩/侵害の攻撃（n=5,212）

資産

図22. データ漏洩/侵害された資産（n=4,384）.

VERISについて「知らない」人のために（でも、もし知っていたら、それはすごいことです！）、資産とは攻撃の対象となる「もの」です。つまり、エクスプロイトによってハッキングされたもの（おそらくサーバー）、攻撃者によってソーシャルエンジニアリングされた人、紛失や盗難にあった「もの」が観察される場所です[5]。断固たる防衛者にとって、これは攻撃の標的を理解する助けとなり、インフラに必要な防御の種類の優先順位を付けるための有用なツールにもなるはずです。

図22は、データ漏洩/侵害によって影響を受けた資産の上位が、サーバー、人、およびそのデバイスであることを示しています。具体的なサーバーの種類に注目すると（図24）、Webアプリケーションサーバー（56%）とメールサーバー（28%）が上位2種類を占めており、どちらもインターネットに接続される可能性が最も高い資産であることを考えると、これはむしろ直観的に納得できます。そのため、サーバーは、盗まれた認証情報のような巧妙な手口を使って（ネタバレになりますが）、組織の「境界」をすり抜けるのに便利な場所となっています。

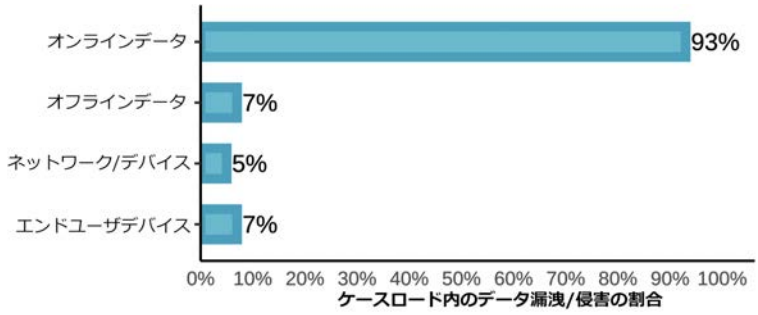


図23. 侵害された資産（2008年DBIR、図18）

過去を振り返る

2008年のDBIRでは（何年も前のこと）、資産を分類する方法が現在とは異なっていたのにも関わらず、調査結果は比較的類似しています。ほとんどのインシデントが、多数のユーザとネットワークデバイスを接続したサーバー（オンラインデータ）に影響を与えています。サーバーは、データ漏洩/侵害において、JNCOジーンズやオートクチュールのスパイクヘアのように時代を超越しているようです。

リストの次に来るのは、ソーシャルエンジニアリングの犠牲になる人たちです。たいていは、会社のお金を扱い、そのお金を使って何かをすることができる（たとえば、預金先を変更する）個人がこれにあたります。

資産の話をするときは、IT資産だけでなく、OT（オペレーショナルテクノロジー）も重要であることを忘れてはいけません。現在の政治情勢により、OTの話題は多くの人の頭に（そしてニュースにも）上っています。OTは国家インフラを動かすコンピューターシステムです。事例も散見されますが、インシデントデータ全体に占める割合は約3%に過ぎません。技術に関わる問題としては、昨年（約1%）より増加しています。これは、インフラを稼働させるために、バックグラウンドで静かに動いているシステムを保護するための、穏やかな注意喚起であるとお考えください。重要インフラと呼ばれる所以です。

図24. データ漏洩/侵害された上位の資産の種類（n=2,796）

5 「スクールハウス・ロック」の曲が聞こえてきそうです。

属性

関連する属性がセキュリティインシデントになければ、情報セキュリティ専門家の仕事はもっと楽になるはずです。しかし、残念ながら、属性は存在します。機密性、完全性、可用性（一般にCIAの3要素とも呼ばれる）といった属性は、インシデントの多くの側面（通知すべき人、取るべき行動、上級管理職に説明すべき内容など）に大きな影響を及ぼしかねません。図25は、DBIRのデータセットにおけるCIAの3要素（セキュリティインシデントに関して）の経時的変化を示したものです。

DBIRはデータ漏洩/侵害を「機密性」属性の侵害と定義しており、「機密性」が侵害された場合は常に、どのような種類のデータが関与していたのかという疑問を提起します。

15年前（2008年DBIRの図20）には、カード決済のデータが群を抜いてトップを占めていました。しかし、この数年間は徐々に減少しています。この減少は、この種のデータを保護するために近年追加されたセキュリティ管理がある程度反映されていることは間違いありません。それにもかかわらず、図27は、上位2つが「認証情報」と「個人情報」であることを示しています。認証情報は、システム上の正当なユーザに簡単になりすますことができるため、犯罪者が好んで使用するデータの種類であると、長い間考えられてきました。羊の皮を被ったオオカミのように、攻撃されるまでは無害に見えます。また攻撃者は、金銭詐欺に役立つメールアドレスなどの個人情報を頻繁に流出させています。個人情報を転売できる巨大な市場もあり、まさに「贈り物」であり続けます。ただし贈り物といっても、そのほとんどがデータ主体（データの対象者）に迷惑をかけるものです。

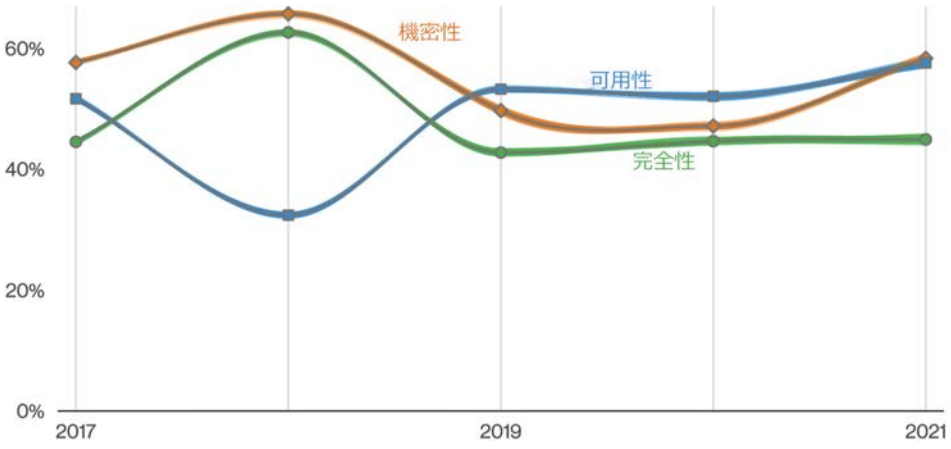


図25. インシデントの属性の経時的変化

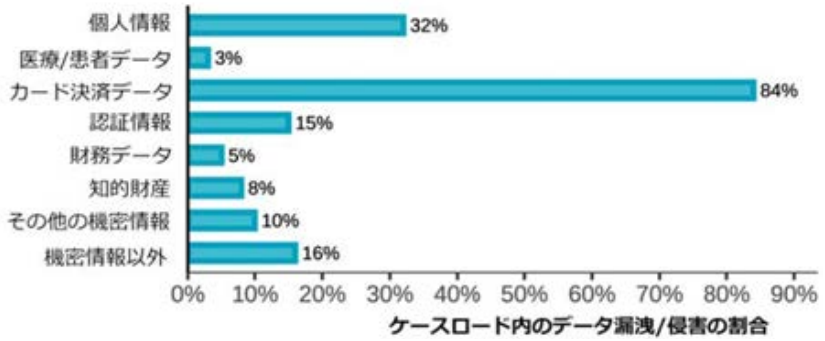


図26. 侵害されたデータタイプ（2008年 DBIR 図20）

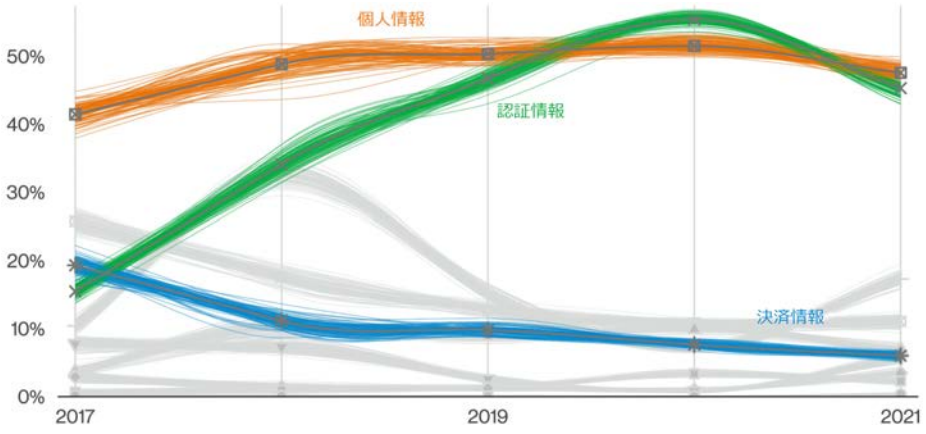


図27. データ漏洩/侵害の上位の機密性の種類の経時的変化

攻撃者は標的のネットワークに侵入すると、しばしばマルウェアをインストールし、システムの「完全性」を侵害します（他の不正な変更と同様に）。また、攻撃によって人の行動が改ざんされれば、一人の人間の「完全性」が侵害される可能性があります。例として、フィッシングメールへの応答や、なりすましのシナリオの犠牲となることが挙げられます。これらが、DBIRのデータで見られる完全性への 侵害の主な2つのタイプであり、どちらもすべてのレポートに存在していましたが、必ずしも同じ用語で呼ばれていたわけではありませんでした。初期のDBIRの頃は、フィッシングのようなソーシャル攻撃は今ほど普及していませんでした。しかし、マルウェアのインストールは当時もかなり一般的で、今年のデータでも例外ではなく、データ漏洩/侵害の30%以上に何らかのマルウェアが含まれ、ソーシャル攻撃が含まれるケースは約20%となっています。

ランサムウェアの全盛期は続いており、今年のマルウェアによるデータ漏洩/侵害の約70%を占めています。ランサムウェアは、CIAの3要素のうち最初の2つにまたがる攻撃であり（ランサムウェア攻撃の38%は「機密性」の侵害）、3つ目の「可用性」も影響を受けます。ランサムウェアが起動すると、データへのアクセスがブロックされるため、組織でのデータの可用性が失われることになります。図28に示すデータセットでは、「難読化」がその典型的な例です。

可用性に影響を与えるもう1つの一般的な形態は、「分散サービス拒否（DDoS）」攻撃から生じることが多いサービス中断です。このような攻撃で多数のインシデントが発生しますが、データ漏洩/侵害のケースは比較的少ないものとなっています。しかし、DoSが特に懸念される方には、それ専用のパターン全体をご用意しています

図28. データ漏洩/侵害の上位の可用性の種類（n=1,109）

タイムライン

タイムラインを見る際には、検出時から始めるとよいでしょう。図29は、数か月ではなく数日以内にデータ漏洩/侵害を検知する可能性が高いという、一見良いニュースのように見えますが、いくつかの要因に目を向けると、少し不安が生じます。データ漏洩/侵害の検出方法の最上位（50%以上）は、「攻撃者による開示」です（通常、ランサムウェアのメモが資産上に表示されるか、またはデータを販売したり侵害を公表するための犯罪フォーラムに掲載される）。どちらも望ましいことではありません。「知らぬが仏」は、データ漏洩/侵害には当てはまりません。

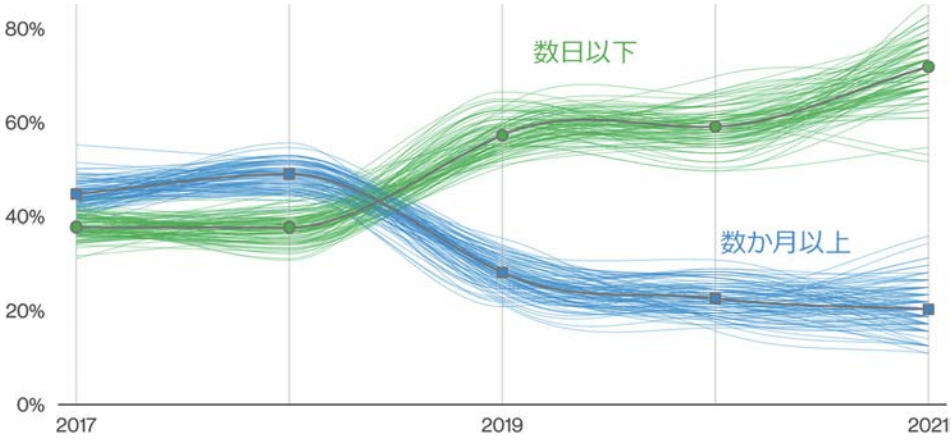


図29. 攻撃者による開示以外のデータ漏洩/侵害の検出

イベントチェーン

図30では、1つの攻撃にかかった時間を単純に分析するのではなく、「攻撃」に関連した時間がどのくらいかかったかを分析することもできます。この攻撃のタイムラインは、「イベントチェーン」データで見ることができます。イベントチェーンは攻撃がたどった経路を記録したものです[6]。図30は、ほとんどのデータ漏洩/侵害がわずかなステップしか含んでいないことを示しています。3つの攻撃（フィッシング、ダウンローダー、ランサムウェア）が最も一般的で、5つ以上の攻撃を利用したものはごくわずかです。防御側の仕事は、この攻撃経路を長くすることです。攻撃者は、攻撃経路を短くしようとする傾向があります。なぜなら、攻撃経路が長くなるにつれ、防御側がデータ漏洩/侵害を防止、検出、対応、回復する可能性が高くなるからです。

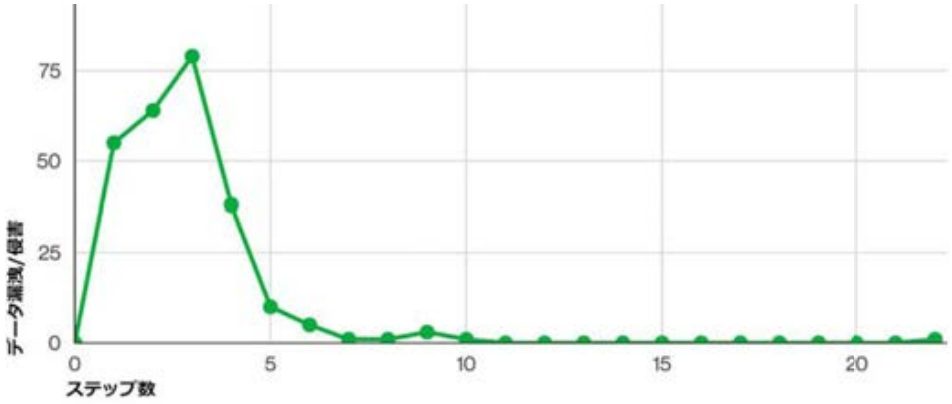


図30. エラーによらないデータ漏洩/侵害の侵害あたりのステップ数（n=258）

6 イベントチェーンは、「付録 B ：VERISと標準」の攻撃フローに似ていますが、より基本的なものです。

バリューチェーン「金を稼ぐには金が必要」

過去2年間、DBIRチームは、バリューチェーン（標的に攻撃する前に、購入または作成への投資によって攻撃者が獲得しなければならない能力と投資）について情報を収集してきました。これまで防御側は、自分たちの境界内で発生する事象に主に焦点を当ててきましたが、それは自分たちで管理するものであるため、理にかなっています。しかし、攻撃者のエコシステムはデータ漏洩/侵害の前と後の両方に存在し、インシデントを煽り、インシデントを糧としています。バリューチェーンで「あのメールアドレスはどこから来たのだろう？」とか、「盗まれた認証情報はどこに行ったのか？」といった疑問が生じます。侵害がさらなる侵害を生み、いわば「侵害の輪[7]」を形成しているように見えることがよくあります。このエコシステムに関連する一連の処理を理解することで、攻撃に関する重要なステップを理解し、力を合わせて、攻撃者にとってこれらの処理がより困難、高価、または持続不可能なものにすることができます。

攻撃者がデータ侵害を行うために必要な投資は次のものです。

- **開発：**ターゲットへの攻撃を遂行するために開発が必要なソフトウェアやコンテンツ。
- **ターゲティング：**攻撃可能な機会を特定する作業。これらは、侵害されたデータの種類と大きく重なる。
- **配信：**メール、侵害されたサーバーやWebサイトなど、攻撃者のコンテンツを配信するために使用されるサービス。
- **非配信サービス：**脅威となる攻撃者が提供および利用する、悪意のあるコンテンツの配信に利用されるもの以外のサービス。
- **キャッシュアウト：**何か（おそらく侵害された属性）を通貨に変換するための方法。

図31. データ漏洩/侵害のバリューチェーンカテゴリー別の上位のバリューチェーンの種類

図31は、バリューチェーンの各パートの上位の種類を示しています。メールは最もよく使われる手段です。メールはバリューチェーンの中で容易に推論できますが、配備されているマルウェアやターゲティング内の認証情報などは推論が難しく、そのため過小評価されている可能性があります。マルウェアは自由に入手でき、認証情報も盗まれる可能性があります。重要なのは、開始と終了という点だけに着目してデータ漏洩/侵害を捉えないということです。その代わりに、スポーツチームを考えるように、フィールドに出ているか、ベンチで控えているかのどちらかだと考えてください。

7 「サークル・オブ・ライフ」に似ていますが、脅威攻撃者のためのものです。

3

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：概要

DBIR データセットは非常に大きく、 時には非常に複雑です。 取得するデータポイントの種類は多岐にわたり、 その規模も年々拡大しています。 増え続ける膨大なデータをより簡単に分析できるよう、 また、 さらに重要なこととして、 調査結果を読者にわかりやすく伝えるために、 2014 年のレポートから 「パターン」 を使用するようにしました。

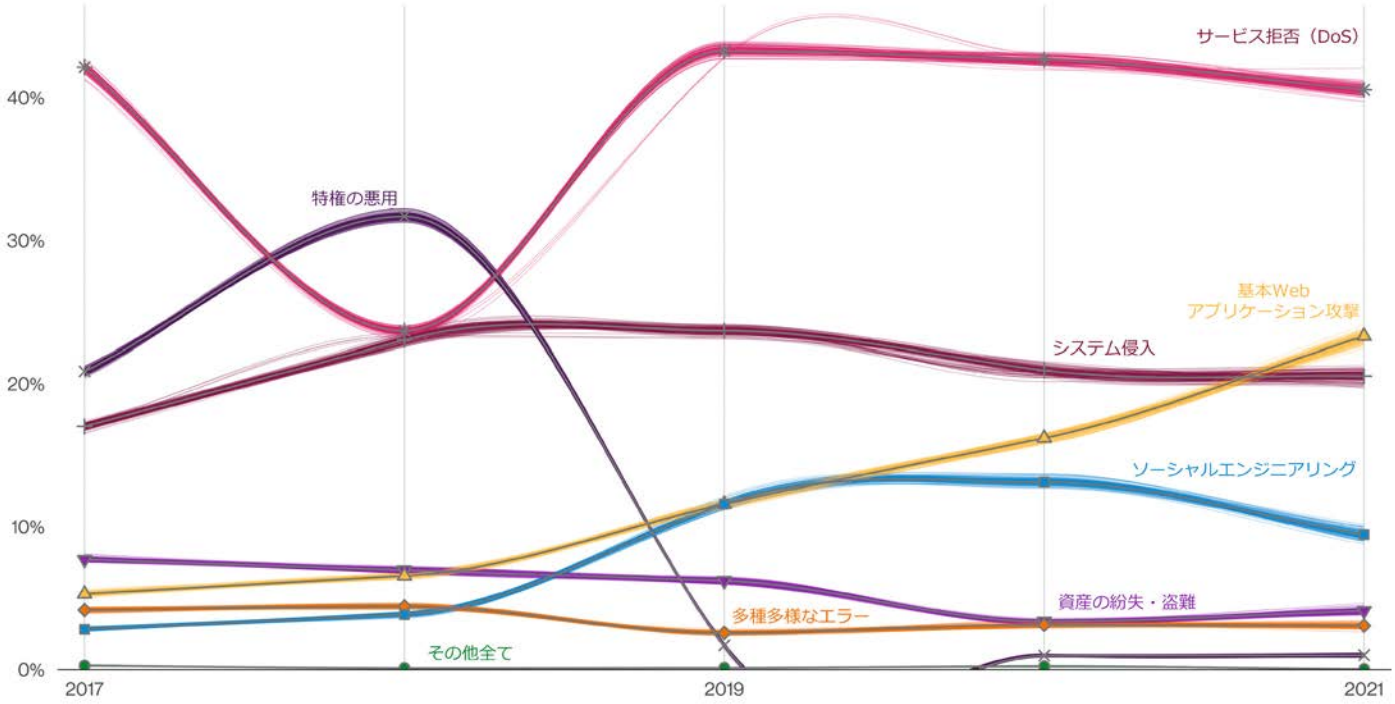


図32. インシデントパターンの経時的変化

パターンとは、基本的に「類似」のインシデントのクラスタです。2014年以降数年間は9つのパターンがありました。昨年、攻撃の種類や脅威の状況の変化により、データの傾向から、これらのパターンを改訂し、組み合わせを検討し、全体的に見直す必要があることがわかりました。そこで、2021年のレポートから、当初の9パターンから、本レポートに掲載されている8つのパターンに変更しました。8つのパターンとその定義については、表1をご覧ください。各パターンの定義の方法については、本レポートの中で言及していくので、必ず熟読してください。

基本Webアプリケーション攻撃	これはWebアプリケーションに対する攻撃であり、最初のデータ漏洩/侵害を行った後は、それ以上の攻撃は行いません。「侵入して、データを取得したら引き上げる」パターンです。
サービス拒否（DoS）	ネットワークやシステムの可用性を損なう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の攻撃が含まれます。
資産の紛失・盗難	置き忘れか悪意によるものかを問わず、情報資産が紛失した場合。
多種多様なエラー	意図しない行動が、情報資産のセキュリティ属性の侵害を直接もたらしたインシデント。デバイスの紛失はこれには含まれず、盗難に分類される。
特権の悪用	正規の特権が不正に、または悪意を持って使用されたことが主な原因であるインシデント。
ソーシャルエンジニアリング	心理的な危害を加えて行動を変容させたり、機密情報を漏洩/侵害させたりすること。
システム侵入	マルウェアやハッキングを利用した複合的な攻撃で、ランサムウェアの配備などの目的を達成する。
その他全て	この「パターン」は、実際にはパターンとは言えません。例えば、廃棄した電化製品の電源ケーブルを、万が一のために保管しておく容器のように、他のパターンの枠にうまく収まらない、あらゆる事象をカバーします。

表 1. インシデントの分類パターン

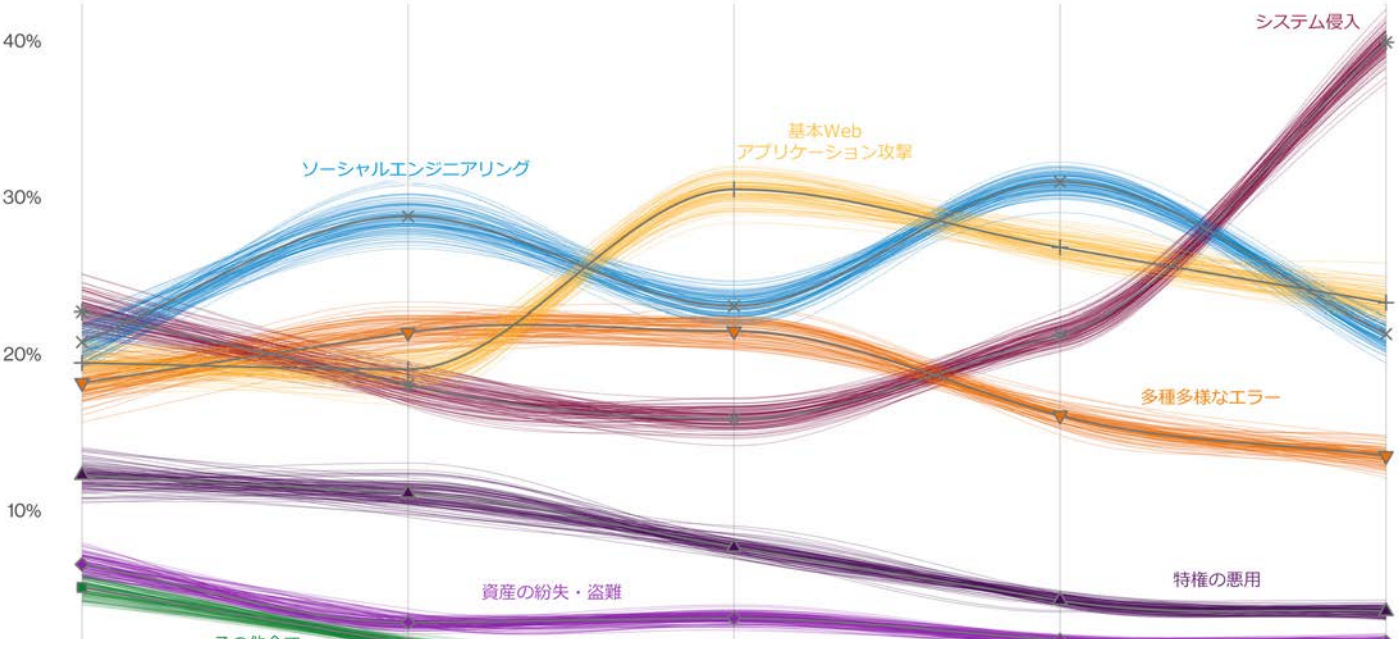


図33. データ漏洩/侵害パターンの経時的変化

システム侵入

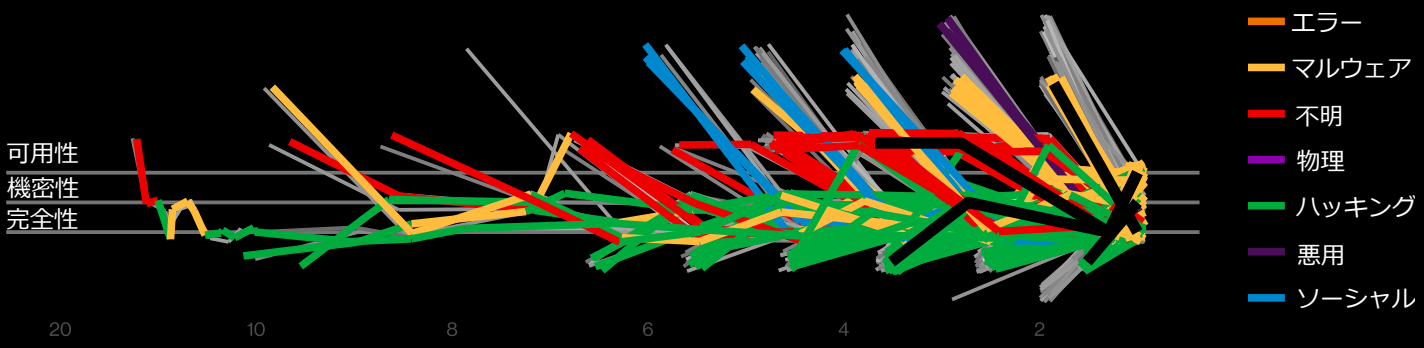


図 34. システム侵入インシデントの経路　（n=228）

複雑なパターン

このレポートでは、すでにシステム侵入パターンの定義を行いましたが、良い例が必要かもしれません。持続的な標的型脅威（APT）やその他の形態の有能な攻撃者が、環境内を移動して砲弾を発射し、マルウェアを投下し、認証情報をダンプし、予想外のレッドチームの演習で期待されるあらゆる楽しいことを行っていると考えられる場合、それはまさに「システム侵入」と言えます。

サマリー

このパターンは、ソーシャル、マルウェア、ハッキングなど、複数の異なる行為の組み合わせを活用した、より複雑な侵害や攻撃で構成されており、今年劇的に増加したサプライチェーン侵害やランサムウェアが見られる場所でもあります。

昨年との比較

このパターンでは、「窃取した認証情報の使用」とランサムウェアのようなマルウェアが引き続き最大の懸念事項となっています。

頻度	7,013件のインシデント、確認されたデータの暴露1,999件
攻撃者	外部（98%）、内部（2%）（漏洩/侵害）
攻撃者の動機	金銭目的（93%）、スパイ活動（6%）（漏洩/侵害）
侵害されたデータ	認証情報（42%）、個人情報（37%）、その他（35%）、内部（16%）（漏洩/侵害）

今年のデータを見ると、特にランサムウェアの増加やパートナー（ベンダーを含む）から受ける脅威など、防御側が多くの課題に直面しているように見えます。

このパターンを良く理解するために、インシデントを構成する攻撃の種類と経路を見てみましょう。図35は、上位の「攻撃の種類」を示したもので、「バックドア（マルウェアが提供）」と「ランサムウェア」が1位を競い、「窃取した認証情報の使用」がそれに続いています。図36では、インシデントの経路として、「パートナー」と「ソフトウェアアップデート」が上位に挙げられています（驚）。これは主に、昨年非常に大規模に公然と発生したあるセキュリティインシデントに起因するものです。ヒントは、"PolarShins"と韻を踏んでいることです。詳しくは、「パートナー、サプライチェーン、サードパーティ」のセクションを参照してください。しかし、「パートナー」と「ソフトウェアアップデート」の次を見てみると、インシデントの14%はデスクトップ共有ソフトウェアが主な経路となっており、次いでメールが9%となっています。

図35. システム侵入インシデントの上位の攻撃種類（n=5,212）

図36. システム侵入インシデントの上位の攻撃経路（n=3,403）

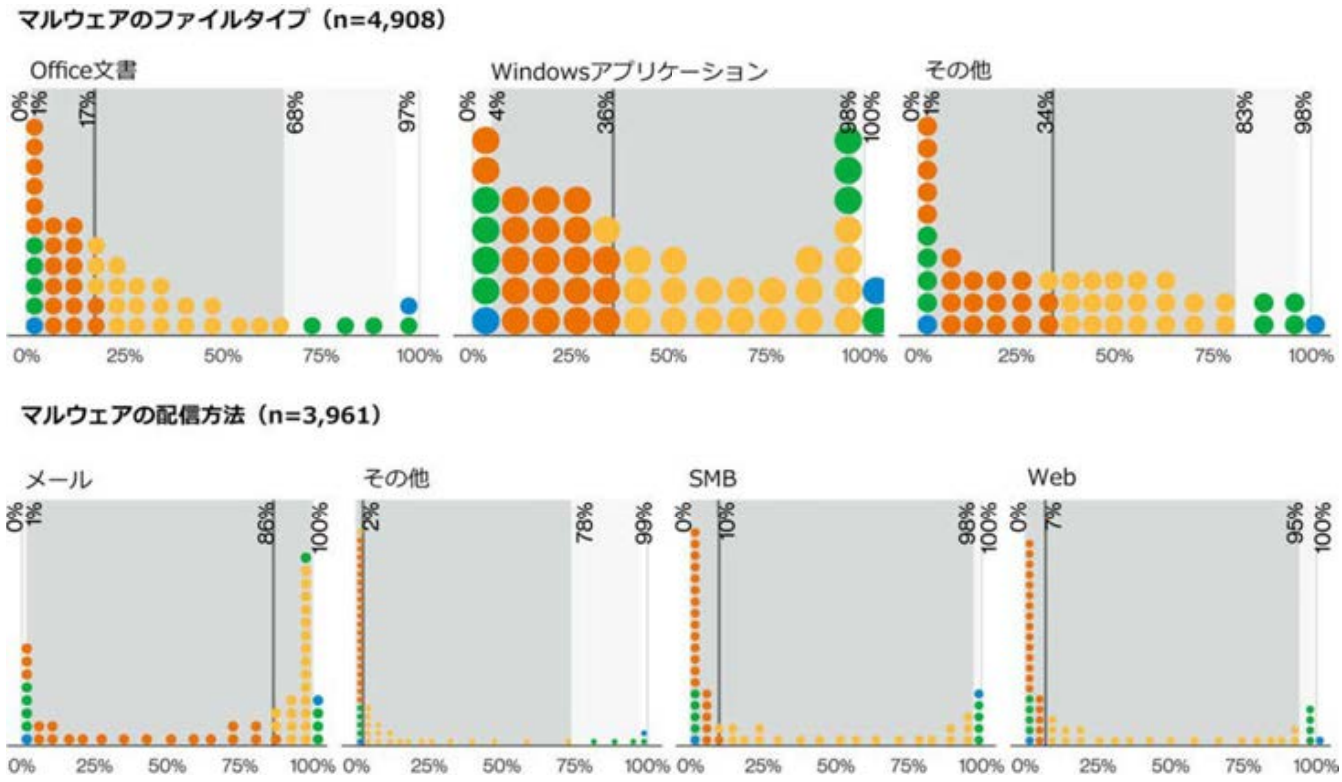


図37. 組織別のマルウェア配信手段の割合

図37は、ファイルタイプの分布と、配信手段の分布を示しています。Office文書やメール8という経路がよく使用されるのは、依然として、ランサムウェアの配備など、さらなる悪事に利用される可能性のある初期ペイロードを配信するための試行錯誤であるかのようです。

暴れ回るランサムウェア

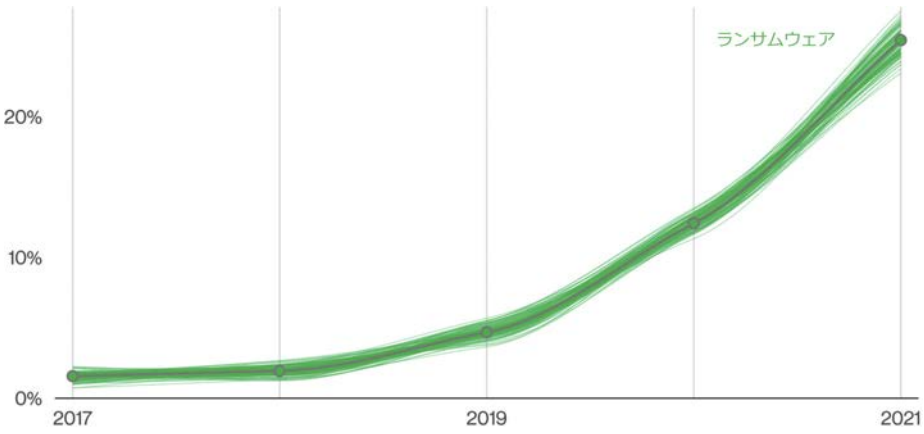


図38. データ侵害/漏洩でのランサムウェアの経時的変化

このセクションは、（私のNFTアート「Unamused Baboons」の値とは異なり）劇的に増加しているというランサムウェアの昨年の調査結果の続編です。この傾向は今年も続いており、約13%増加しています（過去5年間の合計と同程度の増加です）。

ランサムウェアは陰湿なものですが、単に侵害された組織のアクセスを収益化するモデルであり、かなり一般的になっていることを念頭に置いておいてください。ランサムウェアの運営者は、クレジットカードや銀行情報など、価値のある特定のデータを探す必要はありません。データを暗号化することによって、組織の重要な機能を中断する必要があるだけです。

8 中央値の組織では、75%以上のマルウェアをメールで受け取っています。

ランサムウェアの侵入経路

ランサムウェアには様々な種類があり、分かりやすい名前とそうでない名前がありますが、ランサムウェアがシステムに侵入する方法はそれほど多様ではありません。図39は、ランサムウェアを展開するために使用される攻撃とそれぞれの侵入経路の組み合わせを示しています。考慮すべき重要なポイントがいくつかあります。ランサムウェアのインシデントの40%はデスクトップ共有ソフトウェア、35%はメールが要因となっています。ネットワーク内に侵入した攻撃者はさまざまなツールを使用しますが、組織の外部とやり取りするためのインフラ、特にRDPとメールをロックすることは、ランサムウェアから組織を守る上で大きな効果を発揮します。

ブロックされたマルウェアの種類を調べてみると、一般的に「ドロッパー」が2番目に多いことがわかります。これは、メールがよく使われる侵入口であることとよく一致しています。攻撃者は、リモートアクセスの権限があれば、それを直接利用することができます。権限がない場合は、悪意のあるリンクや添付ファイルをメールで送信し、自分自身でリモートアクセスを行う必要があります。

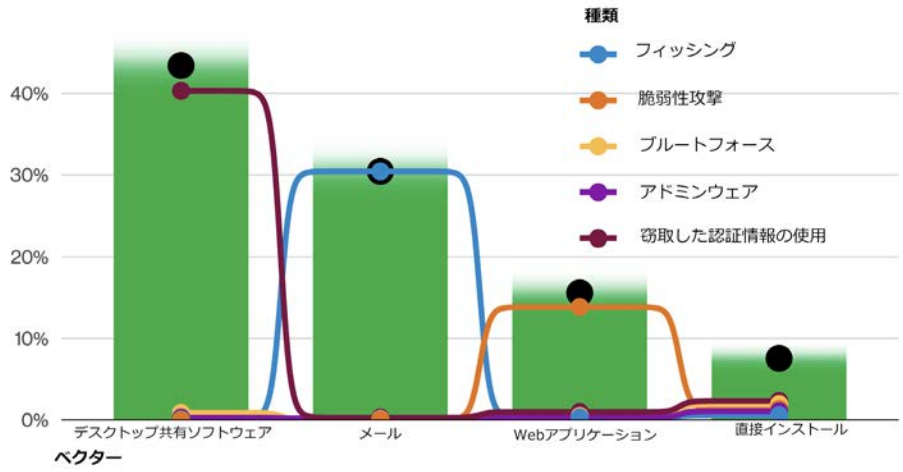


図39. システム侵入型ランサムウェアのインシデントにおける侵入経路内の主な攻撃（n=1,032）

過去を振り返る：ランサムウェア

ランサムウェアの最初のケースは、DBIRの筆者たちの1人がまだおむつをしていた頃（1989年）に発生しましたが、DBIRの主役になるまではかなりの時間がかかりました。ランサムウェアの事例として始めてDBIRに載せられたのは2008年で、それについて何か書くのに十分なデータが揃ったのは2013年になってからです。そして、次のような説明を付けていました。

「企業（一般的には中小企業）を狙う場合、犯罪者はマイクロソフトのリモートデスクトッププロトコル（RDP）を介して、パッチが適用されていない脆弱なポイントからの侵入を試みるか、脆弱なパスワードで標的のネットワークにアクセスします。最初のアクセスに成功した後、彼らは企業のバックアップシステムに変更を加え、バックアップが毎晩実行されても、実際にはデータがバックアップされないようにします。」（2013年 DBIR 31ページ）

9年前と同じことが今も続いているとわかっていれば、この文章をコピーして貼り付けるだけで、時間を節約できたかもしれません。まあ、あと9年もすれば良い方向に変わるかもしれませんが。

パートナー、サプライチェーン、サードパーティ……

サプライチェーン、サードパーティ、パートナーに関わる人にとって、今年は忘れられない1年となりました。2020年は、サイバーセキュリティ業界の勇敢な友人たちによって大規模なスパイ活動が発見され、ちょっとした衝撃とともに幕を閉じました9（それが2021年のDBIRのためのデータ収集期間が終わった直後だったのは、残念でした）。この出来事をきっかけに、サプライチェーン攻撃の影響を受ける可能性のある潜在被害者を特定するという複雑で過酷な、そして至難の業ともいえる取り組みが始まりました。DBIRの調査では、通常、個々のインシデントを検証するのではなく、より大きなトレンドに注目しますが、この1件のインシデントだけでも業界に多大な影響を与え、DBIRのデータセットに驚くべき形で影響を及ぼしました。図36を見れば、この1件がシステム侵入のパターンにどれほど深刻な影響を与えたかがわかるでしょう。ソフトウェアアップデートの急増により、パートナーは、以前は目新しい存在ではなかったのに（DBIRデータの1%未満）、なんと60%ものインシデントに影響を与えるようになりました。しかし、このインシデントは異常な一過性のものに見えるかもしれませんが、実は、私たちが日常的に関わるベンダー、パートナー、サードパーティの間に存在する相互に関連したリスクという点で、この業界で見られるより大きな傾向を表しているように思えます10。

これらの侵害の全体像を理解するためには、サードパーティとサプライチェーンの侵害を定義する必要がありますが、これは少し複雑です。まず私たちは被害者に基づいてインシデントを分類していることに留意する必要があります。したがって、通常は（もちろん、常にではありませんが）、1人の被害者が1つのインシデントとなります。しかし、これでは、サプライチェーンやサードパーティの侵害について議論するときに、実際の環境における相互関係を把握することができません。そこで、最初の侵入によって影響を受けた「第二の被害者」がいる侵害を把握するのに役立つフィールドを追加しました。

サードパーティの侵害を、第三者を危険にさらす単一の侵害と定義しています。DBIRのデータでは、データの所有者と侵害された被害者とが異なる場合に該当します。たとえば、データセンターがランサムウェアに感染し、顧客のデータが暗号化された場合です。この場合、顧客の社内インフラが直接攻撃されたわけではありませんが、顧客は確実に被害を受けています。

2022年のデータセットでは、サードパーティの侵害はDBIRの侵害データのわずか1%でした。それでも、いくつかの興味深いデータポイントを見出すことができます。たとえば、サードパーティの侵害では、「窃取した認証情報の使用」と「ランサムウェア」が上位5つの攻撃のうちの2つであることが分かっています。

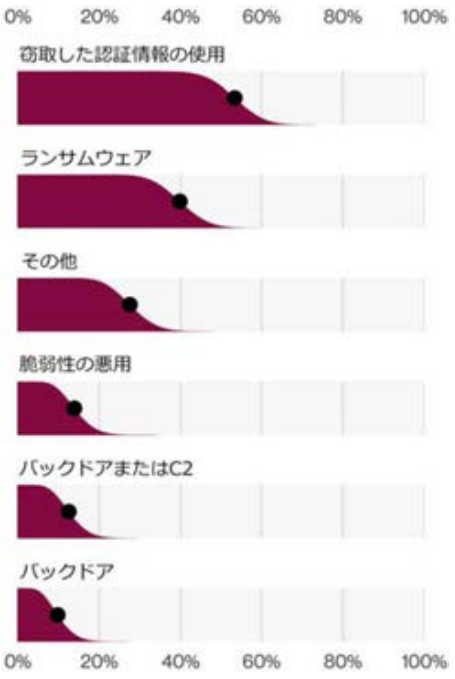


図40. サードパーティインシデントの上位の攻撃（n=73）

9 つまり、終息したと言われていますが、まだ壕の中で間近に迫る世界の終末の到来を待っている我々には、肯定も否定もできません。
10「タイムライン」のセクションでバリューチェーンとイベントチェーンについて述べましたが、これはどちらも攻撃者の「侵害の輪」に含まれるものです。

インシデント経路の種類で次にあげるのは「サプライチェーン」です。DBIRでは、サプライチェーンの侵害を、1つ以上の侵害が連鎖的に発生したものと定義しています。これは第二の犠牲者がいる侵害（第一の犠牲者への侵害から見た場合）、またはパートナー経由の侵害（第二の犠牲者への侵害から見た場合）である可能性があります。また、よくあるパートナー侵害の例としては、侵害されたソフトウェアベンダーから悪意のあるアップデートが組織に送られ、結果としてデータ漏洩/侵害が発生したケースや、パートナーが侵害され、アクセスするために認証情報のセットまたは信頼できる接続が悪用されたケースなどが挙げられます。

昨年の大きな事件がいくつかあった後、これらのタイプのインシデントは、DBIRのインシデントコーパス全体の9%を占め、今年は侵害の0.6%を占めています。2021年に起きた大きな事件では、大規模なネットワーク管理ツールが侵害され、侵害されたサーバーにバックドアを開くために悪用されたこともあり、バックドア11の攻撃の種類の割合が非常に高くなっています。しかし、それ以外の部分では、ランサムウェア、窃取した認証情報の使用、期待される機能を備えた形式の異なるマルウェアなど、注目すべき項目がまだ存在します。過去のDBIRでサプライチェーンへの攻撃事例を紹介したことがありますが、毎年頻繁に使用される手口ではないにしても、このような攻撃の前例があったことを再認識させられます。

最後に

2021年に経験したような大規模な事件が起きると、攻撃に対する防御能力への私たちの自信は揺らいでしまいます。しかし、連邦政府のセキュリティ組織とサイバーセキュリティコミュニティが緊密に連携した結果、今回の事件を数年ではなく数か月で検知・修復できたことを心に留めておいてください。この一連の攻撃について犯人は成功したと思っているのか、それを知るための十分な情報は持ち合わせてはいませんが、業界としても、コミュニティとしても、リソースを共有し、複雑な脅威からお互いを守ることに私たちは最終的に成功したと言えるのではないでしょうか。この取り組みに賛同し、協力してくれたすべての人に感謝します。皆様とご一緒にDBIRチームもグラスを傾けたいと思います。

図41. サプライチェーンインシデントの上位の種類（n=2,103）

11 また、「バックドアまたはC2」の項目にはバックドアが含まれているため、全体として大きな割合を占めています。

侵入の手口

DBIR で取り上げているデータ漏洩 / 侵害の多くは、 フィッシング、 認証情報、 エラーなど、 人的要素に関連するものです。しかし、 このセクションでは、 人的資産に直接関与しない組織への侵入口となる脆弱性について説明します。

脆弱性の悪用の種類は、今年のデータ漏洩/侵害の7%に上り、昨年から2倍に増えています。認証情報やフィッシングに見られるような膨大な数には及びませんが、考えてみる価値はありそうです。まず当然ながら、「攻撃者はどのようにしてこれらの脆弱性を見つけているのか」という疑問があるでしょう。昨年も指摘しましたが、図43に見られるように攻撃者は常に臨戦態勢にあるセールスファネルを持っています。攻撃者は、まずIPとオープンポートをスキャンすることから始めます。次に、特定のサービスのクロールに移ります。その後、特定の脆弱性識別子（CVE）のテストに移ります。そして最後に、リモートコード実行（RCE）を試みて、システムにアクセスするという段取りです。

もし、攻撃者がこのようなプロセスで組織をターゲットにしているとしたら、どのような発見があるでしょうか。図42は、4つの異なるカテゴリー（それぞれ約100組織を含む）に分類された組織のセットを示しています。「安全」（少なくとも積極的に安全確保に努める組織）、「ランサムウェア」（ランサムウェアのインシデントが開示された組織）、「ランダム」（純粋にランダムに選ばれた組織）、「侵害」（侵害が発生した組織）です。ホストサーバーあたり平均でどれだけの脆弱性があるかを調べましたところ12、すべてのカテゴリーの中央値には、ほとんど脆弱性がないことがわかりました（無作為に選んだ組織では、ほんの少し高くなります）。これは、データ漏洩/侵害の多くは脆弱性と結びついていないことを示しています。しかし、分布の両端は異なることを物語っています。「安全」に配慮している組織は、かなり厳重に管理されていますが、他の3つのカテゴリーの組織では、インターネットに接続するホスト1台につき、はるかに多くの脆弱性を抱えていることがわかります。図43で示した攻撃者が誰なのかを考えてみると、それは末端に位置する組織であることがわかります。忘れてはならないのは、多くの攻撃者にとって、攻撃は単なる数合わせのゲームであり、ある程度のアクセス数が欲しいだけですが、それでも、チャンスが訪れるまでエクスプロイトを試行し続ける十分な動機となるということです。

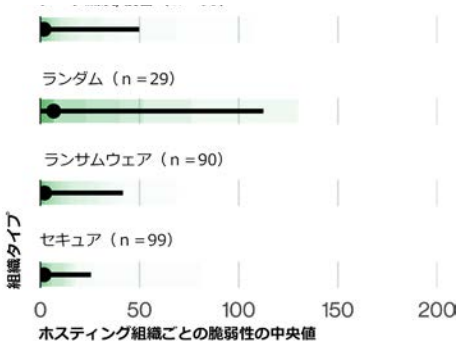


図42. 組織タイプ別のホスト1台あたりの脆弱性（インターネットに接続している組織のみ）

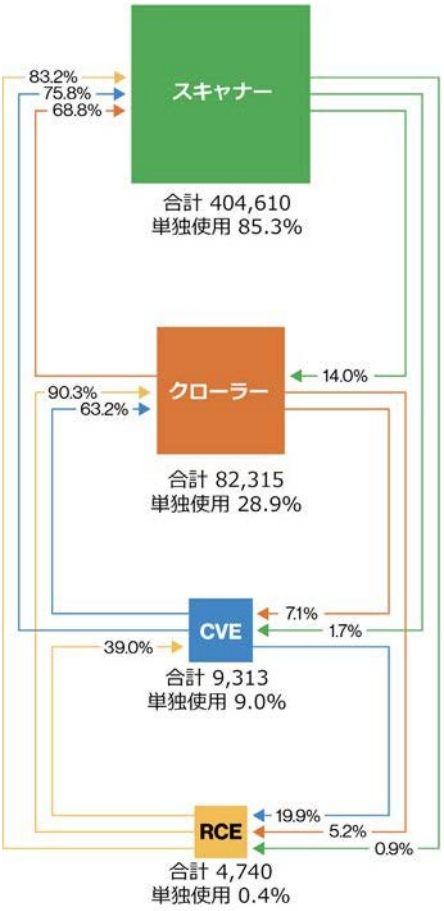


図43. 常に臨戦態勢にある攻撃者のセールスファネル

12 また、統計としてそれほど難しいものではないため、平均を中央値の意味で使っています。モードです。

しかし、ありがたいことに、状況は改善されています。図44は、過去6年間における脆弱性の修正のスピードと完全性を示しています。この図では、値が高ければ高いほどよく、全般的に状況は好転しています。パッチ適用の数もスピードも向上しています。

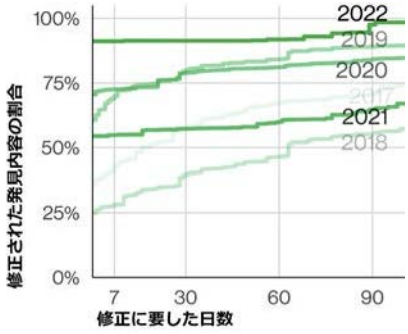


図44. 検出したものを修正するまでの時間

他の点にも着目してみましょう。昨年、ジニ係数（基本的に、少数のことがたくさん起こり、多数のことが数回しか起こらないかどうかを示す尺度）についてお話ししました。図46では、これを「痛みのピラミッド」の各レベルに適用しています。脅威インテリジェンスの専門家でない方のために説明すると、「痛みのピラミッド[13]」とは、脅威情報アナリストが防御者のさまざな指標の価値を分類するために使うモデルです。ピラミッドの底辺は、（ファイルのハッシュのように）攻撃者による変更が容易であるため、防御側にとってあまり有用ではありません。ピラミッドの頂点は、攻撃者が変更することが極めて困難なものです（攻撃者が確立したこのプロセスはTTP（Tactics, Techniques and Procedures）とも呼ばれる）。

ここからわかることは、ハッシュ以外の「痛みのピラミッド」の指標は、ジニ係数がかなり高いということです。つまり、その指標の最初の数パーセントをブロックすれば、悪意の大部分を阻止できるということです。もっともピラミッドの上位に行くほどジニ係数が高くなるであろうとの予想はありましたが、IPアドレスから上はすべてほぼ同じでした。図43に戻ると、IPでも似たようなことがわかります。リモートコード実行（RCE）を試みたIPのうち0.4%しか前段のいずれの段階にも見られませんでした。つまり、恐らくSecOpsは「悪質なIPをブロックせよ！」ということをすでに知っていることを表しています。

ピラミッドの頂点に位置するTTPがないことにお気づきでしょうか。実は、DBIRチームはこのデータを持っていないのです。しかし、付録Bの「VERISと標準」にこのデータ収集の問題に対する解決策を記載してあります。

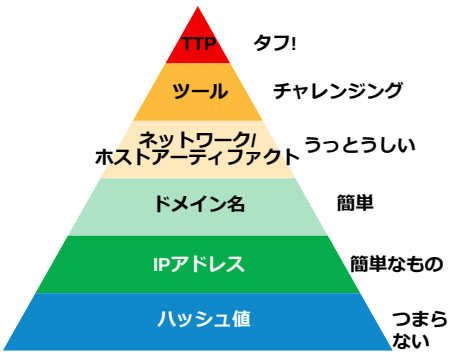


図45. 痛みのピラミッド

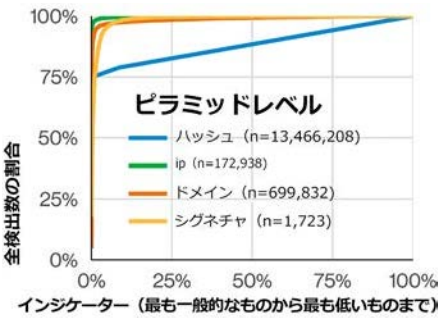


図46. 指標の累積和

13 "The Pyramid of Pain（痛みのピラミッド）" Bianco, David J.、https://bit.ly/PyramidOfPain, 2014年1月。

ソーシャル エンジニアリング

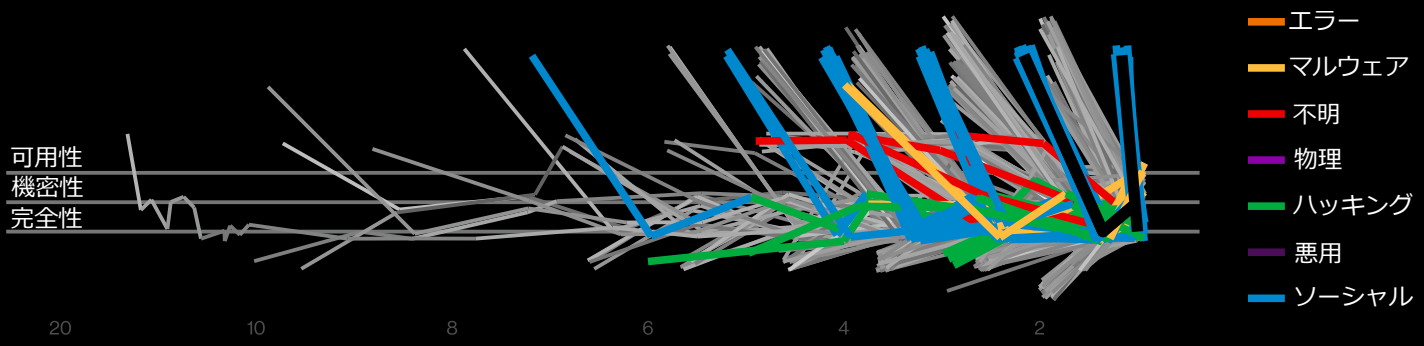


図47. ソーシャルエンジニアリングのインシデントの経路（n=75）

私のせいなの？

今年のDBIRに掲載したデータ漏洩/侵害の82%[14]は人的要因でした。これは、ソーシャルエンジニアリングのパターンが人間を中心とした事象の多くを捉えており、人間をセキュリティ領域の中心に据えていることを示しています。

サマリー

今年もデータ漏洩/侵害の82%の主な要因は人的要素であり、このパターンがこれらのデータ漏洩/侵害の大部分を占めています。さらに、マルウェアや盗まれた認証情報は、ソーシャルエンジニアリング攻撃で攻撃者が侵入した後の第2段階で有効なツールとなります。つまり、強力なセキュリティ啓発プログラムを持つことの重要性を示しています。

昨年との比較

今年も引き続き、これらの攻撃は、「フィッシング」攻撃と、より説得力のある「なりすまし」攻撃（BECによく見られる攻撃）に分かれています。

頻度	2,249件のインシデント、確認されたデータの暴露1,063件
攻撃者	外部（100%）、（漏洩/侵害）
攻撃者の動機	金銭目的（89%）、スパイ活動（11%）（漏洩/侵害）
侵害されたデータ	認証情報（63%）、内部情報（32%）、個人情報（24%）、その他（21%）、（漏洩/侵害）

14 ソーシャルエンジニアリングのパターンだけではありません。

図49を見ると、ソーシャルエンジニアリングのパターンではフィッシングが中心となっています。ええ、わかります。「もう気絶しそう!ソファで横にならせて!」と言いたくなりますね。

しかし、ある意味このグラフは、ソーシャルエンジニアリングによる侵害には数多くの経路があることを示しています。フィッシングで盗まれた認証情報が「窃取した認証情報の使用」で使用されることがわかります。「なりすまし」では、「ビジネスメール詐欺（BEC）」が確認されています（Eはフィッシングと直接結びついているEメール）。「ダウンローダー」と「ランサムウェア」ではマルウェアの投下（ちなみに、データ漏洩/侵害ではなくインシデントの場合、ソーシャルエンジニアリングでの割合は17%に上昇）、「ネットワークのスキャン」「ホストのプロファイリング」ではハッキング、「バックドアまたはC2」ではパーシスタンス（持続性）が確認されています。全体として、フィッシングが組織へ侵入する4つの主要な手口の1つであるという事実が浮き彫りになりました[15]。

フィッシング

サットンの法則によれば、「診断するときは、まず明白なことを考えよ」とあります。したがって、犯罪者がなぜフィッシングを行うのか不思議に思うのであれば、それはメールが彼らにとってターゲットに到達可能な手段だからです。フィッシングメールを実際にクリックする従業員は2.9%に過ぎず、この調査結果は長期にわたって比較的安定していますが、それでも犯罪者がフィッシングメールを使い続けるには十分すぎる数字です。例えば、DBIRで扱ったデータだけでも、1,154,259,736件の個人情報[16]が流出しています。そのほとんどがメールアカウントだと仮定すると、2.9%という数字は33,473,532のアカウントがフィッシングされたことを意味します（ペルーに住む全国民のフィッシングに成功したようなものです）。

良いニュースとしては、フィッシングの報告件数が増えていることです。図48は、フィッシングメールについての報告が過去半年間に約10%増加し、着実に増加していることを示しています。問題は、「報告のあった12.5%に対処し、クリックされた2.9%を見つけることができるのか」という点です。

ビジネスメール詐欺 （BEC）

図49では、ソーシャルエンジニアリングによる侵害の27%が「なりすまし」であり、そのほとんどがBECであることがわかります。このような攻撃をBECと呼びますが、悪質な攻撃者が不正侵入したメールアカウントを使ってただ誰かになりすますというよりも、もう少し複雑なになってきています。BECのうち、フィッシングを伴うものは41%に過ぎません。残りの59%のうち、43%[17]は、被害者の組織で「窃取した認証情報の使用」を行うものでした。残りは、パートナーからのメールを利用したBECか、または「C」[18]を全く必要としない何らかのタイプのフリーメールアカウントを利用したBECである可能性が高いと考えられます。BECにはさまざまな形態があり、パートナーの情報漏洩によって自社の組織が狙われることもあれば、逆に自身のメールの情報漏洩によってパートナーが標的にされたり、自身の侵害によって情報が漏洩し自分が標的にされたりすることもあります。あるいは、先に指摘したように、情報漏洩はまったくなく、ただ攻撃者はあなたの会社の金銭を必要としているという説得力を伴う理由がある場合もあります。

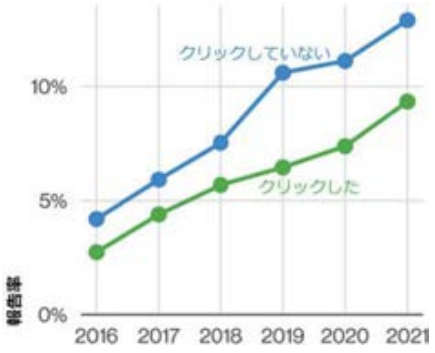


図48. クリック状況別のフィッシングメール報告率（n=295,825,679）

図49. ソーシャルエンジニアリングによるデータ漏洩/侵害の攻撃の種類（n=1,063）

15 残りの3つは認証情報、脆弱性、既存ボットです。

16 「個人情報」はメールアドレスでだけではありません。住所や名前などもありますが、通常はメールアドレスを含みます。また、ユーザ名がメールアドレスであることが多い認証情報はカウントされません。

17 そのとおりです。では、59%×43%で1桁繰り上げ、ローマ数字に変換すると...全BECの25%のようです。

18 つまりBECの「C」（Compromise）=詐欺

図50は、犯罪者がどの程度の金銭を必要と感じているかを示しています。現在のインフレ進行に合わせて、今年、自分たちの昇給を認めたようです。とはいえ、DBIRに詳しい読者なら何かできることがあるはずです。ic3.govで苦情を申し立て、FBI IC3 Recovery Asset Team（RAT）と連絡を取ってください。RATがBECに対処し、送金先の銀行と連携した場合、米国内で発生したBECの半数で93%の資金が回収されたか、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14%でした。

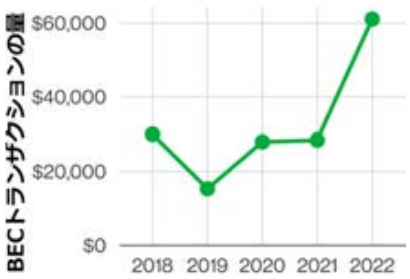


図50. BECのトランザクションサイズの中央値（n=50,342）トランザクションが発生したFBI IC3の苦情に基づく

マルウェア

「またマルウェア？「攻撃」のセクションで読んだのに、なぜまたマルウェアの話？」それは、マルウェアが大量に存在するからです。でも、セクションの間である程度の重複があることは認めます。今年は、2つのパターンに分類されるものが昨年よりも多く見受けられました。その中でも、「システム侵入」と「ソーシャルエンジニアリング」は、その筆頭と言えるでしょう。

「システム侵入」のセクションの図37で指摘したように、少なくとも初期段階では、マルウェアの配布にはメールが最もよく利用されます。図52によると、データ漏洩/侵害では、フィッシングに成功し、マルウェアを送り込んだ後、攻撃者は、バックドアまたはコマンド＆コントロール（C2）の提供とダウンローダーの配信の2つを目的としていることがわかります。フィッシングでドアをこじ開けた場合、図52は、バックドア、C2、ダウンローダーが、他のすべての攻撃を行うためにドアを開けたままにしていることを示しています。注目すべきは、ランサムウェアがデータ漏洩/侵害の約半分を占めているのに対し、インシデントに関する同じ分析では、ダウンローダーとランサムウェアがそれぞれ74%と64%の割合でマルウェアインシデントの上位2位を占めている点です。これは、今年のDBIRでは、ランサムウェアに言及しないセクションは1つもないことを明確に証明しています。

トレーニング

情報セキュリティに関しては、明らかに「人的要素」が多くを占めています。情報漏洩の直接の原因でないとは言え、情報システムは人が構築したものです[19]。率直に言って、AIに頼む方がはるかに厄介に思えるので、問題を解決するのはむしろ人であってほしいのです。

残念ながら、完璧なものはありません。人も、プロセスも、ツールも、システムもです[20]。しかし、私たちは、行ったこと、また構築したことを改善することができます。そのために、トレーニングは改善の大きな部分を占めます。図51は、1年間に従業員が受けるフィッシングについてのトレーニングの量を示しています。ほとんどのトレーニングは予想の2倍時間がかかり、10%は3倍の時間がかかっています。トレーニングは、日常的な行動（「... をクリックするべからず」などの標語やパスワード管理プログラムの使用など）と設計（安全なコーディング、ライフサイクル管理など）の両方において、セキュリティ行動の改善に貢献できる可能性があります。とはいえ、トレーニングを受けるのは簡単ですが、それが機能していることを証明するのは少し難しくもあります。その方法についてのヒントが欲しいなら、付録C「行動を変える」をご覧ください。

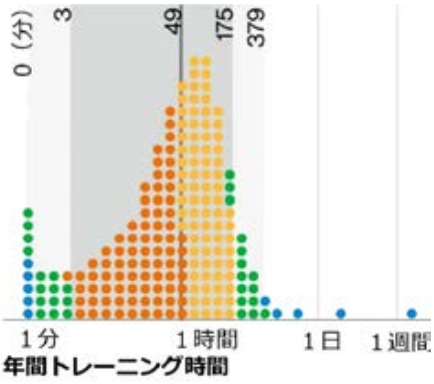


図51. 1年間でトレーニングに費やした1人あたりの時間（分単位）（n=45,372、対数スケール）

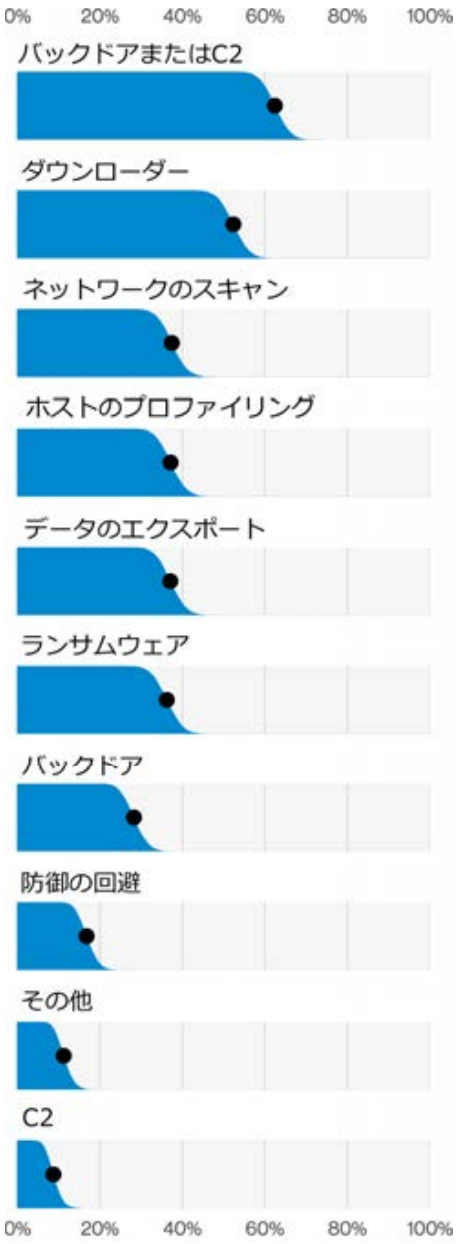


図52. ソーシャルエンジニアリングによる侵害の上位のマルウェアの種類（n=235）

19 すべてのビッグフットの話が真実でない限り。私たちはDaveをカンファレンスに送り、それを確かめようとしましたが、返事はありません。
20 DBIRの執筆者ではありません（これは議論の余地があります。私たちはオラクルに尋ね、サイコロを振ったところ、「おそらく完璧」が出ました）。

基本Web アプリケーション攻撃

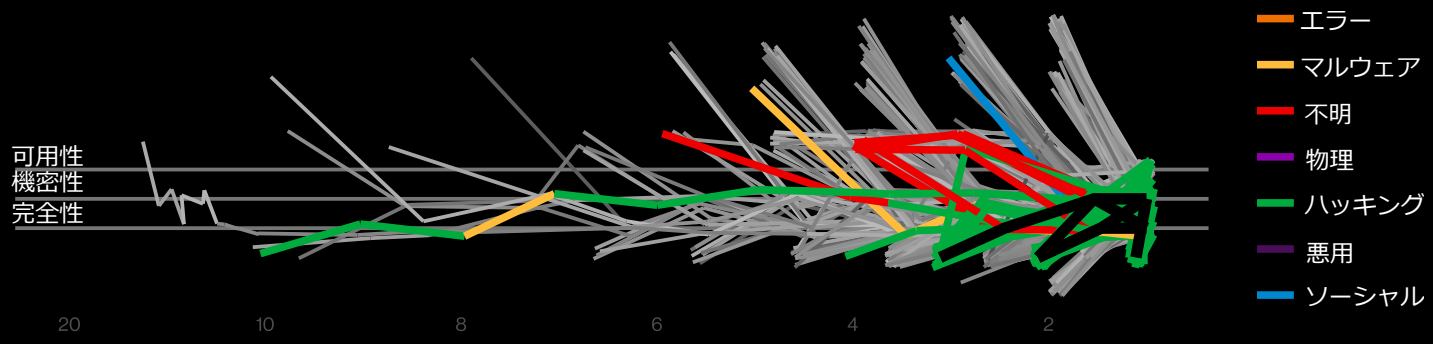


図53. 基本Webアプリケーション攻撃のインシデントの経路（n=92）

これだからインフラは大きく見えてしまう？

「基本Webアプリケーション攻撃」（BWAA）では、Webサーバーなど、組織で最も露出度の高いインフラを直接標的とする攻撃に主に焦点を当てています。これらの攻撃は、「窃取した認証情報の使用」と「脆弱性の悪用」という2つの侵入経路のうち、どちらか一方を利用します。

サマリー

このパターンの攻撃は2つの領域に分かれています。1つは、窃取した認証情報の使用、脆弱性の悪用、パスワードのブルートフォースなど、サーバーにアクセスする手段です。もう1つは、持続性を維持したりアクセスを収益化したりするために、バックドアのような特定のペイロードを使用します。

昨年との比較

今年も引き続き、Webサーバーやメールサーバーなどのインターネットに接続された組織のインフラにアクセスするために、窃取した認証情報を使用することが大きな割合を占めています。

頻度	4,715件のインシデント、確認されたデータ暴露1,273件
攻撃者	外部（100%）（漏洩/侵害）
攻撃者の動機	金銭目的（65%）、スパイ活動（31%）、怨恨（2%）、イデオロギー（1%）（漏洩/侵害）
侵害されたデータ	個人情報（69%）、認証情報（67%）、その他（29%）、医療情報（15%）（漏洩/侵害）

図54. 基本Webアプリケーション攻撃による侵害の上位の攻撃の種類（n=962）

図54は、このパターンの侵害の80%以上が盗まれた認証情報に起因していることから、パスワードの適切な保護の重要性を示しています。図55は、「窃取した認証情報の使用」と「脆弱性の悪用」という観点から、より大きな傾向を明らかにしたものです。2017年以降、「窃取した認証情報の使用」は約30%増加しており、過去4年間、組織にアクセスするための最も確実な方法の1つであることが確定しました。

図55は、Webアプリケーションに関わるインシデントの大半が、窃取した認証情報を使用していることを明確に示しています。図56には、バックドア（侵入後に足場を固めた後に有効）、リモートインジェクション（脆弱性を突かれた後にマルウェアがシステムに侵入する方法）、そしてもちろんデスクトップ共有ソフトウェアなど、他の攻撃経路も散見されます。

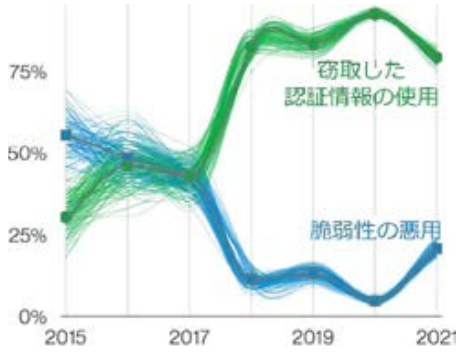


図55. 基本Webアプリケーション攻撃による侵害における脆弱性の悪用と窃取した認証情報の使用の経時的変化

図56. 基本Webアプリケーション攻撃による侵害における上位の攻撃経路（n=972）

メールサーバーが攻撃される

攻撃対象に関して、図59は（このセクションのタイトルから明らかなように）Web アプリケーションが高い比率で侵入されていることを捉えていますが、このパターンでは、メールサーバーは全体の20%未満に留まっています。これらのメールサーバーのうち、80%は盗まれた認証情報で侵害され、30%は何らかの悪用で侵害されています。この30%という数字は、それほど高い数字ではないように思われますが、エクスプロイトを使用したメールサーバーの標的は、3%しか占めていなかった昨年から劇的に増加しています。

基本的＝有用ではない

このようなタイプの攻撃は、脆弱な認証情報を探してインターネット上を飛び回る進取の気性に富んだ犯罪者の仕業であると考えるのは無理もないことかもしれません。しかし、国家に支援された攻撃者もこの低コストで高報酬の戦略を利用しているようで、基本Webアプリケーション攻撃による侵害の20%以上が「スパイ活動」とされています。もし玄関の鍵が弱いのであれば、C2サーバーの高速ネットワークで複雑なポリモーフィックバックドアを開発する必要はないというわけです。

過去を振り返る ：

哲学者のジョージ・サンタヤーナは、「歴史から学ばない者は、それを繰り返す運命にある」という名言を残しています。パスワードの不適切な使用は、2009年から現在までデータ漏洩/侵害の主な原因の1つですので、この名言は事実と言えそうです。

「このグラフから、多くのシステム侵入がIDの基本的な管理（の不備）を悪用していることがわかります。デフォルトの認証情報、共有されている認証情報、窃取した認証情報を使った不正アクセスは、「ハッキング」カテゴリー全体の3分の1以上を占め、記録されたデータ漏洩/侵害の半分以上を占めています。これらの攻撃は比較的容易に防ぐことができるにもかかわらず、デフォルトや共有した認証情報の使用によってこれほど多くの大規模な侵害が発生していることは、特に問題です。」（2009年 DBIR 17ページ）

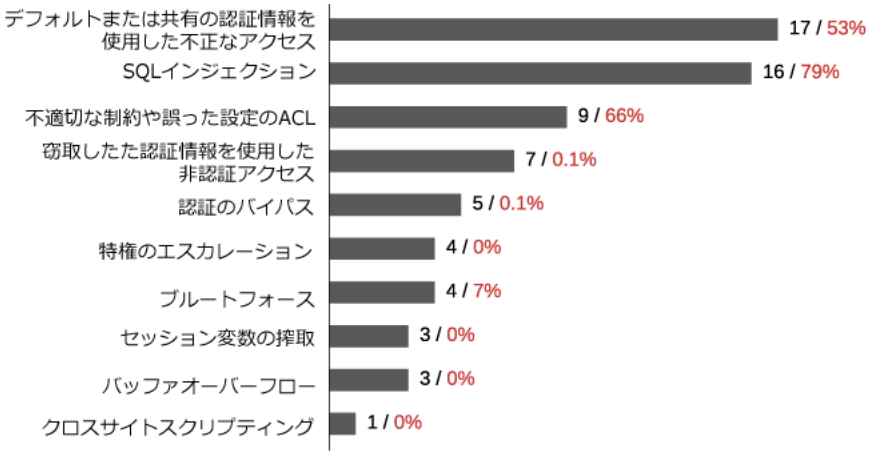


図57. ハッキングのタイプ：侵害の回数（黒）、レコードにおける割合（赤）（2009年DBIR、図15）

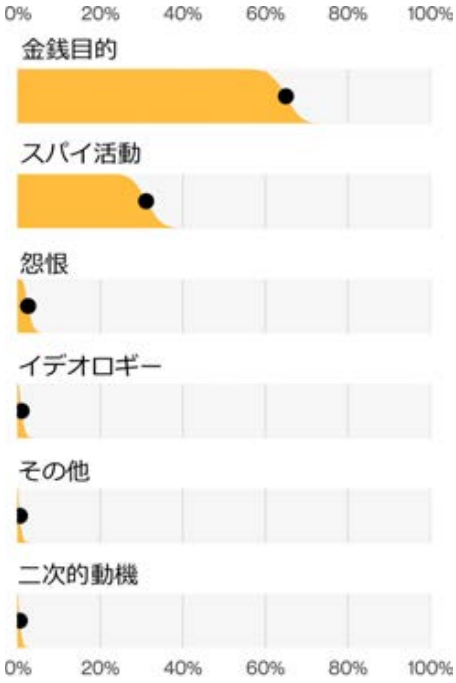


図58. 基本Webアプリケーション攻撃の上位の動機（n=251）

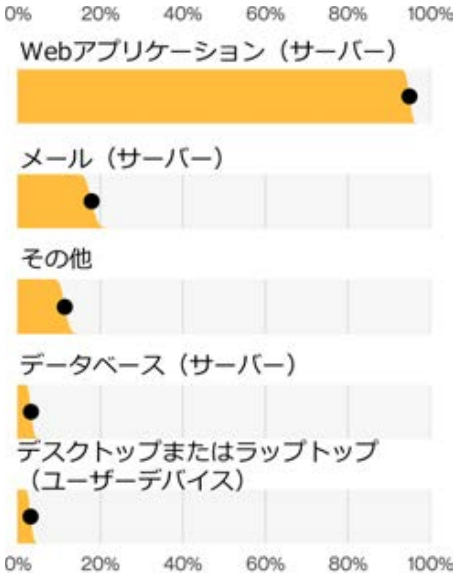


図59. 基本Webアプリケーション攻撃で侵害された上位の資産（n=1,001）

多種多様なエラー

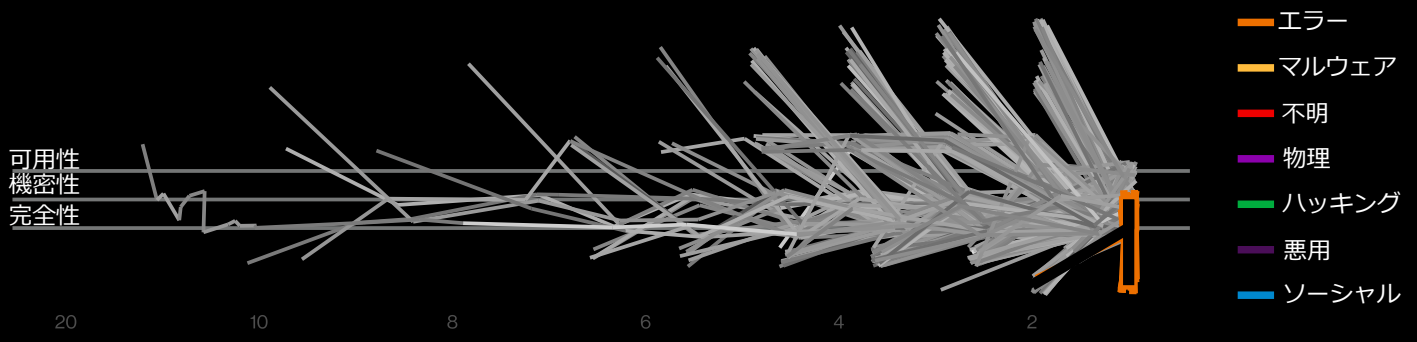


図 60. 多種多様なエラーのインシデントの経路 （n=32）

状況の設定ミス

ほとんどのパターンは長年にわたって変化していますが、不変なのは人々が犯すミスです。2015年、ミスのほとんどはメディア資産（書類）の誤送信であり、一方、設定ミスは侵害全体の10%未満でした。しかし、今年は設定ミスと誤送信ほぼ同程度になりました

サマリー

このパターンの攻撃は、定義では組織内のまたはパートナーの攻撃者によって構成されますが、今年のデータでは、すべて従業員によって構成されていることがわかります。誤送信と設定ミスの2つが上位を占めています。設定ミスは、「セキュリティリサーチャー」という発見方法とよく組み合わされています。

昨年との比較

依然として人は誤りを犯します。そしてその誤りがデータ漏洩を引き起こします

頻度	715件のインシデント、確認されたデータ暴露708件
攻撃者	内部（100%）（漏洩/侵害）
侵害されたデータ	個人情報（81%）、その他（23%）、医療情報（18%）、決済情報（8%）（漏洩/侵害）

設定ミスの増加は2018年に始まり、適切なアクセス制御を行わずに立ち上げたクラウドデータストアの実装が大きな要因となっています。多くのセキュリティ研究者がインターネット上のこれらのデータベースの露出を発見し、その名が知られるようになりました。主要なクラウドプロバイダーがデフォルトの設定をより安全なものにしようと努力しているにもかかわらず（これは称賛に値します）、こうしたエラーは後を絶ちません。

最近の誤送信によるデータ漏洩は、メールによる誤送信が多いですが、物理的な書類もある程度は問題になっています。

これらのデータ漏洩/侵害におけるデータの種類で、圧倒的に多いのは依然として個人情報です。医療や銀行の情報が含まれることもありますが、一般的ではありません。データは顧客から送信されたものであることが多く、また、ほとんどの場合、侵害された組織に通知するのも顧客です。しかし、セキュリティ研究者が依然とこの「ディスカバリー」ショーの主役であることに変わりはありません（その割合は昨年より減少していますが）。

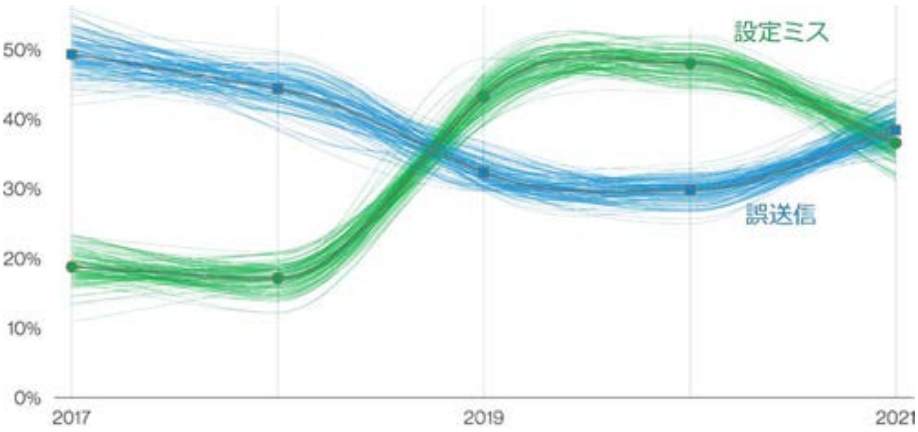


図61. 多種多様なエラーによるデータ漏洩/侵害の上位の攻撃の経時的変化

図62. 多種多様なエラーにおける上位の資産の種類（n=513）

サービス拒否（DoS）

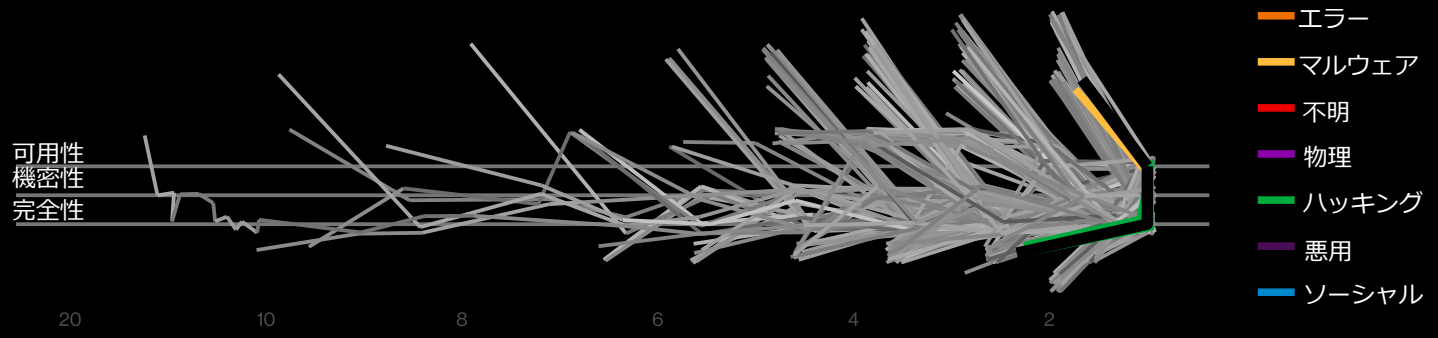


図 63. サービス拒否のインシデントの経路　（n=3）

行けども行けども大渋滞

サービス拒否のパターンは、DBIRのデータセットの中で最も多いタイプのインシデントであり続けているため、おそらく多くの人にとって身近すぎるものと言っても過言ではないでしょう。このパターンは、ボットネットや侵害されたサーバーを利用して、標的のコンピューターにジャンクデータを送信し、「パイプ内のトラフィックジャム」を発生させてサービスを拒否しようとする迷惑な攻撃を主体としています。

サマリー

これらのサービス拒否攻撃は、広範囲にわたり組織に影響を与える厄介なものですが、一部の組織は、これらの攻撃を定期的に受けており、将来的なビジネスの機能に影響を与える可能性があります。

昨年との比較

サービス拒否（DoS）は、サイバーセキュリティに関する最も一般的なインシデントの1つであり続けています。

頻度	8,456件のインシデント、確認されたデータ暴露4件
攻撃者	外部（100%） （インシデント）

このような厄介なインシデントは、特定の業種に限ったことではありません。図64が示すように、情報産業、専門的ササービス、製造業、政府機関など（DBIRでとり上げている多数の業種）、幅広い企業で発生しています。

しかし、DoS攻撃は各業種に偏在しているかもしれませんが、これらの業種の組織が常にDoS攻撃にさらされているわけではありません。DoS攻撃の中央値は 4 時間未満であり（図65）、これらの攻撃を監視している組織の大多数は、年間に受ける攻撃は10件未満であることがわかりました。一方、年間1,000件以上のDDoS（分散型DoS）攻撃を受ける不運な1%の企業のほとんどは、この事実をすでに認識しており、トラフィックを管理するためのサービスを利用しているでしょう。

DDoS 攻撃の実態

DBIRでDDoSを初めてとりあげたのは2013年で、それ以来、毎回話題に上るようになりました。この数年間を振り返って、状況がどのように変化したかを確認するのは興味深いことです。2013年のDDoSでは、攻撃の中央値は約422Mbpsで、100Gbpsの大台に乗るものはごくわずかでした。2016年には中央値が1.1Gbps（3年前の2倍）となり、現在では中央値が約1.3Gbpsとなっています。

DDoS攻撃が狭い範囲に集中している様子も見て取れます。2013年から2016年、そして2021年にかけて、DDoSは中央値を中心に狭い範囲に集中していることがわかります。2013年当時、DDoS攻撃はその場限りの限定的なものでしたが、今日のDDoSインフラははるかに形式化され、反復可能なものになっていると推測21されます。

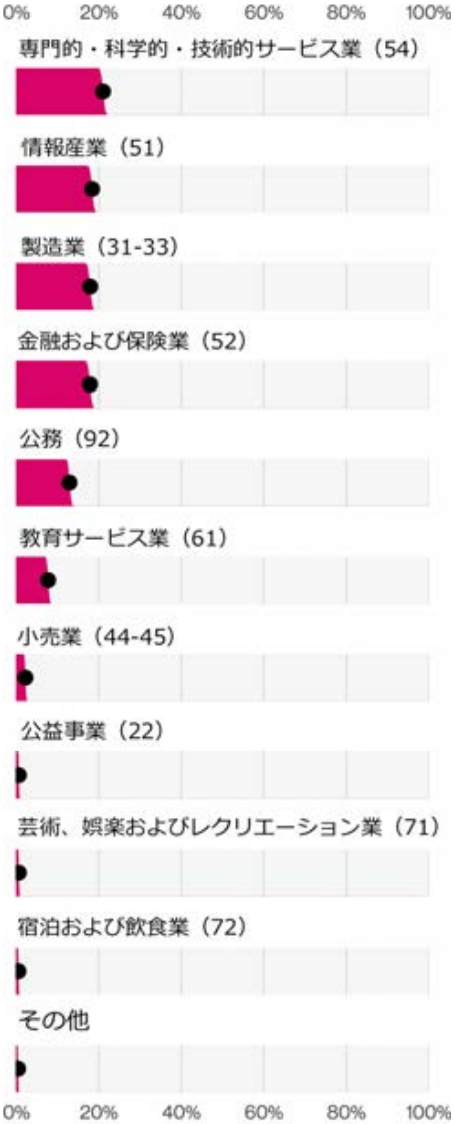


図64. DoSインシデントの上位の業種（n=8,330）

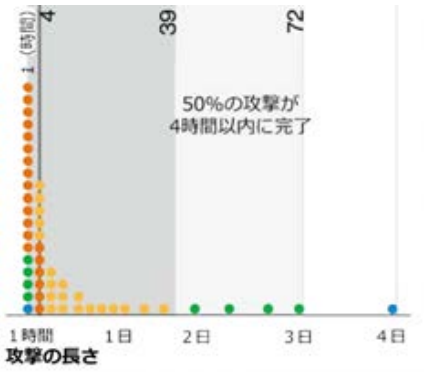
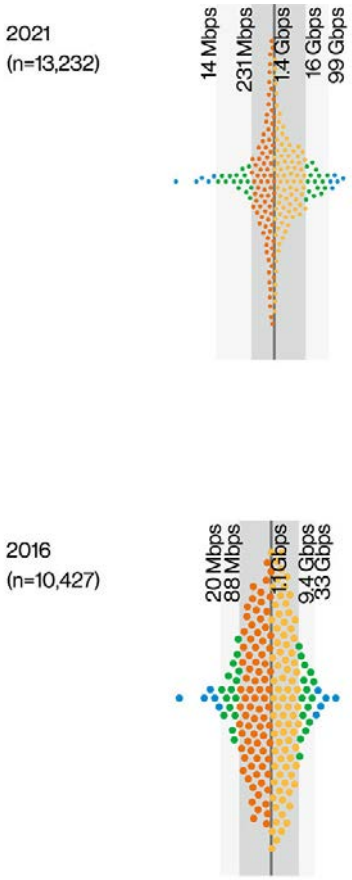


図65. DDoS攻撃の期間（n=15,059、対数スケール）。



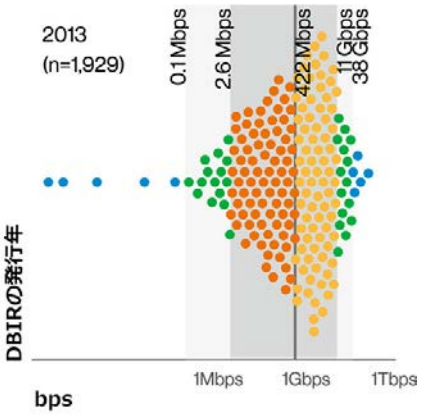


図66. DDoS攻撃速度（bps）の経時的変化（対数スケール）

21 あくまでも「推測」です。

資産の紛失・盗難

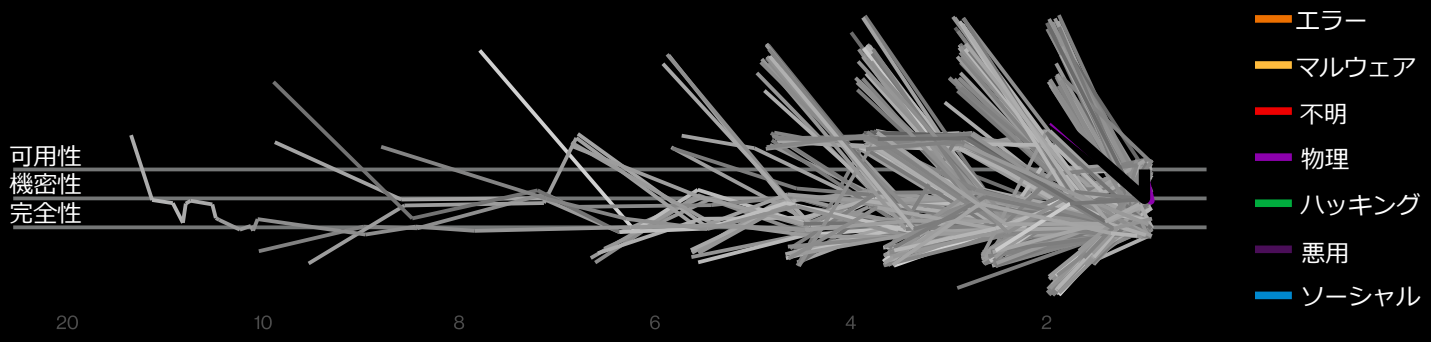


図 67. 資産の紛失 ・ 盗難のインシデントの経路

紛失

昨年のレポートでは、セキュリティインシデント（確認された漏洩/侵害ではない）について、組織のために働いていない人物による盗難よりも、従業員によって資産が失われる可能性の方がはるかに高いと述べました。しかし、漏洩/侵害に着目すると、その逆であることがわかります。

サマリー

このパターンのケースのほとんどは、盗まれたデバイスの性質上、データへのアクセスを確認することが困難なため、「侵害」ではなくインシデント（「事故」）として分類されています。このパターンで盗難が多発しているのは、「金銭的動機」によるものです。盗みを働く者の多くは、盗んだ資産を売却してすぐに現金化するために犯罪に及んでいると考えられます。

昨年との比較

これらの事件で被害を受けたデータのタイプは、昨年と（ほぼ）同じです。通常、盗みを働く者は外部の人物ですが、従業員は資産の行方を見失ったことに責任を負います。

頻度	885件のインシデント、確認されたデータ暴露81件
攻撃者	内部（94%）、外部（6%）（インシデント）
攻撃者の動機	金銭目的（98%）、イデオロギー（2%）（インシデント）
侵害されたデータ	個人情報（77%）、医療情報（43%）、その他（15%）、決済情報（9%）（インシデント）

データ漏洩/侵害の発生が確認できるケースでは、盗まれた資産が原因であることが多くなっています。それでも、盗まれた資産からデータが漏洩したことを確認するのは難しいため、このパターンでは大半（約90%）のケースが「侵害」ではなく「セキュリティインシデント」に分類されています。

パンデミックとそれに伴う出張の減少にもかかわらず、「資産の紛失・盗難」がよくあるパターンとしてDBIRのデータセットに残っているのは興味深いことです。これは、従業員に携帯機器を預ける場合、一定の割合の従業員が機器の置き場所を間違えるか、盗難に遭いやすい場所に置き忘れるということを示しています。自家用車に置き忘れるというのは、データの中で繰り返し出てくるテーマです。以前より自宅の近くで置き忘れるようになっただけかもしれません。

図69は、紛失や盗難が最も多いデバイスを示しています。ユーザのデバイス（デスクトップ、ラップトップ、携帯電話など）は、紛失や盗難に遭う頻度が最も高いアイテムです。それでも、これらの侵害の割合を大きく占めているのは、依然として「書類」です。これは、「公務」や「医療および社会福祉業」の業種で最も多く発生しており、これらのインシデントで医療データの侵害が多いことを説明する一因にもなっています。政府（ほとんどの国）は、健康保険関連のデータを管理する大規模なプログラムを運営しており、もちろん医療業界のメンバーも同様です。保護されるべき健康情報（PHI）を扱う業界は、侵害を報告するための規制要件が高い傾向にあるため、他の業種よりも多くこれらの事象を把握することができます。

図69. 資産の紛失と盗難の侵害における上位資産の種類（n=76）

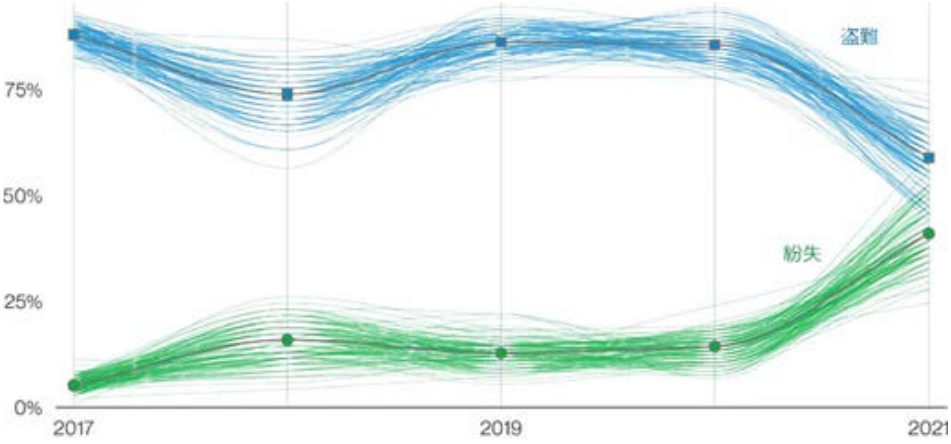


図68. 資産の紛失・盗難のデータ漏洩/侵害における上位の攻撃の種類の経時的変化

「オーガニックフリーレンジ」データ

携帯電話のデータは、 DBIR でとりあげることはほとんどありませんが、 私たちの現状を考えると皮肉なことです。

残念ながら（あるいは幸いにも）、携帯電話はDBIRの侵害データセットの1%以下であり、関連する原因も定まらない傾向があります。これは、データに偏りがあるためと思われます。携帯電話が認証情報のフィッシングに使われた場合、報告されるのはたいていメールサーバーであり、アクセスに使われた端末ではありません。携帯電話のマルウェアが関与したデータ漏洩/侵害が発生した場合、データ収集を行うためにマルウェアがインストールされていることは珍しくありません。そして、データ収集が目的であれば、最初にデバイスに侵入することの難しさを考えると、見つからないようにひっそりとしているのもわかります。

しかし、インシデント以外のデータに目を向けると、セキュリティエコシステムにおいてモバイルが果たす役割がより明確に見えてきます。図70は、携帯電話が目にする脅威のイメージを示しています。

84%のデバイスが不要なアプリの使用を回避していますが、すべてのURLへのアクセスをブロックして回避しているデバイスは42%だけです。つまり、残りの58%のデバイスでは、少なくとも1つの不正なURLがクリックされ、16%のデバイスに少なくとも1つのマルウェアまたはリスクウェアのアプリがインストールされていることになります。この数字はそれほど多くないと思われるかもしれませんが、モバイルデバイスの管理コンソール（または従業員数）を見れば、この数字がどんどん増えていくことがわかるでしょう。

また、携帯電話のユーザを誘惑するのはテキストだけではありません。電話への攻撃を誘い出すハニーポット（おとり）のデータでは、ハニーポットの5%が少なくとも1日に1回は電話を受けていることが判明しました。もちろん、彼らハニーポットは学生ローンの借り換えや延長保証付きの車を所有する必要がない（彼らはリースを好みます）ことは約90%わかっています。図71からは、こうした電話の内容をうかがい知ることができます。約3分の1は音声がほとんどないか、無音で、まるで通話中の電話番号に対してビッシング（ボイスフィッシング）しているようです[22]。

さらに29%は既知の詐欺で（29%のうち7%は特に企業をターゲットにしたもの）、残りはその他のもの、あるいは単に不明なものです。

セキュリティ業界にとって、モバイル端末が狙われることが大きな驚きではない点は心強いです。OSのサンドボックス化と脆弱性防御への資金投入は、モバイルセキュリティがパーソナルコンピューター（PC[23]）から学んだ多くの苦労した教訓を継承していることを示唆しており、モバイル機器には当初からセキュリティが組み込まれていました。

ソーシャルエンジニアリングのパターンでは、データ漏洩/侵害の82%に人的要因があることを指摘していますが、これはシリコンチップでは軽減できるものではありません。また、クリックされたフィッシングメールの18%がモバイル機器から送信されています。確かに、携帯電話やパソコンでクリックする人が多いかどうかは、携帯電話が報告されているわけではないので、わかりません。しかし、フィッシングの成功例の5分の1がモバイル端末からのものであることから、フィッシング詐欺はセキュリティの対象であることを十分に確認することができます。

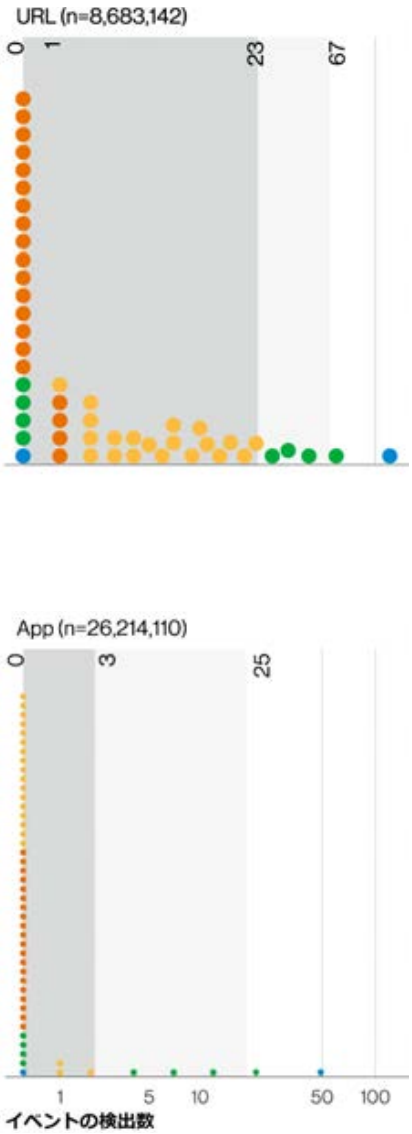


図70. モバイルデバイスで検出されたイベントのタイプ別（対数スケール）

22 まあ、音は鳴らないのですが。まあ.....おわかりですね。

23 そう、ここは「PC」と言い換えました。だって、大人はPCが何であるか知っていますが、最近の子供たちが手にするのは携帯電話やメタバーズですから。気にしなくていいです。

問題の1つは、ユーザのセキュリティ行動を改善させることです。そのアプローチの1つとして、モバイルアプリの形で、親指の届く範囲で重要なセキュリティ情報の知識クイズにアクセスさせるというものがあります。あるセキュリティダッシュボードのアプリでは、利用規約に同意したユーザの66%がダッシュボードを操作していません。操作した人のうちの99%が2回以上操作していますが、図72に示すように、操作時間の中央値は15秒です。それでも、約半数の人が数分後、数時間後、あるいは数か月後に元に戻って来ます。

具体的なセキュリティリスクに関する情報をユーザが利用できるようにすることは、行動を変えさせるための最初のステップです。次に、これらのリスクが自分自身に及ぼす影響をユーザがイメージできるようにすることです。最後に、ユーザに改善させる手段を与える必要があり、これがトレーニングの出番になります[24]。壁にスパゲッティを投げて何が刺さるか見るような感じかもしれませんが、時にはそれが、より良いものを作るために必要なものなのです。

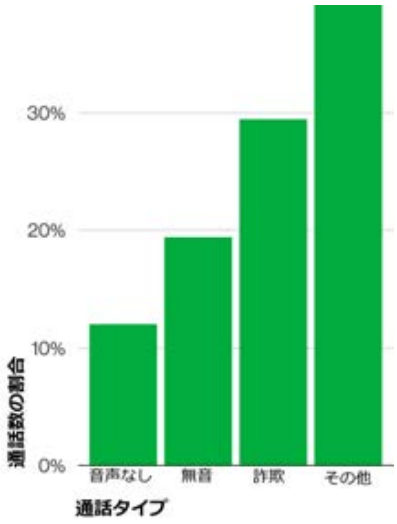


図71. 電話のハニーポットコールのタイプ別（n > 10,000）

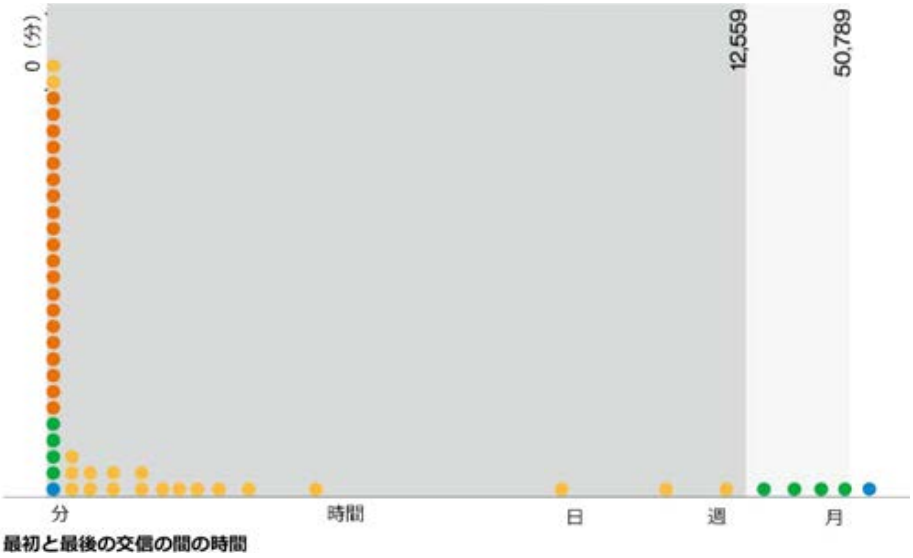


図72. モバイルセキュリティダッシュボードの操作時間（n=22,086、対数スケール）

24 そして、トレーニング方法が気になる方は、付録「行動を変える」をご覧ください。

特権の悪用

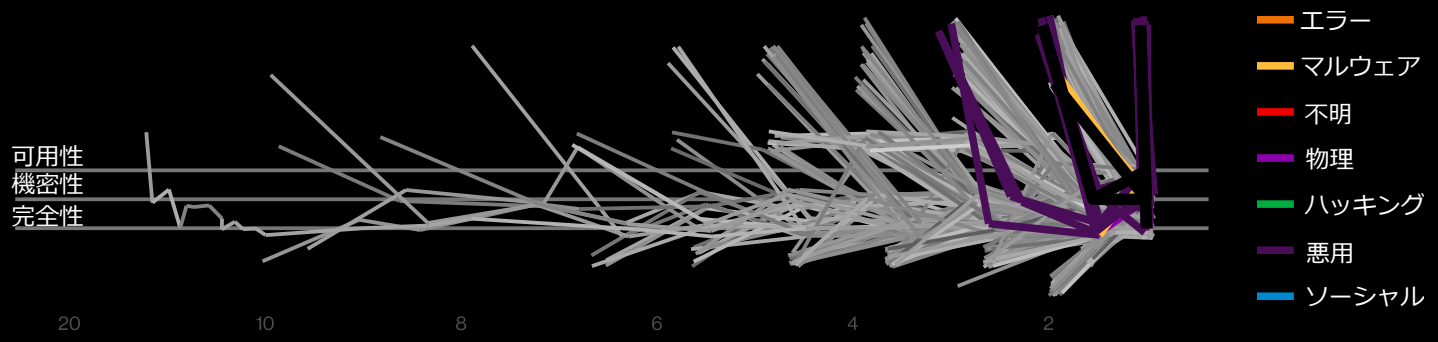


図 73. 特権の悪用インシデントの経路　（n=33）

計画どおりにはいかない

その通りです。採用プロセスを細かいところまで磨き上げ、最も優秀な人材だけを組織に迎え入れるために、十分な準備を整えています。しかし、最善を尽くしても、なぜかうまくいかないことがあります。特権の悪用とは、従業員に与えられる正当なアクセス権を利用してデータを盗むというパターンです。多くの場合、彼らは単独で行動しますが、時にはグループで行動することもあります。いずれにせよ、データ漏洩/侵害が発生したら、その影響に対処しなければなりません。

サマリー

このパターンは、ほぼ完全に内部関係者が悪意を持ってアクセス権を使用し、侵害を引き起こしています。金銭的な動機が依然として最も多いものの、スパイ行為、便宜的な動機、そして単なる恨みも含まれます。個人情報が最も一般的なデータ型であることに変わりはありませんが、医療情報も引き続き狙われています。

昨年との比較

このパターンのインシデントのほとんどは、データ侵害の成功につながります。これらの攻撃者は、依然として強欲（金銭的利益）を動機としており、収益化が容易であるため、個人データを盗んでいるのです。

頻度	275件のインシデント、確認されたデータ暴露216件
攻撃者	内部（100%）、 外部（4%）、 複数の関係者（4%） （漏洩/侵害）
攻撃者の動機	金銭目的（78%）、 怨恨（9%）、 スパイ活動（8%）、 利便性（6%） （漏洩/侵害）
侵害されたデータ	個人情報（70%）、 その他（28%）、 医療情報（22%）、 内部情報（12%） （漏洩/侵害）

そう簡単にはいかない

このパターンで最も多く行われる攻撃は、特権の悪用です。しかし、データの誤操作も、はるかに低い程度とはいえ増えており、通常は「便利さ」という動機と関連して引き起こされます。データの漏洩を防ぐために設計されたセキュリティ管理を回避するために、安全でないことをする場合もあります。セキュリティ管理によっては、従業員にとって業務の遂行がやりにくくなるかもしれませんが、少なくともそのプロセスの背後にある「理由」を理解させるために、教育をこれらの管理と組み合わせることが重要です。いずれにせよ、組織がこの種の事象に何度も見舞われる場合には、安全を確保しながら手間のかからないプロセスを検討すべきと思われます。

このパターンでは、脅威者はすでに日常業務を遂行するためのアクセス権を持っているため、影響を受けるデータのタイプの中には認証情報は見当たりません。その代わりに、（顧客、従業員、パートナーなどの）個人情報が、アクセス権を利用しようとする者にとって最も関心の高いデータとなっています。

医療情報は、このパターンのデータ漏洩/侵害の22%です。このパターンで最も多い業種が医療および社会福祉業であることを考えると、納得がいきます。実際、医療機関では長い間、正当な理由なく内部の関係者がデータにアクセスするという問題が続いていました。現在では医療および社会福祉業のパターンの上位クラスではありませんが、解決済みの問題として片づけるべきではありません。

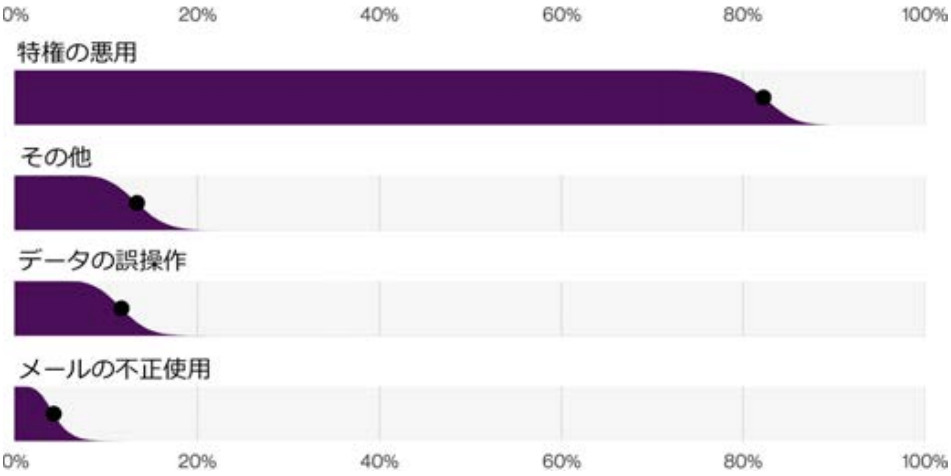
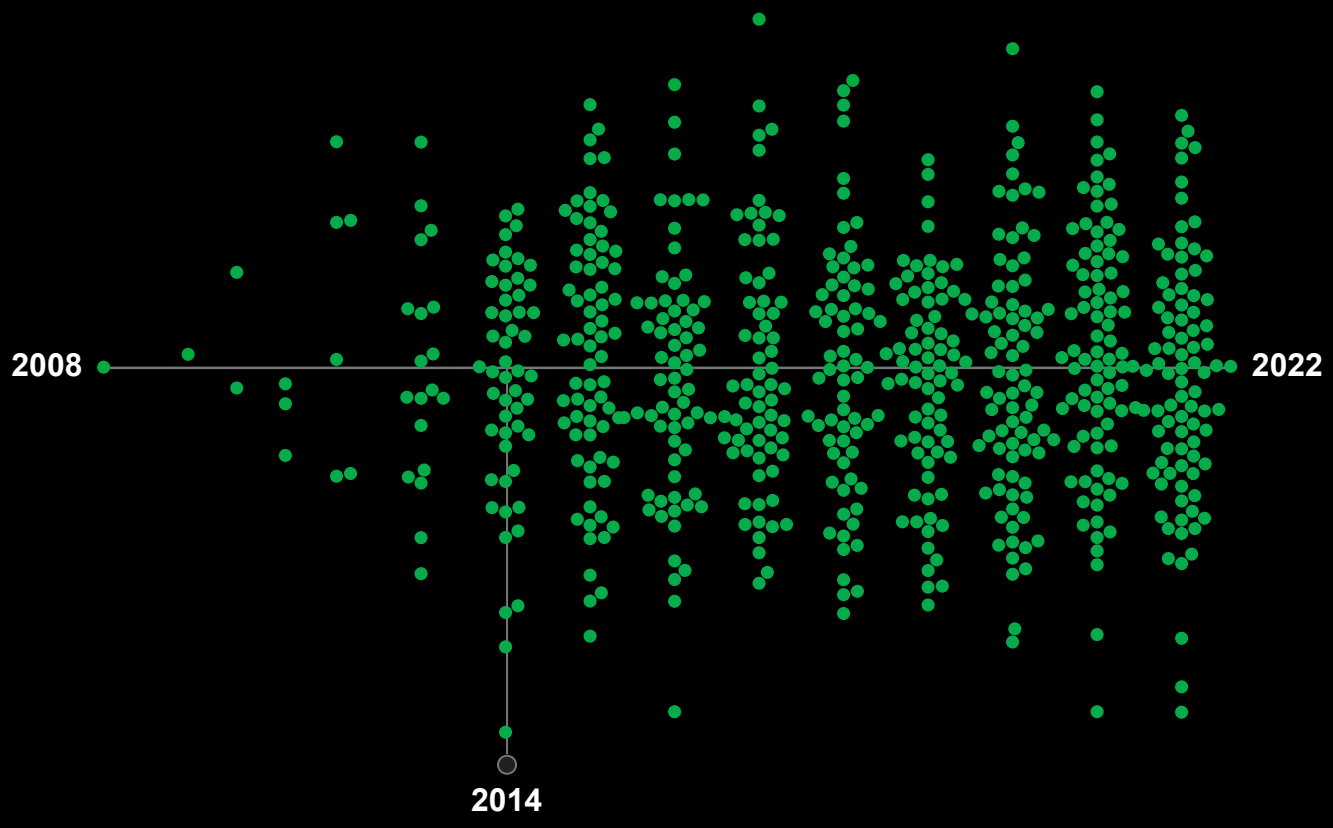


図74. 特権の悪用によるデータ漏洩/侵害の上位の攻撃の種類（n=176）



4 業種別のハイライト

各業種の概要

このセクションは、以前からDBIRをご愛読されている方には重複する内容もあるかもしれませんが、新しい読者の方にはお読みになるだけの価値があります。今年度は23,896件のインシデントを調査し、そのうち5,212件のデータ漏洩/侵害が確認されました。いつものように、これらのインシデントやデータ漏洩/侵害を各業種に分類し、すべての業種が同じような状況ではないことを説明します。少なくとも、攻撃対象や脅威という点では同じではありません。各業種で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、人々（顧客、従業員、その他すべての人々）がどのようにそのデータと関わっているかに大きく関係しています。

ビジネスモデルが完全にモバイル機器に集中しており、顧客が携帯電話のアプリを使用する大企業と、インターネットには接続していないが、POSベンダーにシステムを管理してもらっている小さな個人商店では、リスクが異なります。インフラ（攻撃側から見た攻撃対象）がリスクを大きく左右するのです。

したがって、ある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のみに基づいて、その業種のセキュリティ意識や体制（またはその欠如）について推論しないようご注意ください。これらの数字は、攻撃の被害の報告に関する法律やパートナー情報の公開など、いくつかの要因に大きく影響されます。このため、一部の業種は非常に低い数字となっており、サンプルが少ない場合と同様に、少ない数字から得られる統計の信頼性も低くならざるを得ないことを理解していただく必要があります。

サンプル数が少ない業種の調査では、実際の値が存在する可能性のある範囲を提示しています。これにより、信頼区間を維持しつつ、十分なサンプル数があれば、実際の数値がどの程度になるかをつかむことができます。例えば、「宿泊および飲食業では92%の攻撃が金銭目的の動機によるものであった」とする代わりに、「金銭的動機による攻撃は86%～100%の間であった」と表現することができます。本調査報告書で使用されている統計的信頼性の背景については、「方法論」のセクションをご覧ください。

ご自分の業界のことを知りたくて読まれている方は、各業界のセクションにあるサマリーの表で上位のパターンが何かを確認し、それらのパターンのセクションにも目を通していただくことをお勧めします。また、各業種のセクションでは、セキュリティ対策の戦略を立てたいという方のために、CIS（Center for Internet Security）のCritical Security Controlsの中から優先的に取り組むべきものを提示しています。

	インシデント				データ漏洩/侵害			
業種	合計	中小企業（1～1,000人）	大企業（1,000人以上）	不明	合計	中小企業（1～1,000人）	大企業（1,000人以上）	不明
合計	23,896	2,065	636	21,195	5,212	715	255	4,242
宿泊および飲食業（72）	156	2	1	153	69	1	1	67
官公庁（56）	39	5	7	27	19	3	5	11
農業（11）	243	1	1	241	39	1	0	38
建設業（23）	127	21	7	99	57	8	5	44
教育サービス業（61）	1,241	112	48	1,081	282	57	15	210
芸術、娯楽、およびレクリエーション業（71）	215	12	5	198	96	6	3	87
金融および保険業（52）	2,527	103	50	2,374	690	56	32	602
医療および社会福祉業（62）	849	36	14	799	571	14	10	547
情報産業（51）	2,561	59	25	2,477	378	27	10	341
管理業（55）	8	1	2	5	2	0	0	2
製造業（31-33）	2,337	168	74	2,095	338	54	22	262
鉱業、採石業、石油・ガス採掘業（21）	231	0	0	231	132	0	0	132
その他のサービス（81）	180	16	1	163	101	8	1	92
専門的・科学的・技術的サービス業（54）	3,566	1,095	144	2,327	681	263	52	366
公務（92）	2,792	110	88	2,594	537	74	25	438
不動産業（53）	118	31	5	82	76	19	2	55
小売業（44-45）	629	157	68	404	241	54	35	152
運輸および倉庫業（48-49）	305	26	38	241	137	17	23	97
公益事業（22）	172	20	14	138	47	14	3	30
卸売業（42）	166	79	33	54	68	38	8	22
不明	5,434	11	11	5,412	651	1	3	647
合計	23,896	2,065	636	21,195	5,212	715	255	4,242

表 2. 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

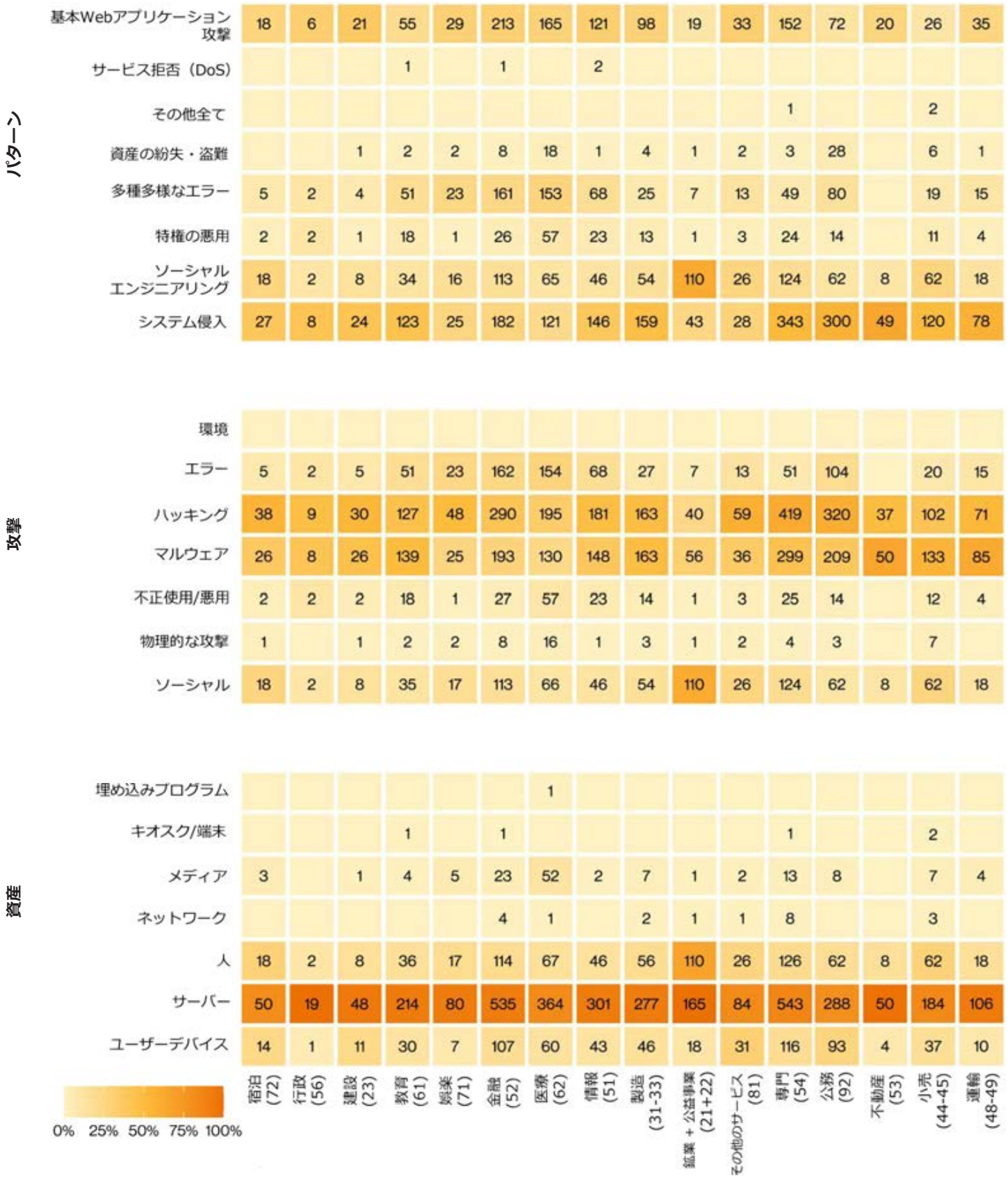


図75. 業種別のデータ漏洩/侵害

インシデント

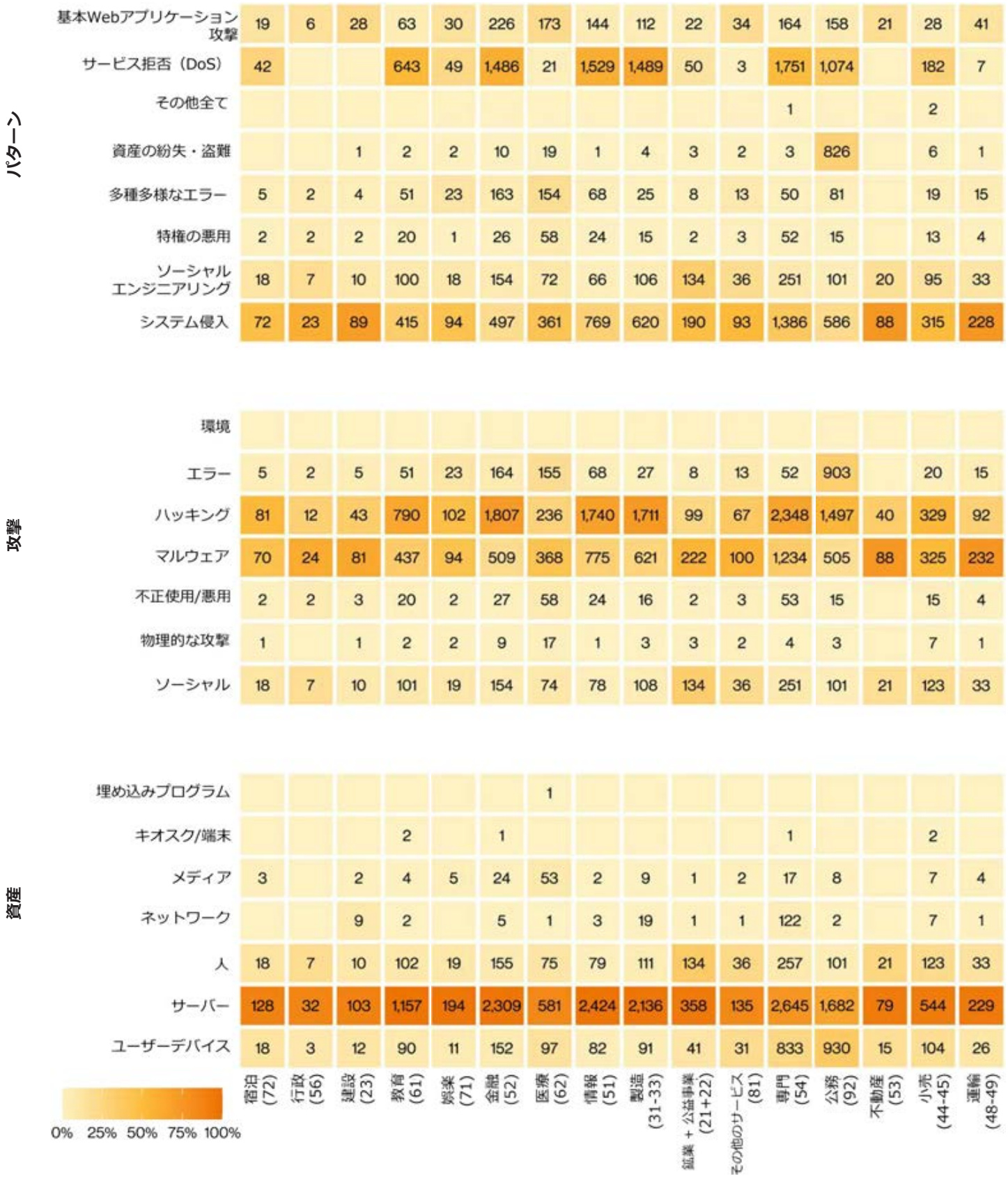


図76. 業種別のインシデント

宿泊および飲食業 NAICS 72

頻度	156件のインシデント、確認されたデータの暴露69件
上位3つのパターン	「システム侵入」、「サービス拒否（DoS）」、「基本Webアプリケーション攻撃」がデータ漏洩/侵害全体の90%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（91%）、スパイ活動（9%）（漏洩/侵害）
侵害されたデータ	認証情報（45%）、個人情報（45%）、決済情報（41%）、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のトレーニングプログラムの実施（CSC 14）、アクセス制御管理（CSC 6）、企業資産およびソフトウェアのセキュアな設定（CSC 4）
昨年との比較	この業界は、依然として決済情報や個人情報を狙う金銭目的を動機とする犯罪者に狙われています。

サマリー

宿泊および飲食業は、2016年以降、「システム侵入」のパターンは減少しているものの、メールで配信された「マルウェア」や、Webアプリケーションに対する「窃取した認証情報の使用」による被害が発生しています。

過去のパターン	5年前との比較	3年前との比較	他の業種との比較
システム侵入	減少	減少	同傾向
ソーシャルエンジニアリング	増加	同傾向	同傾向
基本Webアプリケーション攻撃	増加	増加	同傾向

この業種は、システム侵入の観点では減少した数少ない業種の1つです。しかし、「基本Webアプリケーション攻撃」と「ソーシャルエンジニアリング」に関しては、他の業種と同様の傾向を示しています。これらは過去5年間増加傾向にあり、現在では他の業種が受けている攻撃の種類と同じベースラインに少し近づいています。

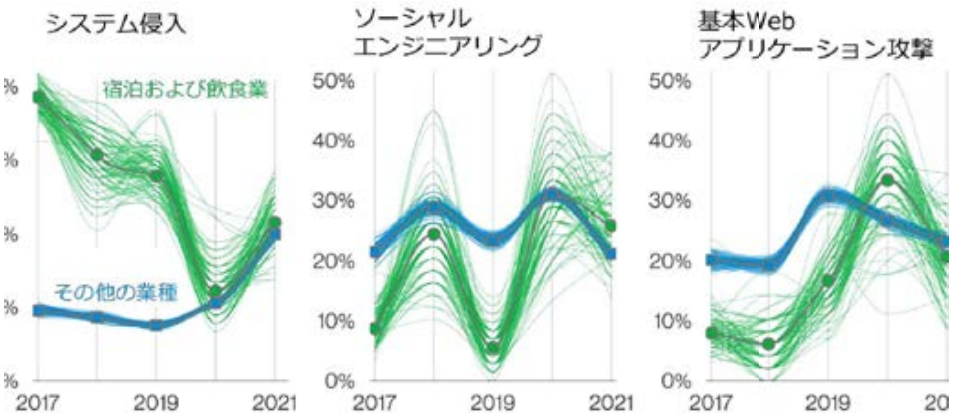


図77. 宿泊および飲食業におけるデータ漏洩/侵害の上位パターンの経時的変化

図78は、この業界で見られる上位の攻撃の種類です。この業界は、ロングテールの長さが非常に長い業種の1つであり、80%以上の侵害には、上位5つに含まれない攻撃も含まれます。この数字は非常に目を引きますが、攻撃経路はメール、Webアプリケーション、デスクトップ共有ソフトウェアなどの他の業種に見られるような普通のものであることに留意してください。

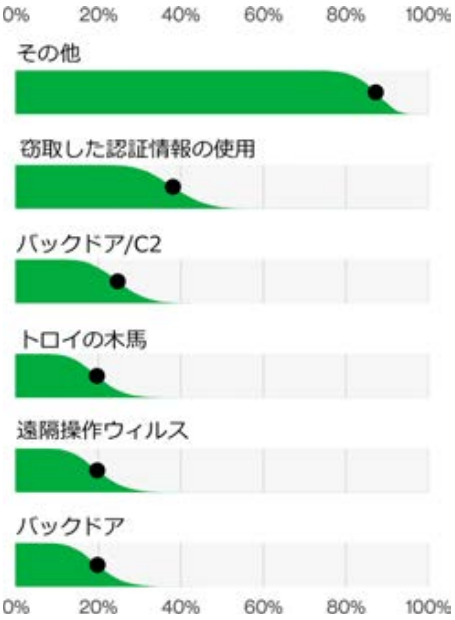


図78. 宿泊・飲食業のデータ漏洩/侵害の上位攻撃の種類（n=58）

過去を振り返る

2012年のDBIRでは、「宿泊・飲食業」はDBIR全体の54%を占めていましたが、その後、2%未満に減少しています。これは、ケースの総数が減少しただけでなく、インシデントが大幅に減少したことを表しており、クレジットカードデータのある組織だけでなく、あらゆる組織をターゲットにして被害を与えるという犯罪エコシステムの大きなシフトを象徴しているのかもしれません。

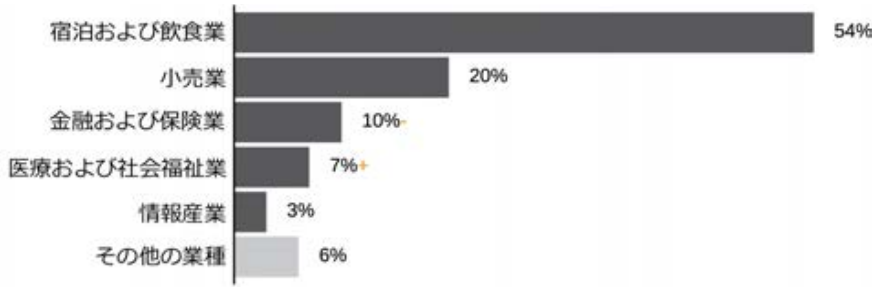


図79. データ漏洩/侵害の割合別の業界グループ（2012年 DBIR 図3）

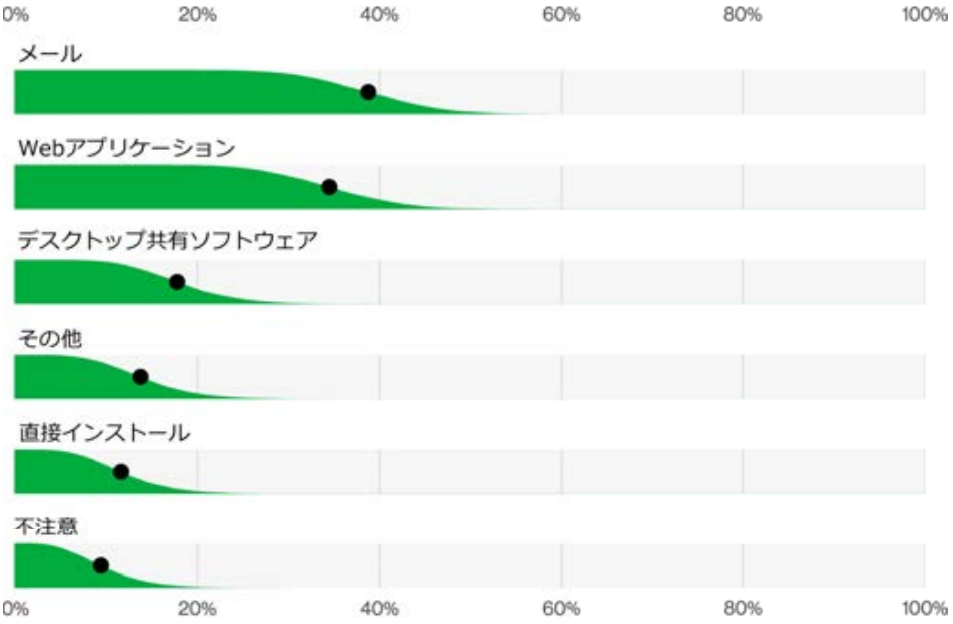


図80. 宿泊および飲食業のデータ漏洩/侵害の上位攻撃の経路（n=47）

芸術、娯楽、レクリエーション業 NAICS 71

頻度	215件のインシデント、確認されたデータの暴露96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」、「多種多様なエラー」がデータ漏洩/侵害の80%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	金銭目的（97%）、怨恨（3%）（漏洩/侵害）
侵害されたデータ	個人情報（66%）、認証情報（49%）、その他（23%）、医療情報（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のトレーニングプログラムの 実施（CSC 14）、企業資産およびソフトウェアのセキュアな設定（CSC 4）、アクセス制御管理（CSC 6）
昨年との比較	上位3つのパターンの顔ぶれに変更はないものの、順位が入れ替 わりました。この業種では、医療データの漏洩/侵害が止まりません。

サマリー

「システム侵入」と「基本Webアプリケーション攻撃」の順位は入れ替わりましたが、「多種多様なエラー」は3位のまま上位3つのパターンに名を連ねています。インシデントについては、「サービス拒否（DoS）」攻撃が、この業種の中でも、特にギャンブル業界において依然として大きな問題になっています。

過去のパターン	5年前との比較	3年前との比較	他の業種との比較
基本Webアプリケーション攻撃	同程度	同程度	同傾向
システム侵入	同程度	同程度	減少傾向
多種多様なエラー	同程度	同程度	増加傾向

この業界は主にライブパフォーマンスを対象としており、ダンス、演劇、スポーツイベントのいずれも共通点は、後で放送するための事前録画をしないことを前提とします。また、ギャンブル産業も含まれます。このNAICSコードに属する無数の組織タイプに、それぞれさまざまな攻撃対象が存在することは想像に難くありません。しかし、これらの組織の多くに共通しているのは、チケット販売や注文（場合によっては賭け事）の受付など、重要な業務を遂行するためにインフラの少なくとも一部をインターネットに依存しているという点です。どのイベントでも、DoS攻撃は招かれざる客として扱われます。しかし、この分野（特にAPAC地域のゲーム会社）では頻繁に発生し、インシデントの20%以上を占めています。

データ漏洩/侵害に関しては、左側の一覧表にある3つのパターンが、サービスの混乱よりもインフラの脆弱性の問題を示しています。攻撃者が侵入すると、本格的に大混乱に陥る可能性があります。これらの攻撃者は、主に金銭目的を動機とする外部の攻撃者ですが、この分野では怨恨を動機とする攻撃も少なからず存在します。

また、あまり複雑でない「基本Webアプリケーション攻撃」が含まれている点が気になるところです。逆に、ランサムウェアが常に好んで使用される「システム侵入」攻撃では、攻撃者はかなり頑張って成果を上げなければなりません。これまで見てきたように、すべての攻撃者は認証情報を好み、それを使って正規の従業員になりすまし、目的のものを手に入れるための時間の間だけ捕捉の手から逃れようとします。

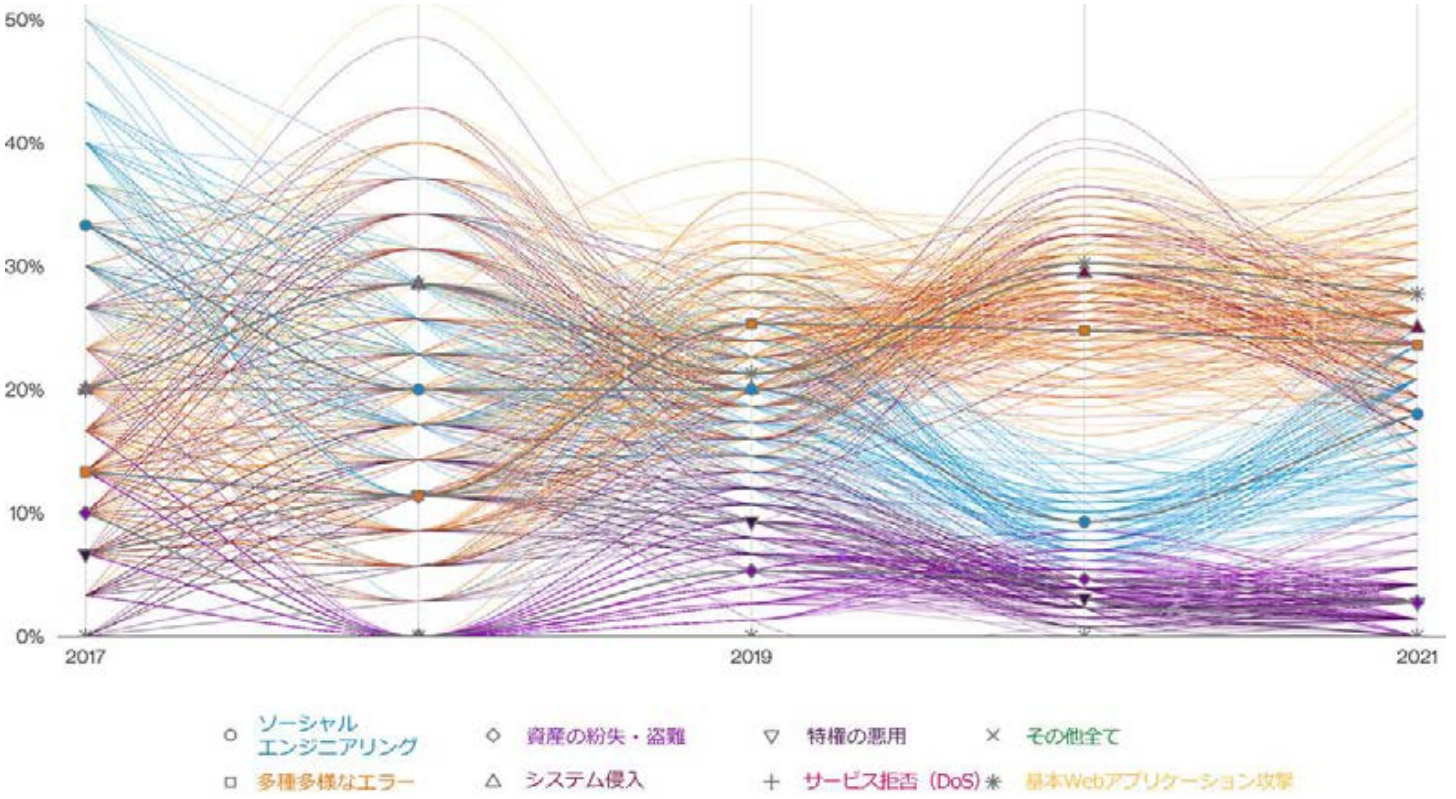


図81. 芸術、娯楽、レクリエーション業のデータ漏洩/侵害パターンの経時的変化

最も多く盗まれているデータは、個人情報（昨年の83%という高い数値からは減少していますが）と認証情報です。奇妙なことに、医療情報も依然として、この分野のデータ漏洩/侵害の15%の割合で掠め取られています（専門用語）。これは昨年（26%）と似たような結果ですが、医療とは無関係のこの分野で医療情報が盗まれるというのは、依然として不可解なことです。この医療情報は、おそらく従業員のために医療保険に加入しているため、その種のデータを保持しなければならない企業から取得したデータであるか、あるいは労働災害補償データ（業務上の負傷）の一形態である可能性があります。また、このNAICSコードにはスポーツチームも含まれているため、医療記録の盗難件数が多くなっている可能性もあります。いずれにせよ、かなり理解の難しい結果です。

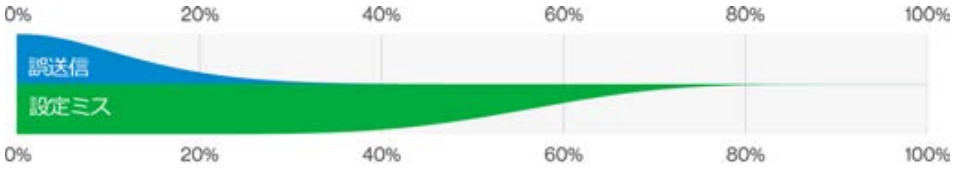


図82. 芸術、娯楽、レクリエーション業のエラーによるデータ漏洩/侵害における誤送信と設定ミス（n=16）。

多種多様なエラーは、今年も上位3つのパターンに上がっています（25%）。設定ミスは最もよく起こりうるもので、データ漏洩/侵害の約15%を占めています。昨年最も多かった誤送信エラーは大幅に減少しているため、この分野では単に1つの問題が別の問題に置き換わっただけのように思われます。

教育サービス業 NAICS 61

頻度	1,241件のインシデント、確認されたデータの暴露282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80%を占めている
攻撃者	外部（75%）、内部（25%）（漏洩/侵害）
攻撃者の動機	金銭目的（95%）、スパイ活動（5%）（漏洩/侵害）
侵害されたデータ	個人情報（63%）、認証情報（41%）、その他（23%）、内部情報（10%）（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トレーニングプログラムの 実施（CSC 14）、アクセス制御管理（CSC 6）、企業資産およ びソフトウェアのセキュアな設定（CSC 4）
昨年との比較	この業界では、依然として外部インフラを標的とした攻撃の影響を受けており、主に金銭の取得を動機とする外部の攻撃者に狙われています。さらに上位のデータ漏洩/侵害の要因の1つである「エラー」にも直面しています。

サマリー

教育サービス業は、他の多くの業種と傾向が奇妙なほど酷似しており、「ランサムウェア」攻撃が著しく増加しています（データ漏洩/侵害の30%以上）。さらに、この業種では、従業員や生徒の個人情報を流出させる可能性のある、「窃取した認証情報の使用」や「フィッシング」攻撃から身を守る必要があります。

過去のパターン	5年前との比較	3年前との比較	他の業種との比較
基本Webアプリケーション攻撃	同程度	増加	減少傾向
システム侵入	増加	増加	減少傾向
多種多様なエラー	同程度	減少	増加傾向

さて、授業が再開されました。NSYNC Trapper Keeperフォルダーをしまって、HBの鉛筆を用意してください。これから、教育サービス業界に影響を与えるデータ漏洩/侵害やインシデントについて学びます。インシデントの主な原因は、「システム侵入」、「ソーシャルエンジニアリング」「DoS」であり、データ漏洩/侵害では「システム侵入」、「基本Webアプリケーション攻撃」、「エラー」が主な原因となっています。また、この業界では、「窃取した認証情報の使用」と「ランサムウェア」が上位2つの攻撃パターンとなっており、これは非常に危険な組み合わせと言えます。噂では、「窃取した認証情報の使用」と「ランサムウェア」は遊ばないので、休み時間で学校を辞めたそうです。

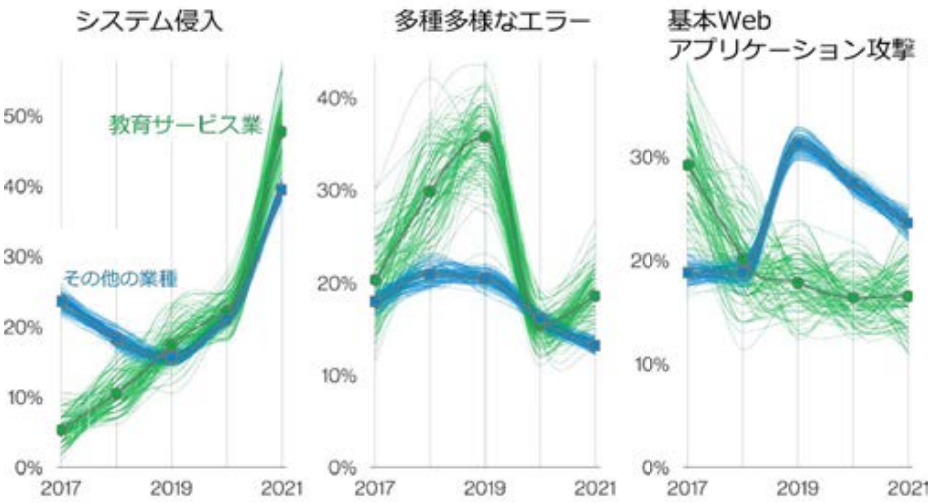


図83. 教育サービス業のデータ漏洩/侵害の上位パターンの経時的変化

計算間違いをしても宿題の点数が少し減点されるだけですが、エンドユーザがエラーを犯すとデータ漏洩につながるかもしれません。この業界で見つかったエラーの34%は、メールの誤送信や添付ファイルの誤りによるものでした。

過去3年間でミスは減ったかもしれませんが、それでも比較的普通の出来事で、特に学校で扱う各種のデータの山を考えると、かわいそうなボビーテーブルのデータを流出させたくありません[25]。

図84. 教育サービス業のデータ漏洩/侵害における上位の攻撃の種類（n=218）

2017年のDBIR

過去を見返しているときに襲ってくる懐かしさほど、素晴らしいものはありません。懐かしい友人たちのサインやメモ、ああ、古き良き時代。2017年のDBIRを再読してみると、この業界の侵害パターンのトップがサイバースパイ活動であったことを知り、同じ感覚に陥ります。しかし、スパイ活動はまだ卒業していませんし、学校を離れていません。今年のインシデントの34%に現れています。図 85 は、データの変化とスパイ活動の劇的な増加を示したものですが、これは現在でも十分に存在するものです。残念ながら、ソーシャルメディア上で偏った意見を持った高校時代の友人とは異なり、あなたのフィードをかき乱さないようにスパイ活動をブロックすることはできません。

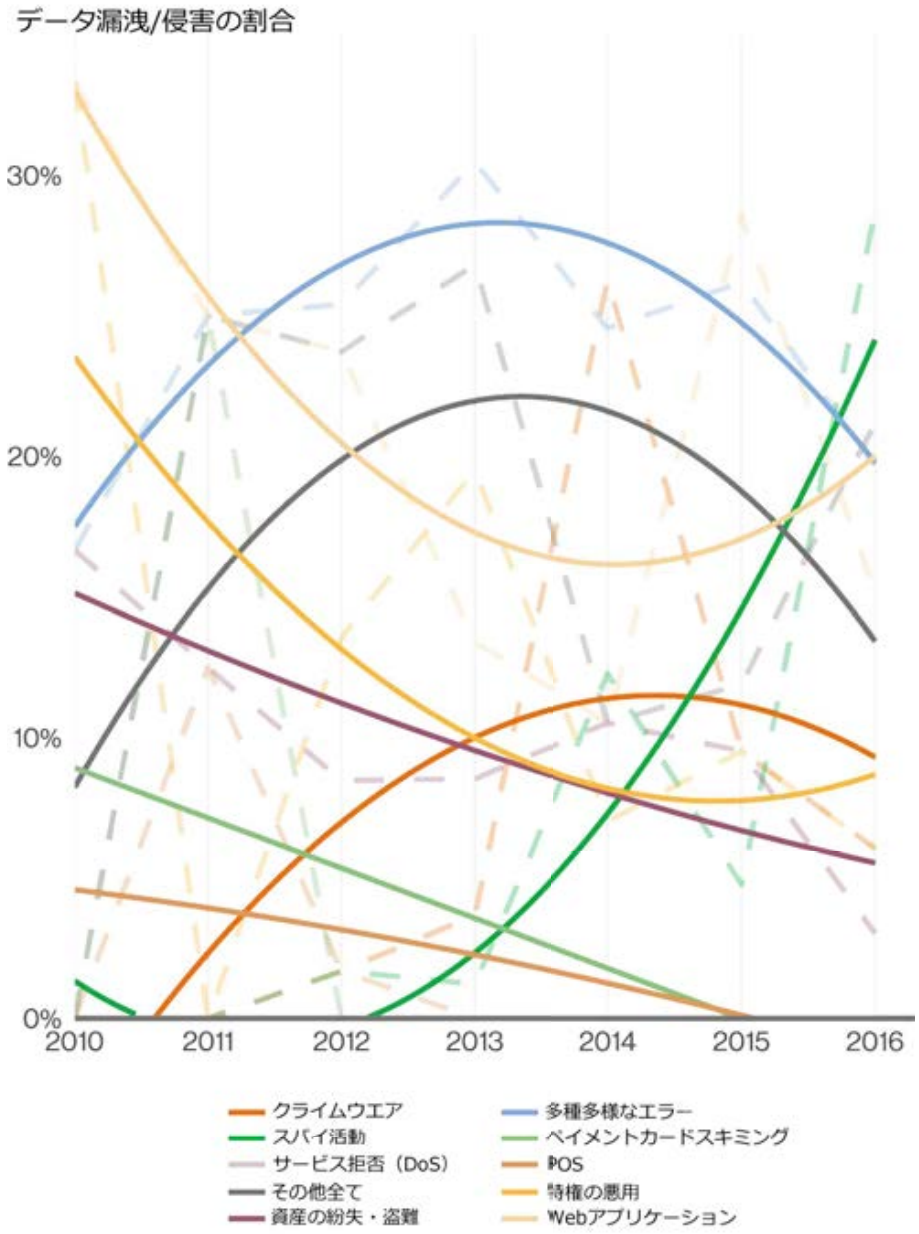


図85. 教育サービス業の侵害分類パターンの割合の経時的変化（2017年 DBIR図17）

25 https://xkcd.com/327、古典的なものです。

金融および保険業 NAICS 52

頻度	2,527件のインシデント、確認されたデータの暴露690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」、「多種多様なエラー」がデータ漏洩/侵害の79%を占めている
攻撃者	外部（73%）、内部（27%）（漏洩/侵害）
攻撃者の動機	金銭目的（95%）、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（71%）、認証情報（40%）、その他（27%）、銀行情報（22%）（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トレーニングプログラム の実施（CSC 14）、アクセス制御管理（CSC 6）、企業資産 およびソフトウェアのセキュアな設定（CSC 4）、データ保護 （CSC 3）
昨年との比較	昨年に引き続き、「基本Webアプリケーション攻撃」と「エラー」が、この業種のデータ漏洩/侵害の大きな部分を占めてい ます。

サマリー

金融および保険業は、「ソーシャル攻撃」（フィッシング）、「ハッキング」（窃取した認証情報の使用）、「マルウェア」（ランサムウェア）などの攻撃を通じて、金銭の取得を動機とする組織犯罪による被害を受け続けています。過去3年連続で非常に多いパターンは、「誤送信」に代表される「多種多様なエラー」です。

過去のパターン	5年前との比較	3年前との比較	他の業種との比較
基本Webアプリケーション攻撃	増加	増加	減少傾向
システム侵入	増加	増加	増加傾向
多種多様なエラー	増加	増加	増加傾向

2016年には金融機関のデータ漏洩/侵害の50%にサーバーが関与していましたが、現在は90%となっています。しかし、「サーバー＋Webアプリケーション」という特定の種類は、同じ期間に12%から51%に増加しており、したがって、「基本Webアプリケーション攻撃」が上位3つのパターンに入ることの裏付けとなっています。これらの攻撃の重要な構成要素は、通常、「窃取した認証情報の使用」であり、これは、この分野の攻撃の種類の第1位です。これらの認証情報は様々な方法で盗取された可能性がありますが、最も疑わしいのは「ブルートフォースハッキング」と「クレデンシャルスタッフィング」です。ひとつ確かなことは、盗まれた認証情報とWebアプリケーションは、ピーナッツバターとチョコレートのように相性がいいということです。

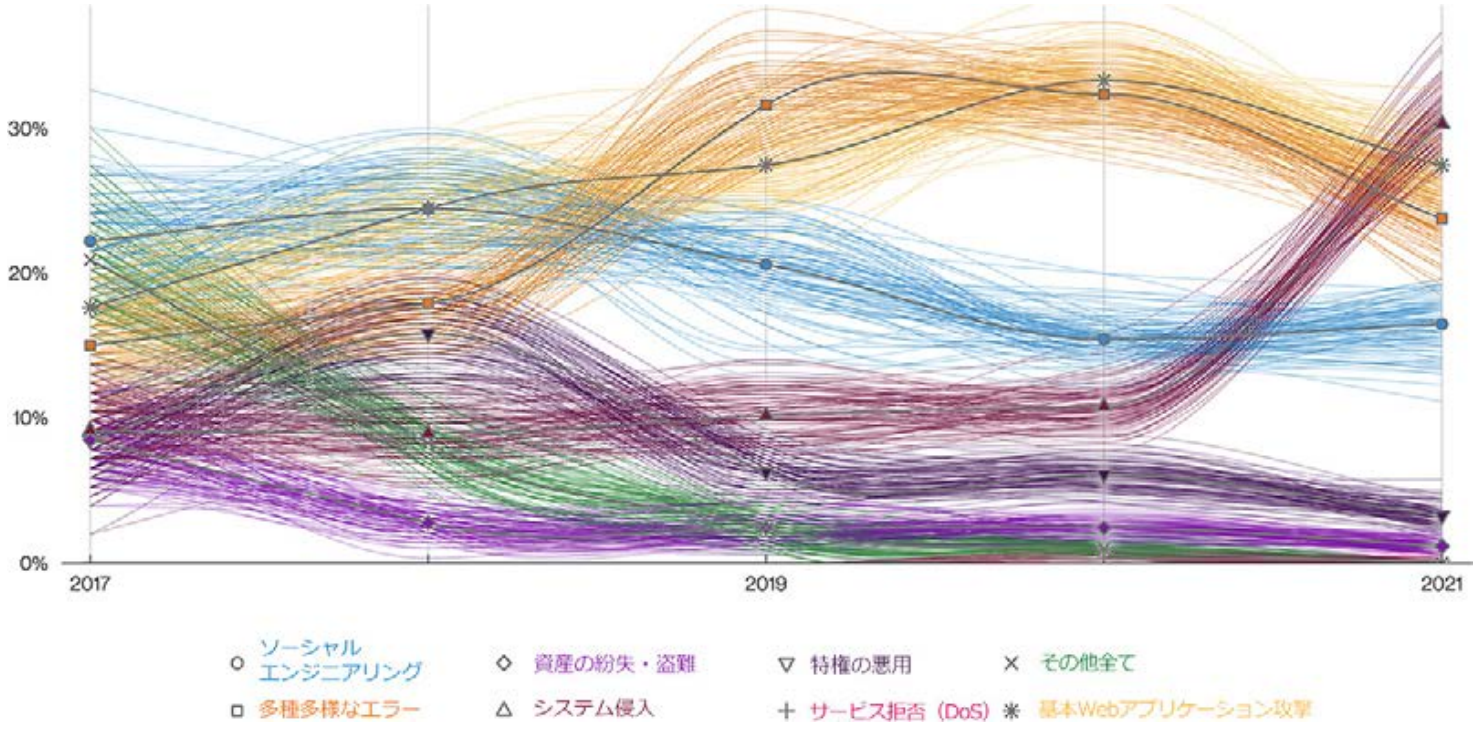


図86. 金融および保険業におけるデータ漏洩/侵害パターンの経時的変化

「そちらが見せてくれたら、こちらも見せましょう。」

誤送信（16%）は、この分野で2番目に多い攻撃の種類です。誤送信とは、その名の通り、個人情報やその他の機密情報を誤った相手に送ることです。公共機関や医療機関では、その性質上、大量のメールを送信するため、このような行為がより多く見られると予想されるかもしれません。しかし、DBIRのデータによると、金融および保険業では他の業種に比べて約3倍も誤送信が多いことが分かっています。私たちDBIRチームはこの発見にショックを受けました。なぜなら、もし権限のない人に自分の小切手が見られ、毎年この報告書を執筆することで何百万も稼いでいることを知ったら、とても恥ずかしいことじゃありませんか[26]。

「年月を経て...」

システム侵入は2016年の14%から今年は30%と倍増しています。組織犯罪は、2018年の侵害の49%に対し、本レポートでは79%でした。可用性は、2016年当時は侵害のわずか6%であったのに対し、現在は14%であり、攻撃の発見手段としては「攻撃者による開示」が、今年のレポートでは58%ですが、2016年は5%でした。これが主にランサムウェアの攻撃によるものであることはほとんど言うまでもありませんが、念のため、とりあえずのように言っておきましょう。

これは主にランサムウェアの攻撃によるものです。ランサムウェアが高収益、低リスクの攻撃であり続ける限り、犯罪者はランサムウェアを利用し続けるでしょう。

DoS攻撃は引き続き大きな問題であり、この分野のセキュリティインシデントの58%を占めていることに触れないのは不注意と言わざるを得ません。これは、他の業種に比べ約2倍もの割合です。

26 たらればの話

医療および社会福祉業 NAICS 62

頻度	849件のインシデント、確認されたデータの暴露571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/侵害の76%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（95%）、スパイ活動（4%）、利便性（1%）、怨恨（1%）（漏洩/侵害）
侵害されたデータ	個人情報（58%）、医療情報（46%）、認証情報（29%）、その他（29%）（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トレーニングプログラムの 実施（CSC 14）、企業資産およびソフトウェアのセキュアな設 定（CSC 4）、アクセス制御管理（CSC 6）
昨年との比較	上位3つのパターンは変わらずに、順位が入れ替わっています。 攻撃者の顔ぶれも昨年と全く同じでした（それぞれの占める割合まで）。

サマリー

この業種では、「基本Webアプリケーション攻撃」が「多種多様なエラー」を抜いてデータ漏洩/侵害を引き起こすようになりました。エラーは依然として重要な問題です。

過去のパターン	5年前との比較	3年前との比較	他の業種との比較
基本Webアプリケーション攻撃	増加	増加	増加傾向
システム侵入	増加	増加	減少傾向
多種多様なエラー	減少	減少	増加傾向

インサイダー？インサイダーとは？

医療および社会福祉業は、私たちがデータの収集と報告を始めて以来、内部関係者による情報漏洩が目立っている業種です。内部犯行の構成は、悪意のある不正使用から、より穏やかな（しかし報告されにくい）その他のエラーへと変化しましたが、内部犯行の脅威を語る上で、この業種は常に信頼できる存在です。「基本Webアプリケーション攻撃」のパターンが増加しており、もはや内部関係者の影響力はなくなってきています。インサイダーの上に移動した大きな犬がここにいるのです。

しかし、従業員は、悪意を持ってアクセス権を悪用するよりも、2.5倍以上も高い確率でミスを犯すのです。誤送信と紛失が最も一般的なエラーです（この2つは非常に接近しており、勝者を決定するには写真撮影が必要なほどです）。

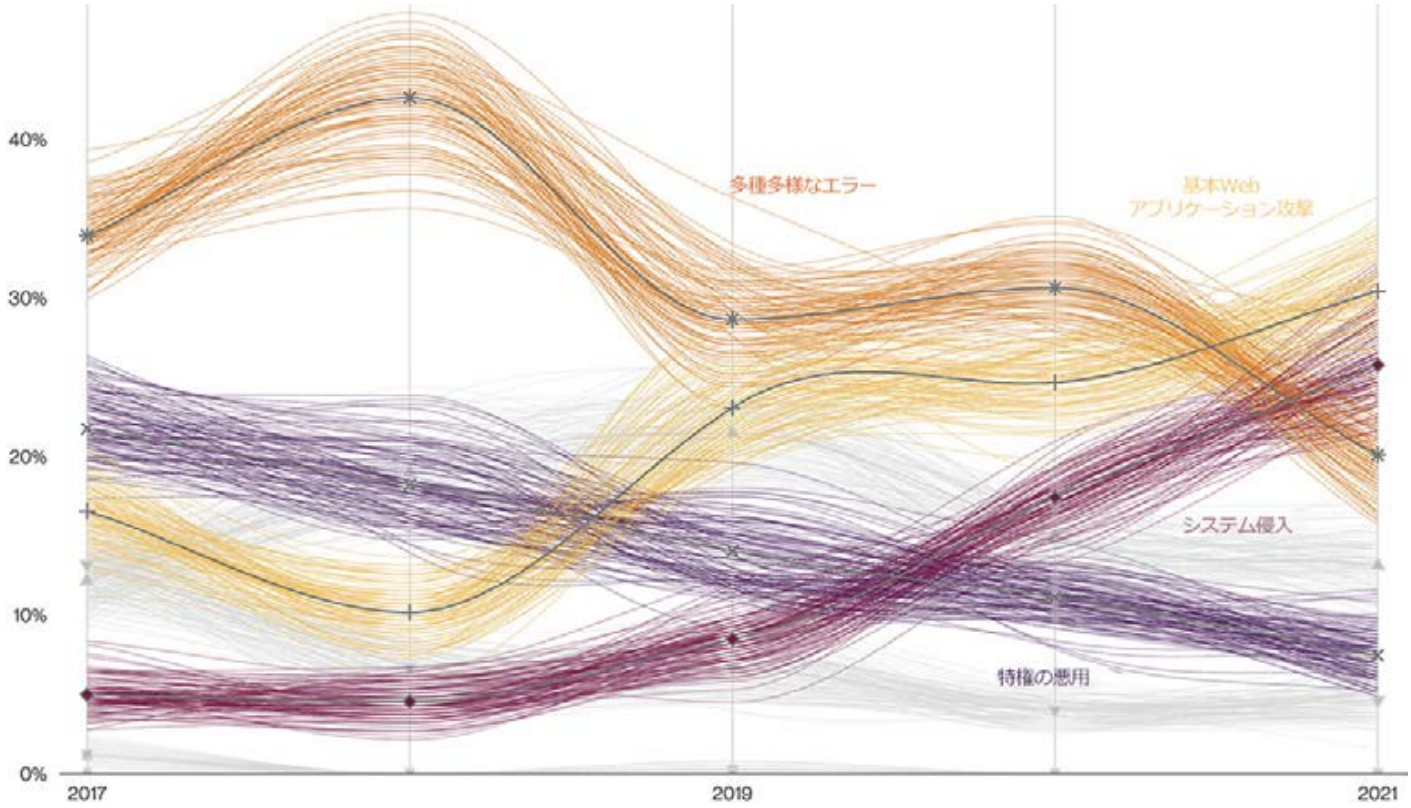


図87. 医療および社会福祉業におけるデータ漏洩/侵害パターンの経時的変化

図87は、医療および社会福祉業のデータ漏洩/侵害パターンの経時的変化を示しています。2015年当時は「特権の悪用」がトップで、「多種多様なエラー」がそれに続いているパターンでした。「基本Webアプリケーション攻撃」の台頭が見られるようになったのは2019年になってからで、この業種だけでなく、明らかにすべての人にとって深刻な問題になっています。この業種は、ありふれたハッキング攻撃や、よりインパクトのあるランサムウェアキャンペーンの標的となることが増えています（どちらも第3位の「システム侵入」パターンからの攻撃）。ランサムウェアの増加に伴い、「攻撃者による開示」という発見手段も増えています。暗号化された後に身代金のメモが表示され、顧客サービス重視の脅威グループにとって便利な支払い方法を指示された日は、最悪と言わざるをえません。（本当に、誰も「お得意様」が簡単に支払えるようにしたくないなんて思いませんよね）。

2年連続で、医療情報よりも個人情報の漏洩が多くなっています。医療情報を大量に保有する業種にとって、これはもはや当たり前のことなのでしょうか。これは、アクセスされないようにしている記録の種類に関係なく、攻撃者がただ侵入して暗号化ゲームをしているためでしょうか？医療データの管理は強化しても、個人情報は控室に置いたままなのか、それは業界関係者のみが知るところです。

情報産業 NAICS 51

頻度	2,561件のインシデント、確認されたデータの暴露378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81%を占めている
攻撃者	外部（76%）、内部（24%）（漏洩/侵害）
攻撃者の動機	金銭目的（78%）、スパイ活動（20%）、イデオロギー（1%）、怨恨（1%）（漏洩/侵害）
侵害されたデータ	個人情報（66%）、その他（35%）、認証情報（27%）、内部情報（17%）（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トレーニングプログラムの 実施（CSC 14）、企業資産およびソフトウェアのセキュアな設 定（CSC 4）、アクセス制御管理（CSC 6）
昨年との比較	驚くことに、過去5年間、ソーシャルのデータ漏洩/侵害はほぼ同じ水準で推移しています。これは、ソーシャルのデータ漏洩/侵害が顧客をターゲットにしているため、ハッキングによるデータ漏洩/侵害が発生し（これもほぼ横ばい）、窃取した認証情報の使用により企業に損害を与えているためと思われます。

サマリー

今年度のデータ漏洩/侵害では、「エラー」と「基本Webアプリケーション攻撃」を抜いて「システム侵入」が首位に立ちました。一方、インシデントでは「サービス拒否（DoS）」が首位を維持しています。「マルウェア」は過去2年間で顕著な増加を示し、「エラー」は5年前の増加から減少傾向にあるようです。

過去のパターン	5年前との比較	3年前との比較	他の業種との比較
基本Webアプリケーション攻撃	同程度	同程度	増加傾向
多種多様なエラー	増加	減少	増加傾向
システム侵入	増加	増加	増加傾向

昨年は、まるで人事考課を行う上司のように、情報産業におけるエラーに焦点を当てました。しかし、図88に示すように、中間の評価見直しで明らかに進展がありました。エラーの数は、5年前の2017年の上昇期から減少してきました。

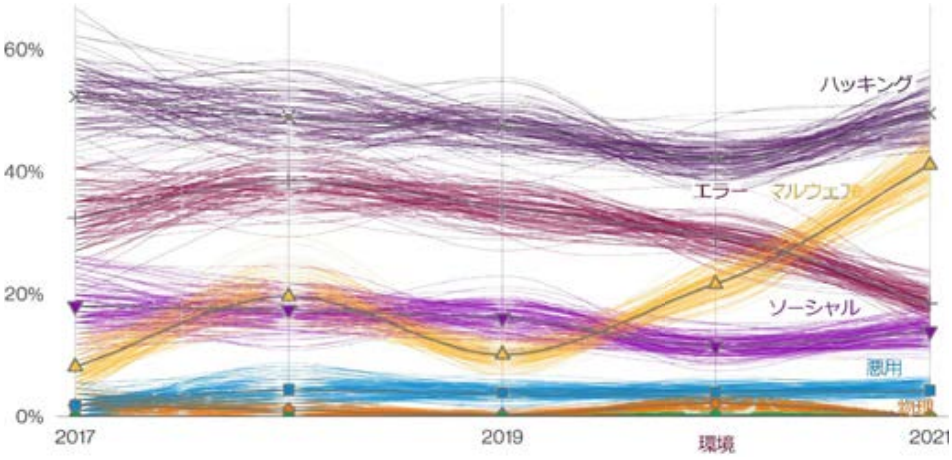


図88. 情報産業におけるデータ漏洩/侵害の攻撃の経時的変化

しかしバランスを維持するためか、過去2年間でマルウェアが顕著に増加しています。その様子を図89に示しました。「システム侵入」は、トップに躍り出て、「基本Webアプリケーション攻撃」をも上回っています。

「システム侵入」が1位になったことの興味深い点は、情報産業には様々な種類の攻撃が存在することです。「窃取した認証情報の使用」が最も多いですが、その後に続いて、「ランサムウェア」、「設定ミス」、「バックドアまたはC2」、「データの抜き出し」などがデータ漏洩/侵害の4%以上に含まれており、様々な攻撃が存在しています。実際、17種類の攻撃が4%を超えているという種類の多さにおいて、情報産業が業種2位タイとなっています。

図90に示したインシデントの上位では、「DDoS攻撃」と「システム侵入」（これはランサムウェアに牽引されている）の2つが大きな割合を占めています。DDoSは、比較的容易に軽減することができますが、なくなったわけではありません。

図91は、忘れられがちなボットネットについての調査結果です。ボットネットでは、情報産業が2年連続でトップになっています。ボットネットによる侵害は被害に遭った組織ではしばしば隠蔽されますが、組織が悪意のあるログインしか監視せず、ボットも認証情報を盗んだということを確認しないためです

図89. 情報産業のデータ漏洩/侵害のパターン（n=378）

図90. 情報産業のインシデントにおける上位のパターン（n=2,561）

図91. 業種別Evil Corpボットネットのデータ漏洩/侵害件数（n=7,072）

製造業 NAICS 31-33

頻度	2,337件のインシデント、確認されたデータの暴露338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」、「ソーシャルエンジニアリング」がデータ漏洩/侵害の88%を占 めている
攻撃者	外部（88%）、 内部（12%）、 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（11%）、 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（58%）、 認証情報（40%）、 その他（36%）、 内部情報（14%） （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トレーニングプログラムの 実施（CSC 14）、アクセス制御管理（CSC 6）、企業資産およ びソフトウェアのセキュアな設定（CSC 4）
昨年との比較	「システム侵入」と「基本Webアプリケーション攻撃」は、この業種が直面する主要パターンの1つであることに変わりはありません。

サマリー

製造業は、引き続き「スパイ活動」の格好の標的となっていますが、「サービス拒否（DoS）」攻撃、認証情報に対する攻撃、「ランサムウェア」など、他の犯罪者の標的になるケースも増えています。

過去のパターン	5年前との比較	3年前との比較	他の業種との比較
基本Webアプリケーション攻撃	増加	増加	増加傾向
ソーシャルエンジニアリング	減少	減少	減少傾向
システム侵入	増加	増加	増加傾向

製造業は、私たちの現代生活を支える重要な部品を製造する機械が大量に存在するため、（主に前のセクションで取り上げた最近の無差別サプライチェーン攻撃によって）引き続きスパイ活動の標的として重宝されています。しかし、製造業は、手っ取り早く儲けようとする金銭的動機のある犯罪者にも狙われています。

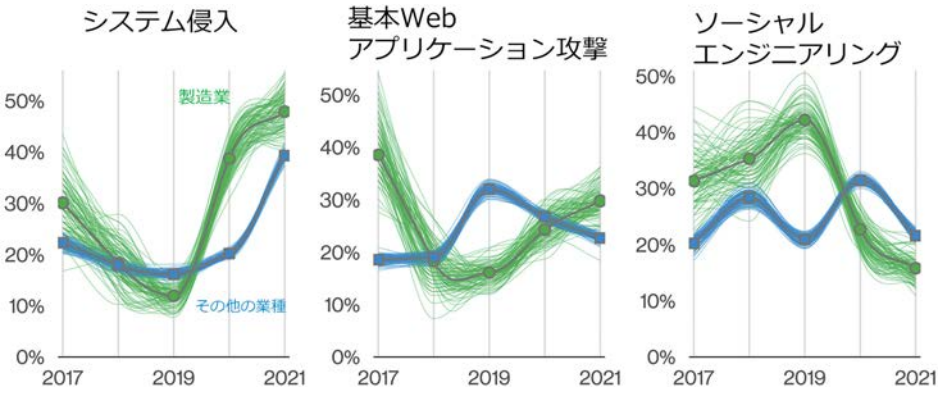


図92. 製造業のデータ漏洩/侵害の上位パターンの経時的変化

過去の報告書では、製造業は金になりそうな回路図や機密情報のために主にターゲットにされていました。例えば、2016年には、この業種におけるインシデントの55%以上がスパイ活動に関係していましたが（図93）、ここ数年は下がってきています。あるいは逆に、スパイがバレない程度にレベルアップしているのかもしれません。

マシンに対するDoS攻撃

可用性＝生産性であるこの業界において、DoS攻撃がここ数年、ヨーヨーのように上下を繰り返すパターンに推移しているのは興味深いことです。DoS攻撃は、2018年のDBIRで最初のピーク（インシデントの40%以上）に達しましたが、2019年以降再び増加しており、現在はインシデントの約70%を占め、他の業種とほぼ同じになってきています。このようにDoSの台頭は、実際に製造プロセスを動かしている重要な資産を妨げる可能性は低いものの、OTとITとの統合が進む中で、留意しておく必要があると考えられます。

この部門に影響を与えるデータ漏洩/侵害については、図95に示すように、窃取した認証情報の使用（39%）、ランサムウェア（24%）、フィッシング（11%）など、お決まりのものが見受けられます。このようなタイプの侵害は、業種に関係なくすべての人に影響を与えているようです。前ページの一覧表に記載したような保護対策を導入することは、この業界の優先事項であるべきです。さもなければ、アニメの女の子をアバターにしているある人物のせいで、あなたの組織が予期せぬ事態に陥ってしまうかもしれないのです。

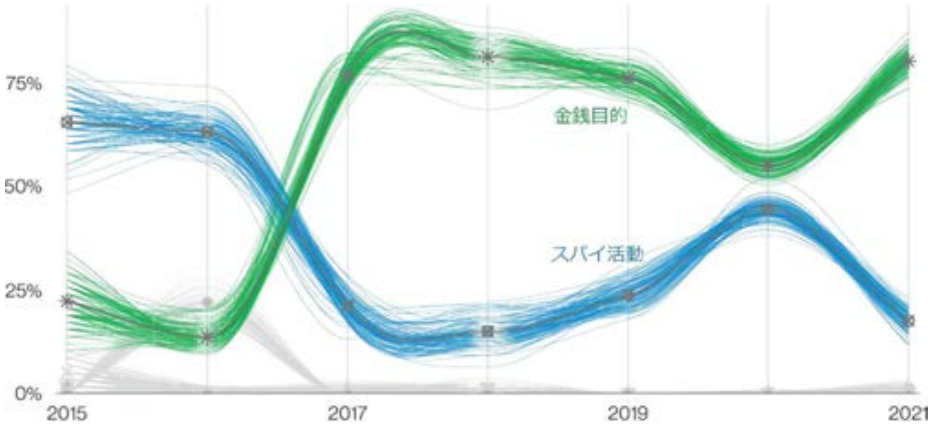


図93. 製造業のインシデントにおける攻撃者の動機の経時的変化

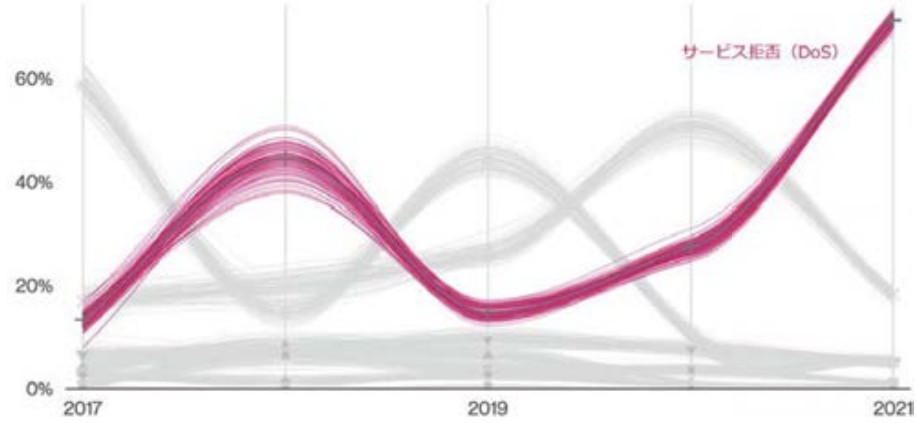


図94. 製造業のインシデントにおけるパターンの経時的変化

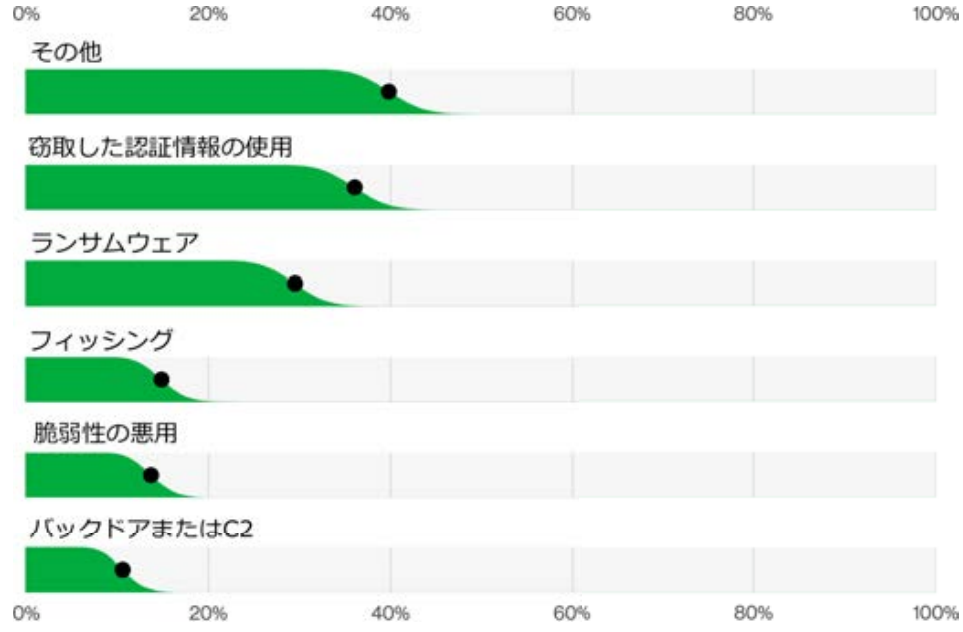


図95. 製造業におけるデータ漏洩/侵害の上位の攻撃の種類（n=259）

鉱業、採石業、石油・ガス採掘業および公益事業 NAICS 21+22

頻度	403件のインシデント、確認されたデータの暴露179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/侵害の95%を占めている
攻撃者	外部（96%）、内部（4%）（漏洩/侵害）
攻撃者の動機	金銭目的（78%）、スパイ活動（22%）（漏洩/侵害）
侵害されたデータ	認証情報（73%）、個人情報（22%）、内部情報（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のトレーニングプログラムの 実施（CSC 14）、アクセス制御管理（CSC 6）、アカウント管理（CSC 5）
昨年との比較	金銭の取得を動機とする攻撃者から引き続き狙われている一方で、スパイ活動に関わる攻撃にも悩まされています。

サマリー

鉱業、採石業、石油・ガス採掘業および公益事業は、認証情報を狙う攻撃や「ランサムウェア」でのデータ利用など、今回調査した他の業種と同様の攻撃タイプに直面しています。しかし、「フィッシング」のような「ソーシャルエンジニアリング」攻撃も高い割合で発生しています。

過去のパターン	5年前との比較	3年前との比較	他の業種との比較
基本Webアプリケーション攻撃	同程度	同程度	減少傾向
ソーシャルエンジニアリング	同程度	同程度	同傾向
システム侵入	同程度	同程度	減少傾向

鉱業、採石業、 石油・ガス採掘業および公益事業（「MQOGEU」とも呼ばれる）の名前は、長くて舌を噛みそうです。興味深いのは、「複合」産業はエンジニアの数が多いということです。この業界は、「エンジニア」のもう1つの形態である「ソーシャルエンジニア」からの攻撃を受けているように見えるので、これはおそらくぴったりと言えます。この業種は、ソーシャルエンジニアリングによる侵害の割合が同業他社よりも高くなっています。

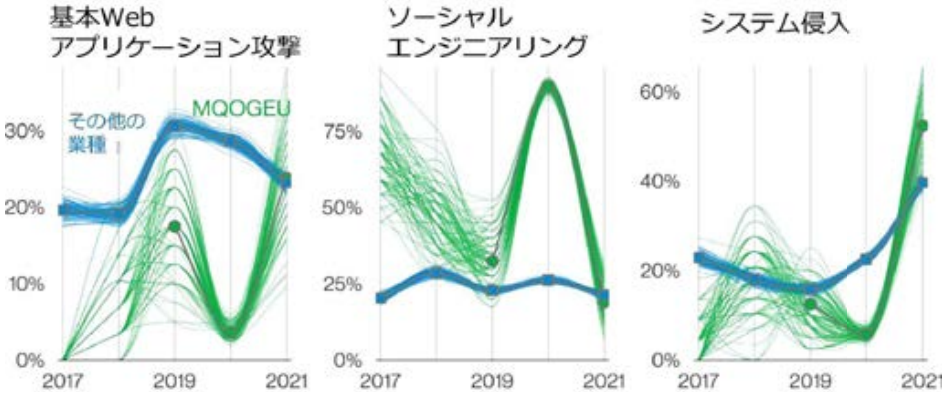


図96. MQOGEUのデータ漏洩/侵害における上位パターンの経時的変化

このことは、データ漏洩/侵害全体の60%以上が「フィッシング」であり（図97）、次いで「窃取した認証情報の使用」（フィッシングで盗取された可能性がある）、「ランサムウェア」（フィッシングと関連する可能性がある）となっていることからもわかります。この業種が私たちの日常生活にとって重要であることを考えると、電力会社や鉱業会社の事業のセキュリティを保護するものがこれらの認証情報だけでないことを強く望みます。なぜなら、このタイプのデータが最もよく侵害されるデータの1つであるからです。

フィッシングや認証情報攻撃の高い普及率を考えると、この業種で最もよく侵害される資産がメールサーバーであり、次いでWebアプリケーションとデスクトップであることは、それほど驚くことではありません。これらの複雑なシステムを実行するインフラは、従来のITインフラではないにもかかわらず、企業は他の組織とまったく同じ脅威にさらされる可能性があります。

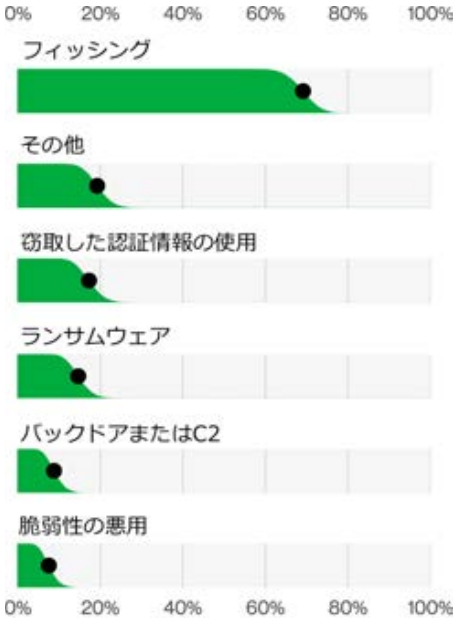


図97. MQOGEUのデータ漏洩/侵害における上位の攻撃の種類（n=153）。

図98. MQOGEUのデータ漏洩/侵害における上位の資産の種類（n=130）。

専門的・科学的・技術的サービス業 NAICS 54

頻度	3,566件のインシデント、確認されたデータの暴露681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」、「ソーシャルエンジニアリング」がデータ漏洩/侵害の89%を占 めている
攻撃者	外部（84%）、 内部（17%）、 複数の関係者（1%） （漏洩/侵害）
攻撃者の動機	金銭目的（90%）、 パイ活動（10%） （漏洩/侵害）
侵害されたデータ	認証情報（56%）、 個人情報（48%）、 その他（26%）、 内部情報（14%） （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トレーニングプログラムの 実施（CSC 14）、アクセス制御管理（CSC 6）、企業資産およ びソフトウェアのセキュアな設定（CSC 4）
昨年との比較	「システム侵入」、「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」の上位3つのパターンは変わり ませんが、昨年の報告書との比較では順位が変わっています。

サマリー

この業種では、「サービス拒否（DoS）」攻撃が深刻な問題となっており、データの漏洩や侵害につながることはほとんどありませんが、それでも大きな影響を被る可能性があります。今年も第1位は「システム侵入」の攻撃パターンです。「ソーシャルエンジニアリング」も突出はしていませんが、上位3つにランキングされています

過去のパターン	5年前との比較	3年前との比較	他の業種との比較
基本Webアプリケーション攻撃	同程度	同程度	同傾向
ソーシャルエンジニアリング	減少	減少	同傾向
システム侵入	増加	増加	同傾向

サービス拒否

NAICSコードに「専門的・科学的・技術的サービス業」とあるように、この業種は、高度な技術を顧客に提供するために、インターネット上でのプレゼンスに依存しています。すなわち、DoS攻撃、特に大量の分散型攻撃を受けた場合、間違いなくその影響を受けることになります。この1年間は、この業種にとって厳しい1年であり、記録されたインシデントのほぼ半分をDoS攻撃が占めています。この種の攻撃は、報告すべきデータ漏洩につながることはほとんどないとはいえ、被害者に大きな損害を与える可能性があります。

身近にいる悪魔

データ漏洩/侵害に目を向けると、「システム侵入」パターンが依然としてピラミッドの頂点にあり、「基本Webアプリケーション攻撃」と「ソーシャルエンジニアリング」がその座を明け渡しています。つまり、同じプレーヤーがフィールド上にいて、ポジションを変えてプレーしているに過ぎないのです。

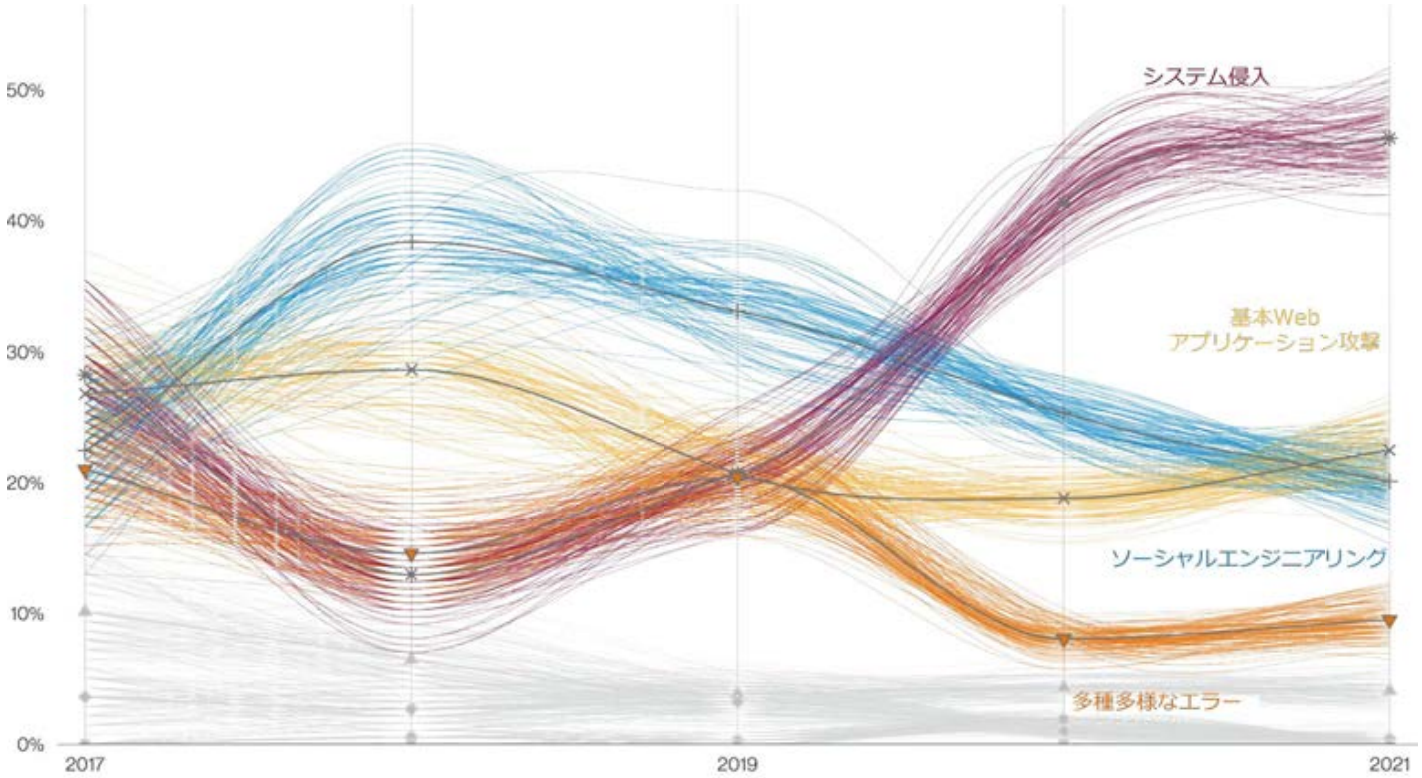


図99. 専門的・科学的・ 技術的サービス業のデータ漏洩/侵害パターンの経時的変化

これら上位3つの攻撃パターンの加害者は、「外部」にいることが多いようです。「内部」の攻撃者によるデータ漏洩/侵害は、今年は昨年よりも減少しています。意外なことに、この分野では今年、複数人による侵害がわずかに増加しました。これは、外部の攻撃者が内部やパートナーの攻撃者をリクルートし、侵害行為に協力させるものです。このような共犯行為には報酬が支払われることもあれば、知人や重要なパートナーがデータへのアクセス権を持つ人物に圧力をかけて、より微妙な形で影響を与えることもあります。いずれにせよ、内部の人間が通常の業務を装ってアクセスするために、結果的に情報漏洩を発見することが難しくなるのです。

過ぎ去りし日々

この部門の過去のデータでは、「多種多様なエラー」が上位3つのパターンに入っていました。しかし、図99が示すように、2019年になると「システム侵入」パターンが急浮上し始め、最終的に「多種多様なエラー」を大きく上回るようになりました。上位の攻撃パターンに関して、この部門には全体のデータセットが反映されています。この上位3つは、全体のデータセットでも上位3つのパターンであり、これらのパターンが多くのビジネスカテゴリーで有力であることは明らかです。

公務 NAICS 92

頻度	2,792件、確認されたデータの暴露537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/侵害の81%を占めている
攻撃者	外部（78%）、内部（22%）（漏洩/侵害）
攻撃者の動機	金銭目的（80%）、スパイ活動（18%）、イデオロギー（1%）、怨恨（1%）（漏洩/侵害）
侵害されたデータ	個人情報（46%）、認証情報（34%）、その他（28%）、内部情報（28%）（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トレーニングプログラムの実施（CSC 14）、アクセス制御管理（CSC6）、アカウント管理（CSC5）
昨年との比較	上位3つのパターンでは、「多種多様なエラー」が昨年と同じ位置を維持しています。

サマリー

この分野では、「システム侵入」パターンが首位に上がってきました。依然として従業員が侵害の原因となっていますが、データ漏洩/侵害を引き起こす可能性は、内部関係者の悪意ある行為よりも操作ミスの方が7倍も高い状況です。

過去のパターン	5年前との比較	3年前との比較	他の業種との比較
基本Webアプリケーション攻撃	同程度	増加	減少傾向
多種多様なエラー	同程度	減少	減少傾向
システム侵入	増加	増加	増加傾向

現在の状況

「システム侵入」は、「ソーシャルエンジニアリング」を「上位3つのパターン」の座から引きずりおろしました。昨年は「ソーシャルエンジニアリング」が1位であったことを考えると、これは非常に画期的なことです。これは、昨年明らかになったサプライチェーンへの大規模な侵害の影響によるものです。

「ソーシャルエンジニアリング」の順位が下がると、「基本Webアプリケーション攻撃」がその空白を埋めるようになりました。「多種多様なエラー」は中位にとどまり、その原因は主に「設定ミス」「誤送信」「盗難・紛失」の3つで、この分野で最も多くの侵害を引き起こしています。

この業界におけるエラーの発生は、内部犯行によるデータ漏洩/侵害の多さを物語っています。この分野では、悪用による侵害も散見されますが、内部関係者は、悪意ある行為を行うよりも、データ漏洩/侵害を引き起こすミスを犯す可能性が約7倍も高いのです。

以前、漏洩/侵害されるデータのタイプとして、認証情報がいかに人気であるかについて述べました。しかし、今年のDBIRでは、2021年にこの業界で80%だった認証情報が低下しています。一方、昨年わずか18%だった個人情報が、今年はトップに躍り出ました。

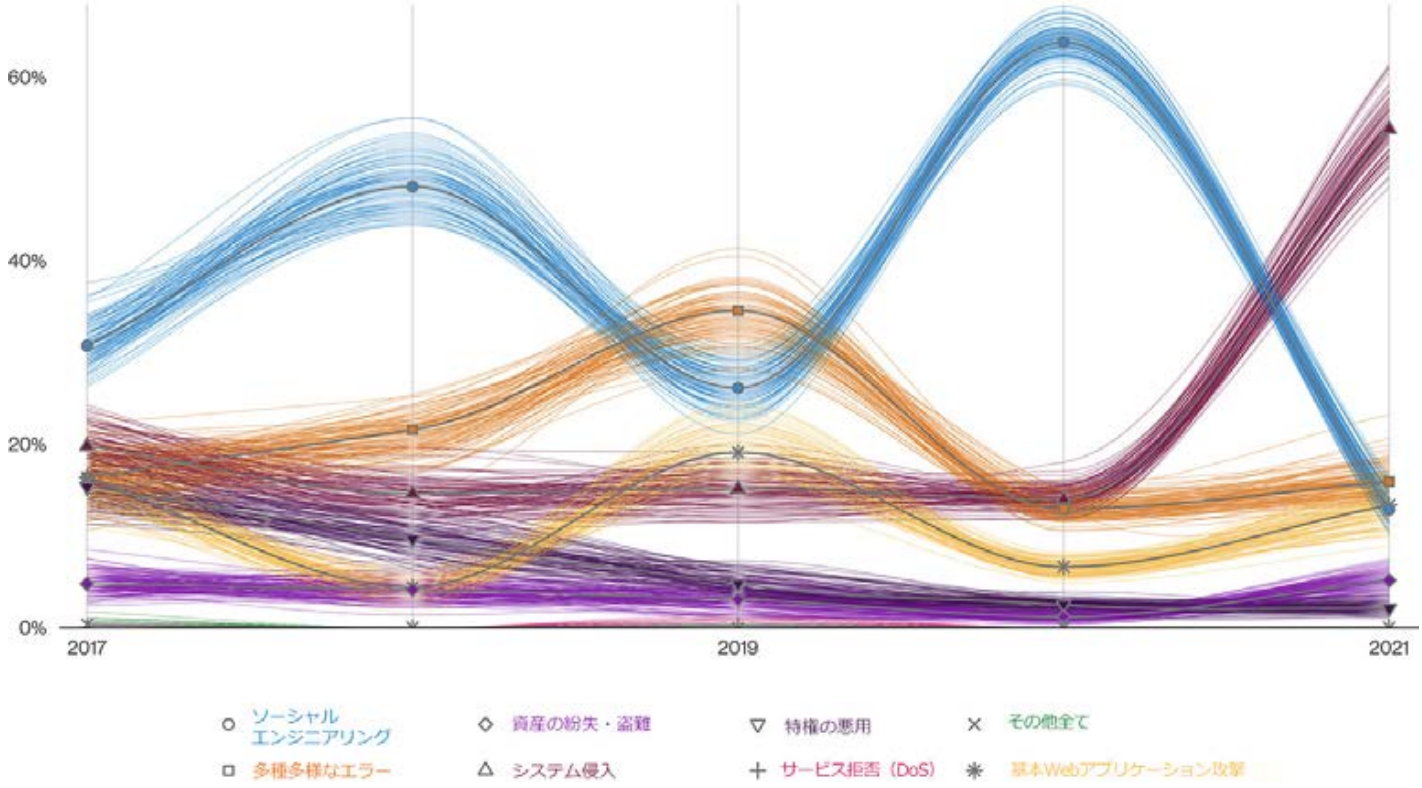


図100. 公務のデータ漏洩/侵害パターンの経時的変化

ぼろぼろのデロリアンに乗り込む

15周年を記念して、この分野で何が変わったのか、過去にさかのぼって考えてみたいと思います。わずか3年前、攻撃者の動機のトップは「スパイ活動」で、66%でした。5年前も64%を占め、政府機関にとって根強い課題であることがわかります。このことは、どの政府機関であっても、その企てを知りたがっている人がいることを考えれば、納得がいきます。悪意があるといえば、動機の「スパイ活動」は、昨年の4%から今年は18%に増加しています。また、内部関係者による犯行も昨年より増加しており、「怨恨」による動機が一挙にリストの上位に上っています。

図101は、2017年以降のこの業界における「スパイ活動」の動機を持つ攻撃者の変化を示しています。ご覧のように、「スパイ活動」の動機が落ちたところで、「金銭目的」の攻撃が増えています。この部門は、一儲けしようとする犯罪者に狙われることで、他の業種に仲間入りしたようです。友よ、パーティーへようこそ！[27]。

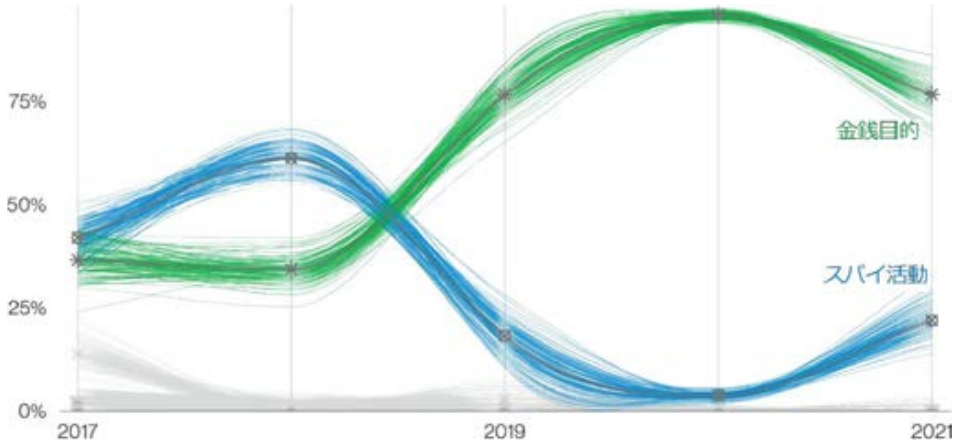


図101. 公務のデータ漏洩/侵害における攻撃者の動機の経時的変化

27 分かっていますよ。あなたはダイハードのジョン・マクレーンを真似てこれを読みましたね。

小売業 NAICS 44-45

頻度	629件のインシデント、確認されたデータの暴露241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/侵害の84%を占めている
攻撃者	外部（87%）、内部（13%）（漏洩/侵害）
攻撃者の動機	金銭目的（98%）、スパイ活動（2%）（漏洩/侵害）
侵害されたデータ	認証情報（45%）、個人情報（27%）、その他（25%）、決済情報（24%）（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トレーニングプログラムの実施（CSC 14）、アクセス制御管理（CSC 6）、企業資産およびソフトウェアのセキュアな設定（CSC 4）
昨年との比較	小売業界は、Webフォームで処理されるクレジットカード情報をキャプチャする「マルウェア」や、「フィッシング」のような一般的な手口など、さまざまな手口を利用する攻撃の影響を受け続けています。

サマリー

小売業界は、昨年と同じタイプの攻撃を受けています。「窃取した認証情報の使用」、「フィッシング」、「ランサムウェア」です。

過去のパターン	5年前との比較	3年前との比較	他の業種との比較
基本Webアプリケーション攻撃	同程度	減少	減少傾向
多種多様なエラー	同程度	増加	増加傾向
システム侵入	増加	同程度	増加傾向

私たちの社会、いや地球全体が、ここ数年で驚くほど大きく変化しています。一方、小売業界は、少なくともデータ漏洩/侵害に関しては、そうではありません。昨年の報告書から、この業界に関する調査結果を単純にカット&ペーストしたいところでしたが、もちろんやりませんでした。しかし、前回調査したときからあまり大きな変化はないものの、注目すべき結果がいくつかあります。

ソーシャル攻撃は、「フィッシング」（53%）と「なりすまし」（47%）に大別されますが、小売業界ではここ数年、増加傾向にあります。2016年は7%、2018年は13%で、今年は29%です。これは、「ソーシャルエンジニアリング」が上位3つのパターンに入ることを物語っています。したがって、この業種で侵害されるデータのタイプは、予想通り認証情報がトップです。多くの場合、これらの認証情報は、後にサーバーへのハッキングやランサムウェアのロードに悪用されます（47%）。そして、犯罪者は大金を手にするまでじっと待っています。

今年の興味深い調査結果の1つは、「アプリデータを取得する」マルウェアの件数が、他の業種に比べて小売業界が7倍も多かったことです。このことは、「システム侵入」パターンがこの業界で1位であることを裏付けるものです。「アプリデータの取得」は、Magecart型の攻撃でよく見られるもので、攻撃者は通常、脆弱性を悪用し、盗んだ認証情報を使ってeコマースサーバーに侵入し、そこでくつろいで、ちょっとしたもの（ほとんどの場合、決済カード情報）を失敬します。

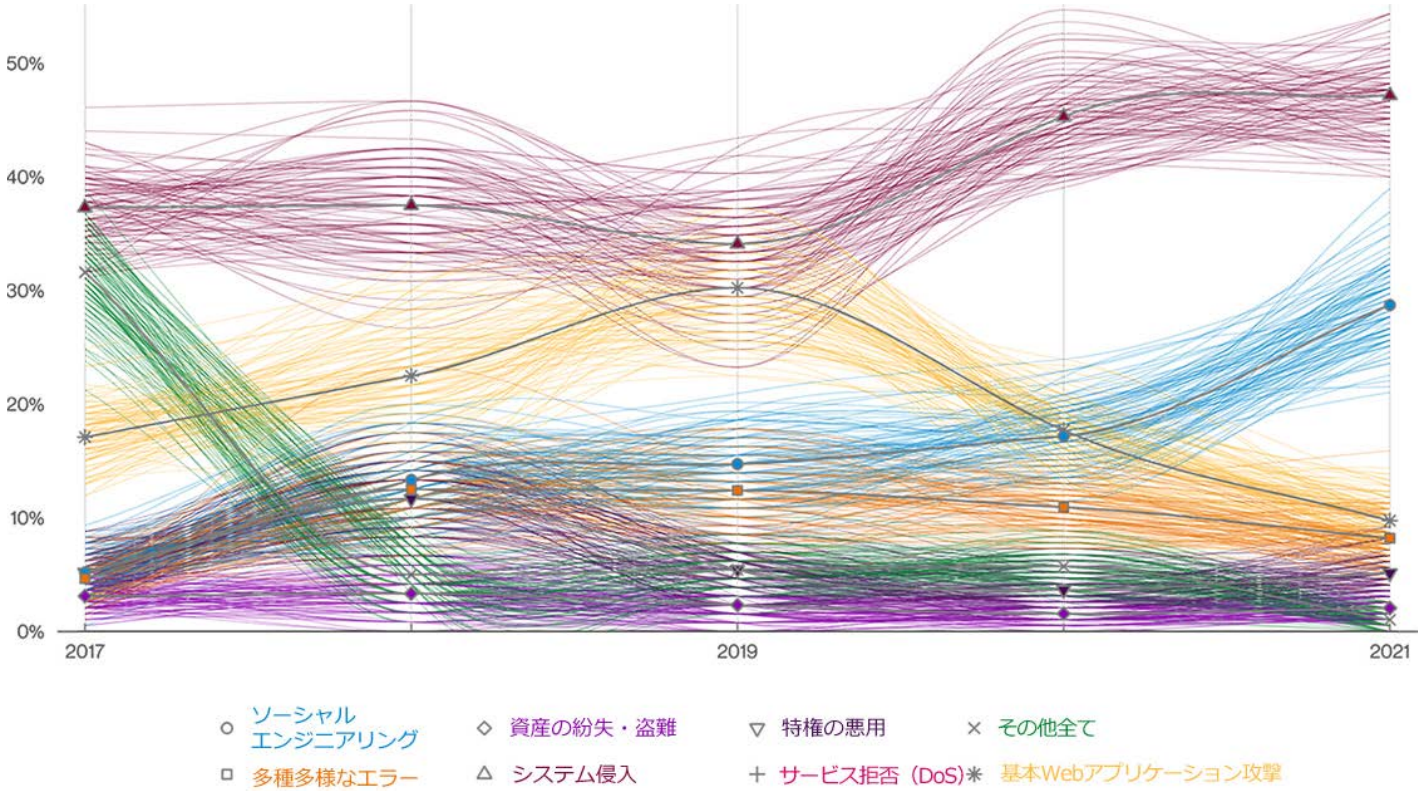


図102. 小売業におけるデータ漏洩/侵害パターンの経時的変化

図103. 小売業界のデータ漏洩/侵害の攻撃（n=241）

小売業界の企業が被害に遭ったことを知るとき、それは他のどの業種よりも不正行為の検知メカニズム（例：Common Point of Purchase（CPP）、法執行機関）を通じて行われます。これは、小売業が非常に多くの取引を担っていることを考えると、直感的に理解できることかもしれませんが、それでも注目すべきことです。

小規模企業向けサイバー犯罪対策シート

頻度	832件のインシデント、確認されたデータの暴露130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」、「特権の悪用」がデータ漏洩/侵害の98%を占める
攻撃者	外部（69%）、 内部（34%）、 複数の関係者（3%） （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	認証情報（93%）、 内部情報（4%）、 銀行情報（2%）、 個人情報（2%） （漏洩/侵害）

サイバー犯罪がニュースになるのは、通常、大企業が攻撃を受けて被害に遭った場合です。しかし、多くの人が考えているのとは逆に、極めて小規模な組織でも、犯罪者にとっては大規模な組織と同様に魅力的であり、ある意味では、それ以上かもし れません。サイバー犯罪において、攻撃者には「手に入るものは何でも手に入れる」という哲学があります。これらのインシデントによって小規模な企業は廃業に追い込まれる可能性があり、実際そうなっている現実もあります。したがって、非常に小規模な企業（従業員10人以下）であっても、攻撃の標的にされないように予防策を講じることが極めて重要です。大企業は大きな資源を持っているので、情報セキュリティの専門家や最先端の技術で自衛する余裕があります。一方、非常に小規模な企業は、資源が非常に限られており、熟練のスタッフに頼ることはできません。このセクションを設けたのは、このような理由です。

ここで、小規模な会社を経営している方に推奨事項やベストプラクティスを紹介します。このセクションを印刷または切り取って、懸念事項が発生したときに参照することをお勧めします。

小規模企業が直面する脅威

今回の調査に使用したデータセットで、小規模企業に対する攻撃タイプで一番多かったのは「ランサムウェア」攻撃です。「ランサムウェア」は、データを暗号化して閲覧や利用ができないようにするマルウェアの一種です。ランサムウェアを起動させると、攻撃者は暗号化の解除と引き換えに（しばしば高額の）身代金の支払いを要求します。そこで、オフライン[28]バックアップが役に立ちます。

2番目に多いのが、窃取した認証情報の使用です。攻撃者が認証情報（ユーザ名とパスワード）を手に入れるには、さまざまな方法があります。「ブルートフォース攻撃」（攻撃者が自動化を使って、文字、記号、数字の組み合わせを数多く試し、認証情報を推測する方法）、さまざまな種類の「マルウェア」（したがって、最新のアンチウイルスが必要）、他のサイトでハッキングされたパスワードの再利用、そして最後に重要なのが、「フィッシング」や「なりすまし」などのソーシャル攻撃です[29]。

ニュース記事などで「ビジネスメール詐欺（BEC）」という言葉を聞いたことがあるかもしれません。「フィッシング」や「なりすまし」などのソーシャル攻撃も、当たり前のように行われています。これらの攻撃は、あまりにも手口が巧妙なため（既知のサプライヤーから来たように見えるが、別の支払口座がある請求書や、またはビジネスパートナーからピンチなので代理で迅速な支払いが必要だというメールなどです）、容易に騙されてしまいます。多くはメールで送られてきますが、犯罪者は電話も利用して要求の正当性を信じ込ませています。このような犯罪者は、しばしば合法的なビジネスのように企業を運営し、犯罪者のコールセンター（実際に存在します）を利用して、自分たちの策略に信憑性を持たせることさえあります。

図104. 従業員1～10人の組織におけるデータ漏洩/侵害の攻撃の種類（n=61）

28 ここでいう「オフライン」の意味がよくわからない場合は、以下の「攻撃の標的にされないためのベストプラクティス」をご覧ください。
29 「フィッシング」や「なりすまし」に馴染みがなくても大丈夫です。定義については、このまま読み進めてください。

フィッシングとは、ソーシャルアタックの一種です（通常はメールを使用）。攻撃者は、ユーザ名とパスワードを教えたり、悪意のあるリンクをクリックさせたりして、ユーザを騙そうとします。例としては、「ここをクリックしてパスワードをリセットしてください」、請求書のダウンロード、添付PDFの閲覧、銀行口座番号の確認、などがあります。このような攻撃は極めて現実的であり、特定が困難な場合も少なくありません。

「なりすまし」は、「フィッシング」に相当するものです。通常、攻撃者は、ログイン情報を得るために、ビジネスパートナー、銀行の従業員、または自分の組織の上司になりすまし、被害者との対話を試みます。「なりすまし」の最終目的は、通常、詐欺の標的にされた組織から犯罪者の銀行口座に資金を自動送金させることです。

被害に遭っていることを知る方法

奇妙なことや通常と変わったことがないか、よく注意してください。たとえば、銀行の明細書や電話の請求書に予期せぬ請求が記載されていることがあります。クレジットカードに覚えのない取引がないか、よく調べてください。友人からメールでギフトカードの購入依頼を受けたというメッセージを受け取るかもしれません。パスワードやクレジットカード番号を尋ねる電話がかかってきたり、口座番号や決められた業者や顧客への支払い方法を変更するよう要求されたりすることがあります。これらはすべて、悪意のあることに巻き込まれているかもしれないという警告のサインです。車と同じように、コンピューターが突然起動しなくなったり、動作が遅くなったり、変な音が聞こえるときは、専門家に見てもらう必要があります。最後に、ランサムウェアのような脅威は、データが暗号化されたことを攻撃者が通知してきます。

攻撃の標的にされないためのベストプラクティス

1. 2要素認証を利用する[30]
2. パスワードの再利用や共有をしない[31]
3. パスワード管理/生成アプリケーションを使用する
4. 機器（POSシステムなど）や他のハードウェア/ソフトウェアのデフォルトの認証情報を必ず変更する
5. ソフトウェアアップデートを迅速にインストールし、脆弱性にパッチを適用できるようにする
6. ベンダーと協力して可能な限り安全性を確保し、ベンダーにも同じ基本的ガイドラインに確実に従わせる
7. バックアップを定期的に行い、オフラインバックアップを必ず行う（コンピューターに接続されたデバイスに保存しない）
8. ラップトップやデスクトップなどのユーザデバイスの内蔵ファイアウォールを必ずオンにさせるようにする（デフォルトで「オン」がなってない場合がある）
9. すべてのデバイスで、ウイルス対策ソフトウェアを使用する。スマートフォン、タブレット、クレジットカードのスワイプも、ラップトップやコンピューターと同様に重要です。すべてをカバーできるわけではありませんが、役に立ちます
10. 迷惑メールやテキストメッセージはクリックしない
11. データや支払いに関する特別の要求を確認できるよう、帯域外認証を設定する
12. 金融取引に使用するコンピューターが、ソーシャルメディアやメールなど他の目的に使用されていないことを確認する
13. フィッシングやなりすましの防御機能を備えたメールサービスを利用し、なりすましの可能性があるWebサイトの警告機能があるWebブラウザを使用する

サイバー犯罪の被害に遭った場合の連絡先

- さまざまな状況に対応できる幅広い情報リソースが、https://fightcybercrime.org/から入手できます。このWebサイトでは、サイバーインシデントが発生した場合にどこに行き、何をすべきかという情報を提供しています。
- Scam Spotterは、一般的な詐欺の見分け方について、シンプルでわかりやすい情報を提供しています。https://scamspotter.org/
- 米国内にお住まいの方は、各州の司法長官事務所のWebサイトにも情報が掲載されていることがあります。

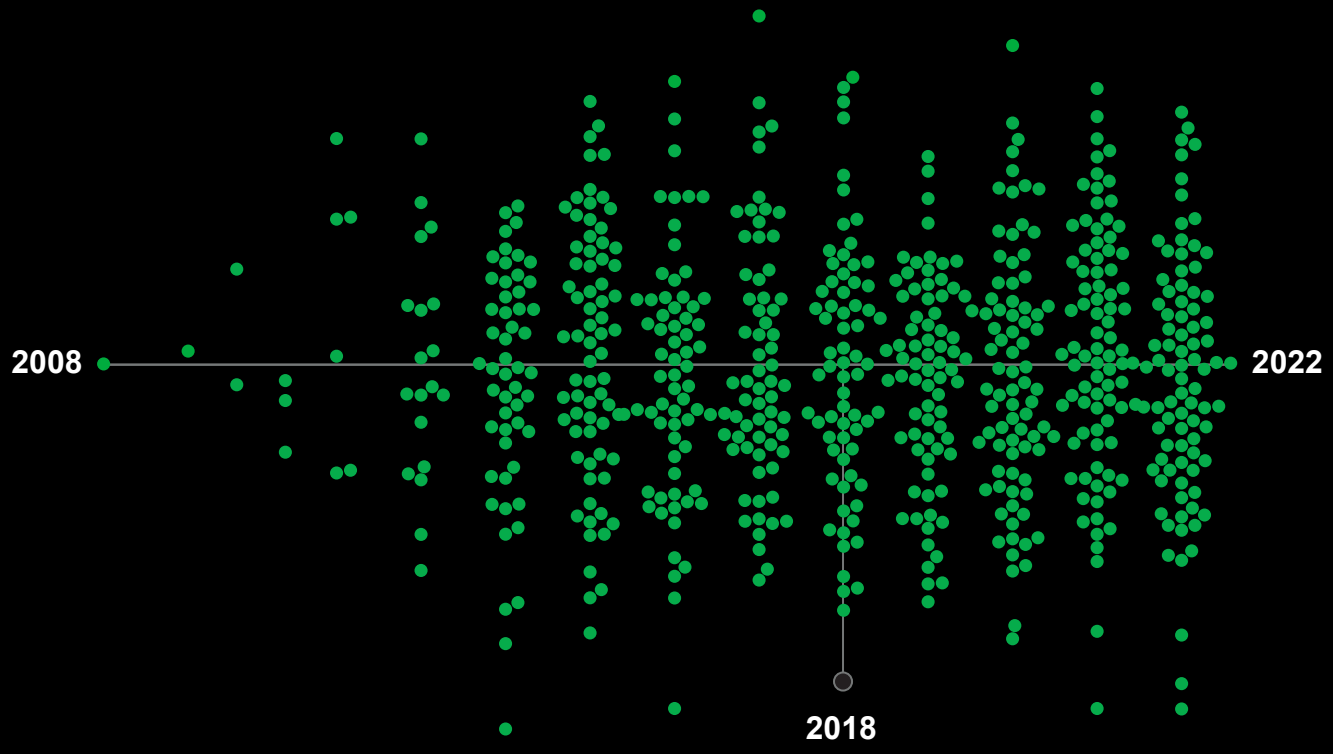
これらの情報リソースを熟知し、自分の組織が被害に遭ったときにどのような手段を取るか、計画を立てください。会社に火が付いてからではなく、前もって計画を立てておくのです。例えば、すべてのベンダーと銀行の詐欺部門の連絡先を記載した文書だけでも、第一歩を踏み出したことになります。プリントアウトして、すぐ参照できる場所に貼っておきましょう。コンピューターにファイルを保存しておくだけでは、攻撃に遭ったときに利用できなくなる可能性があります。

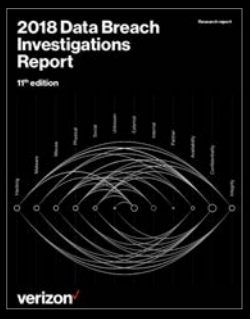
このような攻撃に遭う可能性の高い人たちを少し教育することと、あなたの側で少し計画を立てることが、あなたの小さな会社をより安全にするために大いに役立つのです。

30 ユーザ名とパスワードの組み合わせだけでなく、さらに別のレイヤーが追加されます。登録した携帯電話にテキストで送られるコード、GoogleやMicrosoft Authenticatorのような認証アプリの使用、またはUSBドライブに差し込む小さなデバイスの使用などが考えられます。ベンダーが2要素認証（多要素認証（MFA））を提供していない場合は、対応するように働きかけてください。

31 他の人と共有したり、複数のアプリケーションやWebサイト間で使い回したりしてはなりません。パスワード管理アプリを使えば、簡単に防ぐことができるようになります。

5
地域別の分析


2008
2022
2018


2018 Data Breach Investigations Report
11th edition
verizon

地域別分析の概要

各地域のインシデントをマクロ的観点から紹介するインシデント分析は、 今回の DBIR で 3 回目を迎えます。 サイバー犯罪をよりグローバルな視点で捉えたこれらの分析が、 読者の皆様のお役に立てば幸いです。 これまでにも述べてきたように、 地域における協力関係者の存在や情報開示規制、 ベライゾンが調査した事案など、 さまざまな要因によって、 それぞれの地域についての可視性は変動します。

以下のページに記載されていない地域にお住まいの方やお仕事をされている方で、 データ提供者になることを希望されている場合は、 ベライゾンまでお問い合わせください。 また、 地域内の他の組織にも同じことを勧めていただければ、 年ごとに DBIR の調査範囲を広げ、 改良していくことができます。 あなたがお住まいの地域の掲載がない場合でも、 それは必ずしもその地域を全く把握していないわけではなく、 単に独立したセクションを設けるにはその地域のインシデントが統計的に十分でないからであるということを頭に入れておくことが重要です。

世界の地域は、 国連の M49 基準に従って定義してあり、 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ています。 そうすることで、 今回の調査対象となったのは以下の地域です。

APAC （アジアと太平洋地域） : 南アジア （034）、 東南アジア （035）、 中央アジア （143）、 東アジア （030）、 オセアニア （009） を含む

EMEA （ヨーロッパ、 中東、 アフリカ） : 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

NA （北アメリカ （021）） : 主に米国とカナダで起きたデータ漏洩 / 侵害から構成される

LAC （中南米とカリブ海諸国）: 南米 （005）、中米 （013）、カリブ海諸国 （029） で起きたデータ漏洩 / 侵害から構成される

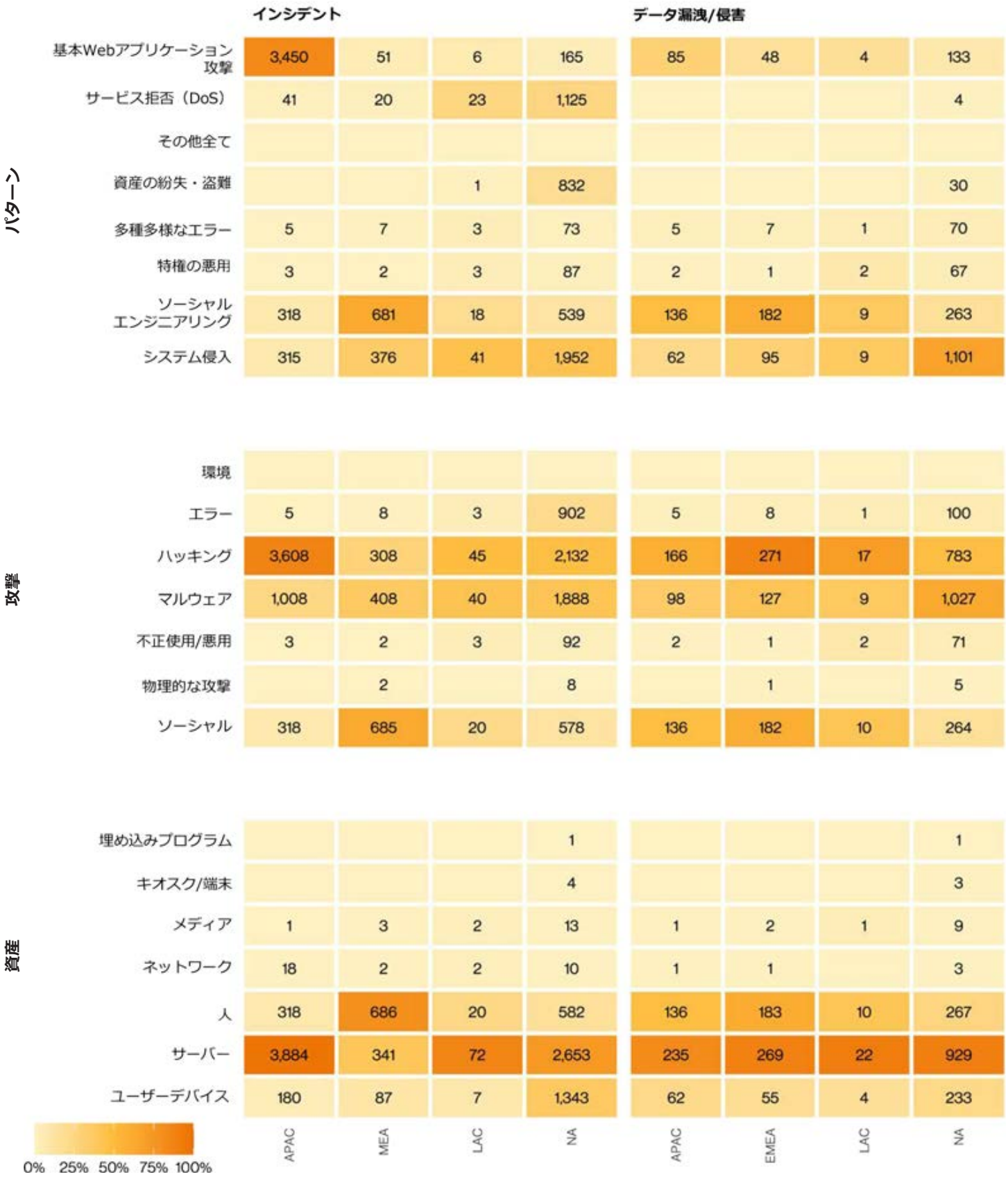
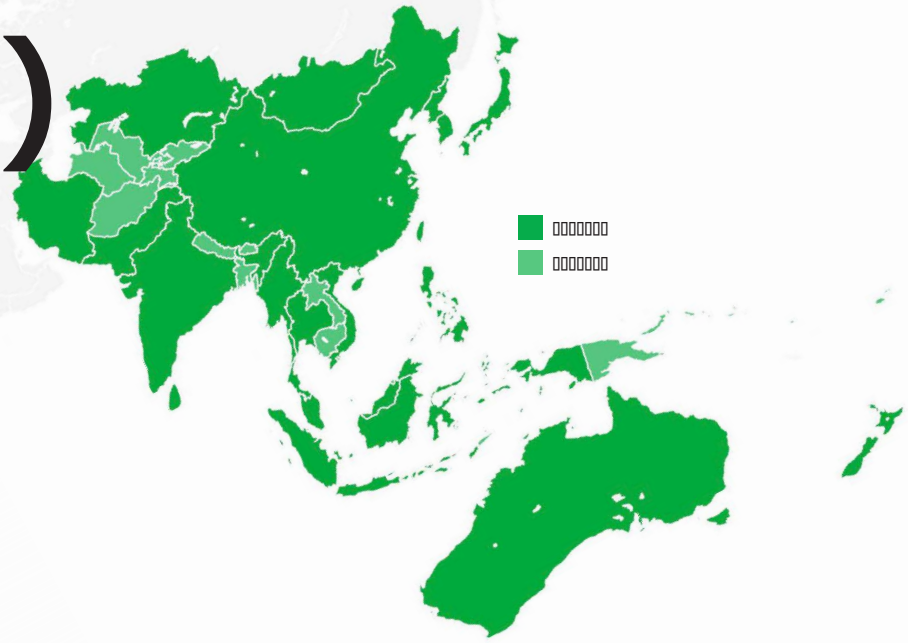


図105. 地域別インシデントとデータ漏洩/侵害

アジア太平洋地域（APAC）



頻度	4,114件のマルウェア、確認されたデータ暴露283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」、「システム侵入」がデータ漏洩/侵害の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（54%）、スパイ活動（46%）、二次的動機（1%）（漏洩/侵害）
侵害されたデータ	認証情報（72%）、内部情報（26%）、機密情報（18%）、その他（11%）（漏洩/侵害）
昨年との比較	この地域では、「基本Webアプリケーション攻撃」と「ソーシャルエンジニアリング」攻撃が依然と根強い脅威となっています。

サマリー

APACでは、ソーシャルおよびハッキング関連の攻撃が多発していますが、ランサムウェアの件数は他の地域よりもはるかに少なくなっています。

今年、APAC地域では、「ハッキング」（58%）、「ソーシャル」（48%）、「マルウェア」（36%）のよく知られた3つの脅威が中心となっています。インシデントの大半は、金銭目的（81%）を動機とする攻撃者によって引き起こされました。しかし、APAC地域では、スパイ活動（19%）を動機とする国家関連（19%）および国家支援（1%）の攻撃者もよく見受けられました。

ハッキング行為としては、「窃取した認証情報の使用」（83%）が最も多く、そのほとんどがWebアプリケーションを侵害するために使用されています（60%）。ソーシャル攻撃は他の地域の約2倍で、ほぼフィッシング（99%）で構成されています。昨年と同様、APAC地域ではランサムウェアの件数は比較的少なくなっています。データセット全体の平均が25%であるのに対し、APAC地域でランサムウェアが関与したデータ漏洩/侵害は10%でした。

この地域では、今年、相当数の改ざん攻撃が発生し（2,800件以上）、「完全性」の属性が全インシデントの75%に上昇しました。これは、世界の他の地域での改ざん件数の多さがDBIRのデータに反映されていないという点で興味深いものです。また、厄介なものではあるとはいえ、ランサムウェアなどのケースに比べると、通常、影響は小さいと言えます。

図106. アジア太平洋地域におけるデータ漏洩/侵害の上位のパターン（n=283）。

ヨーロッパ、中東、アフリカ（EMEA）

頻度	1,093件のインシデント、確認されたデータ暴露307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/侵害の97%を占めている
攻撃者	外部（97%）、内部（3%）（漏洩/侵害）
攻撃者の動機	金銭目的（79%）、スパイ活動（21%）（漏洩/侵害）
侵害されたデータ	認証情報（67%）、内部情報（67%）、機密情報（20%）、その他（18%）（漏洩/侵害）
昨年との比較	パターンの上位3つは変わらず、順位が入れ替わっています。この地域のデータ漏洩/侵害の大部分は、依然として外部要因によ るものです。

サマリー

この地域では、 「ソーシャルエンジニアリング」 のパターンが増加しており、 この攻撃タイプを迅速に検出するためのコントロールが必要であることを示しています。 また、 EMEA 地域では、 「基本 Web アプリケーション攻撃」 のパターンが依然として多いことからもわかるように、 認証情報の盗難も引き続き大きな問題となっています 。

ヨーロッパ、 中東、 アフリカをカバーする EMEA 地域では、 過去 1 年間にソーシャルエンジニアリングのパターンが急増しました （データ漏洩 / 侵害の約 60%）。 同じ上位 3 つのパターンが引き続きこの地域を苦しめていますが、昨年のデータでは 「ソーシャルエンジニアリング」 は3位でした。同時に、 「基本 Web アプリケーション攻撃」 が急減しています （次ページの図 108）。 昨年の DBIR では、 この地域のデータ漏洩 / 侵害の 50% 以上を占めていましたが、 今年は 15% 台にまで低下しました。 しかし、 より複雑な 「システム侵入」 パターンは今年も賑わいを見せており、 30% の割合で 2 位を維持しています。

この地域では、 依然として認証情報の盗難が問題となっており、 攻撃者がどのように認証情報を盗取するかにかかわらず （「ソーシャルエンジニアリング」 の台頭がおそらくその答え）、 入手した認証情報は企業のインフラに対して悪用されます。 このような足がかりを得た攻撃者は、 そのアクセス権を活用し、 「フィッシング」 の手口でさらに認証情報を入手したり、 ビジネスメール詐欺 （BEC） 攻撃の一環として企業のメールから得た情報を利用して、 巧妙ななりすましを働いたりすることができるようになります。

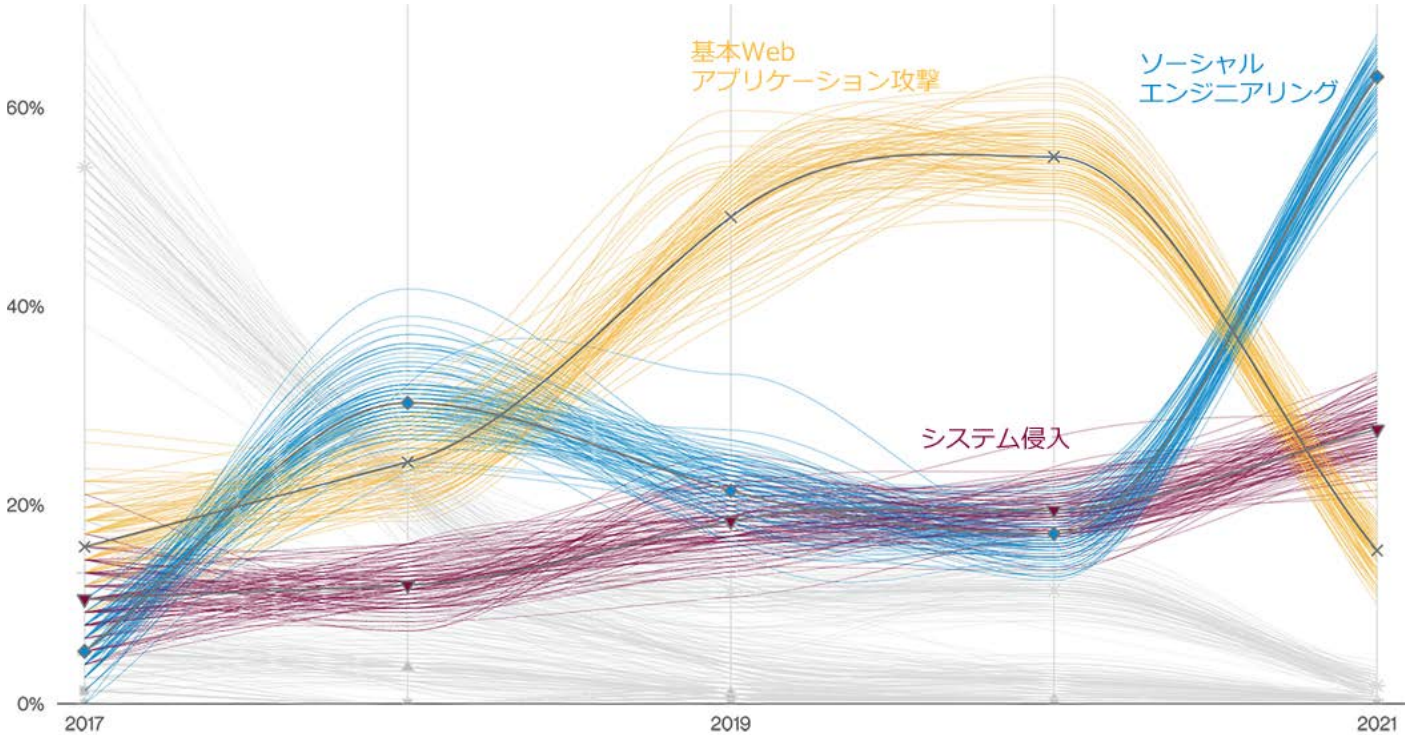


図108. ヨーロッパ、中東、アフリカ地域のデータ漏洩/侵害パターンの経時的変化

攻撃者がよく使用する手段は、 インターネット経由で最も容易にアクセスできるWeb アプリケーションサーバーやメールサーバーへの攻撃です。 メールサーバーは、 アカウントのコンテンツを採掘して、 スパイ活動に使える興味深い機密情報を得る機会になると同時に、 他の従業員を騙してさらに多くのアクセス権を取得できる場にもなります。 フィッシングの標的にされやすいのは、 当然のことながら、 会社の送金システムに容易にアクセスできる財務部門の人々です。 正規の取引を偽装し、 このような標的を騙して金銭を送金させることができれば、 データの現金化に悩む必要もありません。

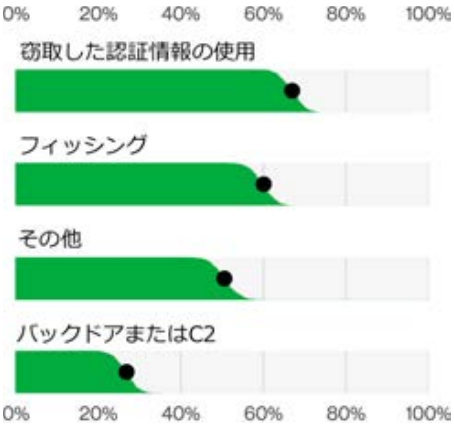


図107. ヨーロッパ、中東、アフリカのデータ漏洩/侵害における上位の攻撃の種類（n=283）

北アメリカ（NA）

頻度	4,504件のインシデント、確認されたデータ暴露1,638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/侵害の90%を占めている
攻撃者	外部（90%）、内部（10%）、複数の関係者（1%）（漏洩/侵害）
攻撃者の動機	金銭目的（96%）、スパイ活動（3%）、怨恨（1%）（漏洩/侵害）
侵害されたデータ	認証情報（66%）、内部情報（21%）、個人情報（20%）、その他（20%）（漏洩/侵害）
昨年との比較	パターンの上位3つは変わらず、順位が入れ替わっています。この地域のデータ漏洩/侵害は、依然として外部の攻撃者の支配下にあります。

DBIRのデータセットは、北アメリカ（NA）への依存が大きいため、この地域がなくなると、このデータセットもなくなります。このことは、北アメリカの上位3つのパターンを見れば明らかです。この3つのパターンは、全データセットの上位パターンに反映しています。北アメリカへの依存には、いくつかの要因が重なっています。まず、北米の情報漏洩に関する法律は非常に強固であり、さらに強化され続けていることです。北米で情報漏洩を報告しなければならない機関をすべて特定するには、暗号解読リングとマジック8ボールが必要なほどです。これに加えて、データを共有してくれる協力者のほとんどは、官民を問わず、北米地域に対する視認性が非常に高いことです。そして、率直に言って、DBIRチームは英語が得意です。フランス語とポルトガル語も何とかなりますが、それ以上の言語能力はありません。つまり、この北米地域については、他の地域よりもかなり豊富にデータがあるということです。

サマリー

この地域では、「システム侵入」が主流パターンとなっています。「システム侵入」の 増加によって、「ソーシャルエンジニアリング」が首位の座を明け渡す形になりました が、北アメリカでは依然として「フィッシング」などの「ソーシャル」の悪用が大きな 問題として残っています。また、「基本Webアプリケーション攻撃」も相変わらず、こ の地域の組織を苦しめています。

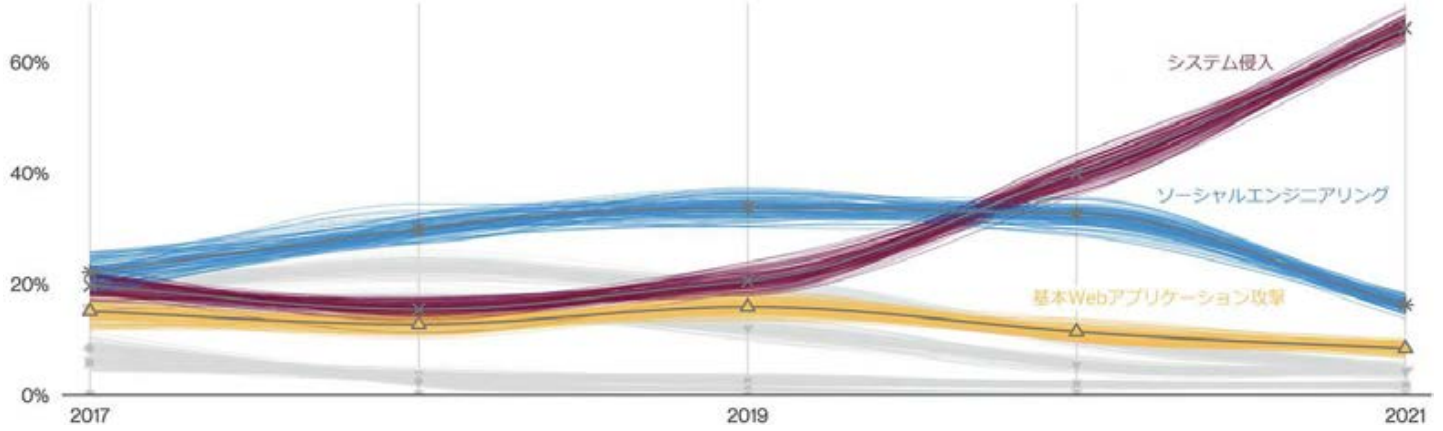


図109. 北米地域のデータ漏洩/侵害パターンの経時的変化

図109を見ると、「ソーシャルエンジニアリング」のパターンがデータ漏洩/侵害の最上位にしばらくの間君臨していましたが、昨年は変化が見られました。今年は「システム侵入」がトップであり、「ランサムウェア」のケースもこのパターンがほとんどです。ランサムウェアがここ数年増加傾向にあり、DBIRのデータ上でもかなり目立つようになったことは周知の事実です。

実際、マルウェアが関わるケースでは、ランサムウェアが圧倒的に多くなっています（図110）。この数年、ランサムウェアによる攻撃では、データへのアクセスができなくなるこに加え、組織のデータのコピーを持ち出されるため情報漏洩の報告が必要になるという、ダブルパンチを受けることが多くなっています。

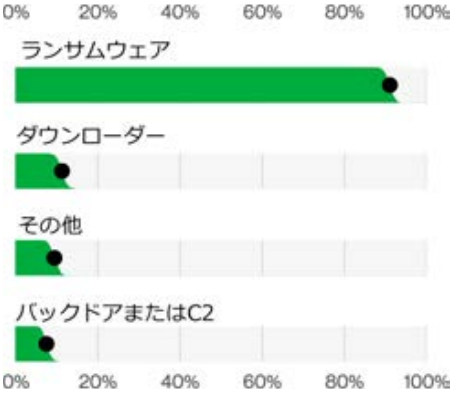


図110. 北米地域におけるデータ漏洩/侵害の上位のマルウェアの種類（n=647）

「ソーシャルエンジニアリング」のパターンには、当然ながら「ソーシャル」攻撃が含まれます。最も一般的なのは、ストレートな「フィッシング」で、2番目が「なりすまし」です（図111）。

図111. 北米地域におけるデータ漏洩/侵害の上位のソーシャルの種類（n=264）

「なりすまし」は手の込んだ手口になるため、より価値の高いターゲットに向けて採用される可能性があります。これは、ビジネスメール詐欺（BEC）攻撃で、偽の請求書などを提示し、相手から金銭や銀行情報を得ようとするケースで見られます。予想通り、組織の財務部門に所属する人々が、高度な攻撃の標的にされる可能性が高いです。

図 **112.** 北米地域におけるデータ漏洩/侵害の上位の機密データの種類（n=944）

データ漏洩が確認された攻撃によって、最もよく盗まれるデータが「認証情報」であるのは、驚くに値しません。認証情報の盗難件数は、次に多く盗まれる2種類のデータを合わせた件数よりも高いのです。おそらく認証情報はポップコーンのようなもので、1つ盗むだけでは飽き足らないのでしょう。

ラテンアメリカ・カリブ海地域（LAC）

頻度	92件のインシデント、確認されたデータ暴露24件
上位 3 つのパターン	「システム侵入」、「DoS攻撃」、「ソーシャルエンジニアリング」がインシデントの88%を占めている
攻撃者	外部（95%）、内部（7%）、複数の関係者（1%）（インシデント）
攻撃者の動機	金銭目的（92%）、利便性（3%）、スパイ活動（2%）、怨恨（2%）、その他（2%）（インシデント）
侵害されたデータ	システム情報（51%）、認証情報（40%）、内部情報（21%）、その他（12%）（インシデント）
昨年との比較	この地域では、金銭取得を動機とする攻撃者が引き続き主な脅威の主体となっています。

南半球では排水口に流れる水が北半球と逆回りなるとのことですが、 データ漏洩 / 侵害やインシデントは他の地域と同じように減少しているようです。 残念ながら、 この地域のデータ収集はまだ十分ではありません。 南半球の友人たちに何が起こっているのか、 理解を深めるためにずっとパートナーを必要としています。 この地域で活動されている企業の方は、 ぜひ力を貸してください。

サマリー

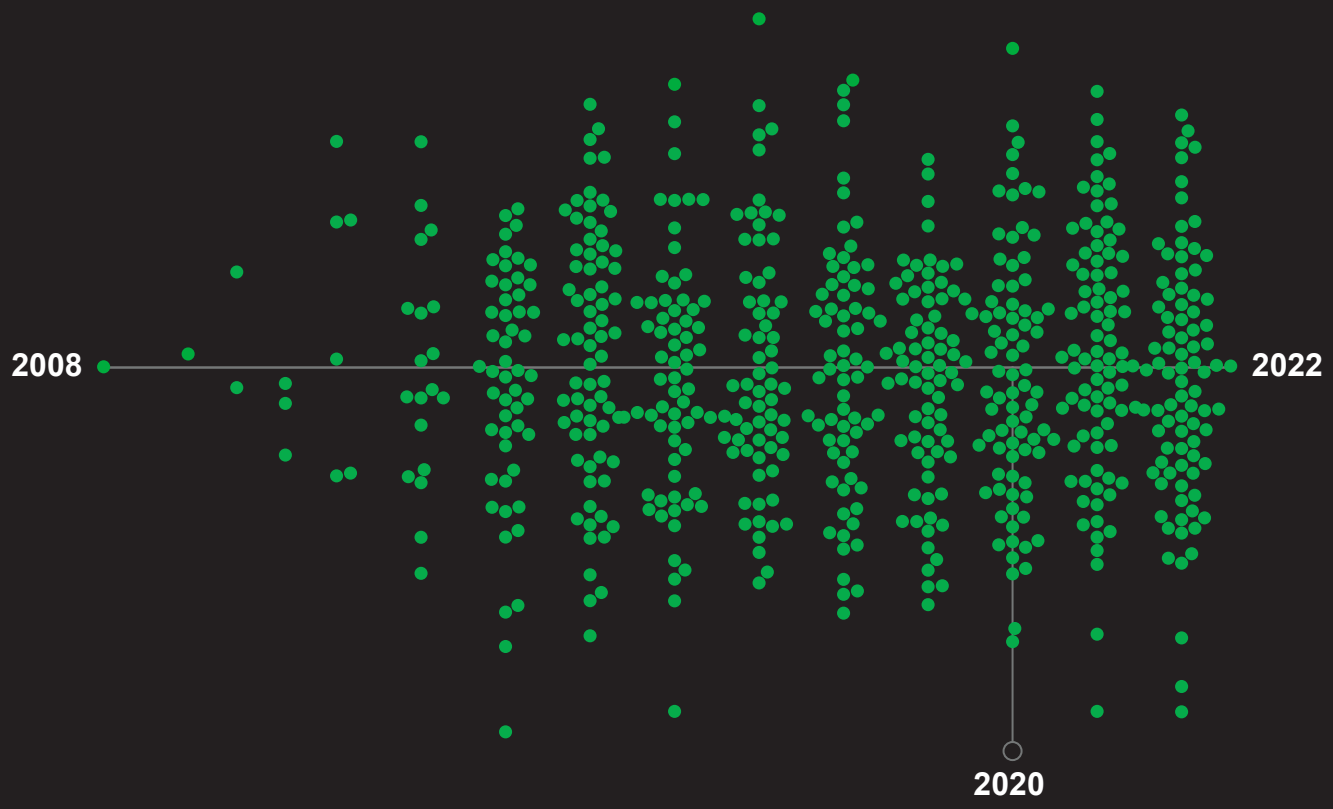
世界の他の地域と同様、ラテンアメリカの企業は、「ランサムウェア」や「サービス拒否（DoS）」攻撃など、企業の業務を標的とした攻撃に直面しています。これらの攻撃は、それぞれインシデントの37%と27%を占めています。

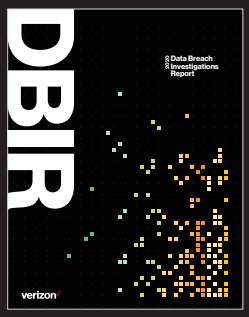
図113. ラテンアメリカ・カリブ海地域におけるインシデントの上位の業種（n=92）

図114. ラテンアメリカ・カリブ海地域におけるインシデントの上位の攻撃の種類（n=89）

図113は、ラテンアメリカでデータ漏洩/侵害された業種の内訳を示しています。中南米では、必ずしも多くの侵害が発生しているわけではありませんが、侵害を受けた組織が多種多様であり、被害者の約20%が上位7社以外の企業であることは確かです。

北米と同様に、ラテンアメリカの産業界にもランサムウェアの脅威が迫っています。このタイプの攻撃は、インシデントの30%以上を占めています。これに続くのが、絶えず存在するDoS攻撃です。そしてこの地域もまた、「フィッシング」攻撃や「盗まれた認証情報」による被害を多く受けています。ほとんど壊れたレコードのように繰り返していますね。あるいは、今風にいうとバッファリングのループ広告でしょうか？この時点で、これらの攻撃のいくつかは、インターネットを利用するすべての人にとって普遍的なものであるように感じ始めています。


2008
2022
2020


DBIR
Data Breach Investigations Report
verizon

6 まとめ

以上で、今年度のデータ漏洩/侵害の調査報告は終了です。

毎年のことですが、本報告書に掲載されている情報が有益かつ実用的であり、また読みやすいことを願っています。私たちは、読者の皆様に時折笑顔をお見せできるよう最善を尽くしますが、サイバー犯罪を真摯に受け止めていることは保証します。私たちDBIRチームの5人は、皆様と一緒に戦えることを幸せに思っています。これからも、DBIRのデータから得られる知見を皆様に提供し続けるとともに、皆様のご成功をお祈りいたします。明るい未来を！また来年もよろしくお願いします。最後に、過去のDBIRで見つけた特に適切と思われる言葉をご紹介します。

「元気で、 豊かで、 何事にも備えあれ」

年間総括

1月

新年を迎え、Verizon Threat Research Advisory Center（VTRAC）では、引き続きSolarWinds関連のキャンペーンの動きを追跡していました。Azure/Microsoft O365環境でセキュリティチームが使用するツールが登場しました。1月のパッチチューズデーでは、Windows Defenderにリモートコード実行の脆弱性が1つ含まれていましたが、これはすでに野放し状態（ゼロデイ）で悪用されていました。SonicWallは、特定のセキュアリモートアクセス製品の「考えられるゼロデイ脆弱性」を悪用した攻撃を調査していました。セキュリティ研究者は、SolarWindsの操作に使用された4つ目のマルウェアを報告しました。Raindropは、Teardropマルウェアのデジタル版といえるものです。Raindropは、特定のターゲットにのみインストールされ、Cobalt Strikeを配信しました。ゼロデイ攻撃の後、AppleはiOS/iPadOSの3つの脆弱性に対してセキュリティアップデートをリリースしました。1月の最大のニュースは、欧州刑事警察機構がEmotetのインフラを閉鎖し、160万台の被害者システムを法執行機関が管理するサーバーにリダイレクトしたことです。

2月

Googleは、2月の初めにChromeブラウザのアップデートを行い、ゼロデイ脆弱性の1つを緩和しました。SonicWall、Cisco、Fortinet、Palo Alto Networksは、VPNおよびリモートアクセス製品へのパッチとアップデートをリリースしました。SonicWallのCVE-2021-20016は、すでに悪用されていました。パッチチューズデーには、さらに2つのゼロデイ脆弱性について、マイクロソフトとアドビがそれぞれ1つずつパッチを適用しました。CERT-FRは、2020年のSolarWinds OrionおよびAccellion攻撃との共通点を示す、ロシアの攻撃者SandwormによるCentrionのサプライチェーン侵害を報告しました。スーパーボウルの2日前、フロリダの小都市の淡水プラントが短い間でしたが侵入されました。ある処理薬品が操作されましたが、すぐに検知され、修正されました。工場のITセキュリティはほとんどすべて間違っていました。攻撃者はWindows 7コンピューターの共有静的パスワードを使ってTeamViewer経由で侵入したのです。

3月

3月は、1月に悪用されたMicrosoft Exchangeの4つのゼロデイ脆弱性に対する不定期更新プログラムで始まりました。少なくとも3万台のExchangeサーバーが、中国の国家安全保障と連携するAPT級の攻撃者であるHafniumの被害を受けたと報告されていました。この欠陥は、「ProxyLogon」と呼ばれ、瞬く間にスキャンされ、悪用されたのです。他のAPTや他の攻撃者は、パッチが適用されていないExchangeサーバーに侵入しました。マイクロソフトは、セキュリティ研究者を標的にした北朝鮮の攻撃者が悪用したInternet Explorerのゼロデイ脆弱性「CVE-2021-26411」を含む89件の脆弱性にパッチを適用しています。この月の締めくくりとして、AppleがApple iOS/iPadOS/WatchOSのゼロデイ脆弱性に対するパッチをリリースしました。

4月

4月上旬、VTRACは、中国とロシアのAPTが、それぞれ日本の製造業とドイツ連邦議会を標的とした攻撃の報告を集めました。最も大きなリスクの変化は、Ivanti Pulse Secure SSL VPNアプライアンスにおける認証バイパスの脆弱性がゼロデイで悪用されたことによるものです。マイクロソフトは114件の脆弱性にパッチを適用しましたが、そのうちの1件はパッチチューズデー以前に悪用されたものです。米国政府は、SolarWinds Orionの操作を、ロシアの情報機関SVRとそのAPT29またはNobelium攻撃者によるものと正式に認定しました。SITAは、世界のほぼすべての航空会社の通信およびITベンダーであり、数百万人の乗客のデータが流出するデータ漏洩/侵害の犠牲となりました。これは今年最大の情報漏洩の1つでした。

5 月

5月は、2021年の最も重要な情報漏洩の1つで始まりました。コロニアルパイプライン社は、DarkSideによるランサムウェア攻撃を封じ込めるため、パイプラインの運用を停止せざるを得なくなりました。いくつかの州は、燃料不足に陥りました。75ビットコイン（～500万米ドル）の身代金を支払っても、閉鎖は6日間続きました。コロニアルが操業を再開した同日、DarkSideは廃業を発表し、関連会社に復号プログラムをリリースするとともにグループのインフラの一部が不特定の法執行機関によって妨害されたと主張しました。その1カ月後、FBIは63.7ビットコイン（ビットコイン評価額の下落により、～230万米ドル）を押収しました。5月のゼロデイ脆弱性は、MacOSの脆弱性1件、Adobe Readerの脆弱性1件、Androidの脆弱性4件でした。ロシアと北朝鮮のAPTの名称を皮肉った「Fancy Lazarus」を名乗る攻撃者が、恐喝型DDoSキャンペーンを開始しました。日本のコングロマリットである富士フィルムと世界最大の食肉加工業者であるJBSフーズが、ランサムウェア「REvil」によって業務停止に追い込まれました。

6 月

北朝鮮のAPTであるKimsukyは、6月に韓国の原子力研究所のネットワークに侵入しました。またElectronic Arts社からソースコードを盗み出した攻撃者もいました。まずはSlack上の同社サポートチャネルに侵入し、同社の多要素認証を回避したのです。マイクロソフトの報告によると、APT29は、IT、シンクタンク、政府機関を標的とし、クレデンシャルハーベスティング攻撃を行ったとのことです。マイクロソフトのパッチチューズデーには、50件のパッチのうち、6件のゼロデイ脆弱性にパッチが適用されました。AppleはiPadOSとiOSの2つのゼロデイパッチを適用し、GoogleはChromeブラウザの1つにパッチを適用しました。

7 月

米国の独立記念日の祝日の数時間前、ランサムウェア「Revil」がKaseya Virtual Systems Administrator（VSA）を悪用して、何千もの企業のインフラを管理するマネージド・セキュリティサービスプロバイダーを攻撃しました。何百万ものエンドポイントシステムのうち、何台が暗号化されたのか、把握している者はいません。数日後、REvilの攻撃者はダークネットウェブサイトを閉鎖し、新たな被害者への感染を停止させました。その月の終わりには、BlackMatterランサムウェアが登場し、「このプロジェクトは、DarkSide、REvil、LockBitの最高の機能を取り込んでいる」との発表がありました。7月には、5つの製品ファミリで合計15件のゼロデイ脆弱性を悪用した攻撃が報告されました。Cloudflareは、金融業界の顧客に対する毎秒1720万リクエストのDDoS攻撃を検知し、軽減しました。この攻撃は、2万台のボットによる30秒間のバースト攻撃でした。マイクロソフトは、ゼロデイ攻撃でSolarWinds Serv-Uを標的とする中国の攻撃者を発見しました。

8 月

8月5日、Black Hatカンファレンスにおいて、ある「研究者」が、Windowsにおける4月の脆弱性2つと5月の脆弱性1つをどのように連鎖させて「ProxyShell」攻撃を作り出したかをを明らかにしました。脆弱性のあるExchangeサーバーの大量スキャンが発生しました。サイバーリーズンは、アジアの通信事業者を標的としたキャンペーン"DeadRinger"について報告しました。サイバーリーズンは、5つ以上の中国の攻撃者グループとのリンクを発見しました。マイクロソフトは、51件の脆弱性にパッチを適用しました（「悪用が検出された」1件のゼロデイ脆弱性も含む）。イタリアのエネルギー企業ERGとアクセンチュアが、ランサムウェアLockBit 2.0の被害に遭いました。T-Mobileは、約4,000万人の元顧客または見込み顧客の個人情報が漏洩したことを報告しました。ブロックチェーン上で動作する「DeFi」、つまり分散型金融プラットフォームであるPoly Networkは、攻撃者に約6億ドルの暗号通貨を盗まれたと発表しました。

9 月

ちょうど米国のレイバー・デーの祝日を台無しにするタイミングで、攻撃者はAtlassian Confluenceサーバーの1週間しか経っていない脆弱性を悪用し始めました。ほとんどの攻撃者はCryptominerをインストールしていましたが、月末までにVTRACは、APT活動家のTTPに似たウェブシェルを含むペイロードの情報を収集しました。レイバー・デーに、マイクロソフトは、Windowsブラウザのレンダリングエンジンの脆弱性に対するゼロデイ攻撃対策として不定期のアドバイザリをリリースしました。マイクロソフトから「マルウェア対策製品を最新の状態にしておくこと」とのアドバイスがありましたが、パッチは1週間後のパッチチューズデーの前夜までリリースされませんでした。アイオワ州の農業サービス会社であるNEW Cooperativeは、BlackMatterランサムウェアに感染し、590万ドルの身代金を要求される被害に遭いました。CISAとFBIは、Zoho ManageEngine ADSelfService Plusの脆弱性を利用し、APTがゼロデイ攻撃として防衛関連企業や学術機関などを標的にしていたため、組織に対してパッチを適用するよう促しました。Googleは、Chromeブラウザのゼロデイ攻撃で悪用されている5つの脆弱性にパッチを適用しました。ゼロデイ攻撃により、AppleはiOS/iPadOSおよびMacOSの3つの脆弱性にパッチを適用しました。

10 月

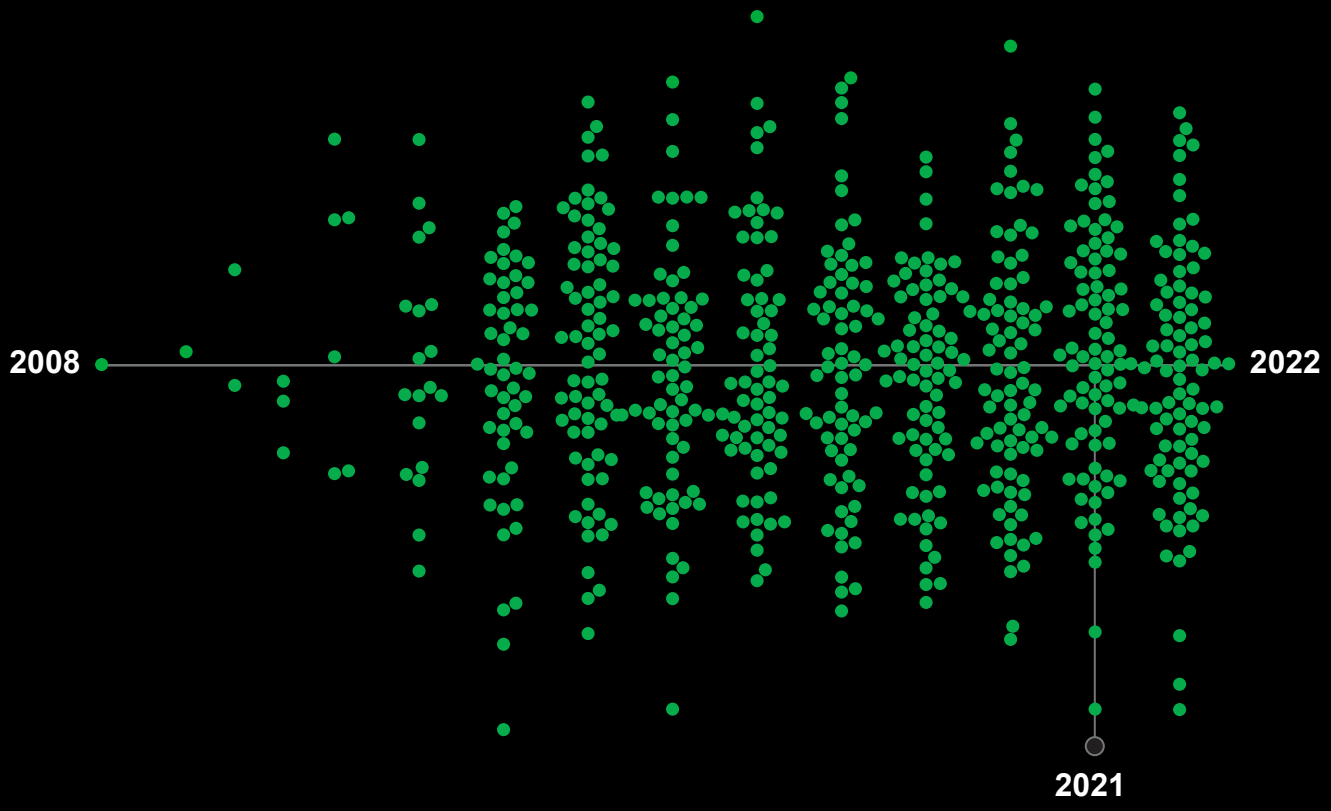
この月は、インターネット上で（Nginxに次いで）第2位のWebサーバーであるApache HTTPDの脆弱性に対するゼロデイ攻撃を緩和するために、パッチを大急ぎで適用することから始まりました。Apache 2.4.50の修正が「不十分」であることが判明した後、新たな脆弱性が導入され、それがほとんど即座に悪用されたのです。Apacheからバージョン2.4.51がリリースされました。ゼロデイ攻撃は、マイクロソフト、アップル、Chromeブラウザにも及びました。ランサムウェア「REvil」は、Tor決済ポータルとデータ流出ブログを何者かに乗っ取られ、再び活動が停止されました。CrowdStrikeは、2016年から通信分野の企業を標的にしていた「LightBasin」と呼ばれる攻撃者の分析結果を発表しました。CrowdStrikeは、LightBasinを国家支援に帰属させませんでした。「サイバー攻撃イベント」によって、数十億ドル規模の酪農企業であるSchreiber Foodsが3日間シャットダウンされました。これにより、米国でのホリデーシーズンのクリームチーズの入手に影響が出ました。CISA/FBI/NSAが、ランサムウェア「BlackMatter」のTTPを詳細に説明する共同警告を発表しました。このランサムウェアは、2021年7月以降、米国の複数の重要インフラ組織を標的にしていました。18日後、BlackMatterは現在の被害者をLockBit 2.0に移行させた後、閉鎖しました。

11 月

Robinhood Marketsは、700万人分の顧客データが流出したことを受けて、ハッカーが金融サービス会社を恐喝しようとしたと述べました。この攻撃者は、「詳細な口座情報」を収集するために10人の顧客をターゲットにしました。Emotetは、配信にTrickBotを使用して戻り、悪意のあるドキュメントを配信する世界的なメールスパムキャンペーンを開始しました。セキュリティ研究者は、このボットネットの復活の背後には、Conti ランサムウェアの一団が関与していると考えています。GoogleのAndroid月例アップデートは、「限定的な標的型攻撃」の下、ローカル権限昇格の脆弱性に対処しています。マイクロソフトは、既に悪用されている2件の脆弱性を含む55件の脆弱性についてのアドバイザリを公開しました。ウクライナのセキュリティ機関であるSSUは、Gamaredonの背後にいる攻撃オペレーターとして、5人のロシア連邦保安庁職員を特定しました。

12 月

Apache Foundation は、広く利用されている Log4j ライブラリに存在するリモートコード実行の重大な脆弱性にパッチを適用しました。しかし、セキュリティ研究者は、パッチ発表の9日前から悪用の兆候を発見していました。VTRACは、Zoho ManageEngineの未知の脆弱性2件を悪用した攻撃について情報を収集しました。ゼロデイ攻撃は、WindowsとChromeブラウザの脆弱性1件にそれぞれ影響を与えました。APT29（Nobelium）の攻撃者は、1年前のSolarWindsの侵害で達成した高い操作性を維持しました。報告書には、このAPTに関連する複数のサイバースパイ活動について以下のように詳述されています。「ほとんどの場合、侵害後の活動には、ロシアの利益に関連するデータの窃取が含まれていました。」


2008
2022
2021


DBIR
2021 Data Breach Investigations Report
verizon

7 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。こうして私たちの方法を詳しく説明することは、その正直さを示すための重要な部分です。

まず前提として、我々は間違いを犯します。コラムが入れ替わっていたり、数字が更新されていなかったりなど、修 正すべき点がいくつか見つかるかもし れません。その際にはその都度、以下の修正ページにリストアップします。https://www.verizon.com/business/resources/reports/dbir/2022/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[32] 、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。

最後に、科学には「創造的探求」と「因果関係の仮説検証」の2種類があります。DBIRはまさに前者です。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（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、無作為化対照試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、概論と言える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か月間、毎晩実行され、データが収集および分析されます。

32 https://github.com/vz-risk/dbir/tree/gh-pages
33 この文章もそうです。

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。

- インシデントには34の分野に少なくとも7つの区分（例：攻撃者の種類、攻撃の種類、完全性喪失の種類など）があるか、DDoS攻撃である必要があり ます。確認されたデータ漏洩/侵害については、区分が7個未満でも例外とな ります。
- インシデントには既知のVERISの攻撃カテゴリー（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、2020年11月1日から2021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2021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Emotet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。

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。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±0.7%、データ 漏洩/侵害では±1.4%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、この信頼度を相補累積密度の棒グラフ（「斜め」の棒グラフ）（斜め）棒グラフ、仮説的結果プロット（スパゲッティ）線グラフ、分位点プロット、ピクトグラムで示しています。

2つ目のバイアスは、サンプリングバイアスです。DBIRチームは、さまざまな協力者からデータ漏洩/侵害のデータを収集することで、「入手可能な最善の真実のバージョン」を目指しています。それでも、サンプリングが偏っていることは明らかです。例えば、公に開示されているデータ漏洩/侵害のようなものは、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。

データ漏洩/侵害

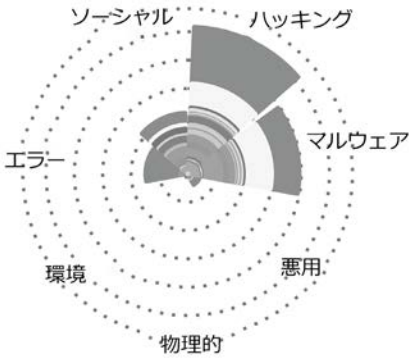


図115. 攻撃別の各貢献度

データ漏洩/侵害

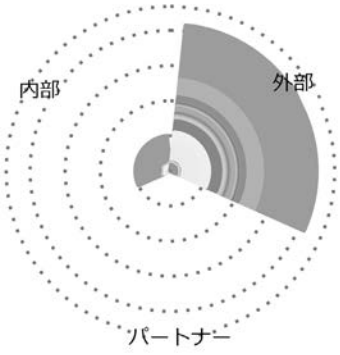


図116. 攻撃者別の各貢献度

データ漏洩/侵害

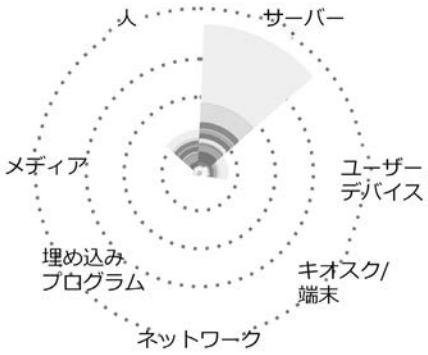


図117. 資産別の各貢献度

データ漏洩/侵害

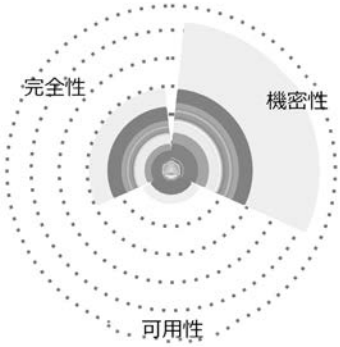


図118. 属性別の各貢献度

図115～118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に使用し ているため、特定の仮説検証は行いません。便宜的なサンプル以上のデータ漏洩/侵害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）[34]。また、リリースに先立って、特定分野の主題専門家と調査結果を検討するようにしています。

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。ただし関連する結果がきちんと得られなかった場合は記載しない可能性があります。今年度の報告書では、データセット全体の一部として分析されないインシデン トのサブセットが2つあります。

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。**

両サブセットは、過去5年間においても個別分析されています。

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、企業から提供されたデータはその数によって加重されるため、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、可能な限り分析できるようにしています。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。

34 ユニークな発見は、予想外の結果というよりも、データ収集の問題など、ありふれたものである可能性が高いです。

付録B：VERISと標準

DBIRが15歳の誕生日を迎える一方で、VERIS（DBIRの基礎となるデータ基準）は12歳という熟年になろうとしています。この基準は、インシデントの主要な構成要素を再現可能な方法でカタログ化する手段として、必要に迫られて誕生しました。これにより、何が起こったのか、誰が影響を受けたのか、どのように発生したのかを分析することができます。それ以来、VERISは多くの異なるタイプの利害関係者が採用できる基準に成長し、成熟してきました。VERISは、コミュニケーションを容易にするだけでなく、CIS（Center for Internet Security）のCritical Security ControlsやMITRE Adversary Tactics, Techniques & Common Knowledge（ATT&CK）など、他の業界標準やベストプラクティスへの接続ポイントを提供する基準となるよう調整されています。私たちは、これらすべての基準などに対応できる一つのフレームワークの開発は不可能だということは分かっています。しかし、私たちは、このコミュニティの成長を可能にしたすべてのフレームワーク間の平和的共存の重要性を確かに信じています。以下は、VERISと共存する素晴らしいプロジェクトや接続ポイントの一部であり、この基準によってサイバーセキュリティ界で活躍するプレーヤーが増えることを私たちは願っています。

CIS Critical Security Controls

CIS Critical Security Controls[35]（CIS CSC）は、コミュニティによって構築され、優先順位で並べたサイバーセキュリティのベストプラクティスのリストであり、さまざまな成熟度の組織が脅威から身を守るために役立つものです。組織がサイバーセキュリティインシデントを分類、評価できるようにDBIRは構築されているため、CIS CSCはVERISとうまく連携しています。このマッピングは、問題となっている事象と、組織の保護に役立つ対策とを結びつけます。2019年以降、ベライゾンは、組織が最も懸念するパターンと、そのパターン内の攻撃から組織を保護できるセーフガードを結びつけるのに役立つマッピングガイドを公開しています。各組織は、自分たちの業界のセクションに記載される上位パターンに基づいて防御策を改善するため、その出発点として使用できる「実装グループ1」のコントロールセットを見つけることができます。

MITRE ATT&CK

MITREのATT&CKは、攻撃者が攻撃プロセスの一環として何をするかという観点から、技術的な戦術情報を収集する決定的な方法の1つになっています。この豊富なデータセットには、個々の技術だけでなく、各技術に関連するソフトウェア、グループ、緩和策、そして今年の初めからは、関連するVERISコンポーネントも含まれています。技術的な戦術情報を戦略的な洞察に変換する組織を支援するため、ベライゾンはCenter for Threat Informed Defense（CTID）のパートナーと協力してVERIS対ATT&CK[36]の公式マッピングを作成し、インターネット接続環境があれば誰でも無料で利用できるようにしました。マッピングデータは、Structured Threat Information eXpression（STIX）STIXフォーマットで記述され、マッピングを更新するためのツールやスクリプトが含まれており、またATT&CK[37]Navigatorに取り込める可視化レイヤーも備えています。このマッピングを提供することで、組織の様々な関係者が一貫した方法で新しい情報を伝え、共有できるようになることを期待しています。

攻撃フロー

DBIRでお気づきかもしれませんが、「タイムライン」のセクションなど、いくつかの小さな箇所以外では、攻撃経路については触れていません。これは、非アトミックデータ（行動の経路やグラフなど）は、DBIRチームや他の情報セキュリティエコシステムにとって、本当に難しいものだからです。侵害の説明、シグネチャの作成、再現可能なペンテストやコントロールの検証、指導者への伝達など、攻撃経路やグラフを作成、共有、分析することは困難なことなのです。

DBIRチームは、MITRE CTIDとその参加者と共に、攻撃フロープロジェクトでこの困難な状態を変えたいと考えています。攻撃フローは、攻撃の因果関係のある経路と、その周辺のコンテキストデータの両方を「フロー」として捉えるためのデータスキーマです。攻撃は扇状に広がっては元に戻り、経路をたどってサーバーに戻ってくるので、攻撃フローは攻撃と資産の相互作用を示す任意のグラフをサポートします。攻撃に関するさまざまなことを私たち全員が知る必要があるため、ナレッジグラフ構造を使ってフローのコンテキストを把握できるようにしてあります。また、私たちはそれぞれ異なる組織化を行っているため、攻撃フローは複数の名前空間をサポートしています。例えば、攻撃経路分析の一環として、VERIS攻撃、MITRE ATT&CK攻撃、組織固有の攻撃、あるいは上記のすべての組み合わせを使用することができます。

攻撃フローによって、私たちは非アトミックデータの共有に使用できる形式を手に入れました。DFIR（Digital Forensics and Incident Response ）の担当者は、インシデントをフローとして文書化することができました。検出ベンダーは、攻撃フローによってシグネチャを作成することができました。コントロール検証ツールは、それによりインシデントをシミュレーションすることができました。セキュリティエンジニアリングチームは、攻撃フローによって攻撃対象領域のグラフを作成し、緩和策を計画することができます。そして、これらすべてが、この構造を利用してリーダーに伝えることができ、標準化されていながら柔軟性のある構造で、同じ基礎データを互いに共有することができようになります。これを支持できるという方はMITREプロジェクトのhttps://github.com/center-for-threat-informed-defense/attack-flowとDBIRチームのグラフベースの作業用ツールhttps://github.com/vz-risk/flowをチェックしてみてください。

35 https://www.cisecurity.org/controls
36 https://github.com/center-for-threat-informed-defense/attack_to_veris/
37 https://oasis-open.github.io/cti-documentation/stix/intro

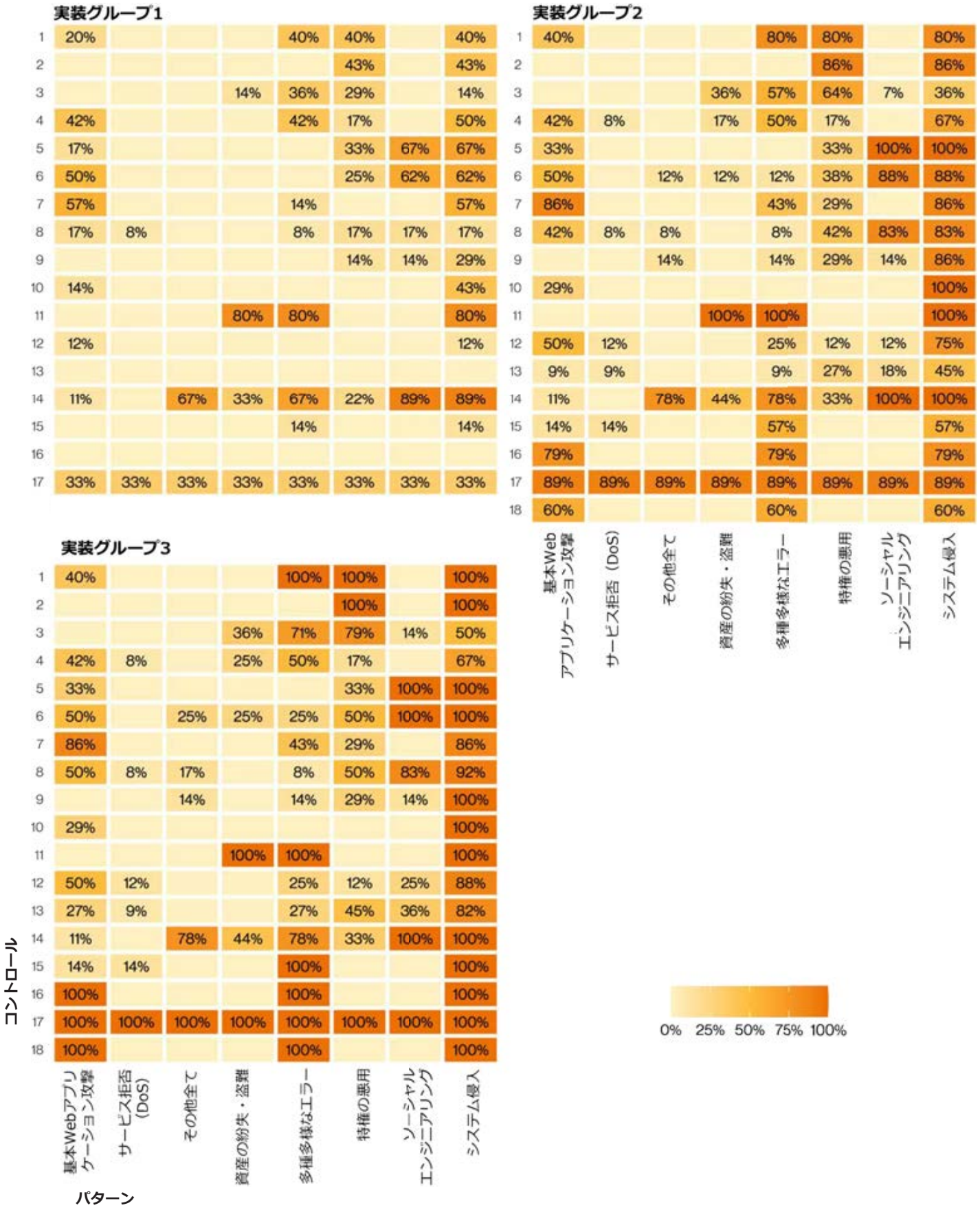


図119. CISからパターンへのマッピング

付録C：行動を変える

2021年に私たちは、人的要素がデータ漏洩/侵害の85%に影響を与えていると報告しましたが、今年はわずかに減少し82%になりました。残念ながら、強力な資産管理や優れた脆弱性スキャンプログラムでも、この問題を解決することはできません。

その代わりに、人々の行動を変える必要があり、それは非常に困難な作業です。どのような方法（変更する理由を与える、トレーニングを行う、またはその2つを組み合わせる）で行うにしても、それがうまくいったかどうかを判断する方法、つまりテストをする必要があります。ここでは、トレーニングの実施に責任を持つ社内部門やベンダーが提供すべきものをまとめた早見表を紹介し、トレーニングが有益かどうかを判断できるようにします。

- あなたが関心を持つ人々の母集団。（テストを医療法人や特定の部署だけで実施した場合、母集団は「誰でも」ではなく「医療法人の社員」とすべき）
- 証明または反証できる測定可能な結果。（例えば、「トレーニングの1日後に届いたフィッシングに関するアンケートの正解率が上がった」、「フィッシングメールをクリックした人が減った」など。）
- 結果を変えるかどうかをテストするための介入。（「フィッシングをクリックしないための15分間のビデオを見る」）
- 結果のベースラインを提供するための対照。（「何もトレーニングを受けなかった」、「フィッシングに関する文章を一段落読んだ」、「マンガを読んで昼寝をした」など。）
- 無作為割り当て。（「200人の従業員が研究に参加するために選ばれ、100人を対照に、100人を介入として無作為に割り当てた」）
- テストの条件も共有すること。（「参加者は、毎年の必須トレーニングとして、会社のトレーニングツールを介して、対照または介入を送られた。」）

このテストは、あなたのために特別に実施されたものかもしれませんし、トレーナーがすでに実施したテストかもしれません。母集団や結果などがあなたの会社に近いものであれば、問題にはなりません。

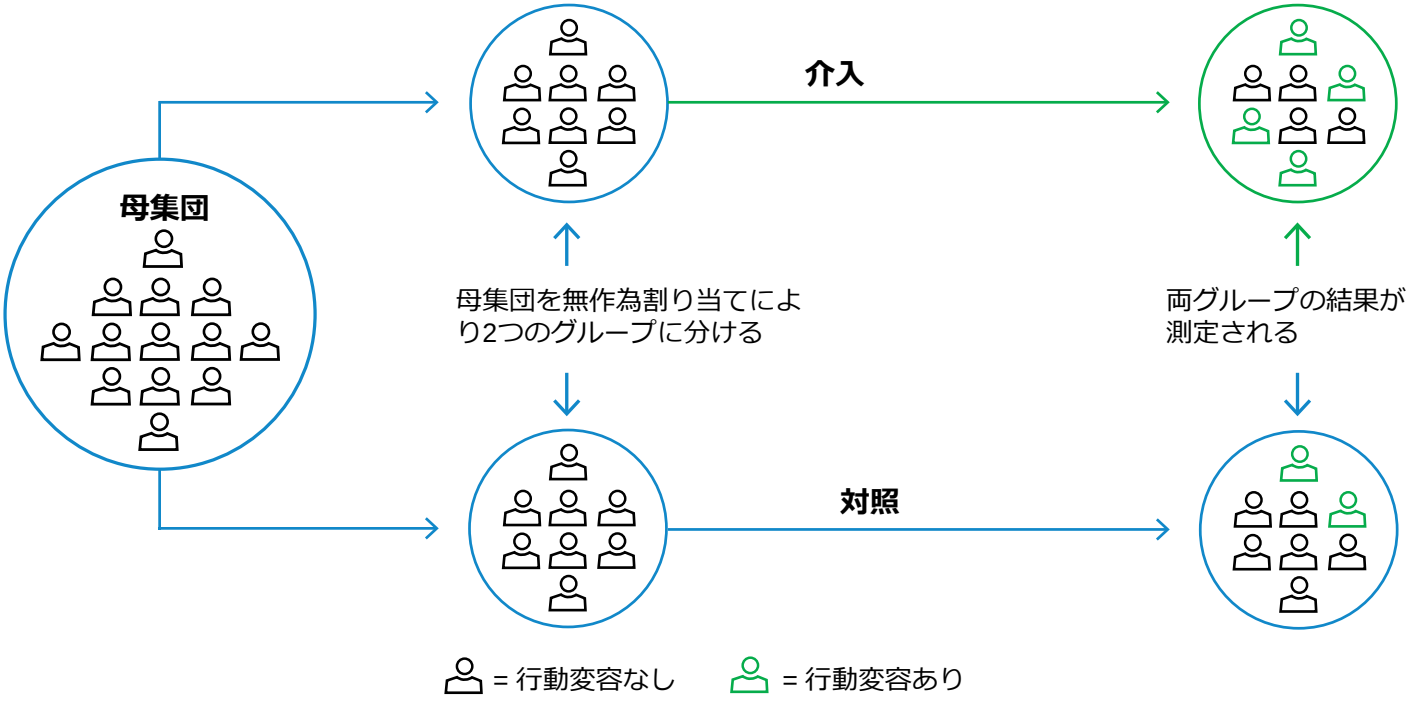


図120. 無作為化対照試験

結果の報告の仕方は、試験の実施方法と同様に重要です。以下に、結果に期待すべきことをいくつか挙げます。

- 信頼区間のある結果。（対照で10人がフィッシングメールをクリックし、介入で1人しかクリックしなかった場合、10-1=9人がクリックすると思ったが、クリックしなかったということです。これは9/10、つまり90%の効果です）。しかし、この1つの数字がすべてを語っているわけではありません。もし、そのうちの何人かがまぐれ当たりだったらどうでしょう？その結果、DBIRの範囲と同じような範囲（信頼度95%で70%から100%の効果など）が得られるはずです。（ちなみに、範囲に0%が含まれている場合、トレーニングが実際には何もしていない可能性があります）。結果の質問がイエス/ノーの場合、信頼度だけでかまいません。（「介入によって人々は98%の信頼度で変化した」）
- 結果は時間とともに変化することがあるので、結果がいつ測定されたかを知っておく必要があります。「結果は介入後30日目であった。」
- トレーニングを受けるのを拒否する人がいたらどうするか？それはドロップアウトと呼ばれ、結果にとって重要です。結果は、誰が脱落したかを示すべきです（できればフルネームで、同僚の前で恥をかかせることができるように。まあ、実際にはしなくても）。（技術に精通した従業員の20%が介入トレーニングを受けず、対照トレーニングを受けなかったのはわずか2%であった」）。ドロップアウトは、記録された他のどの特性（産業、世界の地域、部署、年齢など）でも起こりうるので、大きな違いが見つかった場合は、その特性でも結果を分ける必要がある。（「ハイテクに精通した人たちは98%変わったが、精通していない人たちは70%しか変わらなかった」）
- また、定性的な質問もあるべきです。時には、何がわからないのかがわからないこともあります[38]。その場合は、より客観的な結果に加えて、トレーニングに関する自由形式の質問も用意する必要があります。また、「コンピューター関連の正式な教育や仕事を持っていますか？」といった質問をする機会もあります。そして、このことの重要性は、上記のドロップアウトの箇所でおわかりいただけると思います。「他に何かお知りになりたいことはありますか？」と尋ねれば、トレーニングは効果的であったが、多くの人がそれを非常に不快に感じていることがわかるかもしれません。

残念ながら、何かがうまくいくことを保証する方法はありません。しかし、上記の情報（母集団/Population、結果/Outcome、介入/Intervention、対照/Control、無作為/Random、条件/Conditions）と（結果/Results、時期/When、ドロップアウト/Dropout、定性/Qualitative ）を得ることができれば、努力に見合う何かを得ていると、それなりに確信することができます。ですから、この簡単な頭文字を覚えておいてください。POICRCとRWDQです。

38 ラムズフェルドのパラドックスと呼ばれることが多いです。

付録D：
米国シークレットサービス

David Smith
米国シークレットサービス
アシスタントディレクター

Jason D. Kane
米国シークレットサービス
犯罪捜査部
担当特別捜査官

変化し続けるサイバー犯罪を阻止するための捜査手法の進化

ここ数年、私たちの生活、仕事、交流のあり方は劇的に変化しています。新型コロナウイルス感染症流行の間にインターネットプラットフォームの利用が増えたことは、人々の情報技術への経済的依存度が高まり、それに伴いサイバー犯罪のリスクも高まっていることを明確に示しています。国際的なサイバー犯罪者は、その能力を拡大し続け、金銭的、政治的な動機に関係なく、危害を加える能力を高めています。

犯罪活動の面では、2021年に暗号通貨が関与する犯罪が増加しました。これには、デジタル恐喝スキーム（ランサムウェアを含む）、デジタル資産の実質的価値をコントロールする認証情報や秘密鍵の盗難、分散型金融（DeFi）システムの操作、多様な違法行為を可能にする新しいマネーロンダリング手法などが含まれます。国際的な犯罪者は、従来の物理的な資産や仲介する金融システムではなく、暗号通貨やその他のデジタル資産を利用するようになってきています。暗号通貨はスーパーボウルの広告に登場したこともあります。かつてはニッチな市場だったものが、今では投資、取引、そして違法行為にも利用されるなど、現代生活の一部として広がりを見せています。

1865年の創設以来、米国シークレットサービスは、我が国の金融システムを守るため、捜査戦略や手法を絶えず進化させてきました。私たちはもはや馬に乗って偽造者を追いかけるのではなく、世界中のサイバー犯罪者を特定し逮捕することで、サイバー詐欺を防止することに注力しています。シークレットサービスがDBIRの開発に初めて参加した2010年、私たちが目にしていた最大のリスクは、詐欺に使用するためのペイメントカードや個人情報データの盗難でした。今年の報告書が示すように、このリスクはまだ存在していますが、インターネットを不正に利用する者たちによって新しいスキームが開発されていることがわかります。

進化する犯罪行為に対応するため、米国シークレットサービスは、企業と法執行機関がリスクを軽減するために効果的な行動を取れるようにするための提携に重点を置いています。DBIRは、この重要な部分を担っており、集約されたインシデントレポートの分析から得られた勧告を提供しています。また、サイバー詐欺対策本部や、2021年度に国立コンピューター科学捜査研究所（NCFI：National Computer Forensics Institute）で訓練を受けた3,000人以上の「州・地方・部族・準州政府（SLTT：state, local tribal and territorial）」法執行官の活動を通じて、パートナーを支援しサイバー事件を防止しています。私たちは、グローバル捜査センター（GIOC：Global Investigative Operations Center）の専門調査員グループを通じて、これらの活動をグローバルに調整し、被害者への盗難資産の回収・返還から責任者の逮捕まで、最も効果的な結果を達成することに重点を置いています。

米国シークレットサービスは、今日の犯罪行為を阻止することに重点を置きながら、すでに将来のサイバー犯罪に備えた訓練と準備を始めています。

昨年は、ランサムウェアが企業、重要インフラ、国家安全保障に対するランサムウェアの影響が増大していることが明らかになりました。ランサムウェアのネットワークが最も盛んなのはロシア語圏ですが、この犯罪は1つの国や地域に限定されるものではありません。ある業界の推計によると、ランサムウェアに対する支払いの74%はロシアが絡んでいました。また、ランサムウェアと機能的に類似しているものの、支払い手段を持たない破壊型マルウェアの使用も確認されています。このような動きは、ランサムウェア対策における一部の国の限られた協力と相まって、政治的および金銭的な動機によるサイバー犯罪の区別を曖昧にするリスクの拡大を物語っています。このリスクは、コンピューターシステムの耐障害性を向上させ、攻撃者を逮捕することによってサイバーセキュリティを改善する上で、なぜパートナーシップが不可欠なのかをより明確に示しています。

国境を越えたサイバー犯罪は困難な課題であるにもかかわらず、米国シークレットサービスはこれらの事件を執拗に追及しています。2021年、シークレットサービスはサイバー犯罪ネットワークに対抗するため、多数の多国籍作戦を主導またはこれらに参加しました。例えば、オランダ警察および欧州警察と多国籍作戦を実施し、71カ国で1,800人以上の被害者を出したランサムウェア攻撃の責任者複数人を逮捕しました。昨年度、シークレットサービスは合計で700件以上のネットワーク侵入に対応し、23億ドル以上のサイバー犯罪による金銭的損失を阻止しました。

個人情報の盗難と詐欺は、現在も国境を越えたサイバー犯罪者の中心的活動であり、盗まれた個人を特定できる情報を利益に変える手段を提供しています。新型コロナウイルス感染症の流行は、犯罪者が救済プログラムを詐取したため、この種の詐欺の新たな機会を生み出しました。これを受けて、米国シークレットサービスは、金融機関と連携して不正な支払いを防止・回収することに重点を置くため、国家パンデミック不正回収コーディネーター（National Pandemic Fraud Recovery Coordinator）を任命しました。こうした努力の結果、米国シークレットサービスは12億ドル以上を回収し、不正に取得された23億ドル以上の資金を返還し、100人以上を逮捕しました。

世界がデジタル化するにつれ、テクノロジーで互いにつながるだけでなく、モノのインターネット（IoT）のような多種多様なデバイスにつながるようになりました。その他、量子暗号、5G無線技術、人工知能（AI）など、近い将来サイバー犯罪者のターゲットになる可能性のある新技術が登場しています。これらの技術は、生活を向上させ、新たなコミュニケーションラインを開く可能性を秘めています。逆に、サイバー犯罪者は、これらの技術を悪意のある利益のために利用する方法を模索することでしょう。米国シークレットサービスでは、今日の犯罪行為を阻止することに重点を置いていますが、すでに将来のサイバー犯罪に備えた訓練と準備を始めています。

サイバー犯罪を防止するには、サイバーセキュリティの強度を高め、犯罪者を追及して不正な利益を押収し、将来の犯罪を抑止・防止するなど、多方面にわたる戦略が必要です。これらの取り組みはいずれも、集約されたインシデントレポートの分析、およびDBIRが提供する証拠に基づく勧告によって強化されます。2022年、米国シークレットサービスはパートナーシップをさらに強化し、変化するテクノロジーの使用とそれを悪用する犯罪者に対して先手を打ち、そしてサイバー犯罪者から彼らが安全に隠れる場所を取り上げることができるのを楽しみにしています。

付録E：ランサムウェアに絡むコスト

過去の報告書では、ランサムウェアやその他の侵害が被害者にもたらす損害について延々と語ってきました。しかし、攻撃者がどのような経済効果をもたらすかについては、これまで検証してきませんでした。このような別の視点から、有益な知見を得ることができるかもしれません。

そこで、バリューチェーンのターゲティングおよび配信データ、フィッシングテストの成功率データ、犯罪者フォーラムのデータ、ランサムウェアの支払いデータなどを組み合わせて、犯罪者側から見たビジネスの実態を推定してみました。

まず、アクセスにかかるコストを検証してみましょう。図121は、攻撃者の汚れた仕事をさせるために（犯罪）専門サービスを雇うコストを示しています。このような（またはアクセスのための内部スタッフを擁するさらに大規模な）犯罪組織は、よりリスクが高く、より大きな報酬を得るための攻撃を行う可能性があります。

小規模な犯罪者は、技術者ではなく、どちらかと言えば経営者です。彼らはコストを最小限に抑えようとするため、専門的なサービスには金をかけません。その代わり、認証情報、フィッシング用メール、脆弱性、ボットネットへのアクセスといった形態のアクセス商品を直接購入します。図122は、そのコストのイメージを示しています。10万ドルどころか、大半のアクセス商品は1ドルもかかっていません。これは、クリック率の中央値がわずか2.9%であっても、ほとんどのアクセスが信じられないほど安価なメールであるためです。ボットへのアクセス、ログイン認証、脆弱性に関する知識といった形態で直接購入もしますが、主体はあくまでもメールです。

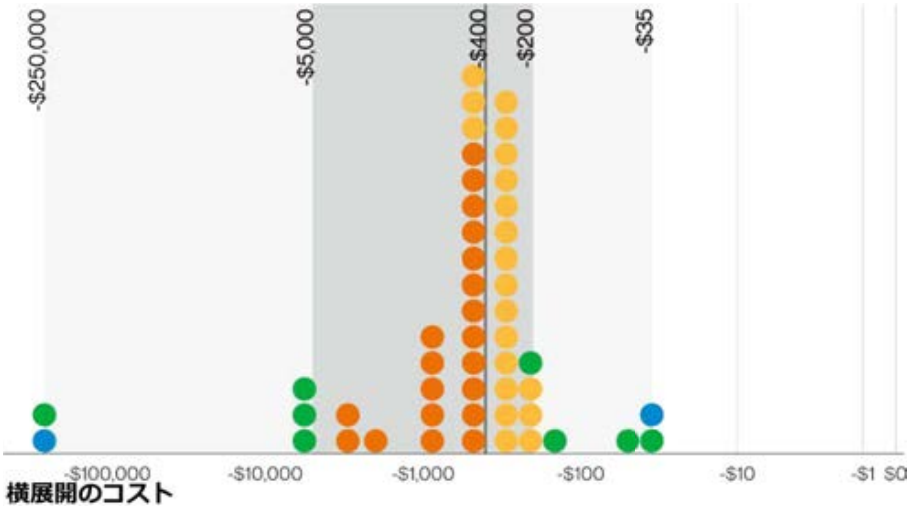


図121. 熟練侵入サービスのコスト（対数スケール）
犯罪フォーラムデータ3,000回分のシミュレーションに基づく

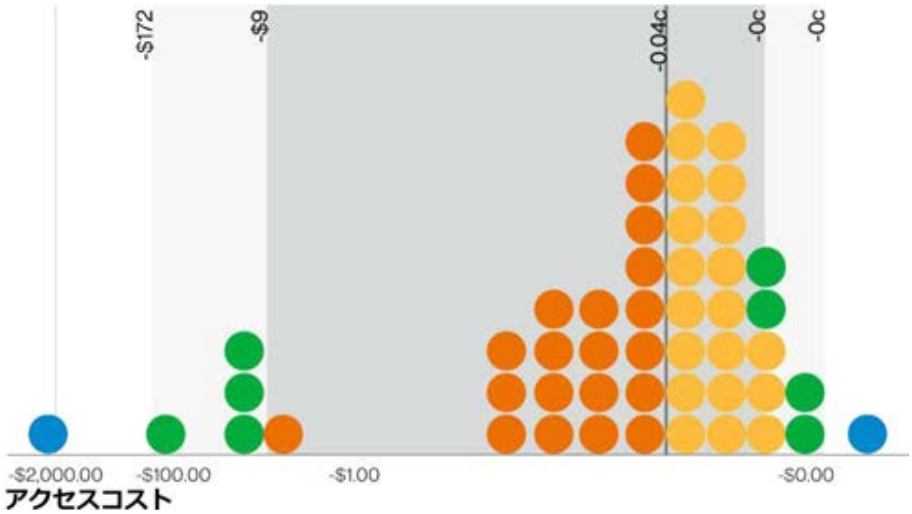


図122. アクセスにかかるコストのシミュレーション（対数スケール100）
（フィッシング、認証情報、脆弱性、ボットネット）

図122のコストと図123の利益を対比してみましょう。ランサムウェアのインシデントの60%は利益がなく、図に表示されていません。1ドル近くの利益が大半です。しかし、中央値は100ドル強です。図124は、同じ利益を時系列で追跡したものです。300回のシミュレーション身代金の後、攻撃者は600,000ドル以上の金銭を得ています[39]。

これが異常であるかどうかを確認するために、500人のランサムウェアの攻撃者をシミュレーションしたところ、1.4%が損失を示しました[40]。しかし、300件のインシデント後の利益の中央値は178,465ドルであり、シミュレーションのトップは3,572,211ドル稼いでいます。

つまり、ランサムウェアはビジネスというよりも宝くじ[41]のようなものだということです。アクセスに賭け、40%の確率で当たりくじを引き当て、数ドルから数千ドルの支払いを受けます。しかし、より実行可能なものを求めて、アクセスに焦点を当てます。もし攻撃者が、侵入するために、アクセス製品ではなく、専門サービスにお金を払わなければならないのであれば、皆様が標的にされる可能性はかなり低くなります。ボットを排除するためにアンチウイルスを使用し、脆弱性の露出を防ぐためにパッチ、フィルタリング、資産管理を実施し、認証情報の露出を最小限に抑えるために2要素認証とパスワード管理アプリの使用を標準化することです。最後に、メールは最大の攻撃経路であるため、人的要素も無視できません。まず、メールとWebのフィルタリングを行い、次にトレーニングを行うことです（トレーニングがうまくいっているかどうかを確認する方法については、付録Cの「行動を変える」を参照してください）。

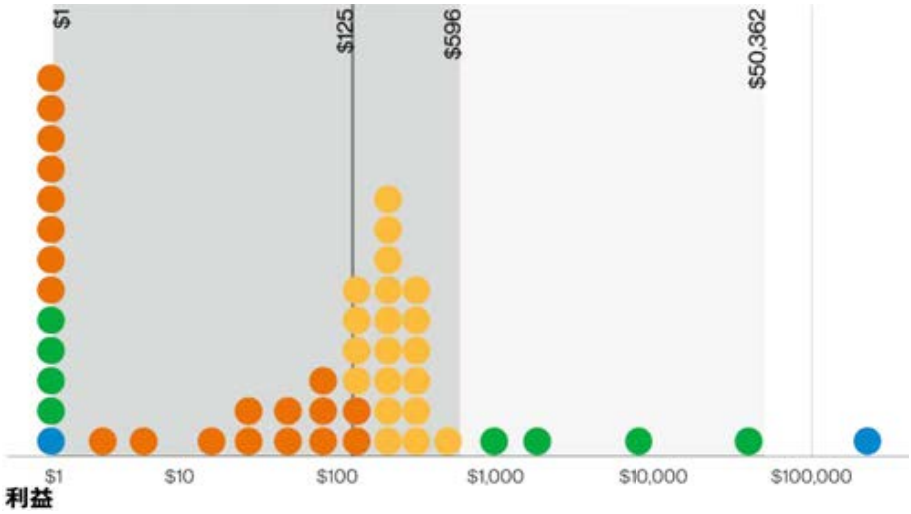


図 123. ランサムウェアインシデントによる利益のシミュレーション （対数スケール）

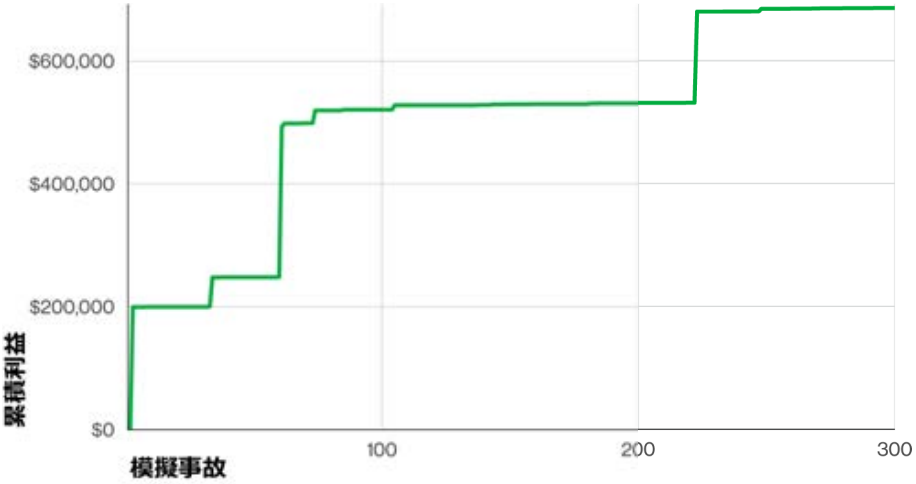


図 124. シミュレーションされたランサムウェア攻撃者の利益の経時的変化

39 非課税を想定しています。
40 誰もが商売上手になれるわけではないと思います。犯罪者であっても。
41 『Winning the Ransomware Lottery:A Game-Theoretic Model for Mitigating Ransomware Attacks』 でErick Galinkinも示唆しているように。https://doi.org/10.48550/ arXiv.2107.14578

付録F：協力企業

A

Akamai Technologies

Ankura

Anomali

Apura Cybersecurity Intelligence

AttackIQ

Atos

B

Bad Packets

bit-x-bit

Bitsight

Blackberry Cylance

C

Center for Internet Security

CERT European Union

CERT Division of Carnegie Mellon University's Software Engineering Institute

Chubb

Coalition

Computer Incident Response Center Luxembourg（CIRCL）

Coveware

Crowdstrike

Cybersixgill

Cybercrime Support Network

Cybersecurity and Infrastructure Security Agency（CISA）

D

Defense Counterintelligence Security Agency（DCSA）

Digital Shadows

Domain Tools（formerly Farsight Security）

Dragos, Inc.

E

EASE（Energy Analytic Security Exchange）

Edgescan

Elevate Security

Emergence Insurance

EUROCONTROL

F

Domain Tools（formerly Farsight Security）

Financial Services ISAC（FS-ISAC）

Fortinet

G

Global Resilience Federation

Grey Noise

H

HackedEDU

Hasso-Plattner Institut

J

Jamf

JPCERT/CC

K

K-12 SIX—（K-12 Security Information Exchange）

Knowbe4

Kordamentha

L

Lares Consulting

Legal Services—ISAO

LMG Security

Lookout

M

Malicious Streams

Maritime Transportation System ISAC（MTS-ISAC）

Micro Focus

mnemonic

N

NetDiligence®

NETSCOUT

NINJIO Cybersecurity Awareness Training

P

Paraflare Pty Ltd

PSafe

Q

Qualys

R

Ransomwhe.re

Recorded Future

S

S21sec

SecurityTrails

Shadowserver Foundation

Shodan

SISAP - Sistemas Aplicativos

Swisscom

V

VERIS Community Database

Verizon Cyber Risk Programs

Verizon DDoS Shield

Verizon Mobile Security Dashboard

Verizon Network Operations and Engineering

Verizon Professional Services

Verizon Sheriff Team

Verizon Threat Intelligence Platform

Vestige Digital Investigations

Verizon Threat Research Advisory Center（VTRAC）

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）

ウォッチガード・テクノロジー

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

デル

は

パロアルトネットワークス

プルーフポイント

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

Akamai

apura

ANOMALI

Atos

ATTACKIQ

BAD
PACKETS

BITSIGHT

bit-x-bit

BlackBerry.
Intelligent Security. Everywhere.

CERT-EU

CIS
Center for
Internet
Security

CIRCL
Computer Incident
Response Center
Luxembourg

CROWDSTRIKE

Cybercrime
SUPPORT NETWORK

CHUBB

CHECK POINT

CYBERSECURITY & INFRASTRUCTURE
CISA
SECURITY AGENCY

Carnegie
Mellon
University
Software
Engineering
Institute

CyberSecurity
MALAYSIA

DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY

COVEWARE

Coalition

cybersixgill

DELL Technologies

digital shadows_

DOMAINTOOLS

DRAGOS

EASE
Energy Analytic Security Exchange

edgescan

Elevate Security

emergence

EUROCONTROL

FEDERAL BUREAU OF INVESTIGATION
INTERNET CRIME COMPLAINT CENTER

FORTINET

FS-ISAC

GLOBAL
RESILIENCE
FEDERATION

GREYNOISE

Hack_EDU

HPI
Hasso
Plattner
Institut
Digital Engineering · Universität Potsdam

IRISS
Irish Reporting and
Information Security Service

jamf

Verizon Cyber Risk Programs

Verizon DDoS Shield

Verizon Mobile Security Dashboard

Verizon Network Operations and Engineering

Verizon Professional Services

Verizon Sheriff Team

Verizon Threat Intelligence Platform

Verizon Threat Research Advisory Center (VTRAC)

verizon