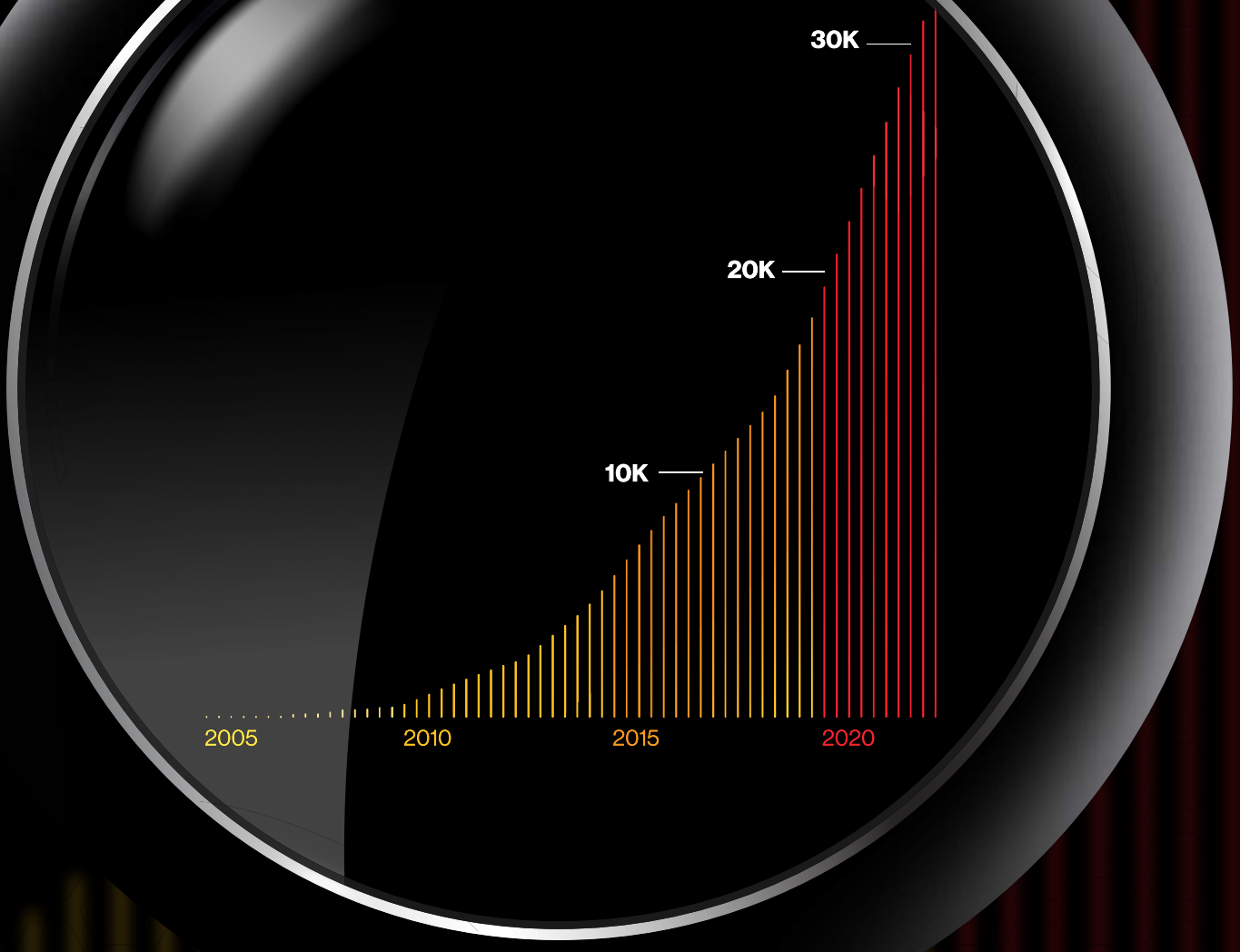
DBIR

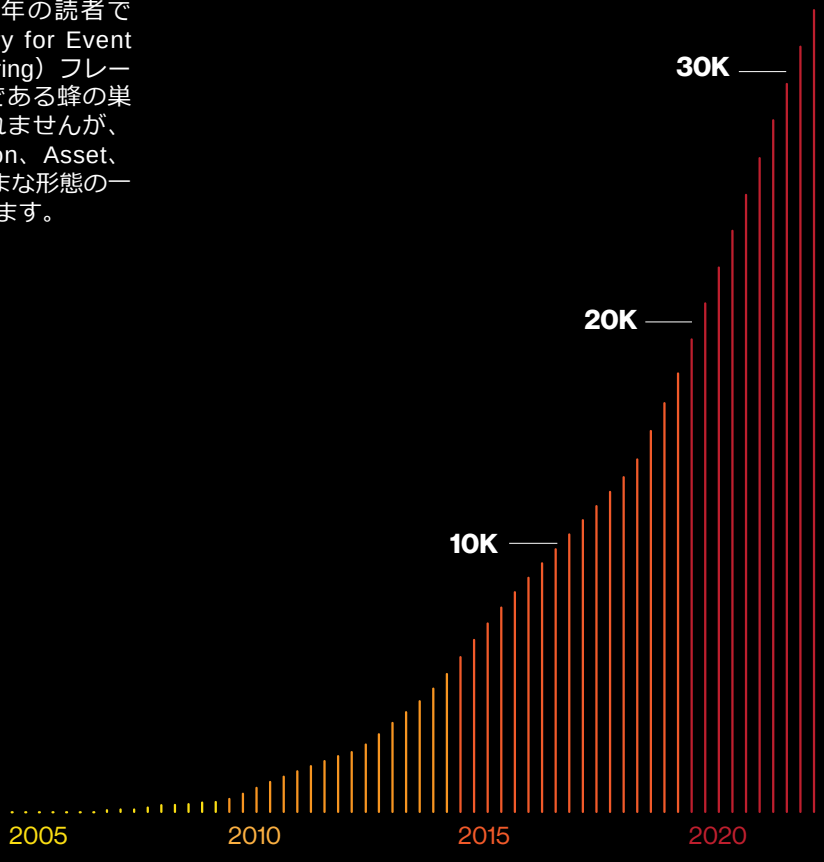
2023年度データ漏洩/侵害調査報告書



verizon

表紙について

表紙の拡大鏡は、コアとなる漏洩/侵害データセットにエネルギーとリソースを再度集中させるためにDBIRチームが行った努力を視覚的に伝える意図があります。拡大されているグラフは、最初のレポートから年月が経つにつれて、データセット内の漏洩/侵害件数を累積的にカウントしたものです。長年の読者であれば、VERIS（Vocabulary for Event Recording and Incident Sharing）フレームワークのトレードマークである蜂の巣パターンにお気づきかもしれませんが、これは4つのA（Actor、Action、Asset、Attribute）とそれらのさまざまな形態の一覧を伝えることを意図しています。



目次

本書の凡例と定義

2023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フレームワークのリソース

「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 Event Recording and Incident Sharing（VERIS）」で使用される用語の一部です。以下に、各用語の定義を示します。

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[1]、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。

- **https://github.com/vz-risk/dbir/tree/gh-pages/2023** – DBIRの結果、図および図内データ。
- **https://verisframework.org**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。
- **https://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。例えば、「分散型サービス拒否（DDoS）」攻撃は、データの流出がないため、ほとんどの場合、データ漏洩/侵害ではなくインシデントに分類されます。だからといって、深刻度が低くなるわけではありません。

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

1 組織的犯罪集団とは、米国人気ドラマの主人公、Tony Sopranoやその愉快な仲間たちではなく、これを生業とし、繰り返し使用する決まったプロセスを持つ集団を意味します。

すみません、これらはすべていつ起こったことですか？

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、2021年11月1日から2022年10月31日の間に発生したものです。**2022年の取扱件数は、2023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。

自分たちのデータに自信をもつ

2019年に斜めカットの棒グラフを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斜めカット、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。

斜めカットの棒グラフとよく似て、スパゲッティチャートも、時間という要素が加わり多少複雑にはなっていますが、信頼区間内に存在する可能性のある値という同じ概念を表しています。個々の糸は、各観測の信頼区間内に存在するポイント間のすべての可能なつながりのサンプルを表します。見てわかるように、いくつかの糸は他よりも緩く、より広い信頼区間とより小さい標本サイズを示しています。

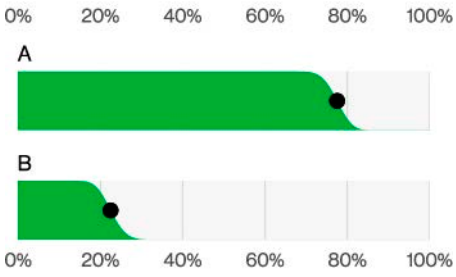


図1. 斜めカットの棒グラフの例（n=205）

斜めカットの棒グラフは、毎号のDBIRの読者にはおなじみのものです。棒グラフの斜めカットは、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）の棒グラフの斜めカット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）。

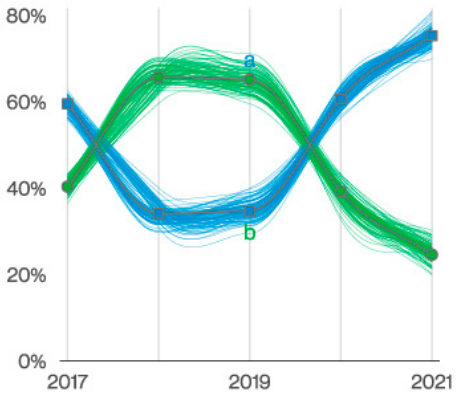


図2. スパゲッティチャートの例

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。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、斜めカット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。

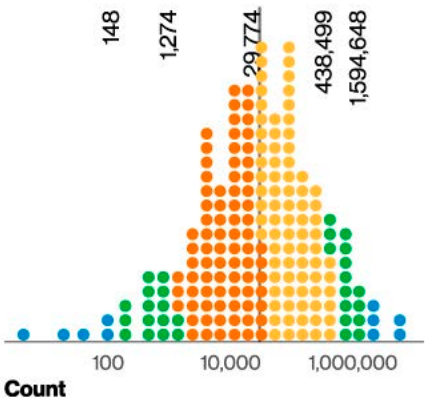


図3. ドットプロットの例（n=672）。各ドットは組織の0.5%を表す。
オレンジ：80%の下半分。黄色：80%の上半分。緑：80%–95%。青：異常値。
組織の95%：148–1,594,648。80%：1,274–438,499。中央値：29,774（対数スケール）

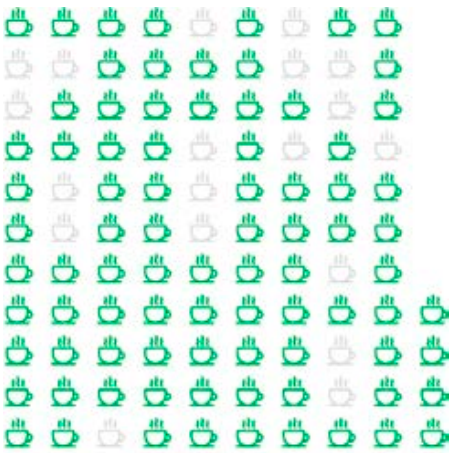


図4. ピクトグラムプロットの例（n=4,110）。それぞれ図柄は40のデータ漏洩/侵害

信用に値するところは信用します

この報告書の内容を引用されたい方がいるらしく、引用する際の条件についてよく質問を受けます。

本DBIRの統計、図表、その他の情報は自由に引用することができます。ただし、（a）出典を「Verizon 2023 Data Breach Investigations Report（ベライゾン2023年度データ漏洩/侵害調査報告書）」と明記し、（b）内容を一切改変しないことを条件とします。正確に引用する場合は問題ありませんが、言い換えをする場合には私たちの審査を受ける必要があります。報告書を他の方に渡したい場合は、このPDFをコピーするのではなく、verizon.com/dbirへのリンクを提供するようお願いいたします。

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、X：
@VerizonBusinesswith #dbir
データにご不明な点がありましたら@VZDBIRにポストしてください。

毎年発行されるこのベライゾンDBIRのデータ提供者になることにご興味を持たれた方は（そうであってほしい）、その手続きはとても簡単でわかりやすいものです。**dbircontributor@verizon.com**宛にメールを送信していただくだけです。

はじめに

「成功とは、意欲を失わずに失敗に次ぐ失敗を繰り返すことである」。
これはウィンストン・チャーチル卿の言葉です。

ベライゾンの2023年度データ漏洩/侵害調査報告書（DBIR）へようこそ。サイバー犯罪の卑劣な実態を調査し、そこからどのような教訓を得ることができるかを探る本報告書に、再びお付き合いいただけることを嬉しく思います。私たちが新しい防衛戦略や機器、あるいはPlease-Save-Us-As-A-Service（サービスとして保存してください）を作成したり、買ったり、借りたりするたびに、敵も同じように素早く適応し、攻撃するための新たな視点を見つけているように感じることがよくあります。このような状況はすでに十分に不幸なことですが、古い戦術でもまだそれなりに通用するために戦術を進化させる必要すらない場合には、さらに事態は悪くなります。

「めちゃくちゃ安全」から「あまり安全でない」までのスペクトルのどの位置にいるかにかかわらず、上記の引用はサイバーセキュリティ（そして人生全般）に対する良いロードマップと言えます。本報告書は、物事が意図したとおりに動かなかった場合に参照し、指弾するためではなく、私たち全員が学び、状況を改善させていくことを目的としています。企業や個人を問わず、ほとんどすべての人がより少ない労力でより多くのことを行う方法を模索している今、私たちの防御策がいつ失敗したかを詳細に分析することは非常に有益であると私たちは信じています。大きな変化の時は常に困難が伴うものですが、そのような時はしばしば自分たちの状況を把握し、必要であれば、自分たちの視点とエネルギーの両方に焦点を当て直すように促されます。今年のDBIRもそうでした。私たちはチームとして、現在の地位を築いた根本的なもの、つまりベライゾン独自のVERISフレームワークを使って分析した実際のデータ漏洩/侵害に集中的に焦点を当てることにもう一度立ち返ることにしました。VERISといえば、MITRE EngenuityおよびCenter for Threat Informed Defense（CTID）との共同作業により、VERISとMITRE ATT&CKのマッピングがさらに強化されました[2]。また、DBIRチームの親組織であるVerizon Threat Research Advisory Center（VTRAC）[3]が、私たちの分析のためにこれまでで最も多くの漏洩/侵害情報を提供してくれたことも助けになりました。ちなみに今年はVTRACが設立されてから20周年にあたります。お祝いのケーキを残しておいてほしいですね。

長年の読者であればご存知のように、ここ数年、さまざまな形の調査や分析を行なう中で、データ漏洩/侵害の発見に深みと奥行きを持たせるために、インシデント以外のデータを活用することが増えてきました。このような取り組みが私たちの仕事の大部分を占めることに変わりはありませんが、前述のとおり、今年はより直接的にデータ漏洩/侵害の側面に焦点を当てるべく、意図的な措置を講じました。この結果、報告書をより簡潔にし、扱いにくさを軽減することができたのです。今年は16,312件のセキュリティインシデントを分析し、そのうち5,199件にデータ漏洩/侵害が確認されました。いつものように、この情報が有益で、役に立ち、理解しやすく、行動に移しやすいものであることを願っています。

最後に、本報告書の作成にご協力いただいた世界中のデータ提供者の皆様に心より感謝申し上げます。もちろん、読者の皆様にも同様のことが言えますので、引き続きご支援を賜りますようお願い申し上げます。

敬具

DBIRの執筆陣（DBIRチーム）
C. David Hylender、Philippe Langlois、Alex Pinto、Suzanne Widup

Verizon Threat Research Advisory Center（VTRAC）のDave KennedyとErika Giffordに対し、本報告書への継続的支援と毎年の貢献、およびVerizon Business Product Data Science TeamのKate Kutchko、Marziyeh Khanouki、Yoni Fridmanの貴重な支援に対し、心より感謝いたします。
Gabriel Bassettには、長年にわたり統計計算とチャートをご提供いただきました（そしてひどいジョークも！）。新天地でのご活躍を祈ります。

2 https://mitre-engenuity.org/cybersecurity/center-for-threat-informed-defense/
3 https://www.verizon.com/business/resources/reports/verizon-threat-research-advisory-center/

主な調査結果

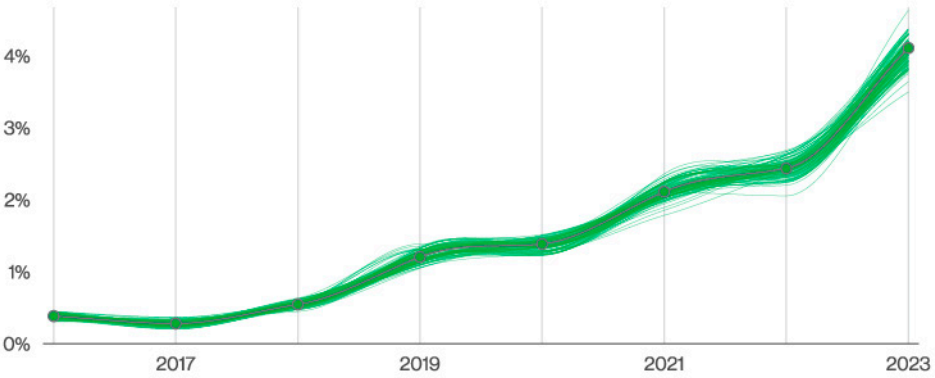


図5.「なりすまし」（プレテキスティング）インシデントの経時的変化

「ソーシャルエンジニアリング」攻撃は、通常、サイバー犯罪者にとって極めて利益の出る、効果の高い攻撃です。図5に見られるように、「ビジネスメール詐欺（BEC）」攻撃（要するに「なりすまし」（プレテキスティング）攻撃）がインシデントのデータセット全体でほぼ倍増し、「ソーシャルエンジニアリング」パターンにおけるインシデントの50%以上を占めるまでになったのは、このためかもしれません。

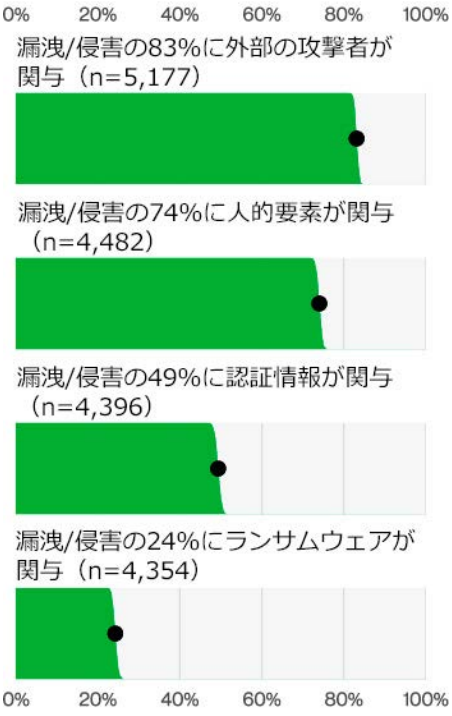


図6. 主な要因の上位一覧

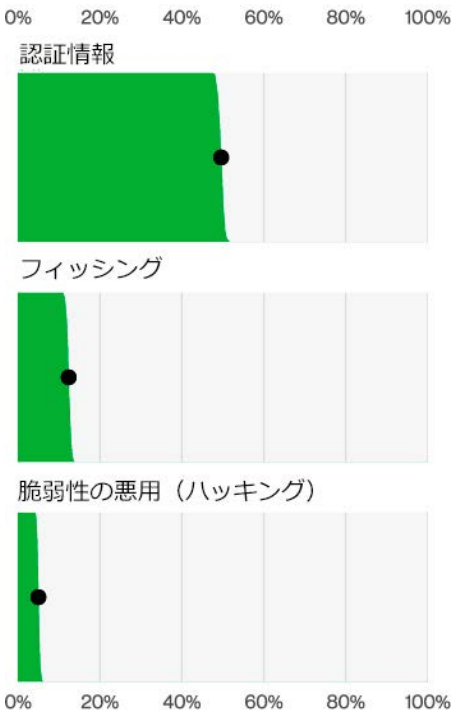


図7.「エラー」/「悪用」を除いたデータ漏洩/侵害の要因の上位一覧（n=4,291）

データ漏洩/侵害の74%が人的要因となっており、「エラー」、「特権の悪用」、「盗まれた認証情報の悪用」、「ソーシャルエンジニアリング」などのすべてに人が関与しています。

データ漏洩/侵害の83%は「外部」の攻撃者が関与しています。また、攻撃の主な動機は依然として金銭目的であり、その割合は95%に達しています。

攻撃者が組織内に入り込む主な手段は、盗まれた認証情報、フィッシング、脆弱性の悪用の3つです。

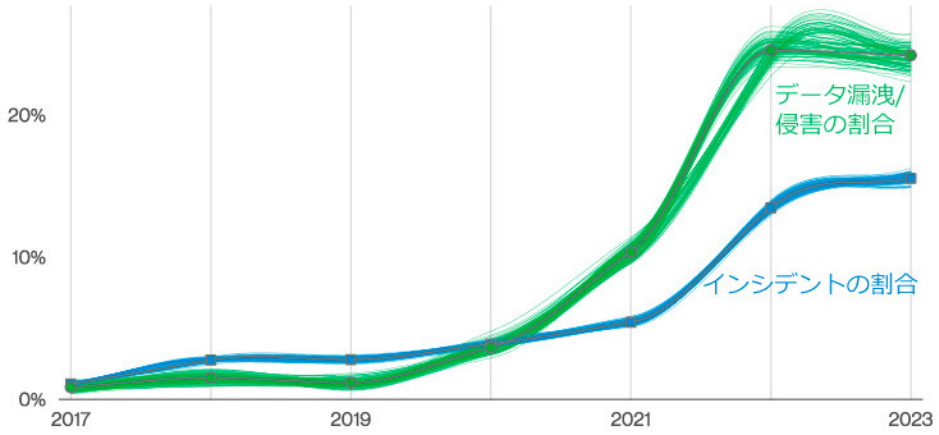


図8. ランサムウェア攻撃の経時的変化

「ランサムウェア」は、データ漏洩/侵害を引き起こす「攻撃」タイプの上位に君臨し続け、実際には増加しなかったものの、統計的には24%で安定した状態を維持しています。「ランサムウェア」攻撃は、あらゆる規模および業種の組織にわたり、広範に発生しています。

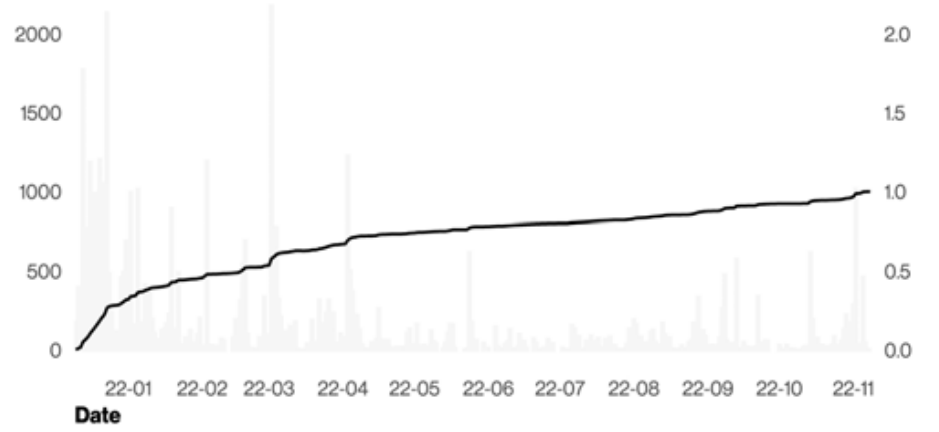


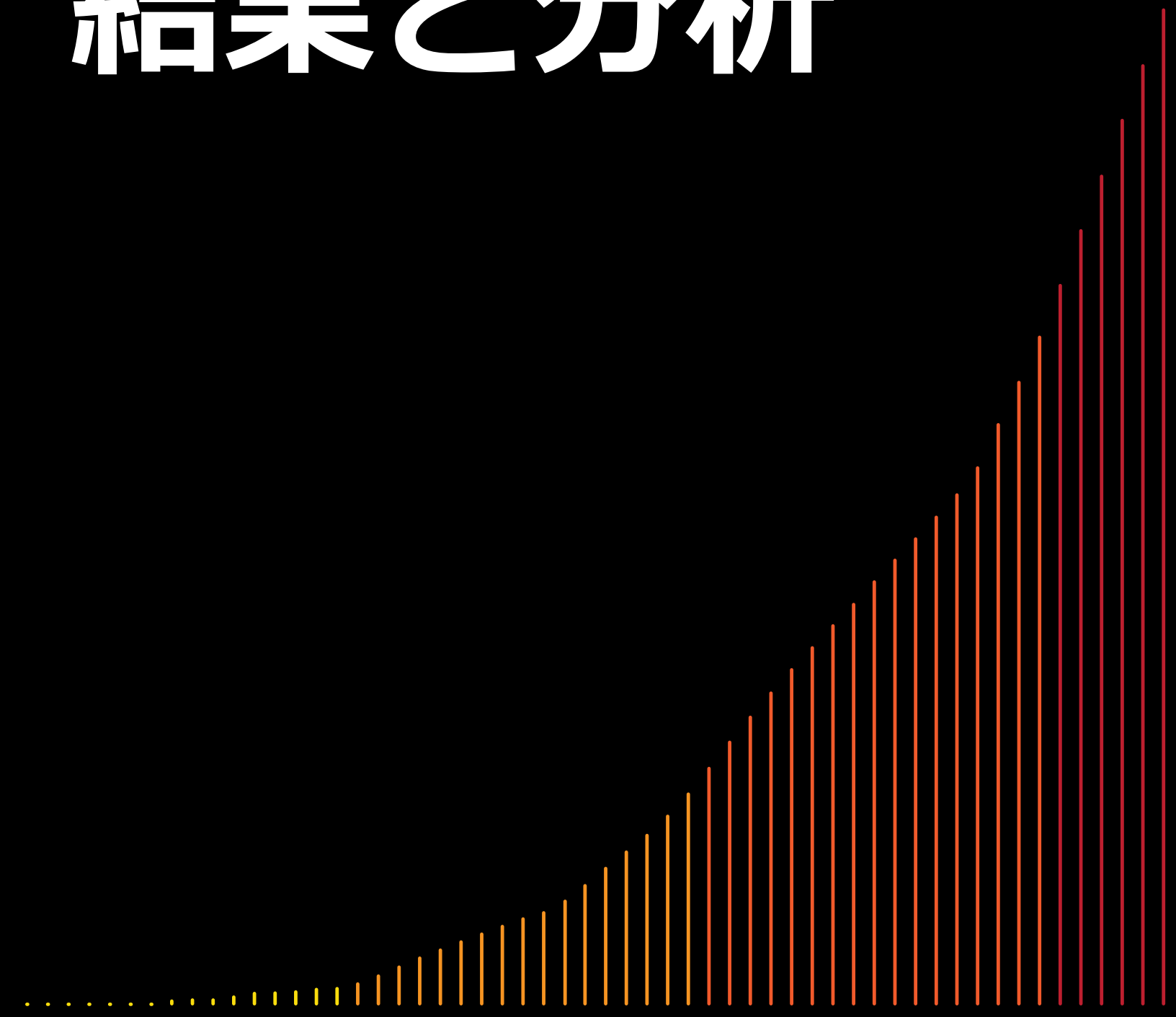
図9. 2022年のLog4jスキャニングの割合

この1年間に発生したLog4jスキャニングの32%以上がそのリリースから30日以内に実行されています（最も急増したのは17日以内）。

図10. 確認された脆弱性の悪用がLog4j関連であった割合（n=81）
コーヒーカップはそれぞれインシデントを表す。

Log4jは、データ提供者のインシデント報告において非常に重要視されており、「脆弱性の悪用」を手口とするインシデントの90%は、コメント欄に「Log4j」または「CVE-2021-44228」と記載されています。ただし、コメントが付けられたインシデントは全体の20.6%に過ぎません。

2
結果と分析



結果と分析：概要

この「結果と分析」セクションでは、今年の分析データから見つかった主なものを紹介します。このデータセットは、ベライゾンのVTRACスタッフによる調査、データ提供者からの報告、一般に公開されたセキュリティインシデントなど、さまざまな情報源から収集されたものです。

データ提供者の入れ替わりが激しいため、さまざまなタイプのセキュリティインシデントとその発生国に関する幅広い情報を確実に入手することを優先事項のひとつとしました。このような貢献者の入れ替わりは、明らかに分析対象となるデータセットに影響を与えるため、そのような潜在的な偏りについて、可能な限り背景情報を提供するつもりです。

長年にわたりお気づきの方もいらっしゃるかもしれませんが[4]、DBIRチームが行っているインシデントデータ収集は、VERISフレームワークに基づいています。VERISフレームワークは、私たちチームの複数年にわたるデータセットを構築してきた基盤であり、攻撃状況の傾向が明らかになったときに自信を持って説明できるようにするものです。DBIRのデータセットには現在953,894件のインシデントが含まれており、そのうち漏洩/侵害が認定されているのは254,968件です。インシデントが100万件[6]に達した暁には、皆さんとご一緒に祝杯を上げたいと思います[5]。

VERISでは、インシデントを説明するために、主に「攻撃者」（誰が）、「攻撃」（手口）、「資産」（対象）、「属性」（何を）の4つのカテゴリーを使用しています。「紛れもなく」インシデントであることを特定するには、これら4つがすべて揃っている必要があります。たとえインシデント調査の1日の終わりに、いずれかが見つからなかったとしてもです。VERISのカテゴリーについての詳しい背景については、各サブセクションの説明コラムを参照してください。

それでは、各カテゴリーについて調査結果を見ていきましょう。

4 決まり文句ですので、あしからず。

5 セキュリティインシデント件数を祝うべきかどうかは別として、誰もが四捨五入をしたがります。

6 億万長者になることが私たちのデータセット頭をよぎり、「一斉辞職」に加わって南国のタックスヘイブンでの隠居を決めることにならないことを祈りたいです。

攻撃者

人生は恐ろしく、予測不可能なもの。であればこそ、結果考察を慣れ親しんだ「攻撃者」の分析から始めてみたいのです。人生において確実なのは、死と税金と「外部」の攻撃者だけであると言われますが、まったくそのとおりです[7]。

図11が示すように、「外部」の攻撃者はデータ漏洩/侵害の83%を占めており、「内部」の攻撃者は19%です。「内部」攻撃者は、このようなケースで意図的な被害の要因になっているだけでなく、「エラー」攻撃の要因となる可能性も同様に高い[8]ことを思い起こさせます。いずれにせよ、データ漏洩/侵害の扇動者としての「外部」攻撃者の頻度は、この調査を始めて以来ずっと高止まりしているデータポイントです。

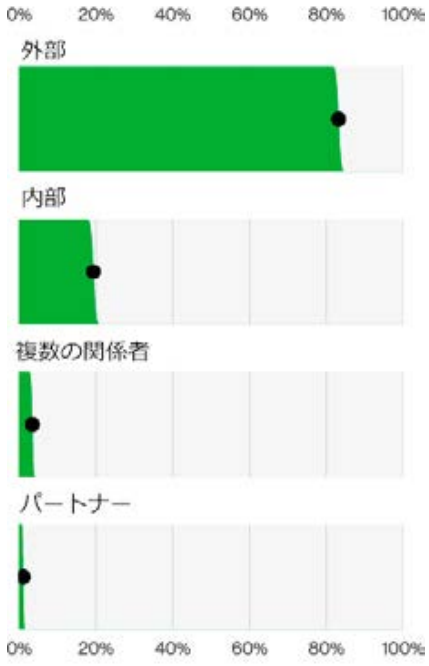


図11. データ漏洩/侵害の要因である攻撃者（n=5,177）

攻撃者のタイプ[9]

外部：外部からの脅威は、組織とそのパートナーのネットワーク以外のソースから発生するものです。たとえば、犯罪グループ、単独ハッカー、元従業員、政府機関などの外部ソースです。これには、神（の「御業」）や「大自然」、偶然といったものまで含まれます。一般的に、外部のエンティティには信頼も特権も存在しません。

内部：内部の脅威は、組織の内部で発生するものです。これには、正社員、契約社員、インターン、その他のスタッフが含まれます。内部関係者は信頼され、特権が与えられています（人によって程度は異なりますが）。

パートナー：パートナーには、サプライヤー、ベンダー、ホスティングプロバイダー、外注ITサポートなど、組織とビジネス上の関係を有する第三者が含まれます。通常、ビジネスパートナーシップには、ある程度の信頼と特権が存在します。攻撃者がパートナーを攻撃経路に利用する可能性がありますが、その場合、パートナーが「攻撃者」になるわけではありません。パートナーがインシデントの引き金になります。

7 そう言われていますよね。
8 本当のところ、実際には2倍にもなります。
9 https://verisframework.org/actors.html

図12. データ漏洩/侵害における攻撃者の「動機」（n=2,328）

DBIRの長年の読者は、「金銭目的」の動機が依然として侵害の大部分を引き起こしているのを見て、同様にショックを受けていることでしょう（図12）。昨年よりもさらに増加し、データ漏洩/侵害の94.6%に達しています。最も活発に活動している外部攻撃者は、「組織犯罪」です（図13）。

しかし、図13で最も興味深いのは、外部の様々な「国家支援型」攻撃者よりも、内部のさまざまな「エンドユーザ」が頻繁に現れていることです[10]。これら組織の従業員は、主に「悪用」（内部での悪意のある行為）と「エラー」（事故）に関与しており、日々のセキュリティ管理で監視を強化すべき対象であることを示唆しています。

このことは、「スパイ活動」を目的とするものであるかどうかにかかわらず、ウクライナ紛争が続いていることから、「国家支援型」の攻撃が増加すると予想されていたことと関連しています。たとえ地政学的な議論に起因するイデオロギーやハクティビズムに関連する攻撃が増加しているという証拠が裏付けの乏しいものであったとしても、それは統計的に大きな意味を持ちません。また、この種の活動は、平均的な読者の組織を混乱させる可能性が低いとも考えられます[11]。

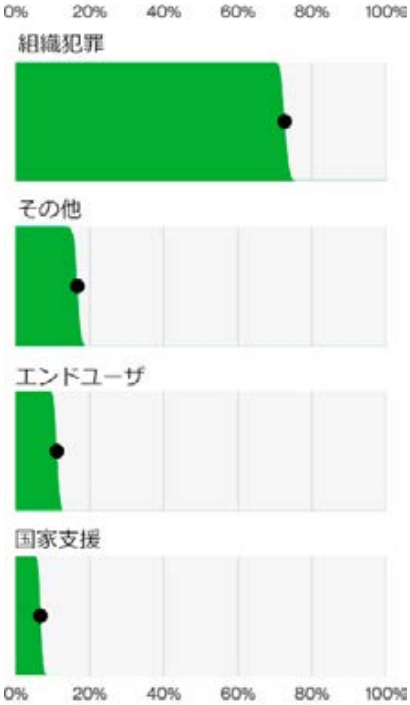


図13. データ漏洩/侵害における攻撃者のタイプ（n=2,489）

10 言ってみれば、アナーキストやその他の国家転覆のイデオロギーにとって大勝利ということです。
11 いいえ、ボンドさん、MI6は平均的な読者の代表ではありませんよ。

攻撃

攻撃とは、その名の通り、私たちの報告内容に大きな影響をもたらすものです。攻撃者はどのような卑劣な行為を企んでいるのでしょうか？この問いに「ランサムウェア」と答えるとしたら、想像力に欠けると言いたいところですが、正解とも言えます。この厄介な「マルウェア」の一種はもう何年も私たちの話題をさらっており、身代金を支払うのに十分な暗号通貨をかき集めることができていません！

図14～図17は、上位を占める「攻撃」の種類（攻撃の詳細）と攻撃の経路（攻撃の手口）を説明しています。

図14. データ漏洩/侵害において上位を占める「攻撃」の種類（n=4,354）

攻撃の種類[12]

ハッキング（hack）：論理的なセキュリティ機能を迂回したり妨害したりすることで、権限なく（または権限を越えて）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（mal）：デバイス上で実行され、所有者の同意なくデバイスの状態や機能を変更す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（err）：誤って、または不注意によって行われた（または行われずに放置された）こと。

ソーシャル（soc）：欺瞞、操作、脅迫などを用いて情報資産の人的要素（ユーザ）を利用すること。

悪用（mis）：委託された組織の資源や権限を、意図された目的または方法に反して使用すること。

物理的（phy）：接近、所有、または力づくの故意の脅威。

環境（env）：地震や洪水などの自然災害だけでなく、資産が置かれている身近な環境やインフラに関連する危険も含む。

12 https://verisframework.org/actions.html

図15. インシデントにおいて上位を占める「攻撃」の種類（n=14,829）

図16. データ漏洩/侵害において上位を占める「攻撃」経路（n=3,194）

図17. インシデントにおいて上位を占める「攻撃」経路（n=10,502）

予想通り、このグラフは、最初のまたは一回の攻撃、特にデータ漏洩/侵害では「盗まれた認証情報の悪用」、インシデントでは「サービス拒否（DoS）」で占められています。これは例年と変化はありません。意外ではないものの、「ランサムウェア」がインシデントの第2位に上り、全インシデントの15.5%を占めていることが気にかかります。一方、データ漏洩/侵害では、「ランサムウェア」の割合は増えておらず、（少なくとも統計的には）24%を維持しています。図18は、両者の推移を示しています。

データ漏洩/侵害のほぼ4分の1に「ランサムウェア」のステップが含まれているというのは、依然として驚異的な結果です。しかし私たちは、「ランサムウェア」がまもなく理論上の上限に達するだろうと予想していました。つまり、「ランサムウェア」の可能性のあるインシデントはすべて「ランサムウェア」によるものになると。「ランサムウェア」は現在、組織的犯罪者によるインシデントの62%以上、および「金銭目的」を動機とするインシデントの59%を占めているため、悲しいことにまだ伸びていく余地があります。

観察眼の鋭い読者は、昨年の「サプライチェーンポカリプス（Supply Chain pocalypse）[13]」（ベライゾンの造語）とは対照的に、今年はインシデントの攻撃経路として「パートナー」や「ソフトウェア」が更新されていないことに気づくでしょう。代わりに、私たちのクリスマス休暇は、また別の「過去の技術的負債の怨霊」（CVE-2021-44228として広く知られているLog4jの脆弱性）によって台無しにされました[14]。

Log4jの脆弱性については、後述の「システム侵入」セクションで詳しく説明しますが、「脆弱性を悪用」した攻撃の存在がインシデントにおいて安定しているものの、実際には漏洩/侵害ではあまり目立たなくなり、7%から5%に低下していることは注目すべきです。では、セキュリティ業界全体がクリスマス休暇を犠牲にしたことは無駄だったのでしょうか？そういうわけではありません。これは、代替の攻撃手段がより一般的になっているケースの1つです。現在のトップに立つ「盗まれた認証情報の悪用」は、41.6%から44.7%に伸びており、「脆弱性の悪用」の減少を補って余りある形になっています。

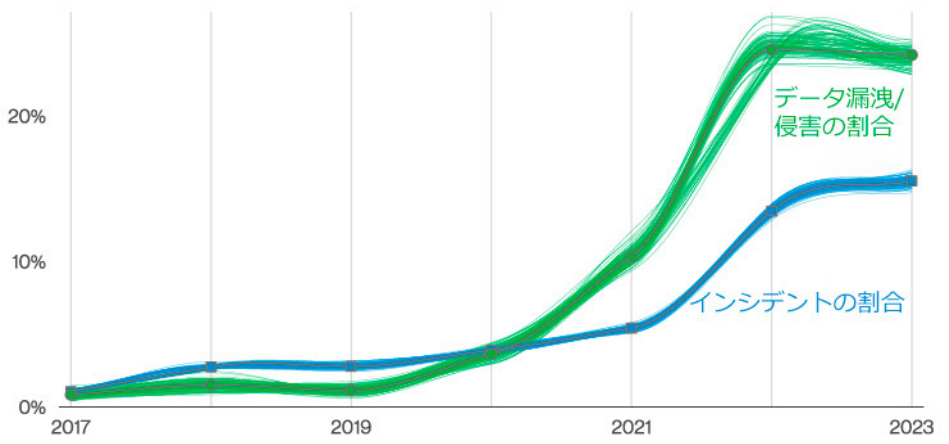


図18. ランサムウェア攻撃の経時的変化

より重要なことは、広く注意を喚起し、Log4jを含むすべての各種システムにパッチを当てるためにコミュニティが迅速に対応したことです。これによって、確かに被害の拡大を抑えられたため、その成功の結果としてインシデントが大したことではなかったように見えたのです[15]。実際は、データ提供協力者のインシデント対応においてLog4jが最重要視されたため、「脆弱性の悪用」によるインシデントの90%に「Log4j」または「CVE-2021-44228」のコメントが付けられていたほどでした。もっとも、コメントが全くなかったインシデントは全体の20.6%に過ぎなかったので[16]、データセット全体を完全に表すことはできないとしても、2021年後半から2022年前半にかけて、インシデント対応チームにとってこの脆弱性がいかに重要であったかを物語っていることにはまちがいありません。

最後に、読者の皆さまの注意が散漫にならないうちに、「紛失」について触れておきます[17]。この種の行為は、物理的なデバイスやメディアを偶然に失くすことですが、「不注意」による攻撃経路と対になることがよくあります。インシデントにおいて「紛失」はかなり高い頻度で発生していますが、これは多くの場合、データにアクセスされたことが確認できず、データ漏洩/侵害ではなくリスクと見なされたためです。しかし、これらのインシデントは、この種の事象がより厳しく報告される公共部門のデータに集中していたことは指摘に値します。何であれ、新型コロナウイルス感染症の流行が去り、誰もが再び家を出ることに胸を躍らせていたことは理解しますが、カフェのテーブルで仕事をする際には、自分の荷物から目を離さないようにしてほしいものです。

13 ご存じないでしょうが、私たちのデータセットに関連性のないものがあると述べた瞬間、何か新しいことが起こり、変化だけが唯一の不変であることを思い出させてくれます。2023年3月下旬に発生した3CXのサプライチェーン攻撃に対応しているチームの皆様の幸運を祈って、このセクションを終わります。また、今後の報告書で取り上げてもらえるよう、メモを大量にとっておくことをお忘れなく。

14 なんともやりきれません。

15 2000年問題のバグに対処していたのはどこの誰でしたっけ？帯状疱疹ワクチンの接種予定をお忘れなく！

16 皆の弁明によれば、ここで行われているデータ共有のほとんどは、マシン間で行なわれているものだということです。ほとんどのデータ提供者にとって、職人技でオーダーメイドされ、VERISで分類されたインシデントの時代はとっくに終わっていたのです。

17 オンライン中心で仕事をされている方々には、精神的なダメージを与えたことを謝罪いたします。

資産

会計学の初級の授業を抜け出してきた人のために説明しますが、ここでの「資産」とは貸借対照表の左側に記載されている数字以上のものです[18]。資産には、インシデントやデータ漏洩/侵害で影響を受ける可能性があり、攻撃者の悪意のある目標のために操作されることになるエンティティが含まれます。囲みコラムには、VERISで最も一般的な上位の「資産」と、それを標的とする最も一般的な攻撃パターンがいくつか記載されています。

図19. データ漏洩/侵害のあった「資産」（n=4,433）

侵害の被害を受けた「資産」の種類の内訳を示した図19では、「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」が今年の攻撃パターンの上位を占めており、ほぼ予想通りの結果となっています。

上位3つのパターンについて、被害を受けた「サーバー」が若干減少し、「ユーザデバイス」がわずかに増加したため、若干の変動が見られますが、この順位は「人」が2位の座を奪って以来、少なくとも数年間は変わっていません。VERISでは、人も資産であり[19]、ソーシャル攻撃によって影響を受ける「場所」であることを忘れてはなりません。

資産のカテゴリー[20]

サーバー（srv）： 組織をサポートする何らかの機能を実行するデバイスで、通常はエンドユーザとのインタラクションを伴わず、Webアプリケーション、メールサービス、ファイルサーバー、そして情報レイヤーが魔法のように生成される場所。「システムがダウンしている」と言われたことがある人は、一部の「サーバー」について「可用性」に影響が出ていることを確認してください。サーバーは、ほぼすべての攻撃パターンで共通の標的ですが、特に「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」、「サービス拒否（DoS）」の各パターンでよく見られます。

人（per）： その組織で仕事をしている人々（たぶん）。AIチャットは不可。部署によってメンバーとなる「人」のタイプは異なり、その役割によって所属する組織内での権限とアクセス権も異なります。少なくとも、自分専用の「ユーザデバイス」と自身の将来の夢や希望にアクセスすることができます。「ソーシャルエンジニアリング」攻撃パターンでは、「人」が一般的なターゲットになります。

ユーザデバイス（usr）：「人」が組織内で職務を遂行するために使用するデバイス。通常、ラップトップ、デスクトップ、携帯電話、タブレットなどの形態をとります。「システム侵入」パターンでよく攻撃の標的にされていますが、「資産の紛失・盗難」のパターンにもよく見られます。人々は小さなコンピューターをどこにでも持って行きたがるものです。

ネットワーク（net）：概念ではなく、ルーター、電話、ブロードバンド機器、ファイアウォールや侵入検知システムなどの従来のインラインネットワークセキュリティデバイスなど、ビットを世界中に行き渡らせる物理的なネットワークコンピューティングデバイス。そう、ベライゾンは「電気通信会社」ですからね。

メディア（med）：最も純粋で結晶形の貴重な希釈データ、というのは冗談で、ほとんどが親指サイズのUSBストレージと紙の印刷文書。たまに無骨なフルサイズのディスクドライブや実際の物理的なペイメントカードを見かけますが、どちらかというと稀です。ただし、「資産の紛失・盗難」のパターンによく見られます。

18 しかし、それらを適切に管理しないと、負債が右肩上がりになる可能性があります。
19 人事部に聞いてみてください。
20 https://verisframework.org/assets.html

図20で「資産」の種類をさらに詳しく見ると、予想通り、「Webアプリケーション」と「メールサーバー」が上位を占めていますが、興味深いことに、「人-経理」が昨年より増加傾向を示しています。これらに関して、特に「ビジネスメール詐欺（BEC）」については、本報告書の「ソーシャルエンジニアリング」のセクションで説明します。

最後に、コンピューターが重機と重要なインフラと連動する「オペレーショナルテクノロジー（OT）」に関連するインシデントは、私たちが猫の写真やインターネットを通じて広まる情報をため込んでいる「インフォメーションテクノロジー（IT）」に関連するインシデントとは対照的に、非常に少数であることが引き続き確認されています。「製造業」や「鉱業、採石業、石油・ガス採掘および公益事業」[21]のような業種は、私たちのデータセットに比較的多く含まれていますが、OTデバイスへの実際の影響に関する報告は、この報告書で有意義なものとして取り上げるにはまだ事例が少なすぎます。

図20. データ漏洩/侵害において上位を占める「資産」の種類（n=3,207）

これを記録している人で、影響を訴えたのはOT資産の3.4%でした。 つまり、注意レベルを高く保つ必要がありますが、これらのシステムが影響を受けた場合の潜在的な影響を考慮すると、これらの数字は全体として非常に低いか、それぞれの国[22]でセキュリティ上の懸念があるために、単に提供されたデータセットに含まれていないものと考えられます。

21 ええ、本当にそのとおりです。
22 まったく、どの国からの提供データもでした。

属性

VERISが「属性」について説明するとき、それは情報セキュリティ（InfoSec）におけるCIAの三要素、「機密性」（Confidentiality）、「完全性」（Integrity）、「可用性」（Availability）のことを指しています。これは、資産のどのような特性が影響を受ける可能性があるかを記述することによって、インシデントの潜在的な影響を理解する実証済みの方法です。

属性のカテゴリー[23]

機密性（cp）：資産（またはデータ）の閲覧と開示が制限されることを意味します。機密性の喪失は、データが危険にさらされた、危険な状態にあるかまたはその可能性がある（後者は「所有および管理」の属性に該当）のではなく、実際に閲覧された、または権限のない攻撃者に開示されたことを意味します。簡単な定義：アクセス、閲覧、開示の制限。

完全性（ia）：資産（またはデータ）が完全な状態であり、元の状態または承認された状態、内容、機能から変更されていないことを指します。完全性の喪失の要因としては、不正な挿入、改竄、操作などがあります。簡単な定義：完全で、元の状態から変更されていないこと。

可用性（au）：資産（またはデータ）が存在し、アクセス可能で、必要なときに利用できる状態を指します。可用性の喪失の要因としては、破壊、削除、移動、パフォーマンスへの影響（遅延または加速）、中断などがあります。簡単な定義：アクセス可能で、必要なときに利用できる状態。

今度、受難のインシデント対応担当者に会うことがありましたら、彼らの頭の中をよぎるのは、「資産やデータのコピーが外に漏れたか」（機密性）、「既知の信頼できる状態から変更されてしまったか」（完全性）、「まだ自分たちがアクセスできるのか」（可用性）であることを確認してみるとよいでしょう。それは非常に拷問的なことなので、彼らに温かい言葉と飲み物を提供してあげてください。あなたが寒いと感じているなら、彼らも寒いのです。

私たちが毎年追跡している「属性」の種類の中で最も注目しているものの1つは、「機密」データの種類（図21）、つまり漏洩/侵害で流出したデータの種類です。「個人」情報は顧客、パートナー、または従業員の「個人を特定できる情報（PII）」です。世界中でプライバシー関連の法律が制定されるにつれて、通常、企業が規制当局と最もトラブルになるのはこのデータです（ただし、「医療」データはまったく別のものです）。

図21. データ漏洩/侵害において上位を占める機密情報の種類（n=5,010）

仮想通貨、現実の問題

今年、DBIRチームが特に注目したデータの種類は仮想通貨です。暗号通貨が関係するデータ漏洩/侵害の件数が、昨年から4倍も増加しました。2020年以前は毎年多くても1件か2件だった牧歌的な時代から、大きく様変わりしました。もし私たちの漫画動物のNFT（Non-Fungible Token：代替不可能なトークン）でこれほどの収益を得ていたら、大きな家に住み、この報告書を両親の家の地下室ではなく、ランボルギーニを豪華に乗り回しながら書いていたことでしょうね[24]。

図23と図24は、仮想通貨を含むデータ漏洩/侵害における上位の攻撃の種類と経路を示しており、「脆弱性の悪用」、「盗まれた認証情報の悪用」、「フィッシング」の間で激しい戦いが繰り広げられています。これらのタイプの侵害は、アプリケーションやAPIを介して侵害を受ける実際のコインネットワークや取引所、

23 https://verisframework.org/attributes.html
24 うちのランボルギーニは両親の家のガレージに停めてあるかもしれませんが。

「内部」情報と「システム」情報は、通常、メールや文書からの情報が攻撃者によって吸い上げられ、複数の段階を経ることで広範な侵害の副産物となります。「認証」情報は、「盗まれた認証情報の悪用」がデータ漏洩/侵害のとっかかりとして最もよく狙われる標的となったため、この過去5年間で本当に順位を上げてきました。

もちろん、「医療」情報、「銀行口座」情報、「ペイメントカード」のデータなど、特定のデータが狙われるケースも依然として存在します。これらは特定の標的を絞ったものである場合もあれば、ランサムウェア攻撃によるデータ流出で取得されたデータの一部である場合もあります。また、ランサムウェアに関する私たちの嘆きに飽き足らない方は[25]、図22をご覧ください。ここでは、ランサムウェアの増加のもう1つの影響を見ることができます。それは、データの「難読化」が最も一般的な可用性への影響要因となり、従来の単純な「データの損失」をたやすく上回ったことです。

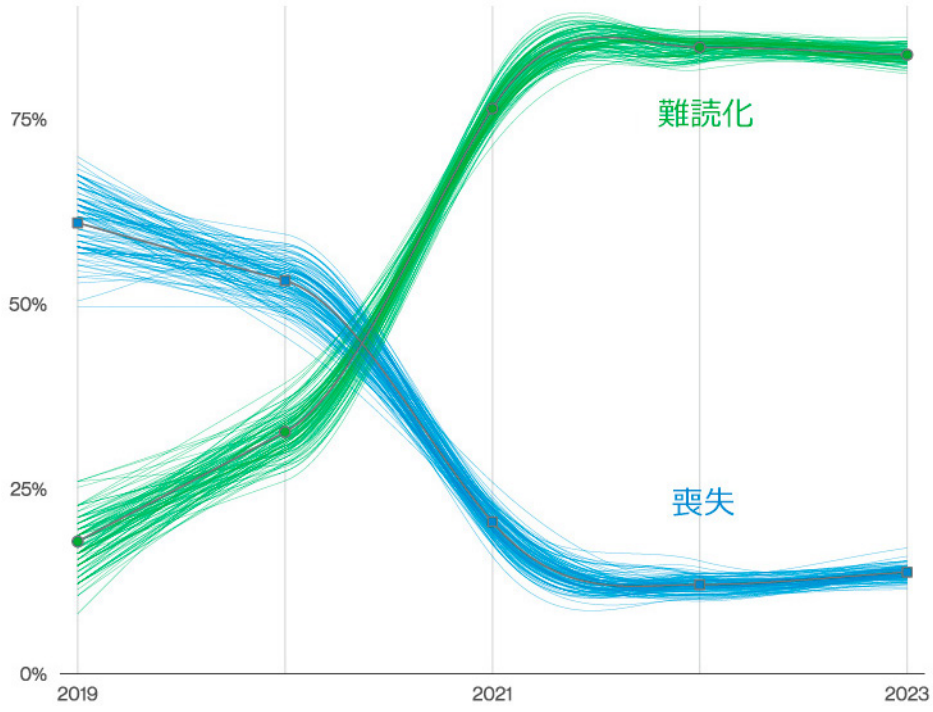


図22. 可用性の種類の経時的変化

またはコインのコミュニティのチャットプラットフォーム（Discordなど）でのフィッシングやなりすまし活動の間に紛れており、リンクをクリックしたとたんに自分の財布が自分ものでなくなるのです。

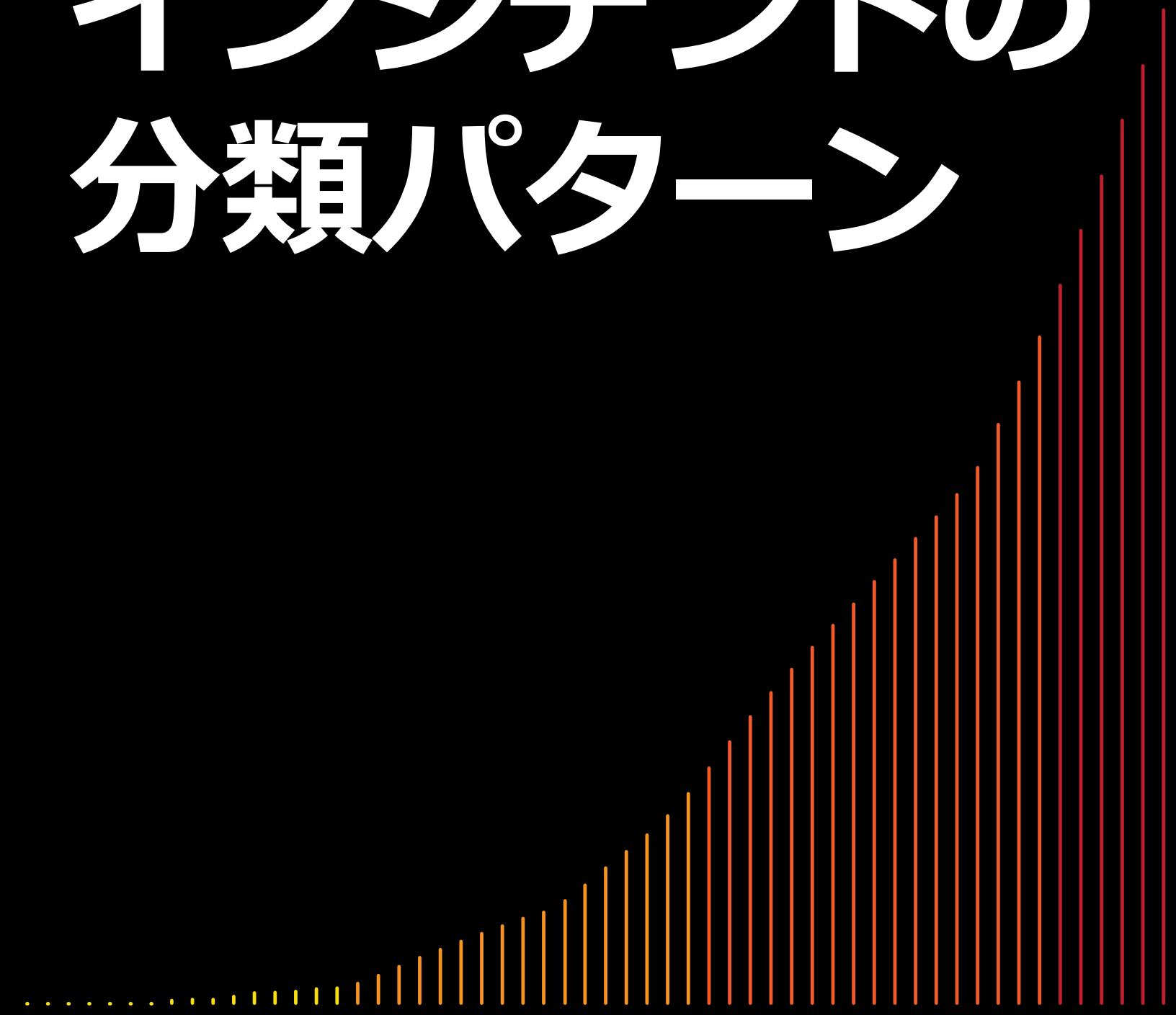
仮想通貨で資産を持つことは、悪質な攻撃者が持ち逃げ詐欺（rug-pulling）[26]に関与していなくとも、大変リスクの高い投機です。このような種類の資産に攻撃者が注目するようになったことは状況を一層難しくしています。つまるところ、仮想通貨市場でセキュリティが真剣に取り組まれない限り、現実には、成功することはないということです。

図23. 仮想通貨に関わるデータ漏洩/侵害において上位を占める攻撃の種類（n=30）

図24. 仮想通貨に関わるデータ漏洩/侵害において上位を占める攻撃経路（n=48）

25 つらいのは私たちでなく、あなたがたですよ。
26 あの絨毯のおかげで部屋がまとまっていたのに！

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

進化が人類に与えた最大の贈り物の1つは、パターンを追求する頭脳です。あれはジャングルで木の葉が揺れているだけなのか、それとも縞模様の虎が我々を襲うために忍び寄っているのか？人類が依然として存続しているという事実は、そうした問いに、間違った答えよりも正解したことの方が多かったことを物語っています。ありがたいことに、私たちはパターン追求の超能力を使って、コンピューターが私たちに間違いを気付かせるさまざまな方法を整理し、理解しようとすることもできるのです[27]。

私たちのインシデントパターンとは、一言で言えば、似たようなインシデントをまとめ、覚えやすい短い言葉にまとめる方法なのです。前述したように、インシデントはVERISの4つのA[28]によって特徴付けられ、この方法でインシデントを分類することによって、毎回長い段落の説明を避けることができます。8つのパターンとその定義を表1に示します。

今年は、特定のパターンに関連するATT&CKテクニック[29]とCenter for Internet Security（CIS）Critical Security Controls[30]の詳細な内訳を紹介します。というのも、この報告書全体を通してその度に同じ説明を繰り返さないようにするためです。ATT&CKマッピングのリリースを私たちが誇りに思うのは、MITRE CTIDの標準とVERISの間の作業関係の構築と維持における、MITRE CTIDとの複数年にわたる協力の集大成であるためです。詳しい説明は付録Bをご覧ください。

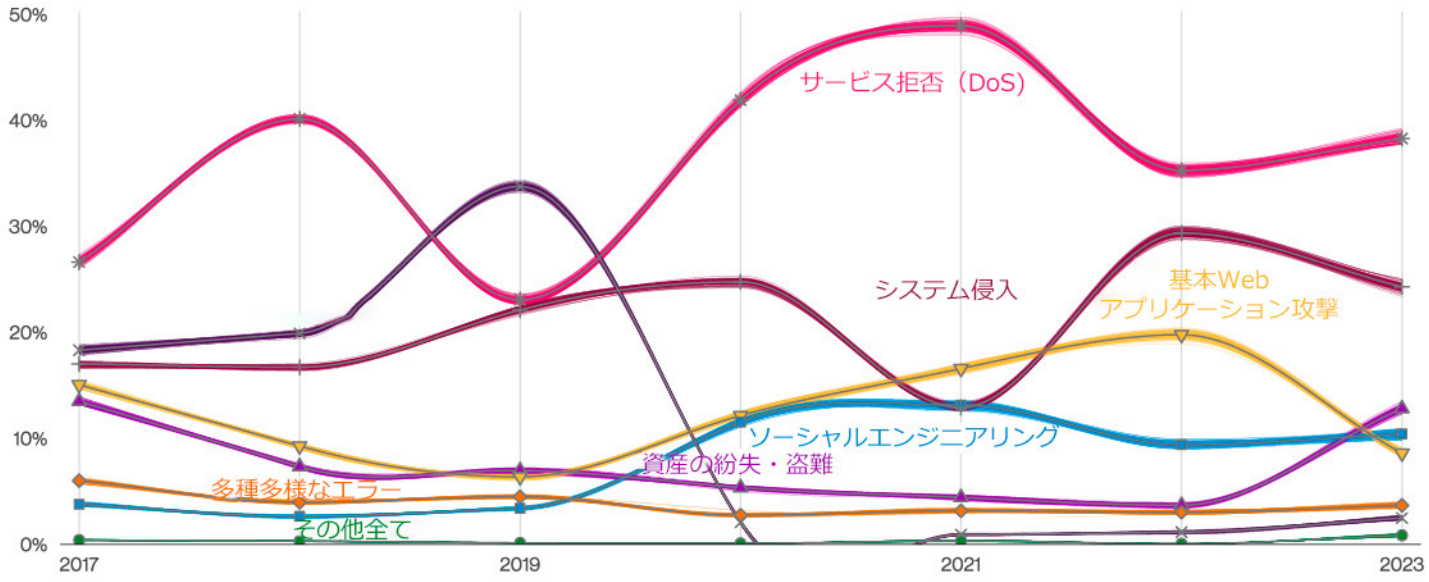


図25. インシデントにおけるパターンの経時的変化

27 人間が間違えであると主張するChatGPTや他のAIプラットフォームとは対照的です。

28 よく言われるように、パターンは攻撃者（Actor）、攻撃（Action）、資産（Asset）、属性（Attribute）の4つの観点から分析されます。

29 https://attack.mitre.org/

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

それでは、各パターンの具体的な結果と詳細な分析を掘り下げることで、（パターンを求める）頭脳から取り除いた認知的負荷を楽しんでください。

例年どおり、ここでは「インシデントの分類パターン」（以下パターン）を提示し、それらが年々どのように変化しているかを示します。インシデントのパターンの経時的変化を示す図25では、「サービス拒否（DoS）」が数年前から変わらずトップであることがわかります。

この図と図26を比較し、データの損失が確認されたインシデントに焦点を当てることで、環境がいかに変化しているかがわかります。

より複雑な攻撃を伴う「システム侵入」パターンには、ランサムウェアを特徴とする多段階攻撃が含まれています。しかし、少し話を急ぎすぎたようです。全容を明らかにするために、詳細なパターンのセクションに移りましょう。

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わない、「侵入して、データを取得したら引き上げる」パターン。
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を含む。
資産の紛失・盗難	置き忘れか悪意によるものかを問わず、情報資産を紛失したインシデント。
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がこのパターンに含まれる。デバイスの紛失はこれには含まれず、盗難に分類。
特権の悪用	正規の特権が不正に、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人の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」を仕組むなどの目的を達成すること。
多種多様なエラー	この「パターン」は、実際にはパターンとは言わない。しかし、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。例えば、廃棄した電化製品の電源ケーブルを箱に保管しておくようなもの。もしもの場合に備えて。

表1. インシデントの分類パターン

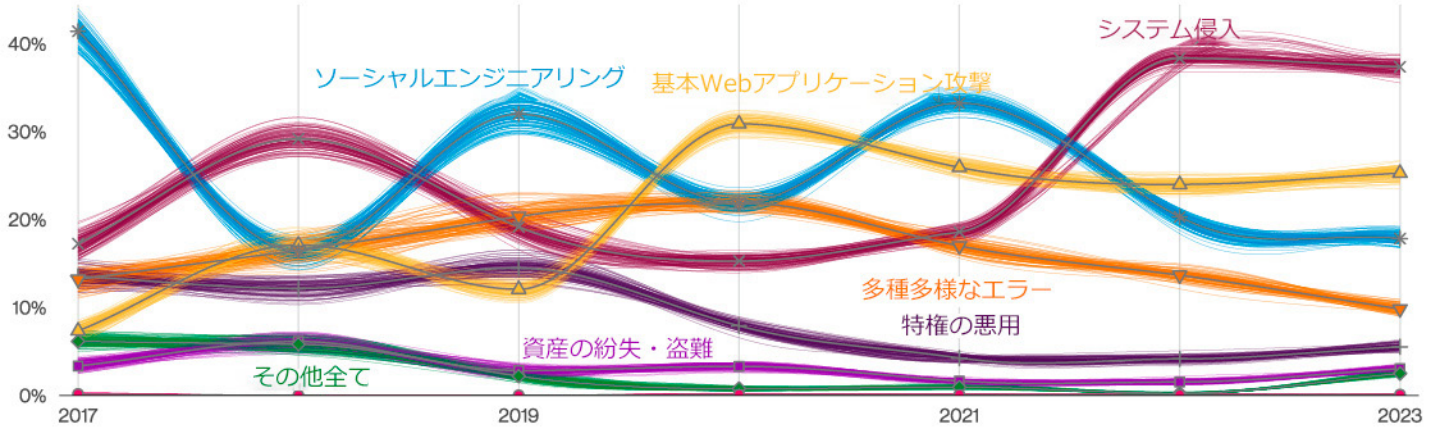


図26. データ漏洩/侵害パターンの経時的変化

システム侵入

サマリー

このパターンは主に、ハッキングの専門知識とマルウェアへの迅速なアクセスを活用し、さまざまな規模の組織に侵入し、影響を与える、より熱心な犯罪者によって実行される攻撃に関連しており、支払日を確実にする手段として「ランサムウェア」を活用することが多いです。

昨年との比較

「ランサムウェア」は、攻撃者がさまざまな手法を駆使して組織を侵害するため、このパターンを支配し続けています。

頻度	インシデント3,966件、確認されたデータの暴露1,944件
攻撃者	外部（96%）、内部（4%）、複数（2%）、パートナー（1%）（漏洩/侵害）
攻撃者の動機	金銭目的（97%）、スパイ活動（3%）（漏洩/侵害）
侵害されたデータ	その他（42%）、個人（34%）、システム（31%）、内部（24%）（漏洩/侵害）

これは私のもの、これも私のもの...

ある朝オフィスに行くと、恐ろしい名前の犯罪グループから、全データの返還と引き換えにビットコイン（BTC）を要求する驚くべき画面がデスクトップに表示されたとします。願わくば、熱心なDBIRの読者であるあなたなら、リストア用に作成され、十分にテストされた最新のバックアップがあるはずです。しかし、この犯罪者があなたのデータを暗号化するだけでなく、お金を払わない限り、機密性の高い情報の一部を流出させると脅してきたら、どうしますか？私たちの防御や対策をどれだけ早く進化させても、攻撃者のほうも同じように早く進化しているように見えることがよくあります。これは永遠の軍拡競争を生み出すようなもので、「システム侵入」パターンほどそれを象徴するものはありません。

関連する ATT&CK テクニック

脆弱性の悪用（VERIS）

- 権限昇格の悪用：T1068
- 一般用アプリケーションの悪用：T1190
- 防御回避のための不正使用：T1211
- 認証情報アクセスのための不正：T1212
- リモートサービスの悪用：T1210
- 外部リモートサービス：T1133
- 脆弱性スキャン：T1595.002

盗まれた認証情報の悪用（VERIS）

- アカウントの侵害：T1586
  - ソーシャルメディアアカウント：T1586.001
  - メールアカウント：T1586.002
- 外部リモートサービス：T1133
- リモートサービス：T1021
  - リモートデスクトッププロトコル：T1021.001
- 代替認証材料の使用：T1550
  - WebセッションCookie：T1550.004
- 有効なアカウント：T1078
  - デフォルトアカウント：T1078.001
  - ドメインアカウント：T1078.002
  - ローカルアカウント：T1078.003
  - クラウドアカウント：T1078.004

- 実行：TA0002
- 永続性：TA0003
- 権限昇格：TA0004
- 防御回避：TA0005
- 認証情報へのアクセス：TA0006

私たちはよく、このパターンの攻撃者を「キーボードを武器とする」タイプの攻撃者と捉えます。足がかりを得るために自動化を利用することもありますが、いったん組織内に侵入すると、研ぎ澄まされたスキルを活用して制御を迂回し、目的を達成します。図28が示すように、このパターンには一般的に「ランサムウェア」が含まれます。この手の攻撃者は、フィッシングや盗まれた認証情報を悪用してアクセス権を取得し、バックドアを追加していつでもアクセスできるようにしたり、脆弱性を悪用して水平方向に移動したりする（ラテラルムーブメント）など、さまざまなツールを使用して被害者の環境を探索した後、足場を築きます。このような攻撃を、より小さく、扱いやすい3つの部分に分けると、より明確に把握することができるのです。すなわち、最初のアクセス段階、侵害の拡大、そして結果です。図27に示したのは、攻撃のさまざまな段階で見られる「攻撃」と「資産」の組み合わせの内訳です。

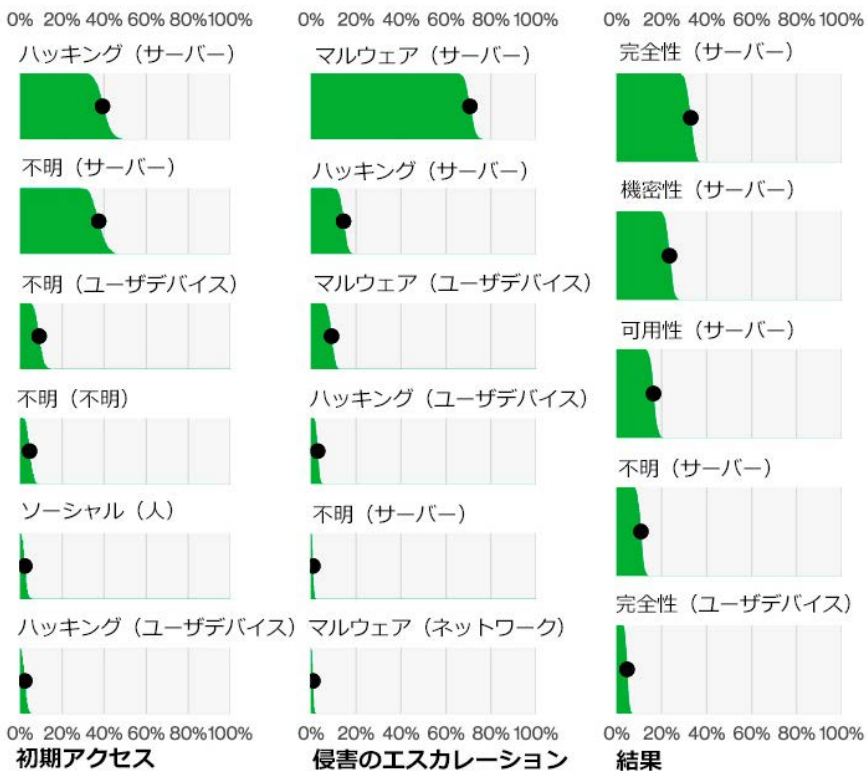


図27. システム侵入によるデータ漏洩/侵害のステップ

図28. システム侵入インシデントにおける攻撃の種類 （n=2,700）

図29. システム侵入インシデントにおける攻撃経路 （n=787）

ロック解除の試み

図27を見ると、最初のアクセスで明らかに上位を占めているのは、多くのサーバーハッキングと、それとほぼ同量の不明な攻撃です。ハッキングに関しては、インシデントの9%に「脆弱性の悪用」、8%に「盗まれた認証情報の悪用」が含まれています。脆弱性の悪用を含むインシデントのみを詳しく見ると、これらの脆弱性は主に「Webアプリケーション」を介して悪用されていることがわかります（図29）。

さらに、いくつかの「ユーザデバイス」が直接狙われており、そのケースの約6%で「フィッシング」も確認されています。「フィッシング」は、使用可能な認証情報を取得するため、あるいはユーザのシステム上にペイロードを展開するために、別の侵入手段を提供するだけのものです。「マルウェア」は主にメールを介して配布され、多くの場合Microsoft Office文書の形で送られてきます（図30を参照）。これらのドキュメントのほとんどが、クライアントシステム上でコードを実行する機能を備えており、攻撃者にとって非常に便利であることを考えれば、これはまさに理にかなっています。

確かに、攻撃者が使用した侵入手段が正確に分からないケースも多くあります。しかし、「脆弱性の悪用」、「盗まれた認証情報の悪用」、「フィッシング」といった経路は、例年の調査結果と非常によく似ており、正直に言って、これらは情報セキュリティ初級クラスの内容そのものです。これはまた、抜本的な対策の重要性を示しています。

そう、権限があっという間に昇格

いったん攻撃者があなたの環境にアクセスすると、攻撃者は通常、権限を昇格させる方法を探し、永続性を維持し、最終的な目標を達成するために組織全体にわたって移動できる経路を探します。ATT&CKをよくご存知の方には、そのマ

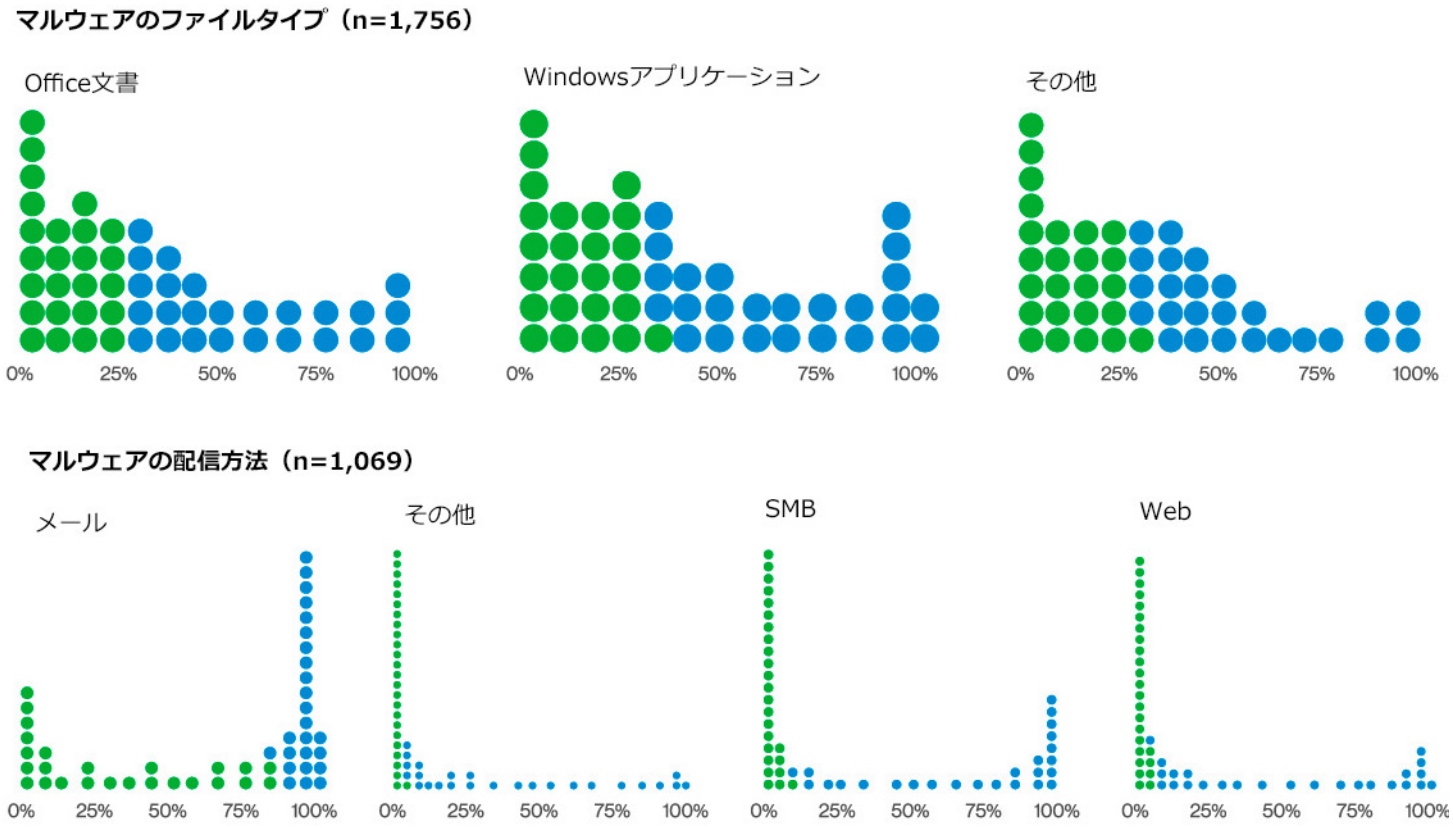


図30. マルウェア配信方法の組織別割合

トリクスの大部分について話しているように聞こえるでしょう。実はその通りなのです。私たちはインシデントを高い視点からは見ていますが、どのような手法が使われたかを正確に知るために必要な遠隔測定をいつでも行なえるわけではありません。しかし、私たちが追跡できるハッキングテクニックとマルウェアの能力については以下で説明します。

システムへのコマンド＆コントロール（C2）アクセスを維持する「マルウェア」は、インシデントの約5%で確認されています。また、ホストのプロファイル更新、ネットワークのスキャン、（ローカルでよく行なわれる）パスワードの破棄などを行なう典型的なタイプのマルウェアも確認されています。最後に、このデータセットには、2010年代はもう過去のものと思っていた暗号マイナーがかなり含まれていました。暗号マイナーの再流行を確信できるほど十分な数ではありませんでしたが、いくつかの組織が、侵害されたサーバーをマイニングのために無料で開放されている“土地”として考えていることを確信するには、十分な数であることは間違いありません。

結果

このようなパターン（「ランサムウェア」、バックドア、ペイメントカードのスキミングマルウェアのいずれかの形態）では、マルウェアのインストールへの依存度が高いため、「属性」と「資産」の最も一般的な組み合わせとして、不正なソフトウェアがインストールされたサーバーが見つかっても、それほど驚くことはありません。2番目に多いのはデータの流出で、3番目に多いのは可用性の喪失、つまりデータを読めなくすることです。これら上位3つのパターンは、こうした攻撃の多くに関連する最終的なステップをよく表しており、攻撃者は、組織全体にペイロードをインストールする方法を見つけ、データを盗み、そしてシステムを暗号化して出て行くのです。

ランサムウェア... もう少しこのセクションは続きます

「ランサムウェア」は、あらゆる規模や業種の組織にとって大きな脅威であり続けており、データ漏洩/侵害全体の24%に存在しています。これらのケースのうち94%は「システム侵入」です。「ランサムウェア」は今年わずかに増加しただけですが、神出鬼没な脅威であるため、常に保護対策を整える必要があります。私たちの業界の91%が「ランサムウェア」を上位3つの攻撃の1つにしています。

図31. ランサムウェアの攻撃経路（n=690）

このような攻撃がどのように発生するかを理解するためには、その上位の「攻撃経路」を見ることが役立ちます。この場合、最も一般的な攻撃経路は、「メール」、「デスクトップ共有ソフトウェア」、「Webアプリケーション」です（図31）。攻撃経路としての「メール」は、すぐになくなることはありません。マルウェアを送信し、ユーザに実行させるという利便性があるため、この手法は時代を越えて存続していきます。次に多い攻撃経路である「デスクトップ共有ソフトウェア」は、これらの侵害やインシデントが頻繁にシステムへのアクセス手段を利用していることを考えると、理にかなっていると言えます。そのためには、RDPのようなビルトインツールやサードパーティのバージョンを使って、犯罪の首謀者に素晴らしいGUIを提供することが一番、でしょう？

Log4jの分割

私たちDBIRの著者たちが大いなる眠りから目を覚まし、サイバーセキュリティの世界で起きている主要な出来事をすべて収集し、書き始めていたところ、データ収集の作業を締め切った後に、また新たなサイバーセキュリティの重要な出来事がゆっくりと進行していました。これはまず2020年にSolarWinds[31]で起こったことですが、2021年にはLog4j[32]で再び歴史が繰り返され、脆弱性の「パンドラの箱」を開けたかのようでした。しかし、待つことには1つの利点があます。つまり出来事を覆っていた霧が晴れ、実際に起こったことについて客観的な分析ができるようになるのです。Log4jの脆弱性に関わるインシデントを取り巻く不確実性と複雑性は非常に大きなものでした。そのうちの1つは、誰も本当にデータ漏洩/侵害の全容を理解していなかったという事実でした。その脆弱性は単に1つのソフトウェア製品にあったのではなく、実際には多数のアプリケーションとプログラム（購入したものとオープンソースの両方）によって使用されるライブラリに存在していたからです。

記憶を呼び覚ますために、簡単にこの出来事を振り返っておきましょう。この脆弱性は2021年11月下旬に公表され、数日のうちに最初の悪用が開始されました。CVE-2021-44228のコードを持つこの脆弱性には、なんと重大度スコア10が与えられました[33]。12月末までに、ハニーポットによって暴かれたスキャン活動の0.003%が、この特定の脆弱性を積極的に攻撃していました。その数は小さいように見えるかもしれませんが、速度はむしろ顕著で、1年間の全Log4jスキャン活動の32%以上が、そのリリースから30日以内に起こりました（活動の最大のピークは、図32が示すように17日以内に発生）。この速度は、組織がパッチを当てるまでの期間と比較すると興味深いものがあります。重要な脆弱性の場合、パッチ当てまでの期間は中央値で現在49日で、この数字は、ここ数年で比較的一貫しています。

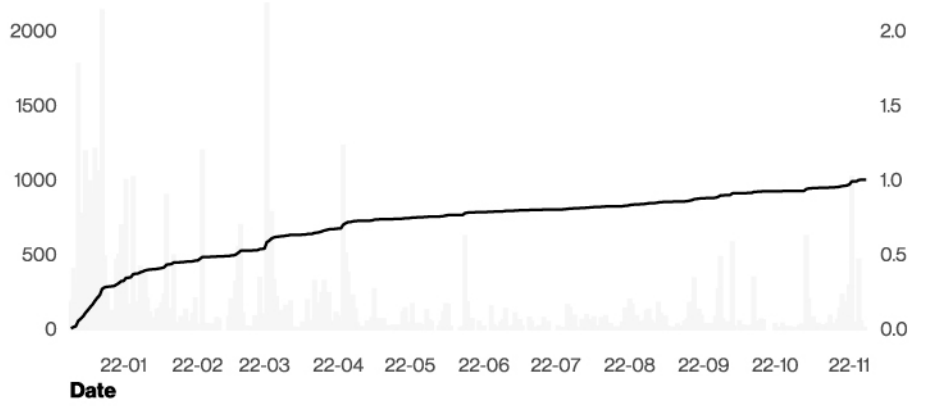


図32. 2022年のLog4jスキャンの割合

ただし、これは多くの人が予測したほど大きな災害ではなかったのかもしれません。DBIRのインシデントのデータセットを分析したところ、実際にインシデントとデータ漏洩/侵害につながる脆弱性の悪用が減少しており、Log4jの報告は全インシデントの0.4%（100件弱）でした。しかし、これらのケースを詳細に調べてみると、Log4jが様々な異なる目的を達成するために多くの攻撃者によって利用されており、「スパイ活動」に関係するケースの73%、「組織犯罪」に関係するケースの26%に関わっていたことが明らかになりました。リモートでコードの実行を可能にするという脆弱性の性質を考えると、追加のホストを引き込むためのBackdoors（バックドア）やDownloader（ダウンローダー）のような、それに関連するマルウェア活動が多く見られたのは予想通りでした。最後に、ケースの約26%で、得ることができるならどんなものでも利用する「ランサムウェア」攻撃の一環でLog4jの脆弱性が悪用されていました。

チームが分析した脆弱性スキャンデータのいくつかで（悪意の行為ではなく、脆弱性の発見のためにスキャンしている善良な人々が行なうのと同じく）、脆弱なLog4jが組織の8%に存在することも発見しました。さらに、やや意外と思われる別の報告の中に、組織の14%で、使用期限（EOL）に達していたLog4jのインストールが大きな割合を占めていたことも分かりました（実際にそのLog4jに明示的な脆弱性があったかは分かりませんが）。最終的に、組織の22%は、それぞれのシステムにLog4jの脆弱性で複数の（2つ以上の）インスタンスを抱えていました。

依存関係に潜むこの脆弱性は、ソフトウェア部品表（SBOM）を持つことに関する議論を呼び起こしました。SBOMは、子供たちが使う「マジだよ」と「最高！」の間に投げかける言葉だと思うかもしれませんが、その目的は、組織が依存するソフトウェアを作るために必要なすべての材料（ソフトウェアパッケージとライブラリ）を理解するのを助けることにあります。SBOMのプロセスをエコシステム全体で成熟させることで、組織は基礎となるライブラリ内の脆弱性を迅速に特定し、Log4jのようなものに対する将来の修復プロセスに役立てることができます。

31 https://www.cisa.gov/news-events/news/cisa-issues-emergency-directive-mitigate-compromise-solarwinds-orion-network

32 https://www.cisa.gov/news-events/news/cisa-issues-emergency-directive-requiring-federal-agencies-mitigate-apache-log4j

33 もっとも、11まで上げても良かったと内部関係者は指摘していますが。

検討すべきCISコントロール

このパターンの中に見られる活動の幅の広さと、攻撃者が幅広いテクニックと戦術の組み合わせを活用することを念頭に置くと、組織が実装を検討すべきセーフガードはたくさんあります。以下に、CIS管理番号を含む小さなサブセットを示しますが、これは、組織のリスクプロファイルに適した管理策を決定するために、独自のリスクアセスメントを構築する際の出発点となるものです。

デバイスの保護

企業資産とソフトウェアのセキュアな設定［4］
- 安全な構成プロセスを確立し維持する［4.1］
- ネットワークインフラの安全な設定プロセスを確立し維持する［4.2］
- サーバーにファイアウォールを実装し管理する［4.4］
- エンドユーザデバイスにファイアウォールを実装し管理する［4.5］

電子メールとWebブラウザの保護［9］
- DNSフィルタリングサービスを利用する［9.2］

マルウェアに対する防御［10］
- マルウェア対策ソフトウェアを導入し維持する［10.1］
- マルウェア対策のシグネチャ自動更新を設定する［10.2］

継続的な脆弱性管理［7］
- 脆弱性管理プロセスを確立し維持する［7.1］
- 修復プロセスを確立し維持する［7.2］

データ復旧［11］
- データ復旧プロセスを確立し維持する［11.1］
- 自動バックアップを実行する［11.2］
- 復旧データを保護する［11.3］
- 復旧データ保管用に隔離された環境を準備し維持する［11.4］

アカウントの保護

アカウント管理［5］
- アカウントのインベントリを確立し維持する［5.1］
- 休止アカウントを無効にする［5.3］

アクセス制御管理［6］
- アクセス権限を付与/停止するプロセスを確立する［6.1］［6.2］
- 外部公開アプリケーションに多要素認証を義務付ける［6.3］
- リモートネットワークアクセスに多要素認証を設定する［6.4］

セキュリティ意識向上プログラム

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［14］

（ランサムウェアについて）メモをもう1つだけ

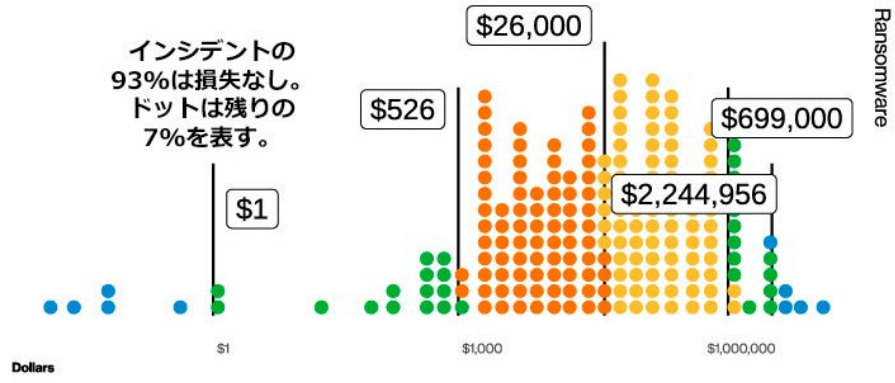


図33. 苦情1件あたりの「ランサムウェア」インシデントコストの95%および80%信頼区間（n=2,575）

ランサムウェアの話題で盛り上がっているので、ベライゾンのパートナーであるFBIのInternet Crime Complaint Center（IC3）が提供する侵害における影響のデータを再検討するのは興味深いことだと考えました[34]。

2021年のDBIRでこのデータのレビューを行なったときに、IC3に報告されたインシデントの 90%に金銭的な損失はありませんでしたが、残りの10%では、損失額の中央値は11,500ドルとなり、そのケースの95%での損失額の範囲は70～120万ドルでした。

図33を見ると、損失が発生したインシデントのうち、計算上の中央値は2倍以上の26,000ドル、95%の損失幅は100万ドルから225万ドルに拡大しており、 小規模企業であればこの上限は恐ろしい領域となっています。FBIの調べでは、このケースで損失を被ったのは全体の7%に過ぎず、悪いニュースばかりではありません。

さて、インフレと経済の基準レートについて嫌味を口にする人が出てくる前に、ここから後は異常な部分を報告します。同じ期間に攻撃者に支払われた取引額を合計すると、中央値は1万ドルとかなり小さくなっており（図34）、この中央値は、DBIRチームがこのデータセットを分析した過去2年よりも低くなっています。

このことが示唆しているのは、身代金の金額が低くなっても、ランサムウェアのインシデントから回復するためのコストは全体的に増加しているということです[35]。この事実は、ランサムウェア被害者の全体的な企業規模が小さくなっていることを示唆している可能性があります。攻撃者が要求する金額は、小規模な企業ほど、より少額になるようですが（彼らはできる限りの金を手に入れたいと考えていますが）、技術的な負債が発生する可能性が高いという背景の下、ITインフラを回復するためのコストが追加されることで、全体的な損失が急増することになります。

このように推測するのは、企業規模のデータがなく、すべての苦情がこの特定のデータセットに関連する取引額のデータを提供しているわけではないためです。とはいえ、ランサムウェアの仕掛け側の自動化と効率化が進んでいるため、このような結果になることは予想されていました。ともあれ、予防の重さは治療の金額に値すると言ってもよいので[36]、次の予定外の暗号化イベントが発生する前に、計画および/またはインシデント対応リソースを準備しておく必要性があることは、いくら強調してもしきれません。

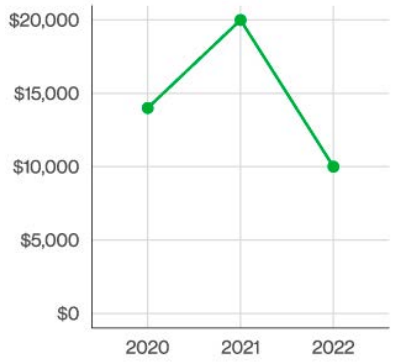


図34. FBIのIC3への苦情に基づくランサムウェアの取引額の中央値

34 https://www.ic3.gov
35 このインフレジョークを遠慮なくお使いください。
36 雷雨の中で鍵を持って凧揚げをした男（ベンジャミン・フランクリン）が言った有名な文句です。考えさせられるでしょう。

ソーシャル エンジニアリング

サマリー

「ソーシャルエンジニアリング」のインシデントが前年より増加した主な原因は、「ビジネスメール詐欺（BEC）」でよく使用される「なりすまし」が昨年の約2倍に増加したことです。これらの攻撃の頻度が増加していることに加え、このような攻撃によって盗まれた金額の中央値もここ数年で増加しており、5万ドルとなっています。

昨年との比較

「フィッシング」と「なりすまし」が引き続きこのパターンを支配しているため、メールが個人に影響を与える最も一般的な手段の1つであることには変わりありません。

頻度	インシデント1,700件、確認されたデータ暴露928件
攻撃者	外部（100%）、複数（2%）、内部（1%）、パートナー（1%）（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（76%）、内部情報（28%）、その他 （27%）、個人情報（26%）（漏洩/侵害）

対応するATT&CK テクニック

アカウント侵害 ： T1586
– メールアカウント ： T1586.002

アカウント確立 ： T1585
–メールアカウント : T1585.002

外部リモートサービス : T1133

内部スピアフィッシング : T1534

フィッシング : T1566
– 添付ファイルによるスピアフィッシング : T1566.001
– リンクによるスピアフィッシング : T1566.002
– サービスを利用するスピアフィッシング : T1566.003

情報のフィッシング : T1598
– スピアフィッシングサービス : T1598.001

代替認証情報の使用 : T1550
– アプリケーションアクセストークン : T1550.001

有効なアカウント : T1078
– ドメインアカウント : T1078.002

プロのエンジニア？

エンジニアリングは、実用的で有意義な目的のために応用される数学と物理学の美しい組み合わせであると、そう私たちは聞かされています。しかし、両親を失望させたように、私たちのほとんどはエンジニアではなく、コンピューターのキーボードに縛り付けられた猿を無限に集められたような集団にすぎません。（伝説によれば、私たちはいつの日か、まったくの偶然から『ハムレット』を作曲するらしいです。せいぜい気を付けて、GPT-4）。

しかし、このセクションでは、社会にとってあまり有益ではない、もう1つのエンジニアであるソーシャルエンジニアを取り上げます。この攻撃パターンの解説では、私たちが生まれながらにして持っている親切な性質を利用して、私たちを操り、被害に遭わせる攻撃者が使う手口に焦点を当てます。このパターンの攻撃者は、私たちに返信や行動を起こさせるために偽りの危機感を与えたり、権威者からの請願書類を作成したり、あるいは既存の通信スレッドを乗っ取って機密データを開示させたり、自分たちのために何らかの行動を起こさせたりするなど、さまざまな戦略を組み合わせてこの攻撃を行います。「ソーシャルエンジニアリング」は、ナイジェリア王子詐欺のような単純なものから、検知するのがはるかに困難な手口へと大きく進歩しています。「ソーシャルエンジニアリング」が増加の一途をたどり、現在、この調査結果の上位3つのパターン（データ漏洩/侵害の17%、インシデントの10%）を占めているのは、このように巧妙さを増した手口によるものです。

今後はこの銀行口座番号を使用してください

フィッシングと、より複雑なソーシャルエンジニアリングの見分け方に関して、よくある誤解があります。怪しげな添付ファイルや、パスワードの更新を要求する悪質なリンクが貼られたメールを受け取ったことがない人は手を挙げてください。誰もいませんか？そうです、私たちの思った通りです。これがフィッシングで、「ソーシャルエンジニアリング」インシデンドの44%を占めています。さて、どうしてもお金が必要な友人や家族からメールやSNSのダイレクトメッセージを受け取ったことがある人はいますか？おそらく少ないでしょう。これはソーシャルエンジニアリング（具体的には「なりすまし」）であり、熟練したスキルを要します。説得力に長けたソーシャルエンジニアは、あなたの心に訴えかけ、あなたの愛する人が危険にさらされていると信じ込ませることができます。攻撃者は、あなたやあなたの大切な人について知り得た情報を使って、そのメッセージが本当にあなたの知っている人からのものだと信じ込ませ、あなたの感情につけ込んで危機感を煽ります。図35に示すように、「ソーシャルエンジニアリング」インシデントでは、「フィッシング」よりも「なりすまし」のほうが多く発生しています。しかし、確認されたデータ暴露では、「フィッシング」が依然としてトップです。

より複雑なソーシャルエンジニアリング攻撃のひとつに「ビジネスメール詐欺（BEC）」があります。このなりすまし攻撃では、攻撃者は既存のメールのスレッドやコンテキストを悪用し、取引業者の銀行口座を変更するなどの比較的日常的なタスクを受信者に要求します。しかし、悪魔は細部に宿るものであり、新しい銀行口座は攻撃者のものであるため、被害者がその口座に支払いをすべて振り込むことで、その取引業者に支払うべき金額はゼロなってしまいます。この種の攻撃は、攻撃者があらかじめ下準備を整えているため、多くの場合、発見がはるかに難しくなっています。例えば、見た目が請求元のドメインに酷似したドメインを立ち上げたり、メール署名欄の取引業者の電話番号を偽装して、自分たちの番号に差し替えたりといった手口があります。これらは、攻撃者が標的をだますために、特に似たような正当なリクエストを日常受けている標的に対して使う数多くの巧妙な偽装のうちの2つの例に過ぎません。おそらくこれが、図36に見られるように、「ビジネスメール詐欺（BEC）」攻撃がインシデントデータセット全体でほぼ倍増し、現在このパターン内のインシデントの50%以上を占めている理由の1つです。

攻撃の種類は、クリック率（開封率）にはあまり影響しないようです。添付ファイル攻撃とリンク攻撃の失敗率の中央値はそれぞれ4%と4.7%で、データ入力攻撃のクリック率の中央値は5.8%です（ただし、データ入力率は1.6%）。

図35.「ソーシャルエンジニアリング」インシデントにおける攻撃の種類（n=1,696）

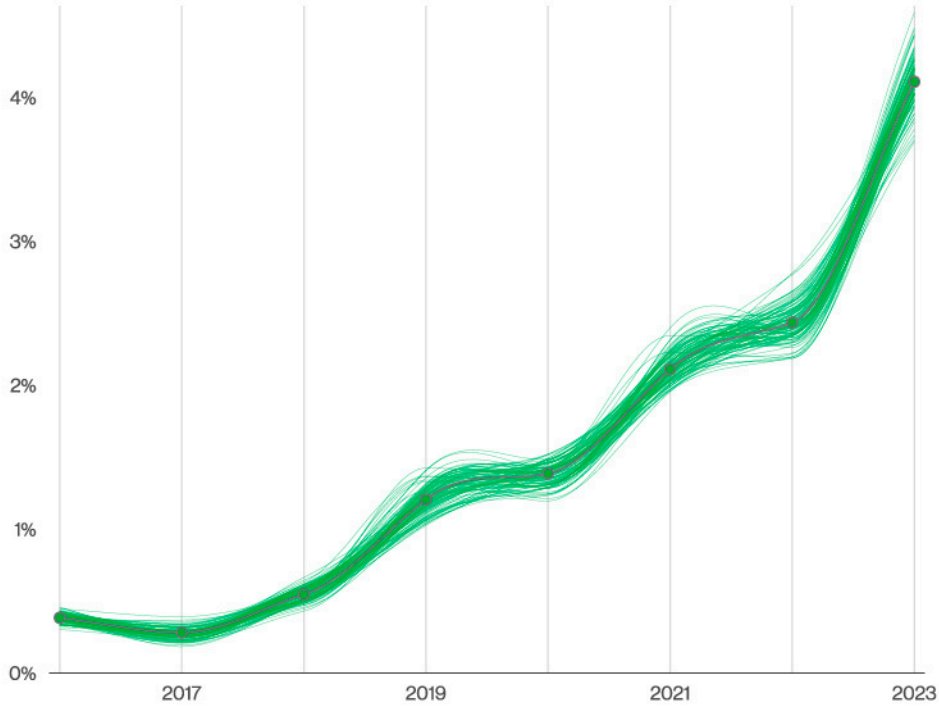


図36.「なりすまし」インシデントの経時的変化

密かな始まり

このパターンは主に人間を標的にした攻撃に基づいているため、このパターンで最初に行われる攻撃が何らかのフィッシングやなりすまし詐欺を行なうメールであることは理にかなっています（図37）。実際、このようなインシデントの攻撃経路の98%はメールですが、電話やソーシャルメディア、あるいは一部の社員には人気のない社内メッセージングアプリ（^_^;）など、他のコミュニケーション手段も時折使われます。

2つの分かれ道、などなど

最初のメールを受けた後が、攻撃の分かれ道になります。攻撃には通常、大きく分けて2つのルートがあります。最も一般的なのは、攻撃者が認証情報を要求し、それを取得した場合、その認証情報を使ってユーザの受信トレイにアクセスする方法です（インシデントの32%に見られる）。メールによるコミュニケーションを頼りに手探りで進み、攻撃者は（別の人間であるにもかかわらず）信用できるストーリーを紡ぎ出し、誰かを説得することができます。例えば、請求先の銀行口座を変更するよう誰かを説得することは、インシデントの56%に見られます。もちろん、複数の手口を組み合わせることもできます。攻撃者は、アクセスが可能になったユーザの受信トレイでハイジャックができそうなメールチェーンを探したり、アドレス帳を検索して、さらに標的にできる人物を探したりすることができます。攻撃者は、自分たちの活動ができるだけ長く発見されないように、転送ルールを追加することも珍しくありません。その理由は...

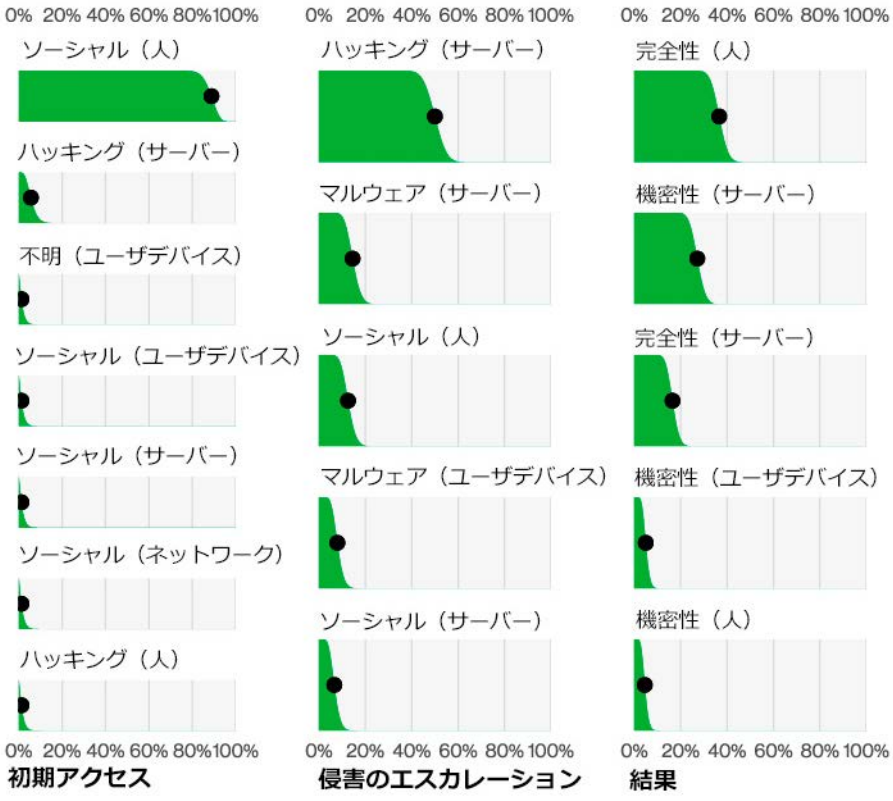


図37.「ソーシャルエンジニアリング」のデータ漏洩/侵害のステップ

時間が最も重要

ソーシャルエンジニアリング攻撃に対応する場合（ほとんどの攻撃についても同じことが言えますが）、迅速な検知と対応が鍵となります。タイムリーな検知が重要であることは、図38に示すように、「ビジネスメール詐欺（BEC）」のコストの中央値が2018年から右肩上がりで上昇し、現在では5万ドル台で推移していることからも浮き彫りにされています。しかし、私たちが現実に生きている時代とは異なり、このセクションは悲観的な情報ばかりではありません。被害者にとっては幸いなことに、法執行機関は銀行と協力して「ビジネスメール詐欺（BEC）」のような攻撃から盗まれた金銭の回収を支援するプロセスを開発しました。被害者の50%以上が、盗まれた金銭の少なくとも82%を取り戻すことができました。このことは、従業員が安心して潜在的なインシデントをセキュリティに報告できるようにすることの重要性を示しています。なぜなら、従業員が進んで報告することで、組織の対応能力が大幅に向上するからです。このことを念頭に置き、企業は「非クリック率が向上するまでフィッシング演習を続ける」というスタンスから脱却し、社内の協力体制が整ったセキュリティアプローチを採用することをお勧めします。

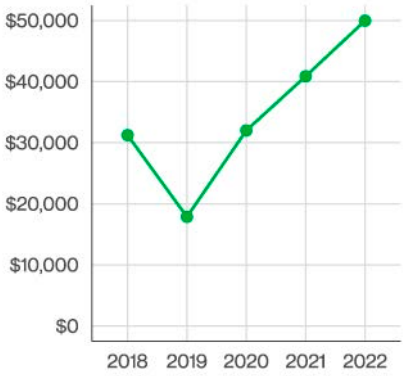


図38. ビジネスメール詐欺（BEC）の取引額の中央値（n=73,420）
取引額が発生したFBI IC3への苦情に基づく

検討すべきCISコントロール

この複雑な脅威に立ち向かう際に考慮すべきコントロールはかなり多く、そのすべてに長所と短所があります。このパターンでは関連する人的要素が強いため、コントロールの多くは、ユーザによる攻撃の検知と報告を支援することと、フィッシングのおびき寄せの被害に遭ったユーザのアカウントを保護することに関連するものとなっています。最後に、「ビジネスメール詐欺（BEC）」への対応において法執行機関が果たす役割は重要であるため、計画や連絡先を事前に用意しておくことが重要です。

ビジネスメール詐欺（BEC）はなぜ機能するのか？

「ビジネスメール詐欺（BEC）」は、組織のネットワークへのアクセスを収益化する「ランサムウェア」と同様に、犯罪者が ユーザの受信トレイや連絡先へのアクセスを収益化する数ある手段の1つに過ぎません。

- 「ビジネスメール詐欺（BEC）」は組織の内部を標的にすることができます。つまり、攻撃者は侵害された従業員のメールアカウントを使って、ユーザになりすますことでその組織を標的にします。一般的に、攻撃者は給与振込先を自分の管理する口座にリダイレクトしようとします。
- あるいは、従業員のメールアカウントにアクセスすることで、パートナーを標的にすることもできます。つまり、そのユーザになりすまし、自分の銀行口座を含めるために支払いの更新を要求するのです。

アカウントの保護

アカウント管理［5］
- アカウントのインベントリを確立し維持する［5.1］
- 休止アカウントを無効にする［5.3］

アクセス制御管理［6］
- アクセス権限を付与するプロセスを確立する［6.1］
- アクセス権限を停止するプロセスを確立する［6.2］
- 外部公開アプリケーションに多要素認証を義務付ける［6.3］
- リモートネットワークアクセスに多要素認証を設定する［6.4］

セキュリティ意識向上プログラム

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［14］

CISコントロールには含まれませんが、「ビジネスメール詐欺（BEC）」と銀行口座の更新に関連するプロセスに特に重点を置く必要があります。

インシデントレスポンスの管理

インシデントレスポンス管理［17］
- インシデントハンドリングをサポートする管理担当者を指名する［17.1］
- セキュリティインシデントを報告するための連絡先を収集し維持する［17.2］
- インシデントの報告に関する組織全体の基準を策定し維持する［17.3］

基本Web アプリケーション攻撃

概要

DBIRのデータセットの約4 分の1を占める「基本Webアプリケーション」攻撃によるデータ漏洩/侵害やインシデントは、主に認証情報に対する攻撃によって引き起こされる傾向があり、攻撃者は盗んだ認証情報を悪用してさまざまなリソースにアクセスします。

昨年との比較

不適切なパスワード選択と保護は、このパターンにおけるデータ漏洩/侵害の主要な原因の1つであり続けています。

頻度	インシデント1,404件、確認されたデータ暴露1,315件
攻撃者	外部（100%）、内部（1%）、複数（1%）（漏洩/侵害）
攻撃者の動機	金銭目的（95%）、スパイ活動（4%）、愉快（1%）（漏洩/侵害）
侵害されたデータ	認証情報（86%）、個人情報（72%）、内部情報（41%）、その他（19%）（漏洩/侵害）

誰がやったのか？

データ漏洩/侵害の背後にいる攻撃者が、サイバー版「クルー」ゲームの登場人物であると想像することは、私たちの平凡な日常に面白みを与えてくれるかもしれませんが[37]、盗まれた認証情報やよく知られた脆弱性を利用した平均的な名もなき人物である可能性の方が高いでしょう。

このパターンは、DBIRのデータ漏洩/侵害全体の25%を占め、組織の資産へのアクセスを取得するために盗まれた認証情報と脆弱性を利用することで主に構成されています。この前線基地を足がかりにして、攻撃者はメールに隠された重要な情報を盗んだり、リポジトリからコードを抜き取ったりと、さまざまなことが可能になります。このような攻撃は複雑ではありませんが、確かに効果的であり、DBIRのデータセットの中では比較的安定した地位を保っています。そこで改めて（ドラムロールをお願いします）、多要素認証（MFA）とパッチ管理の重要性について説明したいと思います[38]。

関連するATT&CKテクニック

ブルートフォース ： T1110
- クレデンシャルスタッフィング：T1110.004
- パスワード解析：T1110.002
- パスワード推測：T1110.001
- パスワードスプレー：T1110.003

アカウントの侵害：T1586
- メールアカウント：T1586.002

公衆用アプリケーションの悪用：T1190

外部リモートサービス：T1133

有効なアカウント ： T1078
- デフォルトアカウント：T1078.001
- ドメインアカウント：T1078.002

代替認証情報の使用：T1550
- アプリケーションアクセストークン：T1550.001

アクティブスキャン ： T1595
- 脆弱性スキャン：T1595.002

37 データ漏洩/侵害は、インターネットからアクセス可能なサーバー上の複雑なゼロデイを介した謎のSpiderladyによって引き起こされたのでしょうか？それとも、Kubernetesクラスタ内でドローンを使ったSophisticated Pandaによる犯行なのでしょうか？

38 そう、これは情報セキュリティのトピックにおける春の訪れを占う「グラウンドホッグ・デイ」のようなものです。きっと過去の報告書にも載っているはずです！

図39.「基本Webアプリケーション攻撃」によるデータ漏洩/侵害において上位を占める攻撃の種類（n=1,287）

初期アクセス

図39が示すように、データ漏洩/侵害の86%は、「盗まれた認証情報の悪用」が関与しています。そして、私たちの機密情報を含む様々なWebサーバーに対して、これらの認証情報を使用するのに最も適した場所はどこでしょうか？このパターンにおけるパズルのもう1つの主要な部分は、セキュリティ上の弱点を突くツールの使用です。これは、攻撃者がセキュリティ上の弱点を突くツールを持っていて、被害者がたまたま脆弱性（犯罪者にとって便利なもの）を抱えている場合です。これは通常、データセットのわずか10%程度で発生しており、侵害の数としては取るに足らないもののように聞こえるかもしれませんが、パッチが適用されていない脆弱性は、多くの攻撃者にとって依然として好物であり、50%の組織が今年39件以上の「Webアプリケーション」攻撃を経験しています[39]。

侵害のエスカレーション

私たちがこれらの攻撃を「基本的なもの」と呼んでいるとしても、Webアプリケーションに対して認証情報が利用され、攻撃者がそのまま去っていくというような、単純に「1回で終わる」インシデントではありません。多くの場合、何らかの中間ステップが存在します（図40）。例えば、マルウェアは「永続化」（見てください、ATT&CKの用語を使っていますよ）を維持するための主要な手段の1つであることが多く、インシデントの約2%は「バックドア」または「C2（Command & Control）」です。その他のケースでは、攻撃者は現在のアクセス権を利用して追加攻撃を行います。

39 この種の攻撃を実行する利点の1つは、サーバーが決して疲れることなく、眠ることもなく、昼夜を問わず誰に対してもセキュリティ上の弱点を突くツールを投げ続けることです。これが、少なくとも1日4杯のコーヒーと9時間の睡眠が必要な、謙虚なサイバーセキュリティアナリストとは違うところです。

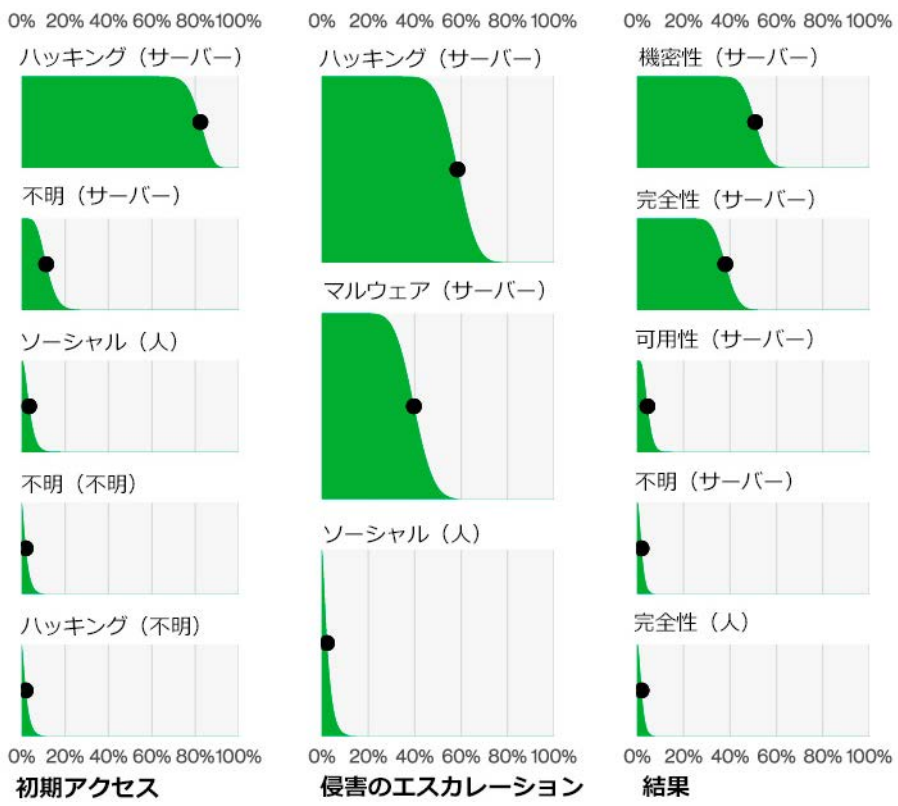


図40. 基本Webアプリケーション攻撃のステップ

影響

影響に関しては、「Webアプリケーション」に続いて、「メールサーバー」が攻撃者にとって好ましい標的の1つであることが一般的です。これは理にかなっており、何百通もの未読メール[40]の受信トレイの中には、しばしば重要な内部文書（侵害の41%はメールサーバーが関係）や、悲しいことに、他のシステムの認証情報が隠されているからです。このパターンの調査結果は、攻撃者が単純な受信トレイマイニングの手口を使って、「内部情報」（41%）、「医療情報」（6%）、さらには「銀行情報」（6%）にアクセスできることを示しています（繰り返しになりますが、メールとサーバーの衛生管理の重要性を再認識させられます）。

40 ごめんね、おばあちゃん。

1つだけを食べるわけにはいかない

「ユーザ名とパスワードをもっと多く覚えられていれば...」というのは、おそらくあまり耳にしない言葉でしょう。認証情報は砂漠の砂のようにどこにでもあり、それを保持することはほとんど困難なのです。同様に、攻撃者は豊富な供給源も持っているようです。しかし、私たちはバイアスと制限に関して明らかにするようにしているのですが、私たちのデータに欠けているのはこれらの認証情報がどこから漏れたのか私たちは必ずしも知らないということです。しかし、DBIRチームはみんなミステリー好きです。犯人は執事か？エイリアンは実在するのか？イエティは？幽霊は？仕事に熱心な人たち？残念ながら、私たちはおそらく知ることはないでしょう。そもそも犯罪者たちがどこで認証情報を手に入れたのかも知り得ないかもしれません。認証情報を取得するさまざまな方法については、ある程度思いつくかもしれません。例えば、ソーシャルエンジニアリングによって認証情報を入手するパスワード窃盗犯から認証情報を買うとか、あるいは総当たりのブルートフォース攻撃で認証情報をまき散らすなど。しかし、データ漏洩/侵害やインシデントのうち、どれだけがそれぞれの手口で引き起こされたものなのか、正確な内訳はわかっていません。古い格言に「知っていることは一滴、知らないことは大海」というのがあります。

しかし、悪いニュースばかりではありません。認証情報を盗む方法はたくさんありますが、守る方法もたくさんあります。その最良の方法のひとつが（このことを聞いたことがある人は私を止めてくださいね）、多要素認証（MFA）の実装です。「さて、実際のところ.....」と椅子に凭れかかる前に、私たちはいくつかのMFAの実装には限界があることを認識しています。皆さんもご存知の通り、今年、いくつかの非常に有名な情報漏洩が、そのような欠点のいくつかを示しました。あるケースでは、犯罪者はソーシャルエンジニアリングを使って、認証情報の入力試行を受け入れるようにユーザを説得しました。また、セッションクッキーを盗み出し、それを使ってユーザになりすましたケースもありました。もちろん、いくつかのMFA回避は、サービスの一部がMFAのみを使用するように適切に設定されていなかったため、実際にはMFAを迂回していました。前述したように、標準のVERISを更新し、データを収集する必要があるため、現時点では、それぞれのMFA回避がどの程度あったかをお伝えすることはできません。これは、最終的にスコアを解決し、どのMFAがより優れているか、どの迂回路が最も利用されているかを議論する素晴らしい機会ですが、私たちはもう1年間、このプレースホルダーを維持しなければならないでしょう。

引用元: Jen Easterly氏

アメリカ合衆国
サイバーセキュリティ・
社会基盤安全保障庁
ディレクター

米国のサイバー防衛機関として、合衆国サイバーセキュリティ・社会基盤安全保障庁（CISA）は、米国の敵対者がどのように活動し、どのようなツールを使用しているかを監視しています。これらの敵の一部は高度なツールやテクニックを使用していますが、ほとんどはパッチが適用されていない脆弱性、不十分なサイバー衛生、またはMFAのような重要なテクノロジーを導入していない組織の失敗を利用しています。悲しいことに、データ漏洩/侵害を経験するまで、MFAがどれほど貴重なものであるかを知る組織はあまりに少ないのです。

CISAに加入して以来、私は、米国の重要インフラをよりよく保護するために、あらゆる部門でMFAの認知度を高めることを優先してきました。重要なことは、私たちがサイバー分野で直面している脅威の範囲と解決策を理解するためには、より多くの優れたデータが必要だということです。私たちは、防衛側が国民、顧客、企業を適切に監視し、理解し、最終的に保護できるようにするため、業界のパートナーに抜本的な透明性を提供するよう求めてきました。特に、システム管理者やSaaS（サービスとしてのソフトウェア）のスタッフのような攻撃者にとって「価値の高いターゲット」がフィッシングに強いMFAを使用することは非常に重要です。

しかし、有用な情報を多く収集することは、始まりに過ぎません。

協力し合い、米国のレジリエントと安全性を高め、測定可能な進歩を示すために、そして来年のベライゾンのデータ漏洩/侵害調査報告書を含め、私たちが一緒に何ができるかを見ていきたいです。

検討すべきCIS コントロール

アカウント保護による盗まれた認証情報への対策

アカウント管理［5］
- アカウントのインベントリを確立し維持する［5.1］
- 休止アカウントを無効にする［5.3］

アクセス制御管理［6］
- アクセス権限を付与するプロセスを確立する［6.1］
- アクセス権限を停止するプロセスを確立する［6.2］
- 外部公開アプリケーションに多要素認証を義務付ける［6.3］
- リモートネットワークアクセスに多要素認証を設定する［6.4］

脆弱性の悪用への対策

継続的な脆弱性管理［7］
- 脆弱性管理プロセスを確立し維持する［7.1］
- 修復プロセスを確立し維持する［7.2］
- オペレーティングシステムへの自動化されたパッチ管理ツールを適用する［7.3］
- アプリケーションへの自動化されたパッチ管理ツールを適用する［7.4］

MFAを回避する攻撃を捕捉するためにVERISをどのようにアップデートしたかに興味がある方は、以下のリストをご覧ください。

1.セカンダリ認証メカニズムの乗っ取り（ハイジャック）を示す新しい攻撃を追加

2.認証情報以外の他の要素が窃取されたかどうかを示す新しいデータの種類「Multifactor credential（多要素認証情報）」を追加

3.ユーザに対して迷惑レベルの認証要求を送信することを目的とした攻撃のために、プロンプト爆撃（Prompt Bombing）[41]というソーシャル攻撃の種類を追加

うまくいけば、既存のリストにこれらの新しいリストを追加することで、我々が遭遇するケースの大半を捕捉することができると思われます。そうでない場合は、VERISの次のバージョンでリストの再検討を行ないます。

41 これは、タイムリーに人々の写真に紛れ込む人をそう呼ぶ（photobomb）ような響きがありますね。

多種多様なエラー

サマリー

「誤送信」、「設定ミス」、「公開エラー」が引き続き主役であり、データの漏洩/侵害につながるエラーは、「システム管理者」と「開発者」が最も多く犯しています。

昨年との比較

従業員は相変わらずミスを犯し続け、時にはそれが組織に大きな損害をもたらすことがあります。

頻度	インシデント602件、確認されたデータ暴露512件
攻撃者	内部（99%）、パートナー（2%）、複数の関係者（1%）、外部（1%）（漏洩/侵害）
侵害されたデータ	個人情報（89%）、医療情報（19%）、その他（10%）、銀行情報（10%）（漏洩/侵害）

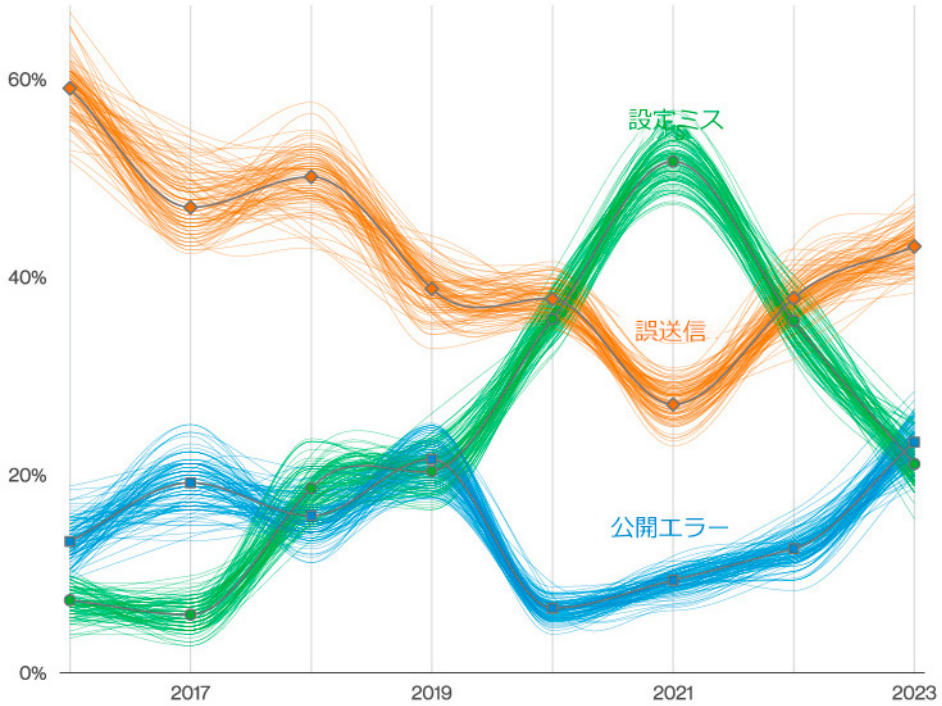


図41. 多種多様なエラーによるデータ漏洩/侵害の攻撃の種類における経時的変化

最近は良いヘルプが見つからない

イギリスの偉大な詩人でありエッセイストであったAlexander Popeは、かつて次のようなことを言いました。「物事を台無しにしない人を雇うのは難しい」と。まあ、多かれ少なかれそのような内容でした。そのまま受け止めてください。誰が何を言ったか（あるいは言わなかったか）にかかわらず、「多種多様なエラー」パターンは、私たちの侵害データのかなりの部分を占めています。もしあなたが「コップにまだ半分も残っている」という楽観的な読者であれば、昨年は13%であったエラー関連のデータ漏洩/侵害が今年は9%に減少しているという事実に安心するかもしれません。あるいは「グラス半分は空っぽ」という悲観的な読者なら、昨年は715件のエラーインシデントと708件のデータ漏洩/侵害が確認されたのに対し、今年は602件のインシデントと512件のデータ漏洩/侵害しか確認されなかったので、単純に報告のせいだと考えるかもしれません。

私のお気に入りのミスだ

「お気に入り」という表現は強すぎるかもしれません。「誤送信」（間違った受信者に何かを送信すること）は、私たちのデータセットにおけるデータ漏洩/侵害関連エラーの43%を占めています（図41）。「公開エラー」（間違った閲覧者に何かを見せること）は23%で2位です。最後に、うっかり者の攻撃タイプとして大人気の「設定ミス」が3位に入り、エラー関連のデータ漏洩/侵害の21%を占めています。これでは、人は信頼できないものだと考えてしまうかもしれません。

しかし、少なくともミスの種類を変えることで、物事を面白くし、あなたを飽きさせないようにすることはできます。

実際、図41が示すように、「設定ミス」と「誤送信」は、ここ数年、まるで天体の振り付けされたダンスの一部のように、浮き沈みを繰り返しています。昨年の報告書では、「誤送信」と「設定ミス」は収束していましたが、今年は「誤送信」がまた台頭しています[42]。一方、私たちと古くから付き合いのある「公開エラー」は坂を下り、再び「設定ミス」に出会っています。

もう少し掘り下げてみると（図42）、これら3つの「エラー」タイプが他のエラーに群を抜いていることがわかります。しかし、「失言」が常に最下位または最下位に近い位置にあることを、チームは残念に思っています（私たち自身がどれだけの失言をしたかを考えると）。

図43に示されているように、データ漏洩/侵害につながるエラーの大部分は「開発者」と「システム管理者」が犯しており、「エンドユーザ」も散見されます。データ漏洩/侵害で最も頻繁に見られる「エラー」のタイプを考えると、データの保守や環境の維持に責任を持つ者たちが、最も頻繁にその発生の責任を負うことは驚くにはあたりません。責任といえば、「不注意」というエラー要因は98%のケースで見らました。なんてことでしょう！Popeは何かつかんでいたのかもしれないですね。

図42. 多種多様なエラーによるデータ漏洩/侵害において上位を占める攻撃の種類（n=450）

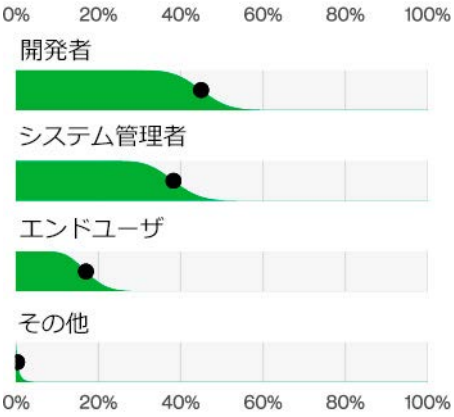


図43. 多種多様なエラーによるデータ漏洩/侵害において上位を占める攻撃者の種類（n=89）

検討すべきCISコントロール

データ管理

データ保護［3］
- データ管理プロセスを確立し維持する［3.1］
- データインベントリを作成し維持する［3.2］
- データアクセス制御リストを設定する［3.3］
- データの保持を徹底する［3.4］
- データを安全に廃棄する［3.5］
- 機密度に応じてデータ処理・保管を分離する［3.12］
- データ盗難防止ソリューションを導入する［3.13］

セキュアなインフラストラクチャ

継続的な脆弱性管理［7］
- 外部公開している組織の資産に対する自動化された 脆弱性スキャンを実施する［7.6］

アプリケーションソフトウェアのセキュリティ［16］
- アプリケーションインフラストラクチャには、標準的なハードニング設定テンプレートを使用する［16.7］
- アプリケーションアーキテクチャにおけるセキュアな設計原則を適用する［16.10］

従業員への教育

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［14］
- データの取り扱いのベストプラクティスについて従業員にトレーニングを行う［14.4］
- 意図しないデータ漏洩の原因について従業員にトレーニングを行う［14.5］

アプリケーションソフトウェアセキュリティ［16］
- アプリケーションセキュリティの概念とセキュアコーディングについて開発者をトレーニングする［16.9］

42 もしあなたが「誤送信」の星の下で生まれたなら、もうすぐ良い知らせがあるはずです。ラッキーナンバーは3、9、13、33です。

サービス拒否（DoS）

サマリー

「サービス拒否（DoS）」がインシデントの大半を占め続ける中、対策サービスの能力も向上しています。しかし、依然として企業に問題を引き起こしている少量の攻撃も復活しています。

昨年との比較

「サービス拒否攻撃（DoS）」は引き続きどこにでも発生し、ここ数年はインシデントの上位を占めています。

頻度	インシデント6,248件、確認されたデータ暴露4件
攻撃者	外部（100%）（インシデント）

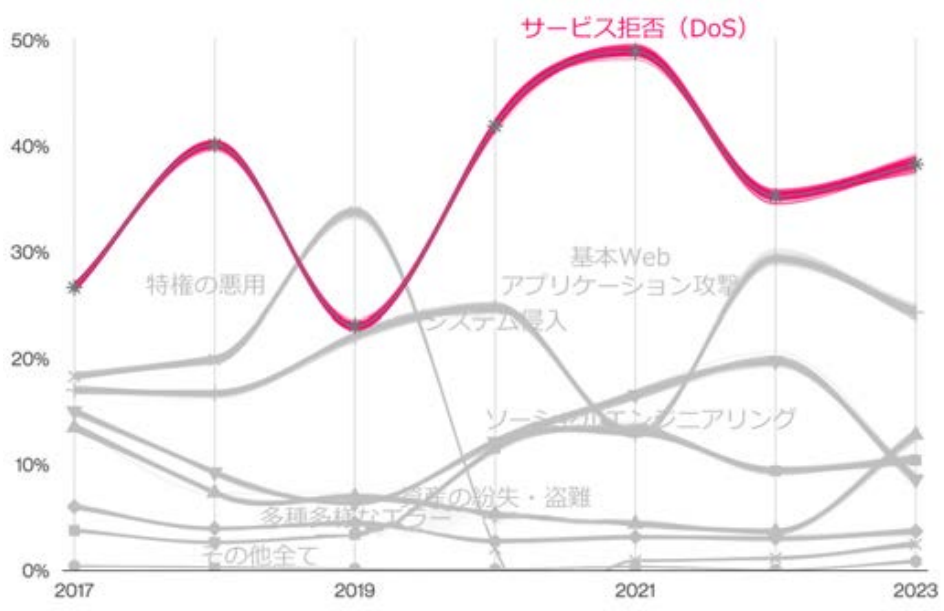


図44. インシデントにおけるパターンの経時的変化

我々は拒否されない

その名前が意味するように、「サービス拒否（DoS）」パターンには、『Below Deck』の次のエピソードをストリーミングしたり、次のTikTokムービーを見たり、X（旧Twitter）のタイムラインを読み込んだりするのを妨げようとする攻撃のすべてが含まれます[43]。悲しいことに、明らかにこうしたことは現実の世界や私たちの周りで起こる迷惑になると認めなければなりません。それは本当にひどいことだと誰もが同意できることです。

しかし、読者の中にはご存知の方もいらっしゃるかもしれませんが、組織がビジネスを行うためには、インターネットを立ち上げ、稼働させる必要があるのです。毎年、「サービス拒否（DoS）」は、ベライゾンのものを含め、いくつかの異なる対策サービスパートナーに起因するインシデントとして、DBIRのデータセットに大量に現れます。こうしたインシデントが組織に重大な影響を与えるのを防ぐため、どの対策サービス会社も素晴らしい仕事をしています。このように考えると、「サービス拒否（DoS）」のパターンがここ数年間一貫してインシデントの首位を占めているにもかかわらず（図44）、インターネット上のネットワークの継続的な可用性を重視するのであれば、何らかの対策サービスに投資することをお勧めします。

43 この件に関して、いつもの攻撃者を非難できるかどうかはわかりません。

これは、「拡散型サービス拒否（DDoS）」データセット全体にニュアンスが欠けているためではなく、「攻撃者」、「資産」、「属性」など、従来分析している典型的な詳細が欠けていることの反映です。

とはいえ、「サービス拒否（DoS）」のセクションを読者に提供しないわけにはいきません。というのも、まだまだ重要なトレンドや見直すべき情報があるからです。たとえ簡単に解決できるとしても、これらの攻撃がまだ存在することを認識するのは重要なことです。また、「ランサムウェア」について2、3ページ書かなくて済むのは、息抜きにもなります。

もっと太い帯域幅が必要だ

重要なポイントとして、「拡散型サービス拒否（DDoS）」攻撃の1秒あたりのビット数の中央値および中央値を超えるパーセンタイルの増加について触れておきます（図45参照）[44]。中央値は昨年の1.4ギガバイト/秒（Gbps）からなんと57%[45]も増加して現在は2.2Gbpsに達し、97.5パーセンタイルは99Gbpsから124Gbpsへと25%増加しています。これは、帯域幅とCPU処理にかかるコストがより身近で利用しやすくなるにつれて予想されることであり、攻撃者と対策サービス間の競争が激化していることから、この傾向はなかなか崩れないことが示唆されます。契約している対策サービスがそのハードルをクリアできることを確認するだけで、ほとんどの影響は吸収できると思われます。映画のトランスフォーマー風にマシンを戦わせ、冷たい飲み物を開けながら、企業を苦しめる他の攻撃パターンを心配するというのはいかがでしょうか。

ネットワーク上のゴミの量が増えても、もっと巧妙な手口の攻撃も行なわれます。私たちのパートナーの何人かから提供された注目すべき情報は、分散型DNS Water Torture（水責め）[46]攻撃が、ご想像の通り、共有DNSインフラで増加していることでした。これは基本的に、DNSキャッシュサーバーにランダムな名前の接頭辞を問い合わせることでリソースを枯渇させる攻撃で、常に失敗し、権威サーバーに転送されます。考えてみればバカバカしいことですが、攻撃者にコントロールされたデバイスで単純な調整を行うだけで、大きな負担となる可能性があります。DNSインフラの回復力を確認し、対策サービスのオプションも確認して、これらの攻撃からも保護されていることを確認する必要があります。

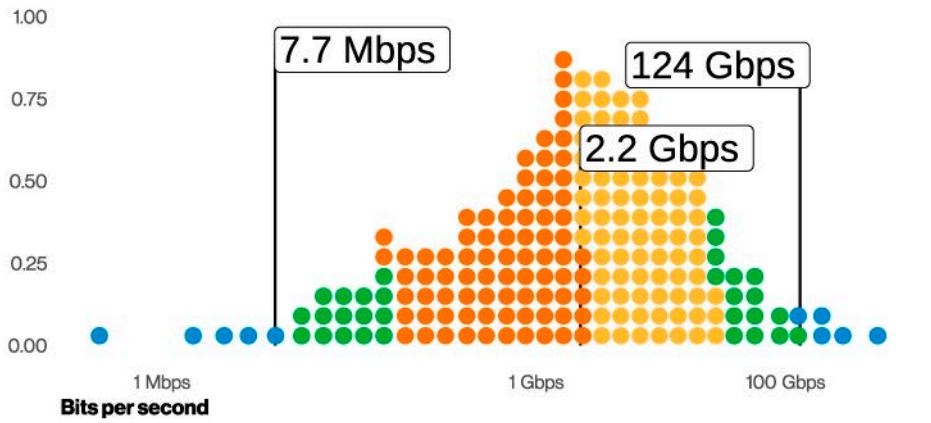


図45. DDoSインシデントにおける1秒あたりのビット数（n=10,622）

44 パーティでは必ずこのことを話題にするとよいでしょう。きっと人気者になれます。
45 アメリカのインフレ率が悪いと思ったのではないでしょうか？
46 これは言い得て妙な名前ではない！

資産の紛失・盗難

サマリー

これらの小型（それほど小型でなくとも）デバイスは非常に携帯性に優れているため、このパターンは組織にとって引き続き問題となっています。私たちは、大量のデータを保存するデバイスの容量が時間の経過とともに増加する一方で、従業員がデバイスを置き忘れる（または「外部」の攻撃者がデバイスを盗む）可能性があることを予見してきました。

昨年との比較

デバイスやメディアの紛失は、「外部」からの盗難よりも「内部」関係者によるものが依然として多くなっています。

頻度	インシデント2,091件、確認されたデータ暴露159件
攻撃者	外部（92%）、内部（68%）、複数（60%）、パートナー（1%）（漏洩/侵害）
攻撃者の動機	金銭目的（100%）（漏洩/侵害）
侵害されたデータ	個人情報（87%）、医療情報（30%）、その他（21%）、銀行（13%）（漏洩/侵害）

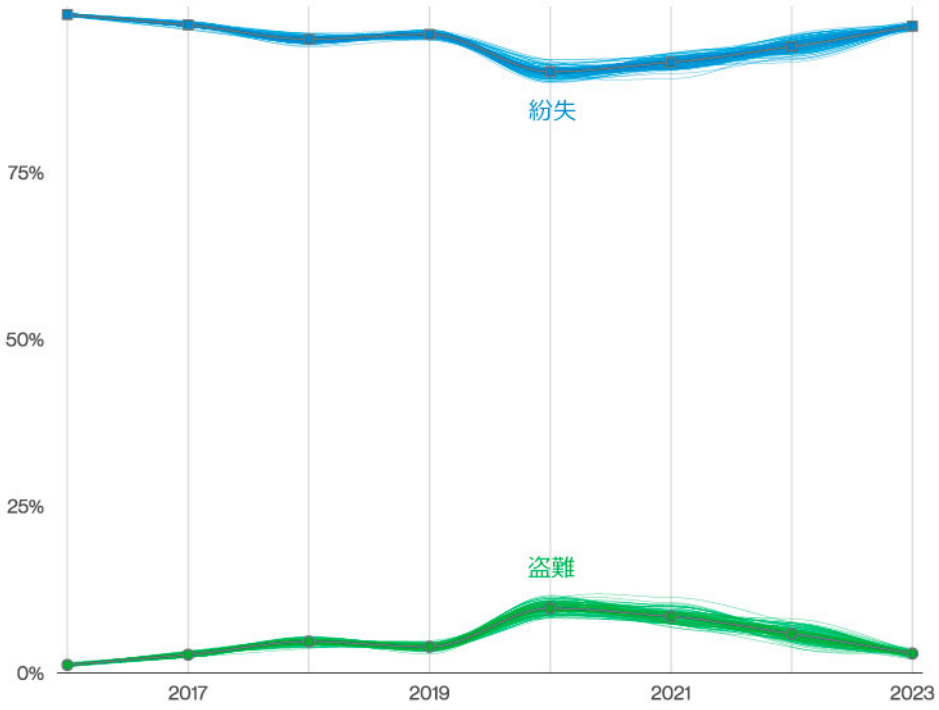


図46. 資産の紛失・盗難インシデントにおいて上位を占める攻撃の種類

私のラップトップはどこ？

このパターンの見出しは「あなたのものがなくなりました」であり、決してニュース速報の見出しではありません。紛失したアイテムが、誰かがノートPCを盗んだという「幇助」があったにせよ、政府高官の住居で機密印刷文書が紛失したような偶発的なものであったにせよ、持ち運び可能な資産であればあるほど、紛失や盗難に対する保護が必要になります。

これは、データ漏洩/侵害が確認されないインシデントの割合が高いパターンであり、その主な理由は、当該資産の保管が失われたことにより、機密漏洩のステータスが「確認」ではなく「危険」のままであるためです。例外は印刷物ですが、これは印刷された文書を閲覧できないようにする管理は存在しないからです。昨年同様、データ漏洩/侵害が確認されたインシデントの割合は10%未満でした。

盗難されたデバイスは確かに組織にとってのリスクではありますが、従業員が紛失することによって偶発的にデータの漏洩/侵害を引き起こす可能性の方がはるかに高くなります。図46に示すように、この事実は毎年一貫した真実であるようです。

何が紛失しているのでしょうか？当然のことながら、ユーザのノートパソコンや携帯電話などのポータブルデバイスです。実際、携帯電話の紛失はかなり日常茶飯事になっています（図47）。誰も手放さないという事実を考えると、これほど多く紛失しているとは信じられません。

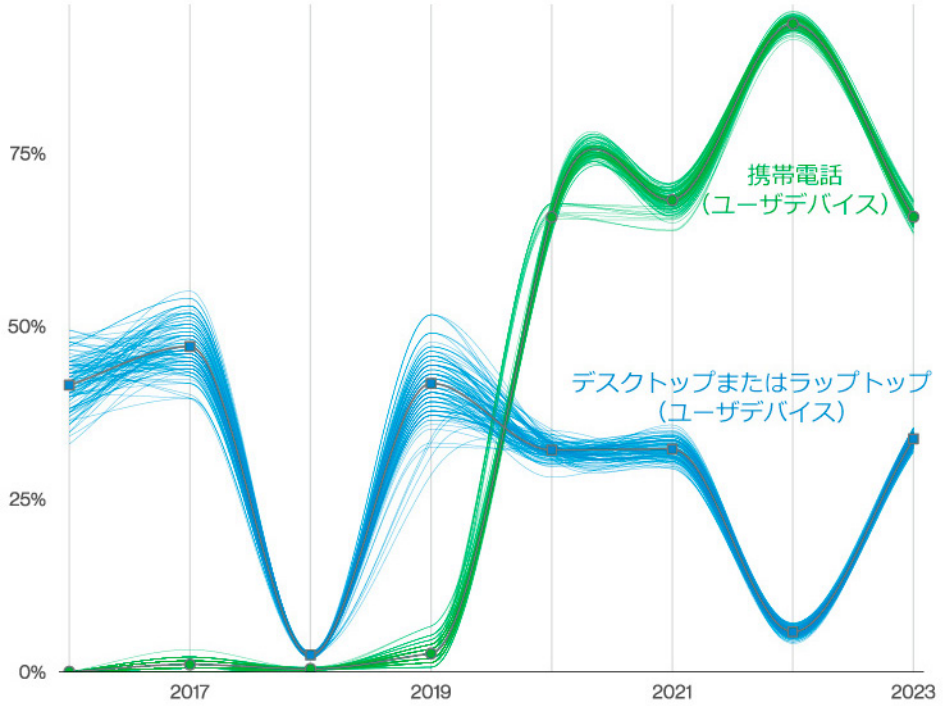


図47. 紛失・盗難インシデントにおける上位資産

検討すべきCIS コントロール

保管データの保護

データ保護［3］
– エンドユーザデバイス上のデータを暗号化する［3.6］
– リムーバブルメディアのデータを暗号化する ［3.9］

企業資産およ びソフトウェアのセキュアな設定［4］
– ポータブルエンドユーザデバイスに自動デバイスロックアウト設定を行う［4.10］
– ポータブルエンドユーザデバイスのリモートワイプ機能を適用する［4.11］

特権の悪用

サマリー

従業員がそのアクセス権を使用して不正侵入をはたらき、場合によっては不正な取引を開始することがあります。今年は、さまざまな種類の攻撃者による共謀が見られました。

昨年との比較

このパターンは、定義どおり、引き続き「内部」攻撃者によって支配されています。大半は金銭の取得を動機としており、「個人情報」は好んで狙われ続けています。

頻度	インシデント406件、確認されたデータ暴露288件
攻撃者	内部（99%）、 複数（7%）、 外部（6%）、 パートナー（2%） （漏洩/侵害）
攻撃者の動機	金銭目的（89%）、 怨恨（13%）、 スパイ活動（5%）、 利便性（3%）、 愉快（3%）、 イデオロギー（2%） （漏洩/侵害）
侵害されたデータ	個人情報（73%）、 医療情報（34%）、 その他（18%）、 銀行情報（12%）、 決算情報（12%） （インシデント）

図48. 特権の悪用によるデータ漏洩/侵害における内部攻撃者の動機（n=59）

従業員に愛されている

従業員は、自分がデータ漏洩/侵害から免れると思っているかもしれません。自社のセキュリティ管理体制に信頼を置き、難攻不落の防御策があると思い込んでいるかもしれません。また、「レーダーの監視下にある」ことに信頼を置いたり、情報漏洩を起こすには規模が小さすぎると考えたりすることもあるかもしれません。しかし、このような考え方はほとんど、侵害が外部から、つまり組織の外部にいる「悪質な攻撃者」からもたらされることを前提としています。内部犯行による侵害のリスクは考慮されていないのです。「もちろん、私の部下はそんなことはしないです！」と彼らは言います。しかしもちろん、彼らはそうするだろうし、 私も「もちろん」なんて信じません。

従業員の中にも、悪意のある理由でデータ漏洩/侵害を引き起こす者がいるという事実を直視するのは難しいことです。事故以外で、最も一般的な内部要因によるデータ漏洩/侵害は、「特権の悪用」です。これはその名の通り、従業員が仕事をするために与えられたアクセス権を悪用し、データを盗むというものです。このような行為は、金銭的な利益のために行われる可能性が非常に高くなっています（図48）。ええ、驚くべきことです。

自分自身を助ける他ありません

ここまで、従業員がこのような行為を行うことについて説明してきましたが、一覧表によると、このパターンには他の種類の攻撃者も含まれています。興味深いことに、7%のデータ漏洩/侵害で複数の種類の攻撃者（「内部」、「外部」、「パートナー」の3つの組み合わせ）が確認されています。これは共謀であり、複数の種類の「攻撃者」が協力してデータ侵害を引き起こしている証拠です。

実際、組織化された詐欺集団が、大規模な詐欺を実行するために企業に雇われることを目的に人を送り込んでいる事例が見られます。私たちはこのような事例を複数の業界で見てきており、組織を長年にわたって悩ませ続けています。このような人物を見分けるのは難しいです。プレゼンテーションやインタビューに長けた人物かもしれません。金銭目的を動機とする犯罪グループによるこうした行為によって、このような人々が可能にする不正なアクセスを捕捉するために、検知制御を導入することの重要性がますます高くなっています。このようなインシデントに対応する際の難しさの1つは、どんな企業でもオンボーディングプロセスは完璧ではなく、ほとんどのオンボーディングでは、IT部門が直接管理しているとは限らないさまざまなグループやシステムに新入社員を配属する必要があることです。こうした調査によって、ITインフラにおけるプロセスに関連した弱点が明らかになることがよくあります。

図49に示すように、「特権の悪用」と「不正取引」が組み合わされたデータ漏洩/侵害が、過去数年よりも今年の方が増加しています。「不正取引」は、「ビジネスメール詐欺（BEC）」の最終目的である完全性（Integrity）の侵害であり、通常は、攻撃者が管理する銀行口座への送金となります。しかし、「内部」攻撃者は、このようなケースで銀行口座やルーティング情報が保存されているシステムにすでにアクセスしているため、あとはおそらく自身で銀行口座の変更を行なうだけでしょう。組織から重要なリソースを吸い上げることができる立場にある人物である可能性を考慮すると、「内部」攻撃者が単に資金をリダイレクトすることが増えている状況は特に懸念されます。

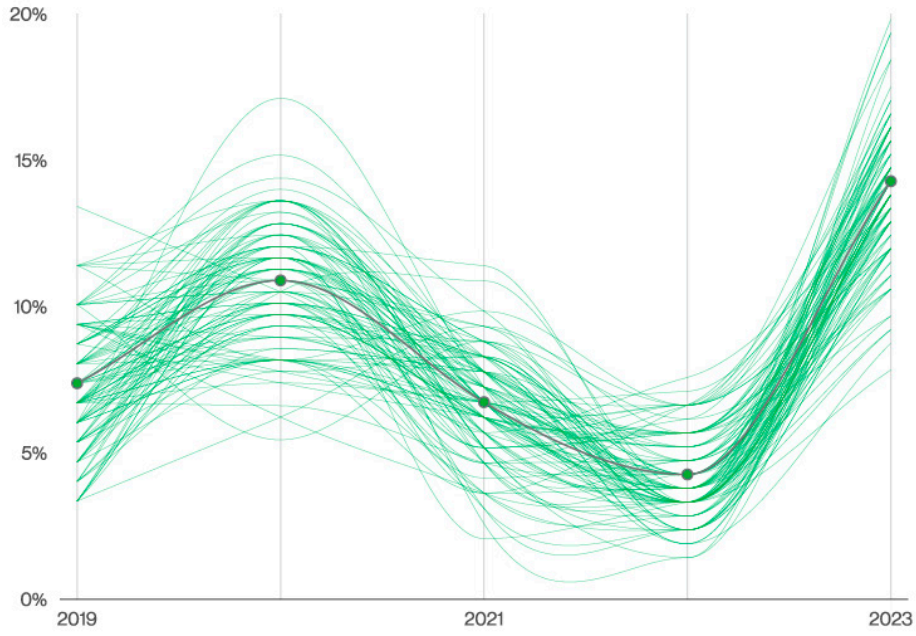
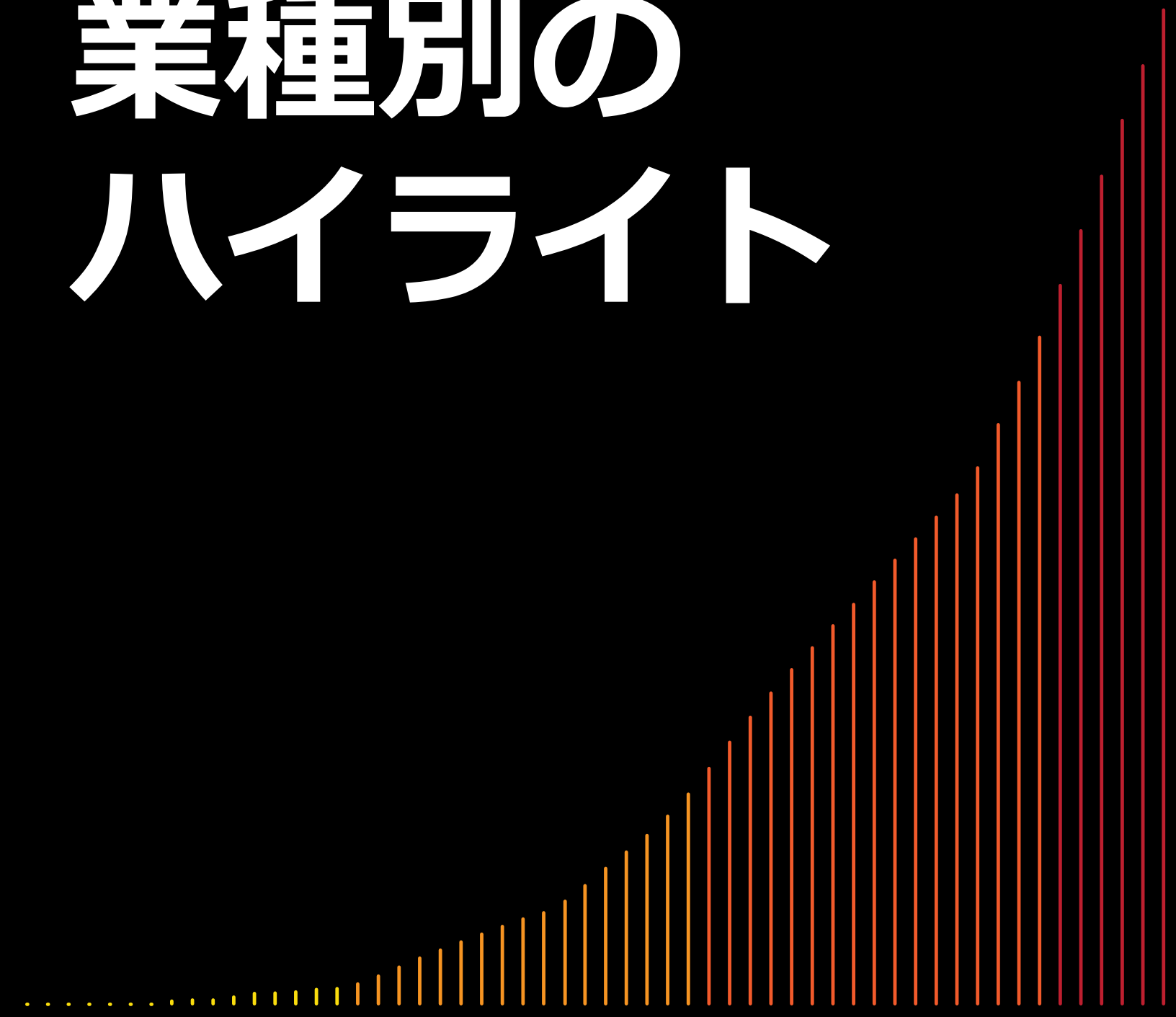


図49. 特権の悪用によるデータ漏洩/侵害における不正取引

4

業種別のハイライト



各業種のハイライト：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、16,312件のインシデントを調査し、そのうち5,199件のデータ漏洩/侵害が確認されました。次のセクションでは、この2つをそれぞれの業種の観点から見てみましょう。ある業種を一貫して食い物にしている攻撃でも、別の業種にはまったく影響を与えないかもしれません。攻撃の対象領域、特定の攻撃者の関心事、および特定の業種が依存するインフラストラクチャなどは、すべてセキュリティインシデントの発生に大きく影響します。また、その業種が扱うデータの種類と量、人々（顧客、従業員など）の関わり方、その他を挙げればきりがないほど多くの要因も、各業種が遭遇する攻撃の種類を決定します。

ビジネスモデルがすべてモバイルデバイスとそれに含まれるアプリに焦点を当てている大企業と、インターネットには接続していないがPoS（販売時点情報管理）ベンダーにシステム管理を委託している超零細企業では、当然ながらリスクが異なります。インフラ、そして逆に攻撃対象領域がリスクを大きく左右します。

したがって、ある業種が報告した侵害やインシデントの件数に基づいて、特定の業種のセキュリティ体制（またはその欠如）について推論しないようにご注意ください[47]。これらの数字は、データ侵害報告関連の法律やパートナーの可視性など、いくつかの要因に大きく影響されます。このため、一部の業種で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、少ない数字から導き出される統計の信頼性も低くならざるを得ないことを、あらかじめお伝えしなければなりません。

もし、ご自分の業種を知るためだけにこのセクションを読まれるのであれば、各業種のセクションに含まれているサマリー欄で上位のパターンが何であるかを確認し、それらのパターンのセクションもお読みいただくことをお勧めします。

47 法務部がこれを言わせたのです。もちろん、他業種の輩を揶揄するのは大いに結構です。

	インシデント				データ漏洩/違反			
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	16,312	694	489	15,129	5,199	376	223	4,600
宿泊および飲食業（72）	254	4	2	248	68	4	1	63
官公庁（56）	38	8	14	16	32	8	11	13
農業（11）	66	1	5	60	33	0	3	30
建設業（23）	87	7	1	79	66	4	1	61
教育サービス業（61）	496	63	15	418	238	28	8	202
芸術、娯楽、およびレクリエーション業（71）	432	13	3	416	93	10	1	82
金融および保険業（52）	1,829	70	30	1,729	477	38	18	421
医療および社会福祉業（62）	522	28	15	479	433	23	15	395
情報産業（51）	2,105	45	110	1,950	380	23	19	338
管理業（55）	9	1	0	8	9	1	0	8
製造業（31-33）	1,814	37	24	1,753	259	18	15	226
鉱業、採石業、石油・ガス採掘業（21）	25	2	0	23	13	2	0	11
その他のサービス（81）	143	7	2	134	100	6	1	93
専門的・科学的・技術的サービス業（54）	1,396	176	54	1,166	421	85	32	304
公務（92）	3,270	87	110	3,073	582	48	39	495
不動産業（53）	83	15	5	63	59	10	2	47
小売業（44-45）	404	62	44	298	191	33	28	130
運輸および倉庫業（48-49）	349	13	25	311	106	8	13	85
公益事業（22）	117	12	6	99	33	3	3	27
卸売業（42）	96	42	22	32	53	23	11	19
不明	2,777	1	2	2,774	1,553	1	2	1,550
合計	16,312	694	489	15,129	5,199	376	223	4,600

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

インシデント

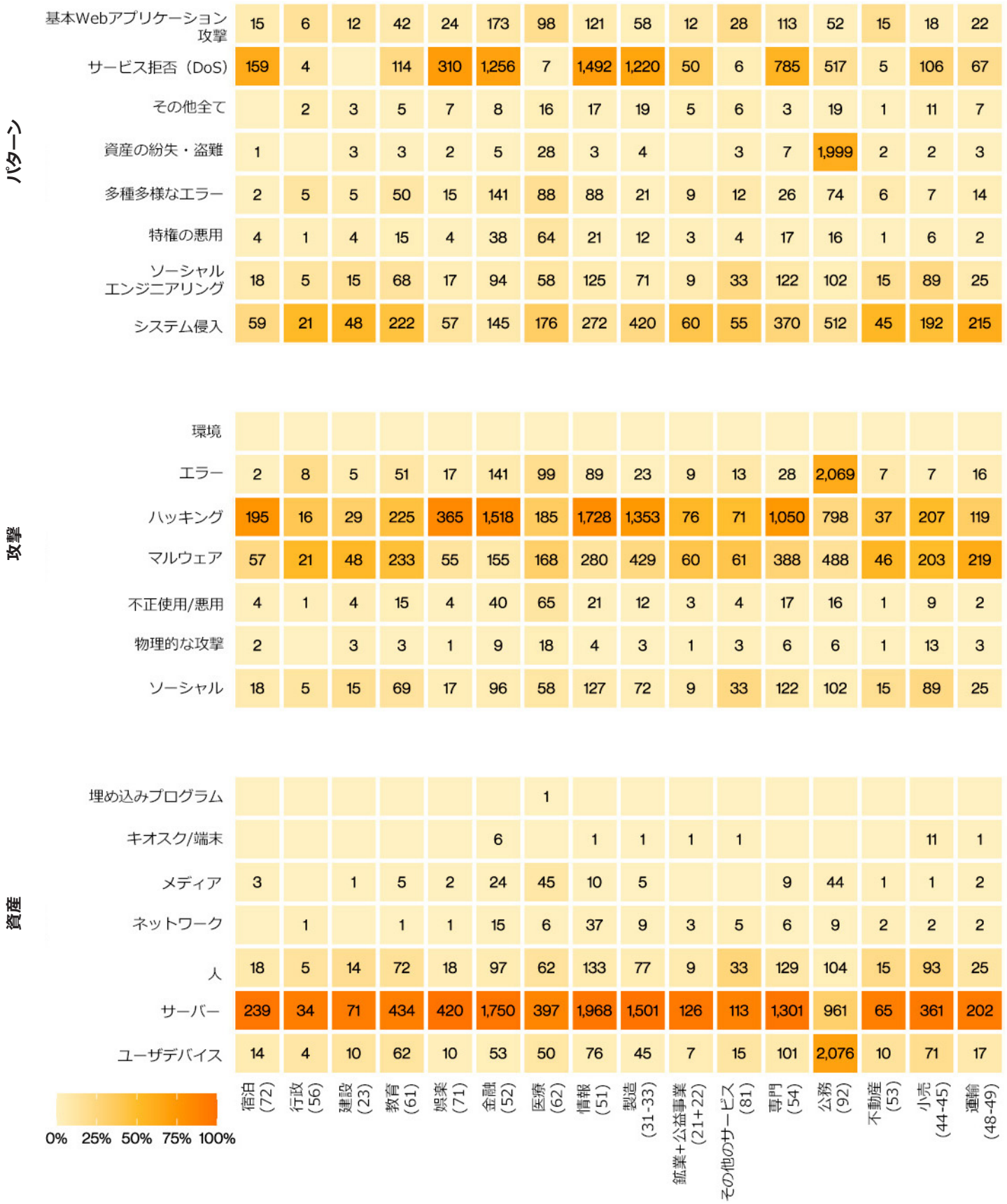


図50. 業種別インシデント

データ漏洩/侵害

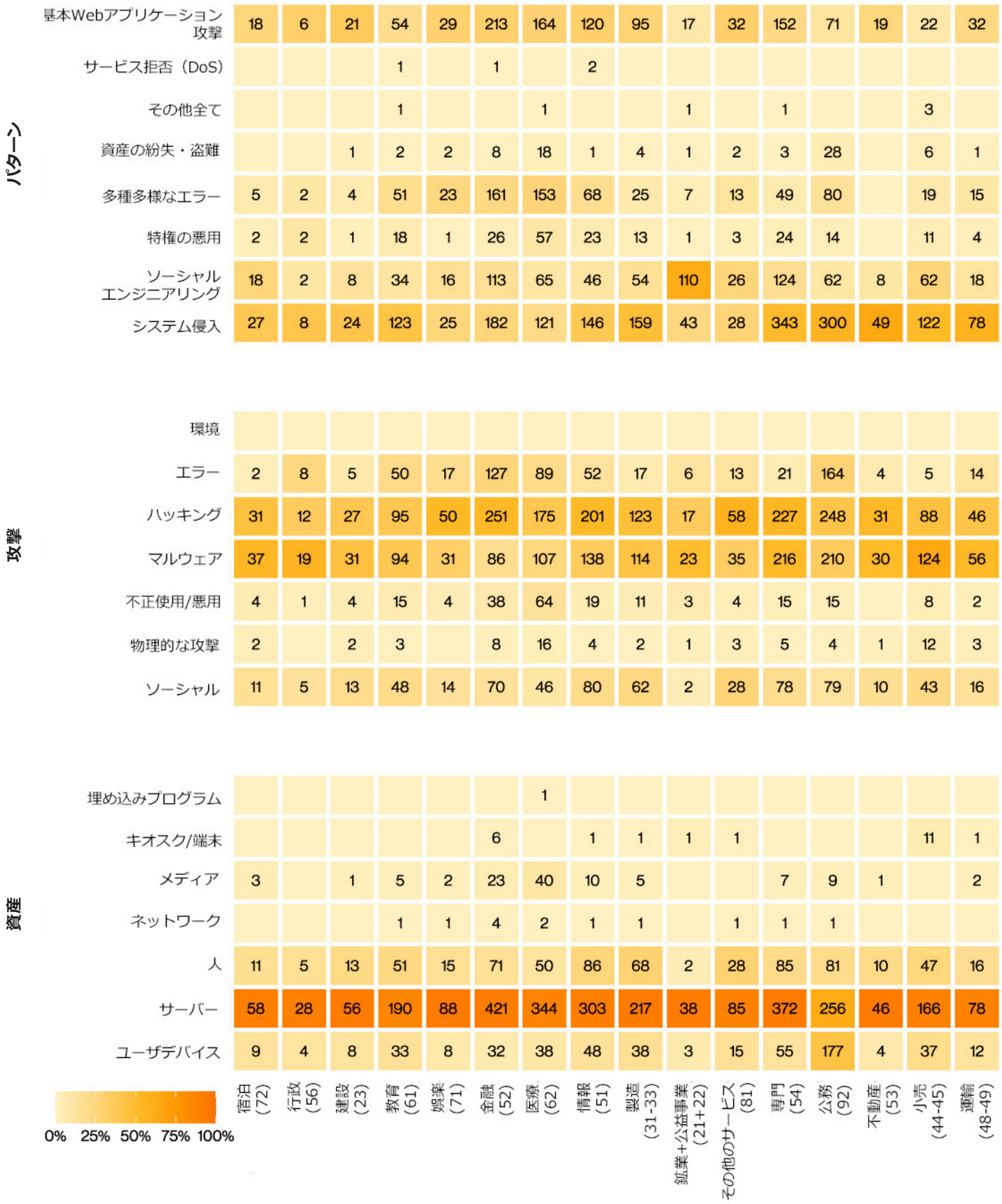


図51. 業種別データ漏洩/侵害

宿泊および飲食業 NAICS 72

頻度	インシデント254件、確認されたデータ暴露68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90%を占めている
攻撃者	外部（93%）、 内部（9%）、 複数の関係者（1%） （漏洩/侵害）
攻撃者の動機	金銭目的（100%） （漏洩/侵害）
侵害されたデータ	決済情報（41%）、 認証情報（38%）、 個人情報（34%）、 その他（26%） （漏洩/侵害）
昨年との比較	この業種を襲っている3つの攻撃パターンに変わりはありませんが、その順序は変わっています。この業種の企業が保有する換金価値の高いデータのために、依然として「外部」の攻撃者に狙われています。

サマリー

ペイメントカードのデータは、当然のことながら、依然としてこの業種で一番よく狙われる「データ」タイプです。「RAMスクレーパー」は、この業種を悩ませ続けている「金銭目的」を動機とする攻撃者のお気に入りのツールとなっています。

私はそれを削り取るだけだ

「システム侵入」パターンは、2年連続でこの業種のトップの座を占めています。このパターンには、とりわけ様々な種類のマルウェアが含まれています。ケースの約3分の1が「ランサムウェア」を使用したもので、残りの多くは「RAMスクレーパー」でした。実際、PoSを標的とした「RAMスクレーパー」は、この分野ではお気に入りのコンボであり、それについては防御体制を維持しようとする人々にとっては驚きではありません。

「ペイメントカード」のデータが狙われた割合は41%で、これは昨年と同じですが、「認証情報」と「個人情報」の全体に占める割合が低下したため、クレジットカードの後塵を拝することになりました。「ペイメントカード」のデータタイプへの注目の高まりとともに、金銭目的の動機も高まっています。昨年は、データ漏洩/侵害の9%に「スパイ活動」の動機が見られましたが、今年は、常に「金銭目的」が動機です[48]。

人にフィッシュを与えれば、1日食わせることができる！

この分野では、ソーシャルが引き続き大きな存在感を示しています。「フィッシング」と「なりすまし」は（両者の主な違いは、敵対者がそれを実現するためにどれだけ努力しなければならないかという点です）、「宿泊業」におけるソーシャルエンジニアリングの主な関心事にはなっていますが、トップの座を主張するにはあまりに僅差です。このようなソーシャル攻撃のほとんどはメール経由で入ってくるので、疑わしい試みを従業員が素早く報告できるようにしておきましょう。従業員が最初の防衛ラインとなることに勝るものはありません。彼らはすでに標的の最前線にいることは間違いないからです。

48 正直なところ、そうでないことがあるでしょうか？

教育サービス業 NAICS 61

頻度	497件のインシデント、確認されたデータ暴露238件
上位3つのパターン	「システム侵入」、「その他のエラー」、「ソーシャルエンジニアリング」が侵害の76%を占める
攻撃者	外部（72%）、内部（29%）、複数（1%）、パートナー（1%）（漏洩/侵害）
攻撃者の動機	金銭目的（92%）、スパイ活動（8%）、便宜（1%）、遊び（1%）（漏洩/侵害）
侵害されたデータ	個人情報（56%）、認証情報（40%）、その他（25%）、内部（20%）（漏洩/侵害）
昨年との比較	「システム侵入」と「多種多様なエラー」が、今年度も上位3つのパターンの2つに入っています。外部と内部の攻撃者の比率は昨年とほぼ同じです。

サマリー

「基本Webアプリケーション攻撃」は上位3つのパターンから脱落し、「ソーシャルエンジニアリング」に取って代わられました。「ランサムウェア」が引き続き、この業種のデータ漏洩/侵害に大きな役割を果たしています。

それを誰が予想しただろうか？

教職員や学生にも衝撃を与えた動きとして、昨年は大人気だった「基本Webアプリケーション攻撃」が上位3つのパターンから脱落しました。「多種多様なエラー」は依然として存在し（いつもそうですよね？）、昨年よりわずかに増加しています。ご想像の通り、これらのエラーはいつもの容疑者たちです。「誤送信」、「公開エラー」、「設定ミス」などです。

「ソーシャルエンジニアリング」は、昨年の14%から2023年には21%に増加し、第3位にランクインしました（図52）。この増加の主な要因は「フィッシング」攻撃で、データ漏洩/侵害の18%に見られ、「なりすまし」シナリオ（4%）でも見られました。

「ハッキング」はデータ漏洩/侵害の40%で見られ、そのうちの 31%で「盗まれた認証情報の悪用」が確認されました。「マルウェア」もデータ漏洩/侵害の40%で見られ、「ランサムウェア」は30%で見られました。試験のために、もう一度おさらいしておきましょう。「ランサムウェア」は、「教育サービス業」における全データ漏洩/侵害のほぼ3分の1を占めています。「ハッキング」と「マルウェア」の両方がこのような印象的な結果を示したにもかかわらず、「システム侵入」パターンは1位を維持しながらも、昨年からわずかに減少しました。

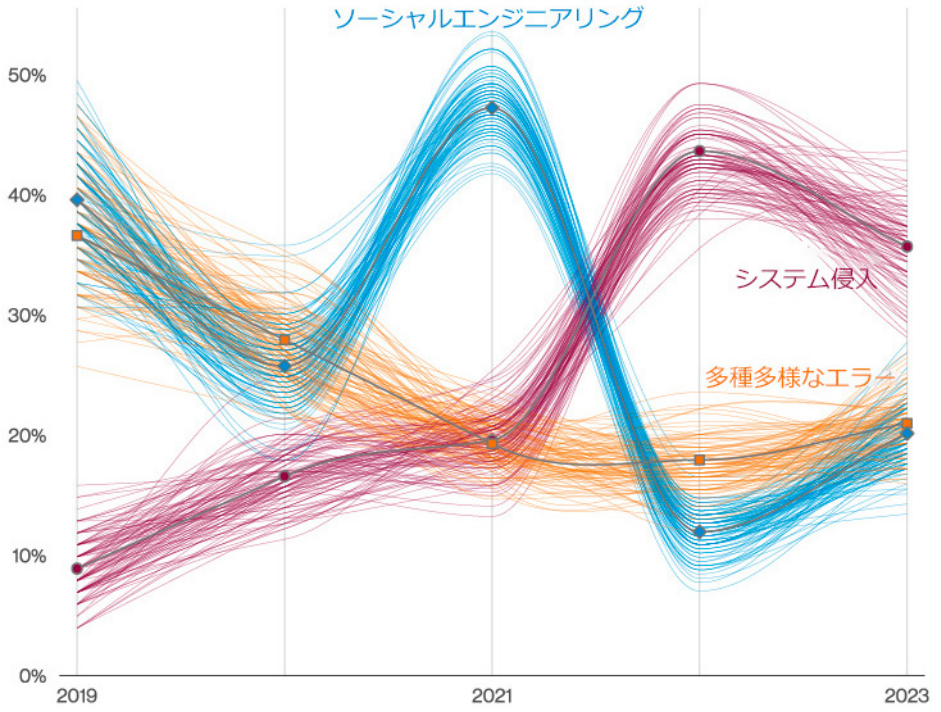


図52. 教育サービス業におけるデータ漏洩/侵害のパターン

金融および保険業 NAICS 52

頻度	インシデント1,832件、確認されたデータ暴露480件
上位3つのパターン	「基本Webアプリケーション攻撃」、「その他のエラー」、「システム侵入」が侵害の77%を占める
攻撃者	外部（66%）、内部（34%）、複数の関係者（1%）（漏洩/侵害）
攻撃者の動機	金銭目的（97%）、スパイ活動（3%）、利便性（1%）、イデオロギー（1%）（漏洩/侵害）
侵害されたデータ	個人情報（74%）、認証情報（38%）、その他（30%）、銀行情報（21%）（漏洩/侵害）
昨年との比較	上位3つのパターンは変わりませんが、順位に変化がありました。「個人情報」は、詐欺に非常に有効なデータであり、依然として最も狙われるデータタイプです。

サマリー

「基本Webアプリケーション攻撃」が最上位にランクインしていることから、攻撃者はそれほど労力をかけずにデータの取得に成功していることがわかります。このことは、「誤送信」と合わせて、この業種における攻撃のかなりの割合をカバーできるよう、対策を強化する余地があることを示しています。

これらの攻撃は非常に基本的なものだ

「我々は非常に巧妙なサイバー攻撃によって侵害された。」データ漏洩/侵害の報告書の大部分はこのように書かれています。しかし、実際、パスワードの総当たり攻撃はどれほど巧妙と言えるのでしょうか？あるいは、もっと巧妙なのは、パスワード（他の侵害から入手した）を推測する必要さえないクレデンシャルスタッフィングでしょう！この分野では、「基本Webアプリケーション攻撃」のパターンが最も一般的です。つまり、それほど複雑ではない攻撃が、敵対者にとって見事に成功しているということです。ほんの少しで済むことに、なぜ多大な労力を費やすのでしょうか？

えーと、それを渡しましたっけ？

もう1つの顕著な攻撃は、「内部」関係者がミスを犯すことです。保護されたデータが間違った受信者に送られる「誤送信」は、最もよく発生します。紙の文書が間違った相手に送られることもあれば、電子版が紛失することもあります。いずれにせよ、この種の「エラー」がデータ漏洩/侵害を引き起こす前に発見するよう、細心の注意を払う必要があります。

そのために努力させるのだ

トップ3の最後を飾るのは、攻撃者が少しだけ努力すれば済む「システム侵入」パターンです。今年は27%から14%に減少しましたが（「多種多様なエラー」が上位を占めました）、依然として深刻な問題であることに変わりはありません。 これは、少なくともある程度の時間内に仕事を終わらせるために、攻撃者が巧妙なテクニックを駆使しなければならなかったことを示しています。興味深いことに、「ランサムウェア」は、この業種のこのパターンでは、お気に入りの手口としては減少しています。この部分については、「インシデントの分類パターン」のセクションで詳しく説明しています。図版のみを見るためにDBIRを読む方もいらっしゃるでしょうが。

医療および社会福祉業 NAICS 62

頻度	インシデント525件、確認されたデータ暴露436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68%を占めている
攻撃者	外部（66%）、内部（35%）、複数（2%）（漏洩/侵害）
攻撃者の動機	金銭目的（98%）、スパイ活動（2%）、愉快（1%）、イデオロギー（1%）（漏洩/侵害）
侵害されたデータ	個人情報（67%）、医療情報（54%）、認証情報（36%）、その他（17%）（漏洩/侵害）
昨年との比較	順位に入れ替わりがあったものの、上位3つのパターンに変更はありません。「内部」関係者が犯すミスは、依然とこの業種において悩みの種となっています。

サマリー

「ランサムウェア」攻撃者は、この業種をずっと標的にしており、その過程でデータ漏洩/侵害が確認されることが多くなっています。また、「エラー」（特に「誤送信」）も常に蔓延しています。最後に、この業種ではインサイダーの脅威も警戒する必要があります。

包囲攻撃にさらされている業種

「医療および社会福祉業」はランサムウェアの標的となっており、その結果、どちらもシステムの利用ができなくなり、データ漏洩/侵害だけでなく、患者の生命を脅かされる可能性があります。この業種におけるランサムウェアのインシデントは2021年にピークを迎え、ここ3年間はランサムウェアによるデータ漏洩/侵害（データが盗まれたことが確認され、暗号化が起動した）が急増しています。このような攻撃の組み合わせにより、より多くのデータが危険にさらされ、さらに職員は頼りにしていたシステムなしで仕事をすることを余儀なくされるという、いつもの混乱も生じています。

このような攻撃に対処するには、たとえ侵害されたシステムの信頼の置けるテスト済みバックアップがあったとしても、時間とリソースがかかります。その両方が不足している組織では、予防と早期発見の対策に頼るほかありません。対策を練る際には、この種の攻撃の脅威を無視してはなりません。

申し訳ありません

「多種多様なエラー」のパターンは、依然として医療および社会福祉業に蔓延しています。「誤送信」の発生パターンは、一貫して人の問題です。これは、特定の人（またはグループ）に行くはずのデータが、実際には全く違う人に行ってしまうというミスです。時には、機密性の高い従業員の医療情報が記載されたスプレッドシートが、予定よりもはるかに広い範囲に誤って送信されてしまうようなケースもあります（これらのメールグループの名前はよく似ていて間違えやすい。オートコンプリート機能に感謝しましょう）。また、封筒の透明窓から多くの情報が見えてしまうように文書を入れた封書ミスというケースもあります。自分の恥ずかしい不手際を郵便局員に知られたいという人がいるはずもありません。顧客（患者）が憤慨するのも無理はありません。

俺の不満はどこに？

ああ、不満を抱えた従業員がしばしば悪意のある行為の加害者となり、内部の関係者だけがなし得る大混乱を引き起こすのです。「特権の悪用」パターンは、この業種ではもはやトップ3には入っていませんが、一貫して問題であることに変わりありません。好奇心からの盗み見はこの業種でもよく行なわれます（積極的な敵対というよりは、退屈している従業員によって）。しかし、この業種では、複数の関係者が共謀して不正侵入の欲望を現実のものにしようとする証拠も見られます。この勤勉さを正当な業務に向けることさえできれば、これらの従業員は一番の業績を納めることができるのに。誰かが不平不満を爆発させた場合の唯一の防御策は、異常なデータアクセスパターンを迅速に検出することしかありません。不平不満は内部攻撃者に問題を引き起こすための動機付けになり、あらゆる業種にとって依然として課題です。

情報産業 NAICS 51

頻度	2,110件のインシデント、確認されたデータ暴露384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77%を占めている
攻撃者	外部（81%）、内部（20%）、複数の関係者（2%）、パートナー（1%）（漏洩/侵害）
攻撃者の動機	金銭目的（92%）、スパイ活動（8%）（漏洩/侵害）
侵害されたデータ	個人情報（51%）、認証情報（37%）、その他（35%）、内部情報（19%）（情報漏えい）
昨年との比較	この業種では、「システム侵入」パターンが依然としてトップの座にあり、「金銭目的」を動機とする外部の攻撃者が圧倒的です。

サマリー

「エラー」は、ここ数年減少傾向にあり、「ソーシャルエンジニアリング」に上位3位のポジションを奪われています。この業種では、「サービス拒否（DoS）」攻撃がインシデントの70%を占めています。

ミスはしないこと、情報は力である

ここ数年、「情報産業」のデータ漏洩/侵害においてエラーの果たす役割は減少しています。その減少傾向は今年も続いており、エラーは4位に転落し、侵害のわずか13%を占めるにすぎません（図53）。「情報産業」の皆さん、お疲れ様でした！知らず知らずのうちに資産を危険にさらすことなく、悪者から自社の資産を守ることはかなり困難なことです。

一方、「ソーシャルエンジニアリング」はじわじわと台頭し、侵害の20%を占め、第3位に浮上しました。業種によっては、より複雑な「なりすまし」よりも「フィッシング」のほうがはるかに多いケースもあります。しかし、「情報産業」では、「フィッシング」は15%、「なりすまし」は11%と、この2つのソーシャル攻撃に大きな差はありません。本報告書の他の部分で述べているように、「なりすまし」は間違いなく増加傾向にあります。

選択肢は変わっていませんので、よく聞いてください

いつものように、この分野のほとんどの攻撃の背後には、外部の攻撃者（その大部分は組織犯罪）がいます。実際、昨年は「外部」および「内部」の攻撃者のみを紹介しました。今年は、「パートナー」および複数の関係者がそれぞれ1%ずつ増加しています（ごくわずかですが）。もちろん、これらは大きな数字ではありませんが、数年ぶりにこの業種に再登場したことは興味深いことです。予想されるように、攻撃の大部分は、誰が行ったかにかかわらず、「金銭目的」を動機とするものでした。「スパイ活動」という動機は依然として8%は存在しますが、昨年の20%よりはかなり低くなっています。この変化の最も可能性の高い理由は、Webアプリケーションやサーバーからスパイ用バルーンやリモートビューイングへと移行していることです。

図53. 情報産業におけるデータ漏洩/侵害のパターン（n=384）

製造業 NAICS 31-33

頻度	インシデント1,817件、確認されたデータ暴露262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83%を占めている
攻撃者	外部（90%）、内部（11%）、複数の関係者（2%）、パートナー（1%）（漏洩/侵害）
攻撃者の動機	金銭目的（96%）、スパイ活動（4%）、利便性（1%）（漏洩/侵害）
侵害されたデータ	個人情報（60%）、認証情報（38%）、その他（37%）、内部情報（18%）（漏洩/侵害）
昨年との比較	上位3つの攻撃パターンに変更はありませんが、順位に若干変化がありました。「金銭目的」を動機とする外部の攻撃者が、依然としてこの業種に大混乱をもたらしています。

サマリー

「ハッキング」と「マルウェア」による攻撃がトップ2の座をめぐって互いにしのぎを削っています。「ソーシャルエンジニアリング」攻撃はまだ3位と健在ですが、他の2つから大きく引き離されています。インシデントでは、この業種のインフラに対する「サービス拒否（DoS）」攻撃も納期を遅らせるものとして見逃せません。

ポストモダンの世界に暮らす私たちは、一日をやり過ごすために、歴史上のどの時代よりも確実に携帯端末やゲーム端末のような多くのガジェットに頼っています[49]。したがって「製造業」の重要性は、私たちが日常的にどのように存在し、どのように相互に影響し合っているかに関連しているため、本当におろそかにはできません。「製造業」はこのことを認識しており、その結果、私たち全員がこれなしでは生きていけないと考える次の大ヒット製品を探し続けています。サイバー犯罪者もそれを承知しており、常に現金化しようと策を練っています。

図54を見ると、順位は若干異なるものの、昨年のレポートと同じ上位3つのパターンが見て取れます。「ソーシャルエンジニアリング」（23%）と「基本Webアプリケーション攻撃」（17%）の順位が入れ替わった一方、「システム侵入」は42%で依然として1位を維持しています。

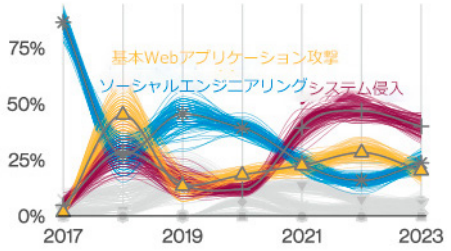


図54. 製造業のインシデントにおけるパターンの経時的変化

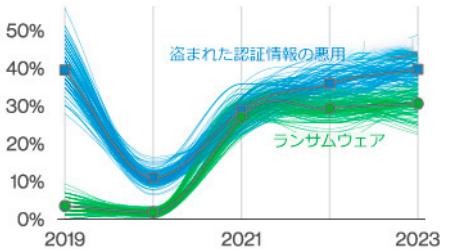


図55. 製造業のデータ漏洩/侵害における攻撃の種類の経時的変化

図56が示すように、「製造業」で最も頻繁に発生する攻撃行為を掘り下げてみると、「ハッキング」攻撃と「マルウェア」攻撃はほぼ同じ割合で発生しており、「ソーシャル」攻撃は引き続き好調であることがわかります。「ランサムウェア」は、「システム侵入」のパターンにおける侵害の大部分を占めており、この分野では3年連続で緩やかな増加傾向が続いています（図55）。

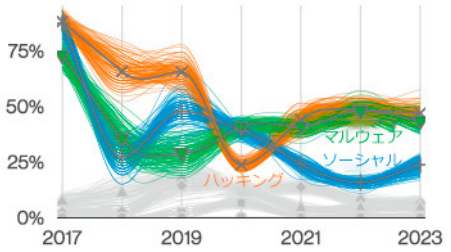


図56. 製造業のデータ漏洩/違反における上位の攻撃の経時的な変化

インシデントの観点からは、依然として「サービス拒否（DoS）」攻撃が中心です。「サービス拒否（DoS）」攻撃は、この分野のインシデント全体の約67%を占めています。これはここ数年増加傾向にあるため、この業種に属する組織であれば、間違いなく注視すべきことです。

49 信じてください、私たちはそのうちのいくつかを経験してきました。

鉱業、採石業、石油・ガス採掘業および公益事業 NAICS 21+22

頻度	インシデント143件、確認されたデータ暴露47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」でデータ漏洩/侵害の81%を占めている
攻撃者	外部（80%）、内部（20%）（漏洩/侵害）
攻撃者の動機	金銭目的（63%〜93%）、スパイ活動（4%〜32%）、怨恨（1%〜21%）、イデオロギー（0%〜15%）、便宜/恐怖/愉快/その他/二次的動機（各0%〜7%）（漏洩/侵害）
侵害されたデータ	個人情報（50%）、内部情報（33%）、その他（26%）、認証情報（24%）（漏洩/侵害）
昨年との比較	この業種では「システム侵入」と「基本Webアプリケーション 攻撃」が、依然として大きな懸念材料となっています。

サマリー

この業種では、「ランサムウェア」が3件に1件の割合でデータ漏洩/侵害の原因となっています。「ソーシャルエンジニアリング」は、全体的に増加しているにもかかわらず、この業種では減少しています。

深く掘り下げてみましょう

NAICS 21および22から報告されたインシデントや侵害の件数が少ないため、統計的に適切な母集団を得るためには、時には深く掘り下げる必要があります。それでも、サンプル数が少ないため、明確な割合ではなく、範囲を使わざるを得ないこともあります。しかし、これらの業種はどちらも重要なインフラであり、それほど似ているわけでもないため、可能な限り有益で興味深い鉱石を掘り当てられるよう最善の努力を尽くしています。あなたはこれらの業種の方ですか？もしそうなら、DBIRのデータ提供協力者になることをご検討ください。

今年の第1位は「システム侵入」です。他のセクションをお読みになった方なら、このことが決してこの産業の人々を「ローンレンジャー」にしているのではないことがお分かりいただけるでしょう。攻撃パターンのセクションで述べたように、「システム侵入」のパターンは、「侵入して、データを取得したら引き上げる」タイプの攻撃とは対照的に、より複雑で多段階の攻撃で構成されています。具体的には、ほとんどのランサムウェア攻撃は「システム侵入」に属し、業種のデータ漏洩/侵害の約3件のうち1件（32%）がランサムウェア攻撃でした（図57）。ランサムウェアの成功率の高さ（攻撃者は暗号化する前にデータを持ち出すことが多く、そのデータを流出サイトに掲載したがるという事実もある）を考えると、重要なインフラ産業でランサムウェアが多発していることは懸念すべき問題です。

図57. 鉱業、採石業、石油・ガス採掘業および公益事業のデータ漏洩/侵害における上位の攻撃の種類（n=37）

昨年、私たちはこの業種で「ソーシャルエンジニアリング」に該当する侵害が多いことを指摘しました。今年は「基本Webアプリケーション攻撃」と「多種多様なエラー」が2位と3位を占め、「ソーシャルエンジニアリング」はトップ3から完全に脱落しました。実際、「ソーシャルエンジニアリング」は上位の5つにも入りませんでした。他の業種ではフィッシングやなりすましが増加しているため、これは少々驚きです。犯罪者たちは、お金を盗むために他人と実際に関わり合いを持ちたくないのだろうか？ それは確かに理解できます。

攻撃者が奪っているものに関しては、個人情報が半分を占め、「内部情報」が大幅に増加しています（図58に示すように、昨年は9%であったのに対し、今年は33%）。これは、前のページで述べた「名指しで恥をかかせる」ランサムウェア攻撃と関連しているのかもしれません。

図58. 鉱業、採石業、石油・ガス採掘業および公益事業で盗まれた上位のデータタイプ（n=46）

専門的・科学的・技術的サービス業 NAICS 54

頻度	インシデント1,398件、確認されたデータ暴露423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90%を占めている
攻撃者	外部（92%）、内部（9%）、複数の関係者（3%）、パートナー（2%）（漏洩/侵害）
攻撃者の動機	金銭目的（96%）、スパイ活動（4%）、利便性（1%）（漏洩/侵害）
侵害されたデータ	個人情報（57%）、認証情報（53%）、その他（25%）、内部情報（16%）（漏洩/侵害）
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」は、この業種の組織にとって主要な脅威であり続けています。

サマリー

この業種では、上位のパターンに変化がないにもかかわらず、「ランサムウェア」が1年間で増加し、前年と同じ主要な攻撃経路をとるインシデントが発生しています。

この業種は、すべての産業を円滑に動かす潤滑油と言えるかもしれません。弁護士の友人［法務に編集されたジョーク］や会計士、その他様々なビジネスサービスなど、多くの異なる専門職で構成されています。この業種も、他の業種と同様、「システム侵入」（47%）、「基本Webアプリケーション攻撃」（25%）、「ソーシャルエンジニアリング」（18%）という3大パターンの影響を受けています。

攻撃の種類に関しては、図59で「サービス拒否（DoS）」と「盗まれた認証情報の悪用」が上位に挙げられている一方で、「ランサムウェア」も多く見受けられます。今年は、「ランサムウェア」がこの分野のインシデントの約23%を占めており、昨年の14%から顕著に増加しています。

このようなデータ侵害がどのように発生するのか疑問に思うのであれば、「Webアプリケーション」（55%）、「メール」（25%）、「デスクトップ共有ソフトウェア」（17%）以外を探す必要はありません。盗まれた認証情報やメールが頻繁に悪用されていることを考えると、強力な認証方法を導入するよう注意を喚起し、チームメンバーに勤勉さを保つことの重要性を心に留めるように促す良い機会かもしれません。

図59. 専門的・科学的・技術的サービス業のインシデントにおける攻撃（n=1,351）

公務 NAICS 92

頻度	インシデント3,273件、確認されたデータ暴露584件
上位3つのパターン	「システム侵入」、「資産の紛失・盗難」、「ソーシャルエンジニアリング」がデータ漏洩/侵害の76%を占めている
攻撃者	外部（85%）、内部（30%）、複数の関係者（16%）（漏洩/侵害）
攻撃者の動機	金銭目的（68%）、スパイ活動（30%）、イデオロギー（2%）（漏洩/侵害）
侵害されたデータ	個人情報（38%）、その他（35%）、認証情報（33%）、内部情報（32%）（漏洩/侵害）
昨年との比較	この業種は、敵対する国の動向を注視するスパイ国家、「金銭目的」の動機で動く外部の攻撃者に狙われ続けています。「個人情報」は、依然として最もよく盗まれるデータタイプです。

サマリー

この業種では、「スパイ活動」を動機とするデータ漏洩/侵害が引き続き上位を占めています。また、複数の攻撃者による侵害が多いことも特徴的です。「外部」と「パートナー」、あるいは「内部」の関係者がグルになってデータを盗むというのは、私たちが望む国際協力とは言えません。

あれは月ではない！

上空を漂うステルス「気象調査」気球（デススター）によってデータが盗まれるにせよ、フィッシングのような従来型の方法によってデータが盗まれるにせよ、外部の攻撃者は公共部門のデータに熱心にアクセスしています。私たちがデータ漏洩/侵害を分類するためにVERISを開発したとき、それが空から飛来するUFOに適用されるとは思ってもみませんでした。しかし、これがトレンドになるまでは、単に「物理的 - その他」とタグ付けして、ひとまず終わりにすることにします。

この業種では、「システム侵入」のパターンが依然として高いままです。「システム侵入」の中には、映画にもなったような、困難な標的に対する複雑な攻撃もあり、経済システム全体にとって大きな賭けとなります[50]。今年は、このパターンでは「スパイ活動」が増加しました。実際、この業種は、「スパイ活動」を動機とする攻撃者が常に最も多いセクターの1つです。

「システム侵入」のパターンでは、「ランサムウェア」が若干減少しています。とはいえ、ランサムウェアを無視すべきだということではありません。つまり、それは攻撃者に収入をもたらしながら、政府の業務を妨害する方法として依然として好まれているからです。

自分たちだけで目標を達成することも可能ですが、このような攻撃者は、組織内部から助けを募ること避けているわけではありません。私たちは、今年の「行政機関」への侵入の16%に共謀（複数の攻撃者が連携して行っている）の証拠を確認しています。この業種では過去2年間、複数の「攻撃者」によるデータ漏洩/侵害は見られなかったし、2020年のレポートではわずか2%であったことを考えると、これは重要なことです。

静かに辞めるより悪いこととは？

このことは、内部攻撃者による「悪用」がこの分野で一貫した問題であり続けていることを示唆しています。蔓延しているとはいえ、増加しているわけではありません。実際、「悪用」は（過去5年間のうち）2019年にピークを迎え、それ以降はやや減少しています。しかし、不幸な従業員とやる気のある外部の攻撃者との組み合わせは、引き続き検知制御の必要性を示しています。この種の「内部」攻撃者が実行する攻撃を初期段階でキャッチできれば、被害を大幅に軽減することができます。

今年の「行政機関」への侵入の16%に共謀（複数の攻撃者が連携して行っている）の証拠が見られました。この業種では過去2年間、複数の攻撃者による侵害は確認されておらず、2020年のレポートではわずか2%であったことを考えると、これは重要なことです。

50 そこには爆発やカーチェイスも含まれています。

小売業 NAICS 44-45

頻度	インシデント406件、確認されたデータ暴露193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88%を占めている
攻撃者	外部（94%）、内部（7%）、複数の関係者（2%）、パートナー（2%）（漏洩/侵害）
攻撃者の動機	金銭目的（100%）、スパイ活動（1%）（漏洩/侵害）
侵害されたデータ	決算情報（37%）、認証情報（35%）、その他（32%）、個人情報（23%）（漏洩/侵害）
昨年との比較	「小売業」は、「ペイメントカード」のデータ収集を目的とするサイバー犯罪者にとって、依然と有益な標的となっています。

サマリー

この業種も他の多くの業種と同じ3つのパターンに占められていますが、「小売業」では、「ランサムウェア」や「基本Webアプリケーション攻撃」といった一般的な脅威に加え、「ペイメントカード」データが狙われるという特徴があります。

今すぐ私を侵害できるか？

世の中には「小売業」での買い物をセラピーとして利用する人もいます。一方、私たちDBIRチームは、ドラゴン、ギター、鳩時計（なぜかは聞かないでください）を必要以上にたくさん持っています。悲しいことに、犯罪者たちは長年この業種を標的にすることで、自分たちなりの「買い物セラピー」を楽しんでいます。彼らは、この業種における決済データの多用に乗じて、そうし続けています。

もっとも上位を占める攻撃/もっとも上位を占める攻撃経路

このような侵害やインシデントがどのように発生するかということになると、「ランサムウェア」と「盗まれた認証情報の悪用」の両方が上位を占め、「メール」と「Webアプリケーション」が攻撃経路となっています。しかし、「データエクスポート」と「アプリデータの取得」という比較的ユニークなアクションもあります。また、この業種は「その他」が上位に食い込んでくる数少ない業種でもあります（図60）。これは、ランサムウェアを展開したり、ペイメントカードを収集する方法を見つけたりするために攻撃者が使用しているさまざまな二次攻撃があることが主な理由です。

もしあなたが「小売業」にいて、eコマースプラットフォームを運営しているのであれば、このセクションは特に注目に値します。「小売業」では、「Magecart」攻撃を[51]行なう攻撃者をよく見かけます。これらの犯罪者は、悪意のあるコードをサイトのクレジットカード決済ページに埋め込む方法を見つけます。これにより、実際にWebサイトの機能に影響を与えることなく、顧客の決済データを静かにさりげなく持ち去ることができます。現在、このような攻撃は「小売業」における不正アクセスの約18%を占めています。これらの「攻撃者」がどのようにしてWebアプリケーションにアクセスし、悪質なJavaScriptをアップロードすることができたのか、私たちが常に把握しているわけではないことを率直に認めますが、これらの攻撃者がいくつかの異なるトリックを使用するところを目撃しています（図61）。

図60. 小売業のデータ漏洩/侵害において上位を占める攻撃の種類（n=182）

51 平たく言えば、魔法使い同士がゴーカートで競争するようなもの。

盗まれた認証情報：$5、ドメインのホスティング: $12、悪意のあるJavaScript：$50、全個人情報の盗用：値段が付けられない

この業種の機能を考慮すると、「ペイメントカード」のデータが最もよく侵害されるデータタイプの1つであり、今年の侵害の37%を占めていることは驚くには値しません。図62を見ると、「ペイメントカード」データは2018年の高水準から減少傾向を示しています。しかし、昨年と比較すると、「ペイメントカード」の盗難件数は比較的増加しています。カードデータを盗むことは、データを収益化するための実証済みの方法ですが、攻撃者は単に迅速な支払日を望んでいる場合もあります。「ランサムウェア」がこの分野のデータを歪めているのは確かですが、「ペイメントカード」のデータは依然として非常に価値があり、今後も人気のターゲットであり続けるでしょう。

ここで疑問が生じます。こうしたデータはどこから盗まれているのか？というのも、何を守っているのか分からなければ、何かを守ることは難しいからです。幸いなことに、私たちはその一助となるデータをいくつか持っています。「小売業」におけるペイメントカードからのデータ侵害に関する分析では、データ侵害の70%が「Webアプリケーション」から、17%が「ガソリンスタンド」から、8%が「PoSサーバー」から発生していることがわかりました。これは、電子商取引によって、盗まれたクレジットカードを含め、欲しいものを手に入れることがあまりにも簡単になったことを改めて示しています。追加的な有益情報をお探しなら、2024年のDBIRが発行される頃には、皆さんはすでにPayment Card Industry （PCI） Data Security Standard （DSS）4.0[52]に準拠しているはずだということを述べておく価値があるでしょう。

図61. 小売業のデータ漏洩/侵害において上位を占める攻撃経路（n=130）

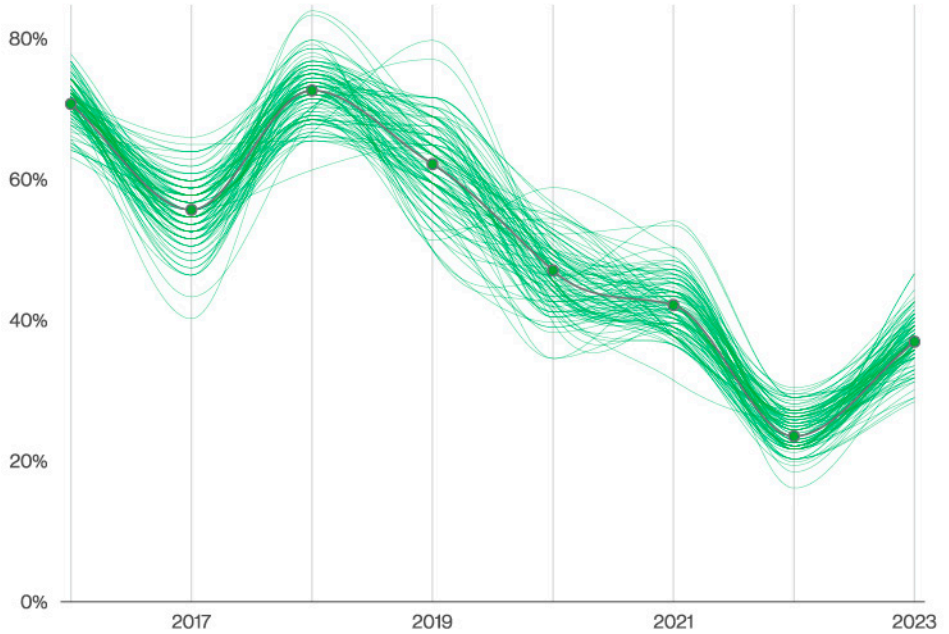


図62. 小売業のデータ漏洩/侵害におけるペイメントカードの経時的変化

52 https://www.pcisecuritystandards.org/resources-overview/

中小企業

「単語問題をやろう！」

誰も言わなかった（数学の先生を除いて）

過去の報告書では、中小企業（SMB）と大企業とを比較対照し、攻撃対象が両者で大きく異なる点について注目してきました。しかし、SMBと大企業が同様のサービスやインフラを利用するケースは増えており、その結果、攻撃対象が以前よりも共通化されてきています。このため、組織の規模に関係なく、攻撃の特徴が近似してきました。しかし、大きく異なるのは脅威に対応する組織の防衛能力です。これは、攻撃を受けた際に展開できるリソースの数によります。

右の表は、SMBと大企業がますます類似してきている事実を示しています。この現象は数年前から始まっており、今では規模による違いはほとんどないため、区別することは困難です。そのため、今年は、SMBにおけるさまざまな企業規模（小規模企業、中規模企業、大き目な企業）のセキュリティ対策の実施状況を調べ、それらがどのように重なっているか、あるいは異なっているかを調べることで、少し違った観点から見る[53]ことにしました。

過去の報告書では、特にMITREと共同で実施したVERISとATT&CKのマッピングなど、管理策に関するベライゾンの調査について説明しました。そこで今年度は、MITREと共同で行ったVERISとATT&CKのマッピングをもう少し現実の世界に落とし込みました。そしてこれらのマッピングを、さまざまな規模のSMBに適した「CIS（Center for Internet Security）実装グループ」の保護コントロールにどのように使用できるか応用してみることにしました。

中小企業（従業員数1,000人未満）	
頻度	インシデント699件、確認されたデータ暴露381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92%を占めている
攻撃者	外部（94%）、内部（7%）、複数の関係者（2%）、パートナー（1%）（漏洩/侵害）
攻撃者の動機	金銭目的（98%）、スパイ活動（1%）、利便性（1%）、怨恨（1%）（漏洩/侵害）
侵害されたデータ	認証情報（54%）、内部情報（37%）、その他（22%）、システム情報（11%）（漏洩/侵害）

表3. SMBの一覧表

大企業（従業員数1,000人以上）	
頻度	インシデント496件、確認されたデータ暴露227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85%を占めている
攻撃者	外部（89%）、内部（13%）、複数の関係者（2%）、パートナー（2%）（漏洩/侵害）
攻撃者の動機	金銭目的（97%）、スパイ活動（3%）、イデオロギー（2%）、利便性（1%）、愉快（1%）（漏洩/侵害）
侵害されたデータ	内部情報（41%）、認証情報（37%）、その他（30%）、システム情報（22%）（漏洩/侵害）

表4. 大企業の一覧表

53 ここでもまた、私たちが話し続けている再度の集中をしました。

小規模であることは容易ではない

あなたがスタートアップ企業、つまり創業間もない小さな会社だとしましょう。セキュリティ対策を実施するためのリソースは非常に限られています。IT担当者はセキュリティ担当者であると同時に、多くのタスクをこなすため、眠らずに働く何でも屋でもあります。

最初のステップは、自社のセキュリティ成熟度とリソースのレベルに応じて、推奨されるセキュリティ対策（コントロール）を確認することです。しかし、どこから始めればよいのでしょうか？CIS Critical Security Controls Navigator[54]は、CISの各コントロールを小分けにして理解しやすくし、組織が採用基準として準拠したいと考えるさまざまなセキュリティ標準にマッピングしたものです。推奨されるコントロールは3つの「実施グループ（IG）」に分けられ、それぞれが組織の成熟度レベルに対応しています。ここでは最初なので、「実装グループ1（IG1）」から始めることにします。これらはすべて優れたセキュリティ対策であり、ロードマップに載せるべきものですが、このシナリオでは、脅威対策に重点をおいたアプローチを取ることにします。

表3と表4を見ると、組織の規模に関係なく、最も一般的に「システム侵入」のパターンに直面することがわかります。昨年のレポートでは、このパターンにコントロールをマッピングし、どのコントロールが最も一般的に攻撃に役立つかを示しました[55]。IG1の結果は、「コントロール14」が89%、「コントロール11」が80%、そして「コントロール5」が67%でした。

「サブコントロール」をさらに掘り下げると、組織のセキュリティ態勢を成熟させるための探求において、よりきめ細かな指針が得られるはずです。各組織は、それぞれのリスクプロファイルと許容度に従ってカスタマイズし、優先順位をつける必要がありますが、少なくともここから始めることができます。最も可能性の高い攻撃パターンを特定したら、次に直面する可能性の高い攻撃パターンを特定し、その対処方法を決定します。最も可能性の高いリスク領域に関するデータ主導の情報を利用することは、少ないリソースで管理の優先順位をつけるための防衛策となります。ある程度進展すれば、きっとあの何でも屋のIT担当者たちも夜は眠りに着けるようになるでしょう。

CISコントロール	概要
14	**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** 企業に対するサイバーセキュリティリスクを低減するために、従業員にセキュリティ意識を持たせ、適切なスキルを身に付けさせるセキュリティ意識向上のトレーニングプログラムを実施し、管理する。
11	**データ復旧** 対象範囲内の企業資産を事故発生前の信頼できる状態に復旧するのに十分なデータ復旧方法を確立し、管理する。
5	**アクセス制御管理** プロセスおよびツールを使用して、企業資産およびソフトウェアのユーザ、管理者およびサービスアカウントのアクセス認証情報および特権の作成、割り当て、管理、および失効などを管理する。

表5. 中小企業が最もよく遭遇する「インシデント分類パターン」に適したCIS「実施グループ1（IG1）」のコントロール

54 https://www.cisecurity.org/controls/cis-controls-navigator/

55 2022年DBIR、付録 B：VERISと標準、p. 96

適正な規模は中堅企業

あなたの会社はそれなりの期間ビジネスを展開してきています。決して小さな会社ではないが、でもまだ大企業レベルには達していません。IT運用と情報セキュリティの両面で、プロセスの成熟化に熱心に取り組んできました。IG1の「コントロール」を導入し、現在はIG2で次のレベルの保護を目指しています。

このことを念頭に置いて、中小企業にとって2番目に大きな脅威である「ソーシャルエンジニアリング」のパターンをカバーするIG2のコントロールを見てみましょう。最初の2つのコントロールは、「システム侵入」の「コントロール5」（100%）と「コントロール14」（100%）と同じ主要カテゴリーです。しかし、3 番目のコントロールは、このパターンでは異なります。

- **コントロール17 – インシデント対応管理**
  攻撃に対する準備、検知、および迅速な対応のために、インシデントレスポンス能力（ポリシー、計画、手順、定義された役割、訓練、およびコミュニケーションなど）を開発し、維持するためのプログラムを確立する。

「インシデント対応管理」の計画は、セキュリティのあらゆる分野においても重要な作業ですが、「ソーシャルエンジニアリング」攻撃に関しては、いくつかの理由から特に重要です。「なりすまし」のような攻撃の多くは、急速にエスカレートする傾向があり、大きな影響を与える可能性があります。おそらく同様に重要なこととして、従業員はこれらのインシデントが発生したときに報告できる場所があると知っていることに安心感を持つ必要があります。

「リソースを手に入れる！あなたはリソースを得る！誰もがリソースを得る！」

では、中小企業の中でもやや大きい企業に目を向けてみましょう。明確にするために、中小企業から離れるのではなく、単にまだ従業員1,000人未満のカテゴリーに分類される大きめの企業を取り上げています。会社がこのレベルに達すると、より多くの人員、より多くのテクノロジーオプション、あるいは単純により多くの資金[56]など、問題に投入できるリソースがより多くなり、それらのリソースを活用することで大きな利益を得ることができます。このレベルでは、IG1とIG2に取り組み、IG3の「コントロール」の準備が整っているかもしれません。

これらの「コントロール」は、組織とともに成熟していいます。そこで、中小企業で3番目によく見られるパターンについて、IG3の対策を検討しましょう：「基本Webアプリケーション攻撃」最初の「コントロール17」（100%）については前のセクションで説明しましたが、「コントロール16」（100%）と18（100%）についてはまだ説明していません。

- **コントロール16 - アプリケーションソフトウェアのセキュリティ**
  自社開発、ホスティング、または買収したソフトウェアのセキュリティライフサイクルを管理し、セキュリティ上の弱点が 企業に影響を及ぼす前に予防、検出、是正する。

- **コントロール18 – 侵入テスト**
  コントロール（人、プロセス、技術）の弱点を特定し、それを疑似的に悪用し、攻撃者の目的と行動をシミュレートすることで、企業資産の有効性と回復力をテストする。

昨年のDBIRで取り上げたSolarWindsの事例と、今年取り上げたLog4jの影響を考慮すると、「コントロール16」は確かに時宜を得たものであり、この「コントロール」の関連性は問題ないでしょう。サブコントロール16.2：ソフトウェアの脆弱性を受け入れ、対処するプロセスの確立と維持、16.4：サードパーティソフトウェアコンポーネントのインベントリの確立と管理、および16.5：最新かつ信頼できるサードパーティソフトウェアコンポーネントの活用は、これら2つのケースに対する防御に大いに役立つでしょう。

56 そして、これは決して困ったことではないですよね？

中小企業でも、組織の規模が大きくなれば、「コントロール18」が重要になります。侵入テスト能力を確立し、その結果をセキュリティプロセスに組み込むことで、大き目な中小企業の情報セキュリティ態勢を改善することができます。これは基本的に、管理策が期待通りに機能しているかどうかを確認するための実世界でのテストです。バックアップと同様、テストされ、検証された管理策だけが信頼されるべきなのです。

これで、すでに「コントロール」に目を通し、優先順位をつけたことで、最も被害を受けそうなものがわかり、最後までやり通すことができます。予防と検知のバランスがとれており、何か悪いことが起こったときにそれを検知するだけでなく、迅速かつ適切に対応できるようになっているのです。これで、計画をまとめるという基本作業から、ロードマップを実行する段階へと移行しました。

最後に、この時点で考慮すべきことをいくつか挙げておきます。特定のコンプライアンスフレームワークとの整合性を検討していますか？自社環境のセキュリティに関する指標を追跡していますか？あなたの取り組みは、セキュリティ態勢の継続的な改善につながっていますか？それとも、「この時点では良好だったが、その後状況が変化した」という時点の状況説明を提供しているだけですか？組織で何が起きているかについての適切な情報をセキュリティ戦略の舵取りに活用すれば、できることはかなりあります。

Center for Internet Security（CIS）について：

ネットワークの所有者が自社の企業資産、実行中のソフトウェア、および重要なデータの所在を把握していなかったために多くの攻撃が成功していることを、各種の報告書や調査に次ぐ調査が明らかにしています。自社の環境を知ることは、サイバーセキュリティプログラムの基礎であり、CISの「重要セキュリティコントロール（Controls）」の最初の3つのコントロールの範囲です。何と言っても、把握していないものを保護することはできません。

自社の環境を理解してこそ、企業全体で適用すべきコントロールとその優先順位を決めることができます。CISでは、この作業には時間とリソースがかかることを承知しています。そのため、セキュリティ改善プログラムの計画を支援するために、「コントロール」とそれをサポートする「セーフガード」に優先順位を付けています。CISは、「実施グループ（IG）」を通じてこれを行います。IGは3つあり、リスクプロフィールと、企業がコントロールを実施するために利用可能なリソースに基づいています。各IGは、前のIGの上に構築されます。つまり、IG2はIG1の上に構築され、IG3はすべての「コントロール」と「セーフガード」から構成されるというように。

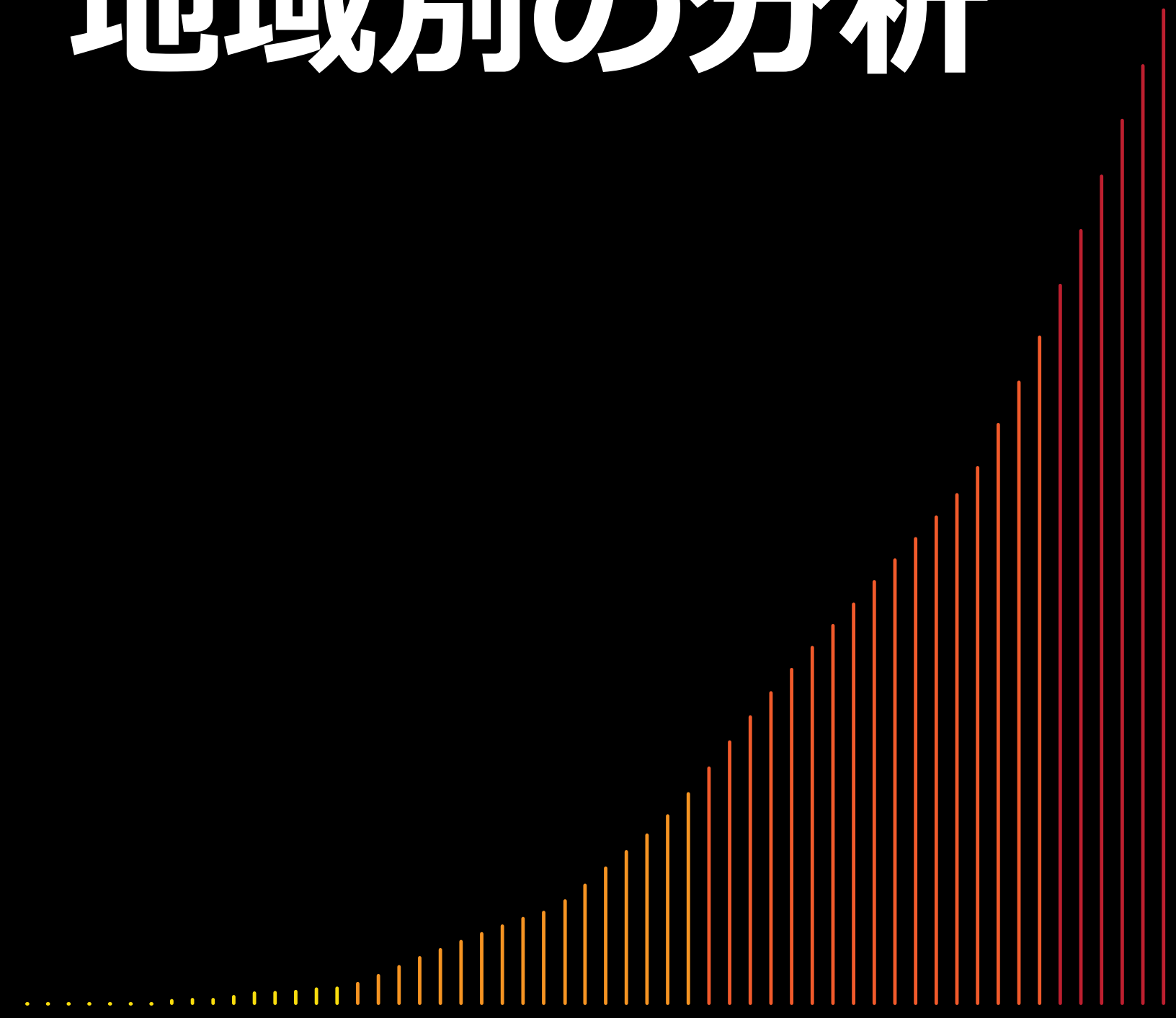
典型的なIG1の企業は、ITとサイバーセキュリティの専門知識が限られており、IT資産と人員の保護に専念できる中小企業です。これらの企業の主な関心事は、ダウンタイムの許容に限界があるため、事業の運営を維持することです。企業のデータの機密性は低く、主に従業員と財務情報を保護対象としています。

IG1で選択される「セーフガード」は、サイバーセキュリティの専門知識が足りなくとも実装可能であり、標的を絞らない一般的な攻撃を阻止することを目的としたものが推奨されます。また、これらの「セーフガード」は通常、小規模またはホームオフィス用の市販（COTS）ハードウェアおよびソフトウェアと連携して動作するように設計されます。

しかし、ビジネスの規模や複雑さにかかわらず、すべての組織がIG1から始めることをお勧めします。IG1は、サイバー犯罪者によって使用されている主要な攻撃タイプから組織を防御するために必要なアクションを提供しているため、私たちはIG1を「基本的なサイバー衛生」とも呼んでいます。IG1は、単にやるべきことのリストではなく、すべての企業が現実世界の脅威から身を守るために不可欠な一連のステップです。そして、サイバー成熟度の向上やセキュリティニーズの変化に対応するための強力な基盤となります。これは強い主張になりますが、（ベライゾンのDBIRのような）攻撃に関する入手可能な最も優れた総覧と、オープンで共有された方法論（CIS Community Defense Model v2.0[57]）を活用することでこの主張は裏付けられます。

57 https://www.cisecurity.org/insights/white-papers/cis-community-defense-model-2-0

5
地域別の分析



地域別分析の概要

各地域のサイバー犯罪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4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。下記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、改善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す。

世界の地域は、国連のM49基準[58]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。その結果、今回の調査対象となったのは以下の地域です。

アジア太平洋地域（APAC）：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）

ヨーロッパ、中東、アフリカ（EMEA）：北アフリカ（015）、ヨーロッパ（150）、東欧（151）、西アジア（145）

ラテンアメリカ・カリブ海地域（LAC）：南米（005）、中米（013）、カリブ海諸国（029）を含む

NA（北アメリカ）：米国とカナダ（021）

例年通り、我々は様々な方法でデータを切り刻みましたが、今回は様々な地域のデータを少し違った形で紹介しています。長年にわたる読者の方は、各主要セクションに掲載した「早見表」をご存じでしょうが、今回は、頻度や上位のパターンなどに関して、各地域がどれだけ似ているか（そして異なっているか）を簡単にご覧いただけるよう、それらを組みわせてみました。

地域	頻度	上位3つのパターン	攻撃者	攻撃者の動機	侵害されたデータ
アジア太平洋地域（APAC）	インシデント699件、確認されたデータ暴露164件	「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93%を占めている	外部（92%）、内部（9%）、パートナー（2%）、複数の関係者（2%）（漏洩/侵害）	金銭目的（61%）、スパイ活動（39%）、利便性（2%）、怨恨（2%）、二次的動機（1%）（漏洩/侵害）	内部情報（56%）、機密情報（42%）、その他（33%）、認証情報（29%）（漏洩/侵害）
欧州、中東、アフリカ（EMEA）	インシデント2,557件、確認されたデータ暴露637件	「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97%を占めている	外部（98%）、内部（2%）、複数の関係者（1%）（漏洩/侵害）	金銭目的（91%）、スパイ活動（8%）、イデオロギー（1%）、愉快（1%）（漏洩/侵害）	認証情報（53%）、内部情報（37%）、システム情報（35%）、その他（15%）（漏洩/侵害）
ラテンアメリカ・カリブ海地域（LAC）	インシデント535件、確認されたデータ暴露65件	「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94%を占めている	外部（95%）、内部（5%）、パートナー（2%）、複数の関係者（2%）（漏洩/侵害）	金銭目的（93%）、スパイ活動（11%）、イデオロギー（2%）（漏洩/侵害）	システム情報（55%）、内部情報（32%）、機密情報（23%）、認証情報（23%）、その他（19%）（漏洩/侵害）
北アメリカ（NA）	インシデント9,036件、確認されたデータ暴露1,924件	「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85%を占めている	外部（94%）、内部（12%）、複数の関係者(9%)、パートナー（2%）（漏洩/侵害）	金銭目的（99%）、スパイ活動（1%）、怨恨（1%）（漏洩/侵害）	認証情報（67%）、内部情報（50%）、個人情報（38%）、その他（24%）（漏洩/侵害）

表6. 各地域の状況

58 https://unstats.un.org/unsd/methodology/m49/

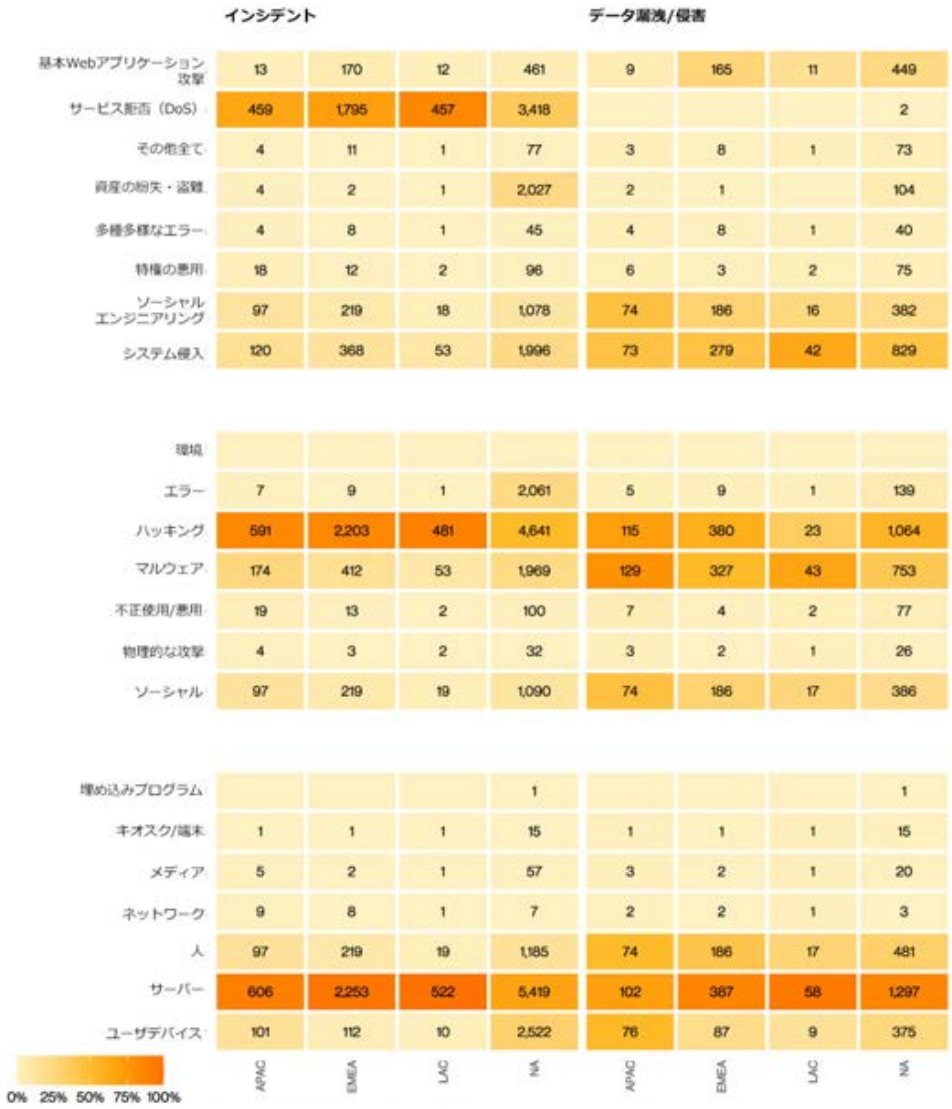


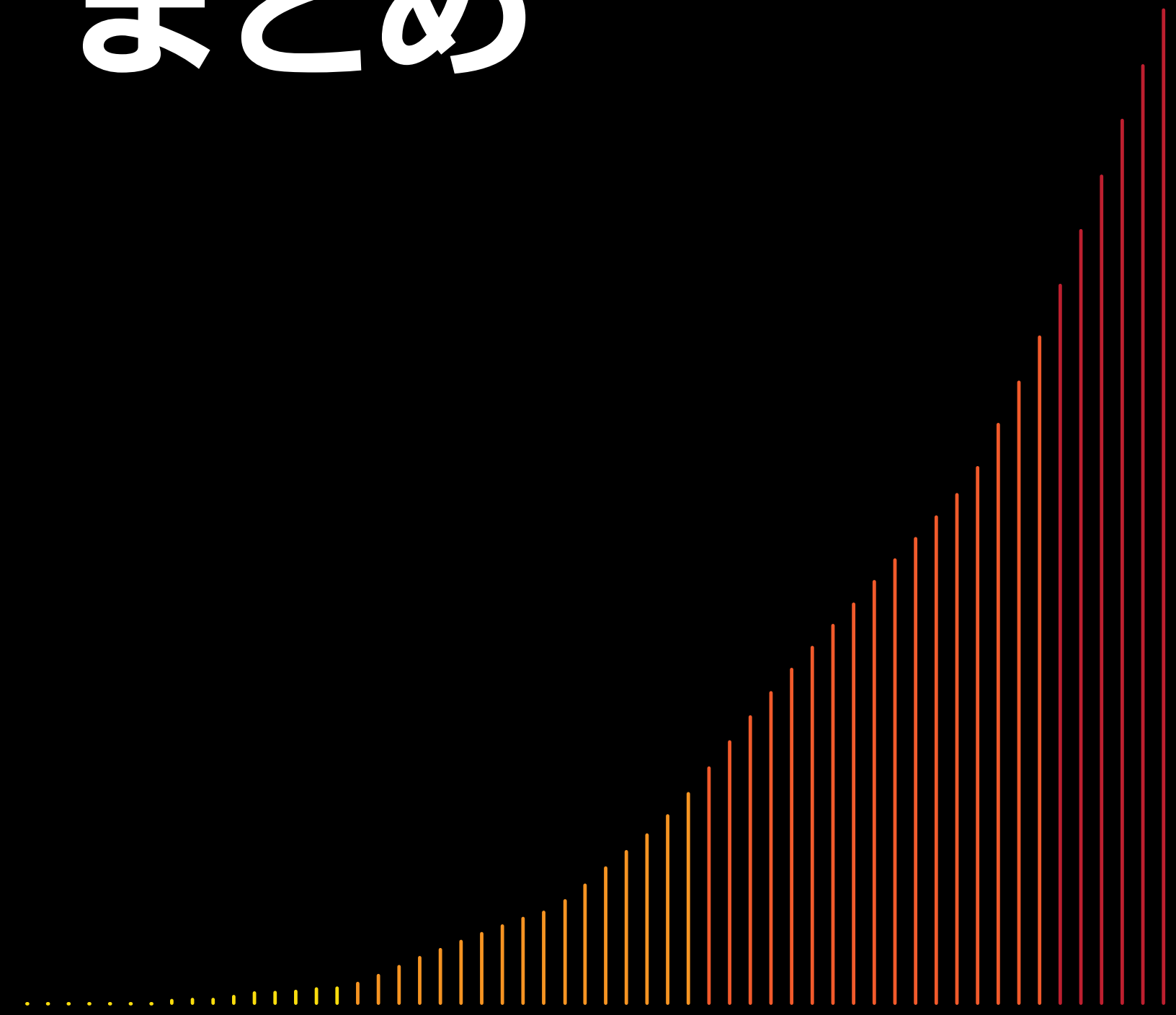
図63. 地域別のインシデントとデータ漏洩/侵害

「システム侵入」のパターンがAPACを除くすべての地域でトップであることは一目瞭然です。また、サイバー犯罪の背後にいるのは、「金銭目的」の動機に基づく外部攻撃者であることも明らかです。このような攻撃者が好むデータの種類は、地域によってより多様であることがわかります。そして私たちのデータはしばしば「何が」を明かしてくれる一方、なかなか「なぜ」を明らかにしてくれません。ある種のデータ型が、ある地域と他の地域とでは、規制要件によってよりよく保護されているのかもしれません。私たちが思いもよらない他の要因かもしれません。しかし、「認証情報」が依然として重要な位置を占めており、侵害される際の価値を下げる必要があることは明らかです（ヒント：MFAに注目すべき）。

図63の素敵なヒートマップをご覧ください。これは、これらの攻撃が地域によってどのように異なるか（または類似しているか）を示す、私たちのお気に入りの方法です。パターン別、地域別に分けてみると、確かに違いはあるものの（その多くは業種とその結果としての共通のインフラパートナーに基づいていることは間違いありません）、地域ごとに、また地域を越えて、いくつかの集中が見られることがよくわかります。

あなたの地域が、そして本報告書の他のデータと組み合わせれば、業種や組織の規模が、どのような攻撃を最も受けやすいかを示すものであり、あなたの防御戦略をより的確なものにできることを願っています。まだ何から手をつけたらよいかわからず、中小企業のセクションを読み飛ばしてしまった場合は、本報告書の情報をどのように適用すればよいかを知るためのよい参考資料となるでしょう。

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[59]。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。また、私たちの忠実な読者の皆様に対して、改めて心からの感謝の意を表したいと思います。長年にわたって皆様からお寄せいただいたご意見やご感想は、私たちがこのレポートを継続的に進化させ、より良いものにしていくための原動力となっています。

「元気で、豊かで、何事にも備えあれ[60]」

59 まあ、少し大げさかもしれませんが。「不眠症の万能薬ではない」というのはどうでしょう？
60 ちなみに、これはDBIRチームの非公式モットーです。

年間総括

1月

VTRACの「インテリジェンスアナリスト」は、2022年の幕開けに、SolarWindsキャンペーンが2021年の幕開けを飾ったのと同じように、Log4jを悪用した攻撃を追跡するというデジャブを体験しました。2021年12月の第1週に、Log4jの脆弱性が情報セキュリティのリスクレーダーで最大の注目を集めました。その約1週間後に、VMwareはLog4Shell攻撃を観測し、「攻撃の大半はLinuxシステムを標的としている」と報告。Log4j、特にVMwareへの攻撃は、2022年の間、持続的なリスク問題であり続けました。1月末までには、悪名高い初期アクセスブローカーであるProphet Spiderが、Log4jを使って侵害したVMware Horizonsシステムの販売を行なっていました。ロシアの攻撃者（TA: Threat Actor）Ember Bearは、ワイパー型マルウェアWhisperGateを使用してウクライナへの攻撃を開始しました。マイクロソフトがWin32k.sysドライバのゼロデイ脆弱性にパッチを適用しました。Appleは、iPhoneやiPadに影響を及ぼすゼロデイ脆弱性にパッチを適用しました。

2月

ロシアの2022年2月のウクライナ侵攻を支援するサイバー攻撃に関する情報の収集と分析は、VTRACにとって2月の最も重要な活動でした。2月24日およびその前に、ロシア軍参謀情報本部（GRU）[61]は、ウクライナのViasat衛星通信端末に対するAcidRainワイパーマルウェア攻撃を開始しましたが、ヨーロッパ全土に散在する端末にも付随的に大きな被害が発生しました。ウクライナは、ロシアのTAによって少なくとも6つの新たなワイパー型マルウェアの標的にされました。2月25日、「サービスとしてのサイバー犯罪」として悪名高いTA「Conti」がロシアへの支援を表明しました。その2日後には、Twitterユーザの"@ContiLeaks"が、6万件のチャットメッセージを含むContiの内部ファイルを400件公開しました。2月の「通常の」サイバー関連情報には、Zimbra、Chrome、Apple OS、Adobe Commerce/Magentoのゼロデイ脆弱性が含まれていました。Emotetを操るサイバー犯罪者は、ロシアとウクライナの紛争を餌にしたマルスパムを発信しました。

3月

3月は、Chrome、Firefox、Trend Micro Apex Central、Mitelのビジネステレフォニーのコンポーネントの脆弱性がゼロデイで悪用されたため、企業のセキュリティチームやパッチ管理チームは多忙を極めました。ロシアとウクライナのサイバー攻撃の証拠を探すために警戒を強化した結果、中国、イラン、北朝鮮のAPT攻撃者に関する情報が得られました。中国のAPT攻撃者Mustang Pandaは、ロシアとウクライナの紛争に乗じて、モンゴル、ベトナム、ミャンマー、ロシアの外交公館、シンクタンク、ISPを攻撃しました。脆弱なWebアプリケーションの悪用を詳細に示す新たな情報により、別の中国のAPT攻撃者であるAPT41（Winnti）は、米国の複数の州政府のネットワークに対する攻撃を水平展開しました。イランのAPT MuddyWaterは、アラビア半島、トルコ、パキスタンを標的としていました。これまでで最大の暗号通貨の盗難は、北朝鮮のLazarusグループがRonin Networkから6億2,000万米ドル以上を盗みました。北朝鮮のAPT Kimsukyは、核関連のシンクタンクを標的として、彼らの特徴である「BabyShark」マルウェアを使用しました。Lapsus$ TAは、戦術、技術、手順（TTP）をランサムウェアからデータ窃盗恐喝に移行し、Microsoft、Okta、Nvidia、Samsungでの侵害を主張しました。

61 現在の名称は「ロシア連邦軍参謀本部情報総局」（少し大げさではないですか？）

4 月

パッチ管理チームは4月、Windows CLFS、Apple OS、トレンドマイクロのセキュリティ製品、Chromeブラウザ、VMwareで攻撃を受けているゼロデイ脆弱性を緩和するために特に奔走しました。Sophosのファイアウォールは、セキュリティ勧告とパッチをリリースした数時間後に攻撃を受けました。SonicWall、Zyxel、FortiGuardもファイアウォールのセキュリティ勧告とアップデートをリリースしました。VTRACはAPTグレードの攻撃者に関して通常以上の情報収集を開始し、他のTAやVerizon Cyber Security Consultingのクライアントが使用できるTTPアップデートを提供しました。中国のAPTグレードの行為者Deep Pandaによる攻撃作戦は、12月のパッチが適用されていないVMware Horizonサーバーの悪名高いLog4Shellの脆弱性を悪用していました。また、2月に発生したViasatへの攻撃の詳細や、北朝鮮のLazarusグループによる4つの作戦など、ウクライナを攻撃しているロシアの国家支援を受けた攻撃者に関する情報も収集しました。LockBit、FIN7、ALPHV、Hive、CL0P、Contiなどのサイバー犯罪TAによる攻撃は衰えることなく続きました。

5 月

2022年には、インフラコンポーネントの脆弱性が繰り返しテーマとして浮上し始めました。F5 BIG-IPアプライアンスの脆弱性（CVE-2022-1388）およびZyxelファイアウォールの脆弱性（CVE-2022-30525）に関するセキュリティ勧告およびパッチがリリースされてから1週間も経たぬうちに、脆弱性の悪用が開始されました。マイクロソフトは5月のパッチチューズデーで、ゼロデイWindows LSAスプーフィングの脆弱性（CVE-2022-26925）を含む74件の脆弱性にパッチを当てました。CISAは当初、この脆弱性をKnown Exploited Vulnerabilities Catalog（既知の悪用される脆弱性カタログ）に追加しましたが、ドメインコントローラーのパッチ適用を急いだ結果、認証に失敗して障害が発生するのを避けるため、すぐに削除しました。EmotetとRevilという2つの悪名高いマルウェアファミリーは、それぞれ活動を停止したと思われていましたが、5月に復活しました。5月が終わると、中国のAPT攻撃者が別のWindowsのゼロデイ脆弱性（CVE-2022-30190）を悪用してロシアとベラルーシの標的を攻撃しているという情報が浮上しました。脆弱性「Folina」は、Microsoft Support Diagnostic Tool（MSDT）のリモートコード実行の脆弱性でした。

6 月

Folinaが発見された数日後、AtlassianはConfluence Data CenterとServerのゼロデイリモートコード実行の脆弱性（CVE-2022-26134）に対するパッチを発表しました。米国のメモリアルデーの週末に、Volexityのインシデント対応者は、おそらく中国の攻撃者によってBehinderのWebシェルがインストールされた、インターネットからのアクセス可能な2つのAtlassian Confluence Serverで不審な活動を検知していました。Volexityはまた、Sophos Firewallのゼロデイ脆弱性（CVE-2022-1040）が"DriftingCloud"と名付けられた中国のAPT攻撃者によって悪用されていることを報告しました。また、悪名高い中国のAPT脆弱性攻撃者Deep Pandaが、パッチ未適用のVMware Horizonサーバーに対しLog4jの脆弱性を悪用した広範な攻撃を継続しているとの情報もありました。

7 月

サイバーインテリジェンスレポートの発表は、通常Black Hat USAとDEF CONカンファレンスに先行して行われます。2022年におけるこれらのレポートの質、量、幅は、7月の最も重要なインテリジェンスとなりました。攻撃者はオープンソースインテリジェンス（OSINT）から学習することに長けているため、成功したTTPを追跡することがインテリジェンスの要件となっており、セキュリティアーキテクチャをすばやく調整することが必須となっています。GoogleのChromeブラウザとWindows CSRSSでゼロデイ脆弱性が悪用されたことで、複数のAtlassian製品における3つの未発見の重大な脆弱性への対応と同様に、パッチ管理チームは多忙を極めました。ランサムウェアと暗号マイニングのTAが、6月以降、CVE-2022-26138の脆弱性の悪用に成功しているという情報も入ってきました。

8 月

"Folina"に加え、Microsoft Windows Support Diagnostic Toolに2つ目のゼロデイリモートコードの脆弱性が発見され、悪用され、8月にパッチが適用されました。Apple、macOS、iOS、iPadOSに加え、Google Chromeにもそれぞれゼロデイ脆弱性が報告され、パッチが適用されました。8月上旬には、Twilioの現従業員と元従業員が、TwilioのIT部門からパスワード変更を求めるスミッシングメッセージを受け取りました。この侵害により、130以上の組織で9,931のアカウントが侵害され、そのほとんどにOktaのIDおよびアクセス管理ソリューションが使用されていました。この攻撃者は、Twilioの多要素認証ソリューションAuthyを利用している93のユーザを侵害しました。これらの攻撃や複数のID攻撃は、少なくとも3月に遡る“Scatter Swine“またはOktapus TAに起因するとのインテリジェンスの報告がありました。

9 月

9月は2022年のゼロデイパルーザの月となりました。新しい月が始まって2日後に、Google ChromeとMicrosoft Edgeは、ブラウザのゼロデイ脆弱性にパッチを適用しました。Trend Microは、同社のApex Oneセキュリティ製品へのIn the Wild攻撃の成功を受けて、今年2つ目のゼロデイ脆弱性を緩和しました。また、Sophosファイアウォールの顧客は、今年2回目のゼロデイパッチを適用する必要がありました。最も重要なゼロデイ攻撃は、Windowsの脆弱性を連鎖させた"ProxyNotShell"というニックネームの中国のAPT攻撃者によるものでした。また、VMwareサーバーは、ESXi、Linux、およびWindowsサーバーに悪意のあるvSphereインストールバンドルを適用する中国のサイバースパイ活動者の標的にされました。

10 月

マイクロソフトは、10月のパッチチューズデーで「ProxyNotShell」にパッチを適用しませんでしたが、特権昇格のゼロデイ脆弱性（CVE-2022-41033）用のパッチをリリースしました。Fortinetは、複数の製品に存在するゼロデイ認証バイパスの脆弱性にパッチを当てました。Zimbra Collaboration Suiteのゼロデイ脆弱性（CVE-2022-41352）が悪用され、それ以前のZimbraの3つ脆弱性のパッチ適用が遅れたために、1,600台以上のサーバーがシステム侵入されました。攻撃は報告されていないものの、Apache Commons Textライブラリに新たな脆弱性が見つかり、“Text4Shell”が情報セキュリティ用語集に登録されました。URSNIFとEmotetの2つの悪名高いマルウェアが、標的を拡大するために再利用されました。これらは、それぞれTTPが大きく変化し、前者はバンキング型「トロイの木馬」からイニシャルアクセスダウンローダーに、後者はフルサービスの「サービスとしてのマルウェア」オペレータのツールとして、4か月の眠りから目覚めました。その他にも、Chromeブラウザや、iOS、iPadOSにおけるゼロデイ攻撃、脆弱性、パッチが報告されています。

11 月

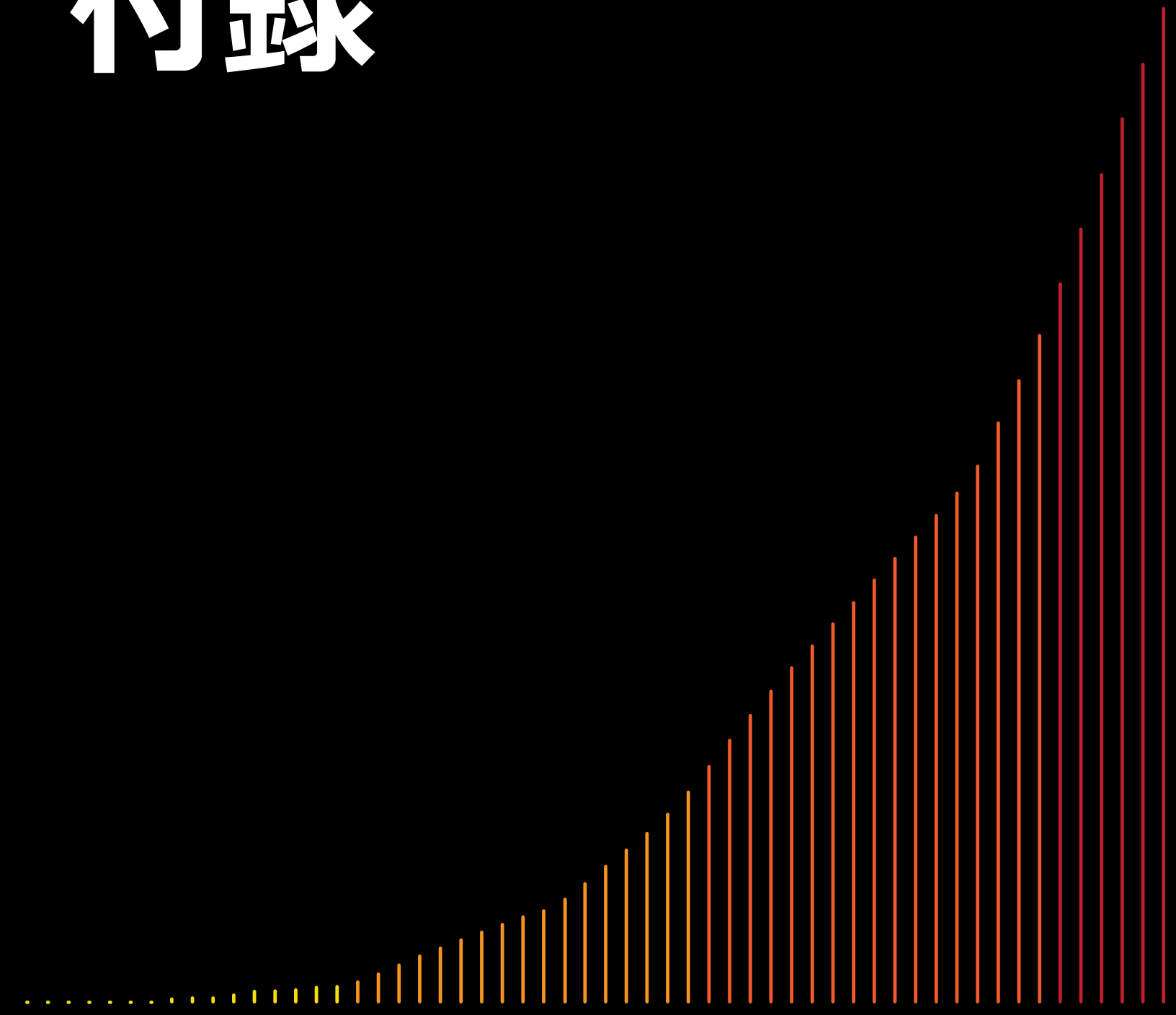
11月には、いくつかの系統のマルウェアが情報セキュリティのリスクインテリジェンスを浮き彫りにした。Exchangeに対するProxyNotShell攻撃の最初の報告から40日を経て、マイクロソフトはこれら2件の脆弱性にパッチを適用しました。また、パッチチューズデーには自社製品の他の4つのゼロデイ脆弱性にパッチを適用しました。Chromeブラウザもゼロデイ脆弱性が緩和されました。VTRACが収集した情報の中では、3つのマルウェアファミリーに関する最新情報が目立ちました。SocGholishは、サイバー犯罪者がドライブバイダウンロードを実行するために使用するJavaScriptフレームワークおよび「サービスとしてのマルウェア」です。新しい悪意のあるローダーであるBumblebeeは、5月に初めて登場し、11月にはMeterpreterとCobalt Strikeのペイロードを配信し始めました。Raspberry Robinワームを操るサイバー犯罪者は、他のペイロードを展開するための初期アクセスブローカーへと転身しました。

12 月

2020年はSolarWinds Orionが、2021年にはLog4jが引き起こした年末の一連の情報セキュリティマイルストーンの連鎖を断ち切ったことで、2022年12月は比較的平穏なものとなりました。インテリジェンスによると、複数の脅威者がマイクロソフトの開発者アカウントを悪用し、プロファイルを利用して悪意のあるドライバに署名をさせ、ランサムウェアやSIMスワッピングなどのサイバー攻撃に利用していたとのことです。マイクロソフト、Apple、Fortinet、Citrix各社の製品への攻撃の被害報告は、ゼロデイ脆弱性を悪用した攻撃が数か月間続いたことを物語っています。OWASSRFは、9月のProxyNotShell攻撃チェーンに対応してマイクロソフトが提供したURL書き換え緩和策を利用して、オンプレミスのExchangeサーバーを悪用する新しい攻撃チェーンです。OWASSRFを悪用するPlayランサムウェアの攻撃者によって、少なくとも8つ組織が攻撃の被害を受けました。収集されたインテリジェンスの中には最も重要な情報として、北朝鮮の軍事情報機関である偵察総局（RGB）の121局配下にあるTAが行なった戦闘の仮想順序がありました。

Verizon Threat Research Advisory Center（VTRAC）のDave Kennedyの継続的な支援と本報告書への毎年の貢献に感謝いたします。

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。verizon.com/business/resources/reports/dbir/2023/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[62]、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を探ることです。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[63]。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 Object Notation（JSON）は、自動化されたワークフローにより取り込まれ、そこに含まれるインシデントやデータ漏洩/侵害を必要に応じてVERIS JSON形式に変換し、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。

62 https://github.com/vz-risk/dbir/tree/gh-pages
63 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、2021年11月1日から2022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2022年の事例ですが、全期間のデータがあらゆる箇所で参照されており、特に傾向を表すグラフで使用されています。また、組織属性の損失に結び付けることのできない個人に影響を及ぼすインシデントおよびデータ漏洩/侵害については、これを除外しました。例えば、ご友人の私用ノートPCがTrickbotの攻撃を受けた場合は、本報告書には含まれません。

最後に、DBIRに含まれるための条件として、私たち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（「斜めカット」の棒グラフ）、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。

図64～67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。

データ漏洩/侵害

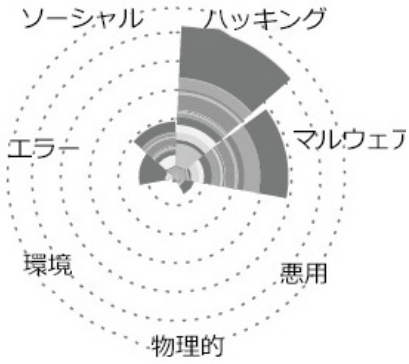


図64. 攻撃別の各貢献度

データ漏洩/侵害

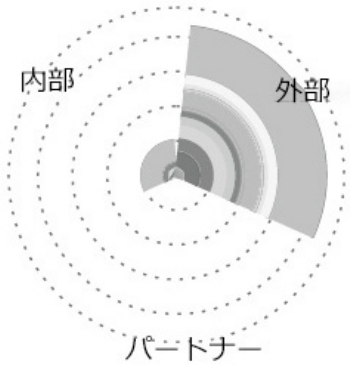


図65. 攻撃者別の各貢献度

データ漏洩/侵害

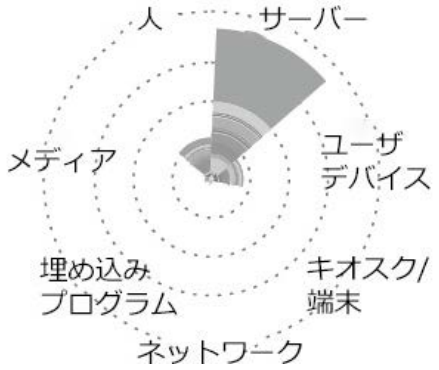


図66. 資産別の各貢献度

データ漏洩/侵害

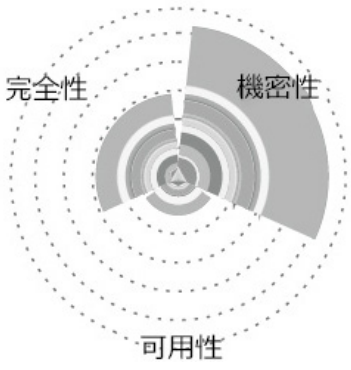


図67.0属性別の各貢献度

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ということです）[64]。

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。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6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、DDoS、その他の種類のデータが挙げられます。インシデント以外のデータのサンプルサイズは、インシデントデータよりもはるかに多い傾向がありますが、データのソースは限られています。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。

64 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のMITRE ATT&CK®へのマッピング

サイバーセキュリティの世界の荒波を航海する際には、方向性を示す地図があると便利です。私たちは、DBIRがそのような地図の1つであり、組織が複雑で変化し続けるサイバーセキュリティの状況をナビゲートするのに役立つと考えています。この地図が可能な限り正確であることを確認するために、私たちはVERISフレームワーク[65]を作成しました。このフレームワークは、疲れたサイバー船員がリスク指向の意思決定を容易にするために、データ漏洩/侵害の重要な構成要素のほとんどを捉えています。

長年にわたり、さまざまな詳細レベルを提供する新たなガイドフレームワークが作成されており、MITRE ATT&CK®が圧倒的に人気があります。私たちは、MITRE EngenuityおよびCenter for Threat Informed Defense[66]と協力し、VERISとATT&CKの関係を把握することで、組織がナビゲーションにおいて両者の利点を活用できるようにしました。

注目に値する成果：ATT&CKは、攻撃者が活用する特定の技術に関する優れた戦術的・技術的な詳細を提供し、一方VERISは、起こり得る災難のより広い範囲をカバーする、サイバー攻撃の状況の戦略的なビューを提供します。例えば、エラーは今年のデータ漏洩/侵害の9%に見られますが、ATT&CKでは対象外です。VERISとATT&CKを組み合わせることで、どのようなタイプの資産が影響を受け、どのようなタイプの被害者がそれらの資産に属していたかを、より明確に把握することができます。

データの漏洩/侵害を政府に報告するという規制上の圧力が高まっているため、このような力の組み合わせは時宜を得たものと言えます。ただし、この報告をどのように行うべきかについては、一般的に受け入れられている形式はありません。もちろん、私たちはそのような規制の必要性について意見を述べることはできませんが[67]、新しい法律が実現するにつれて、組織が負担を軽減するための適切なツールを持っていることを確認するために、私たちの役割を果たしたいと考えています。

2023年4月6日に、このマッピングの第2版がリリースされたばかりであり、私たちは非常に期待しているところです。VERISの戦略的見地からのサイバー攻撃分析に加え、「属性」のマッピングにも多くの工夫が凝らされています。より明確にするために、攻撃者をATT&CKグループにマッピングしました[68]。また、ATT&CK for MobileとATT&CK for ICSへの新しいマッピングもあります。

この作業に少しでも興味がある方は、https://center-for-threat-informed-defense.github.io/attack_to_veris/で作業の詳細をご覧ください。そうでなくても[69]、一部のインシデントパターンに追加したATT&CKテクニックのマッピングのおかげで、あなたはすでにこの作業の恩恵を受けています。

私たちのチームは、VERISフレームワークをより利用しやすく、すべての人に役立つものにするために、多くの考えとエネルギーを注いでいます。もしあなたがフレームワークについて興味があり、過去に試したことがあり、何が新しくなったかを確認したいのであれば、DBIRチームまでご連絡ください（dbir@verizon.com）。

65 https://verisframework.org/
66 https://mitre-engenuity.org/cybersecurity/center-for-threat-informed-defense/
67 誰をからかっているのだろうか？私たちは分析するためのデータがもっと欲しいのです！
68 https://attack.mitre.org/groups/
69 よくそんなことを

付録C：VTRACの20年を振り返る

Chris Novak、ベライゾン サイバーセキュリティコンサルティング マネージングディレクター

Verizon Threat Research Advisory Center（VTRAC）が設立から20年を迎えたとは信じがたいことです！私は、「ゼロデイ」とでも言うべきかVTRACの設立当初からチームの一員であることに、このうえない喜びを感じています。

この20年間、VTRACの名前はいくつか変わりましたが、裏方にいる情熱的なチームはいつも同じでした。当時、私はニューヨークの小さなオタク集団の一員で、常にスーツケースに荷物を詰め込み、次の大規模なデータ侵害調査に挑むため、どこへでも飛行機に飛び乗る準備をしていました。当時の私たちのフォレンジックラボは、フルハイトのサーバーラック1つ分にも満たないシステムの集合体でした。

20年前、「サイバーセキュリティ」という言葉は一般的に使われていませんでしたし、理解されてもいませんでした。一般の人に「サイバー」とは何かと尋ねたら、おそらくSF映画に出てくるような答えが返ってきたでしょう。サイバーセキュリティに関する大学の学位などというものは存在せず、当時存在した最も近いものは、コンピューターサイエンスかエンジニアリングの学位でした。現在では、サイバーセキュリティの学士号だけでなく、修士号や博士号を取得できる大学が世界中に何百とあります。

私が初めて調査したデータ侵害のいくつかは、今でも覚えています。古い人は、私たちが「メディカルバッグ」（通常、起動可能なフロッピーディスクのバインダー、各種ケーブルのコレクション、各種ハードドライブと筐体の入ったバッグ）を持って現場に現れた日々を高く評価してくれるでしょう。前述したように、当時はサイバーセキュリティが何であるかを知っている人はほとんどおらず、一般人はそのメディカルバッグの中の機器の目的を知りませんでした。9.11直後の世界では、その奇妙な電子機器やケーブルの入ったバッグを持って空港のセキュリティを通過すると、私はしばしば「ランダムな」特別検査の幸運な当選者になることがほぼ決まりでした。その幸運がラスベガスへの旅行にも少しは生きていれば。

今日、私たちが出張する必要はほとんどありません。世界中のどこからでも、遠隔地での科学捜査の証拠収集を可能にする企業ツールがあります。電気通信のバックボーンと携帯電話接続の進歩を利用して、5Gを介した即時の緊急通信や帯域外通信を提供することもできます。たとえ被害者組織が独自のネットワークやシステム、インフラに障害があったとしても、1Gbpsを超える速度でフォレンジックデータを収集することができるのです。

当時と現在の過去20年間におよぶ比較は、考えてみれば驚異的なものです。今日、私たちのチームには、経歴も地理的な場所も驚くほど多様な、飛躍的に多くの人材がいます。VTRACは100カ国以上の組織をサポートしています。私たちは世界中に物理的なラボ拠点をいくつか持っているだけでなく、クラウドベースやクライアントのオンプレミスのラボ拠点も持ち、考えうるほぼすべてのデータプライバシーと主権に関する懸念に対応しています。

もちろん、この出版を可能にしているDBIRチームの素晴らしい仕事も忘れてはなりません。多くの人が、DBIRは私の3番目の子供だと言っているのを聞いたことがあるでしょう。DBIRは16年前、VTRAC（当時はRISKチームと呼ばれていました）の初期の活動の一環として、私たちのデータ漏洩/侵害に関するインサイトを世界と共有するというビジョンを持って誕生しました。喩えるなら、私はVTRACが最初の言葉を発するのを聞き、他の共同創造者たちとともに最初の一歩を踏み出すのを見守ったのです。ありがたいことに、私はDBIRのために大学の学費を貯める必要はありません[70]。

私は、VTRACの過去と現在のメンバーが過去20年間に築き上げ、成し遂げてきたことを、これほど誇りに思うことはありません。チームメンバー一人ひとりの情熱と献身が、長い顧客契約、一度も欠かしたことのないサービスレベル契約、世界クラスのソートリーダーシップ、業界アナリストによる一貫したリーダーとしての評価につながっているのです。

次の20年も、冒険、革新、そして興奮の連続となることを楽しみにしています！

VTRAC、20歳の誕生日おめでとう！

— Chris Novak

70 編集部注：私たちは、DBIRがあなたの人間の子供たちの学費の支払いに実際に役立っていることを願っています。

付録D：協力企業

A

Akamai Technologies

Ankura

Apura Cyber Intelligence

B

Bit-x-bit

BitSight

BlackBerry

C

Censys, Inc.

Center for Internet Security

Cequence Security

CERT Division of Carnegie Mellon University's Software Engineering Institute

CERT – European Union

CERT Polska

Chubb

Coalition

Computer Incident Response Center Luxembourg （CIRCL）

Coveware

CrowdStrike

Cybersixgill

CYBIR

D

Department of Government Services, Victorian State Government, Australia

DomainTools

E

Energy Analytic Security Exchange （EASE）

Edgescan

Elevate Security

Emergence Insurance

EUROCONTROL

Eviden

F

Fortinet

G

Global Resilience Federation

GreyNoise

H

HackEDU

I

Ivanti

J

JPCERT/CC

K

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

KordaMentha

L

Legal Services Information Sharing and Analysis Organization （LS-ISAO）

M

Malicious Streams

Maritime Transportation System ISAC （MTS-ISAC）

mnemonic

N

NetDiligence®

NETSCOUT

O

Okta

OpenText Cybersecurity

S

S21sec

SecurityTrails, a Recorded Future Company

Shadowserver Foundation

SISAP – Sistemas Aplicativos

Shodan

Swisscom

V

VERIS Community Database

Verizon Cyber Risk Programs

Verizon Cyber Security Consulting

Verizon DDoS Defense

Verizon Network Operations and Engineering

Verizon Threat Research Advisory Center（VTRAC）

Vestige Digital Investigations

あ

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

アメリカ合衆国サイバーセキュリティ・社会基盤安全保障庁（CISA）

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）


Akamai
ankura
apura
bit-x-bit
BITSIGHT
BlackBerry
censys
CIS Center for Internet Security
CEQUENCE
Carnegie Mellon University Software Engineering Institute
CERT-EU
NASK CERT.PL
CHECK POINT
CHUBB
Coalition
CIRCL Computer Incident Response Center Luxembourg
COVEWARE
CROWDSTRIKE
CISA
CyberSecurity MALAYSIA
cybersixgill
CYBIR
DELL Technologies
VICTORIA State Government Australia
DomainTools
EASE
edgescan
Elevate Security
emergence
EUROCONTROL
EVIDEN
FORTINET
GLOBAL RESILIENCE FEDERATION
GREYNOISE

Hack_EDU	IRISS Irish Reporting and Information Security Service	ivanti	JPCERT CC®	K12 SIX
kaspersky	KordaMentha	LEGAL SERVICES ISAO	Malicious Streams	Maritime Transportation System Information Sharing and Analysis Center
mnemonic Securing your business.	NetDiligence®	NETSCOUT.	okta	opentext™
paloalto NETWORKS®	proofpoint. Security Awareness Training	S21SEC Cyber Solutions by Thales	SecurityTrails A Recorded Future Company	SHADOWSERVER Lighting the way to a more secure Internet
SISAP Sistemas Aplicativos	SHODAN	swisscom		
Verizon Cyber Risk Programs	Verizon Cyber Security Consulting	Verizon DDoS Defense	Verizon Network Operations and Engineering	Verizon Threat Research Advisory Center （VTRAC）
VESTIGE Digital Investigations	WatchGuard