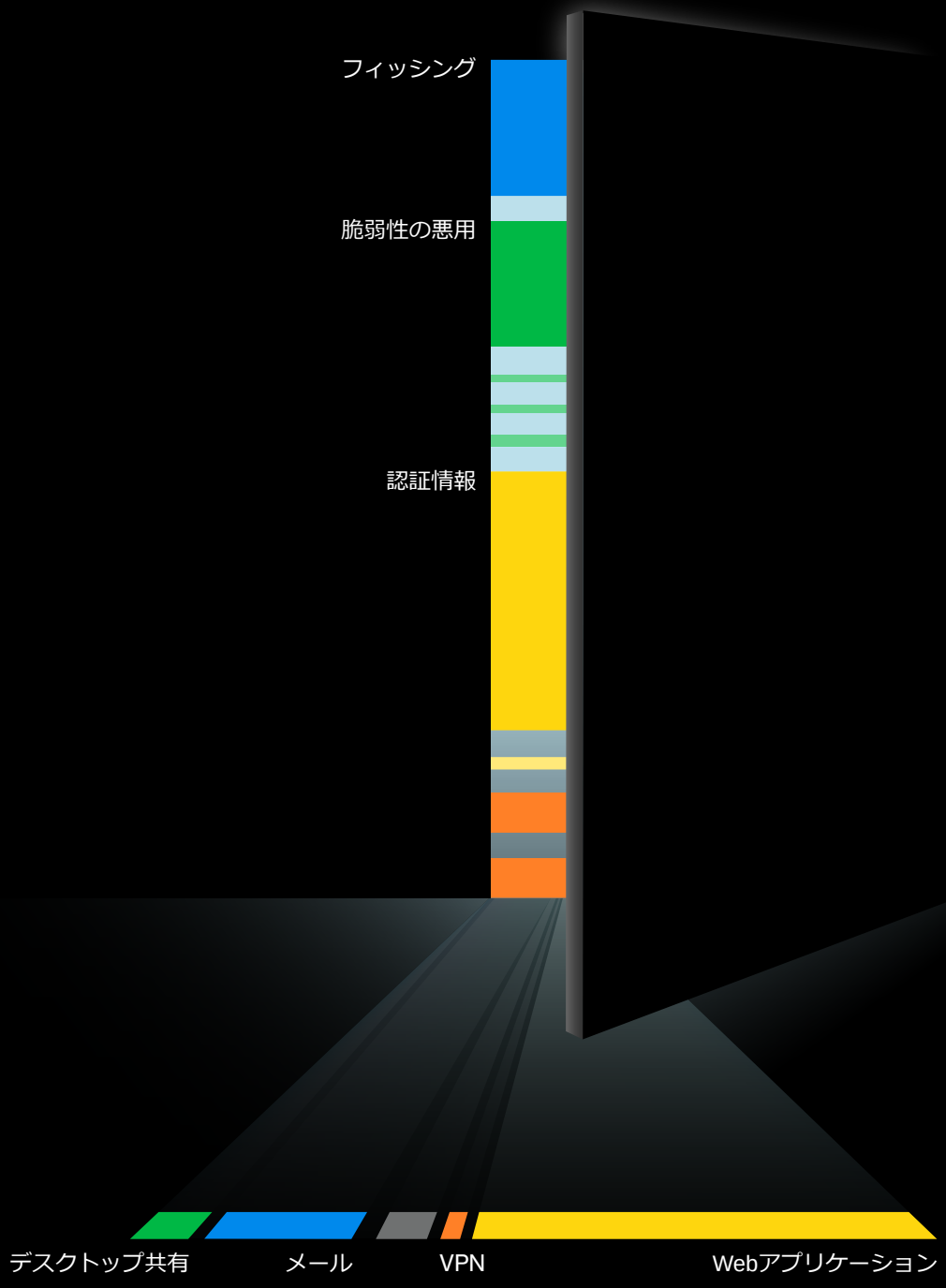
2024年度 DBIR
データ漏洩/侵害調査報告書

verizon business


フィッシング
脆弱性の悪用
認証情報
デスクトップ共有
メール
VPN
Webアプリケーション

表紙について

今年の報告書では、昨今の脅威の状況を踏まえ、データ漏洩/侵害を引き起こす可能性が最も高い攻撃と攻撃経路の組み合わせを特定するため、データ漏洩/侵害に至る経路をより深く掘り下げています。表紙に描かれた、鍵の壊されたドアから漏れ出る光は、部屋の中へ侵入する攻撃者がさまざまな方法を試みていることを表しています。ドアの隙間から見えるパターンは「侵入経路」の組み合わせの割合を示し（図7で詳しく説明）、床の光の帯は攻撃経路の量を示しています。表紙の次の図は、両パターンの割合と量を色付けし具体化したものです。このアートの意味を理解していただければ幸いです。

目次

はじめに

ベライゾンの2024年度データ漏洩調査報告書（DBIR）へようこそ。本書は今年で17回目を迎え、旧来の読者の皆様をまたお迎えするとともに、新しい読者の方に歓迎のご挨拶をさせていただけることを大変嬉しく思います。いつものように、DBIRの目的は、さまざまなタイプの攻撃者と、攻撃者が利用する手口および攻撃するターゲットに光を当てることです。Verizon Threat Research Advisory Center （VTRAC）のチームと共に、私たちにデータやインサイトを共有し続けてくださる世界中の才能ある、寛大で市民意識の高い外部の協力組織の方々のおかげで、私たちは、世界中のあらゆる規模や種類の組織において繰り広げられるサイバー犯罪に関連したトレンドを調査および分析することができるのです。

毎年、私たちは、新しい巧妙な攻撃や、依然として成功が実証されている攻撃バリエーションを目の当たりにしています。MOVEitに影響を与えた脆弱性のような、有名で広範囲に及ぶゼロデイ脆弱性の悪用から、より平凡ではありますが、依然として信じられないほど効果的なランサムウェアやサービス拒否（DoS）攻撃まで、犯罪者は、犯罪は報われないという古い格言が間違っていることを証明するために全力を尽くし続けています。

このようなサイバー脅威の変遷に、私たちは混乱させられ、圧倒され続けています。上記のような攻撃の種類に加え、人的要素やセキュリティ保護が不十分なパスワードなどの要素が加わると事態はさらに混乱します。許されるなら、サイバーセキュリティの現状をサイバー世界のカラフルなマルディグラのパレードに例えてみましょう。沿道で嬉々として「ほら、信用してくれよ!」 と叫ぶ大群衆の攻撃者たちの前を、さまざまな形や大きさの企業の山車が通り過ぎていきます。もちろん、山車に乗った人たちがそのような掛け声に応えてしてしまうことはよくあることです。人間の本性とはそういうものです。そして、こうしたパレードの例に漏れず、通り過ぎた後に残るのは美しい光景とは限りません。昨年はサイバー犯罪にとって多忙を極めた年でした。私たちは、実際に30,458件のセキュリティインシデントを分析し、そのうち10,626件のデータ漏洩が確認され（過去最高！）、被害は94カ国に及びました。

本報告書の全般的な構成は従来と変わりませんが、古くからの読者であれば、いくつかの変更点にお気づきになるかもしれません。たとえば、「本書の凡例と定義」のセクションは、報告書の冒頭ではなく、付録Aに移動しています。しかし、DBIRを初めて読まれる方には、報告書の本文をお読みいただく前にこのセクションを一読されることをお勧めします。その方が、読み進めていくのに役立つはずです。

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組織の皆様に心より感謝申し上げます（皆様のご協力なしには本報告書を刊行することはできませんでした）。もちろん、読者の皆様にも同様に感謝申し上げます（皆様がいなくてはこのような報告書を作成する意味がありません）。どうぞ、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

Christopher Novak氏に対しその継続的なサポートと洞察力に、
VTRACのDave KennedyとErika Gifford、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。

ガイダンス

2024年度DBIRのインシデントデータセットについて

毎年、対象インシデントのDBIR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、本報告書に記載されているインシデントは、2022年11月1日から2023年10月31日の間に発生したものです。2023年の取扱件数が2024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、世界中の協力組織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。悲しいかな、ジョークは自ら書くものではありません。

引用する場合はデータの出所を明記してください

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 2024 Data Breach Investigations Report（ベライゾン2024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、ご不明な点がありましたら、ぜひお聞かせください。

メール（dbir@verizon.com）またはベライゾンのLinkedInまでご連絡いただくか、@VerizonBusinessに、#dbirを付けてポストしてください。データに関するご質問は、X（@VZDBIR）までお問い合わせください。

もしあなたの組織でインシデントやセキュリティ関連のデータを持っており、毎年発行されるベライゾンDBIRへのデータ提供組織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。

主な調査結果

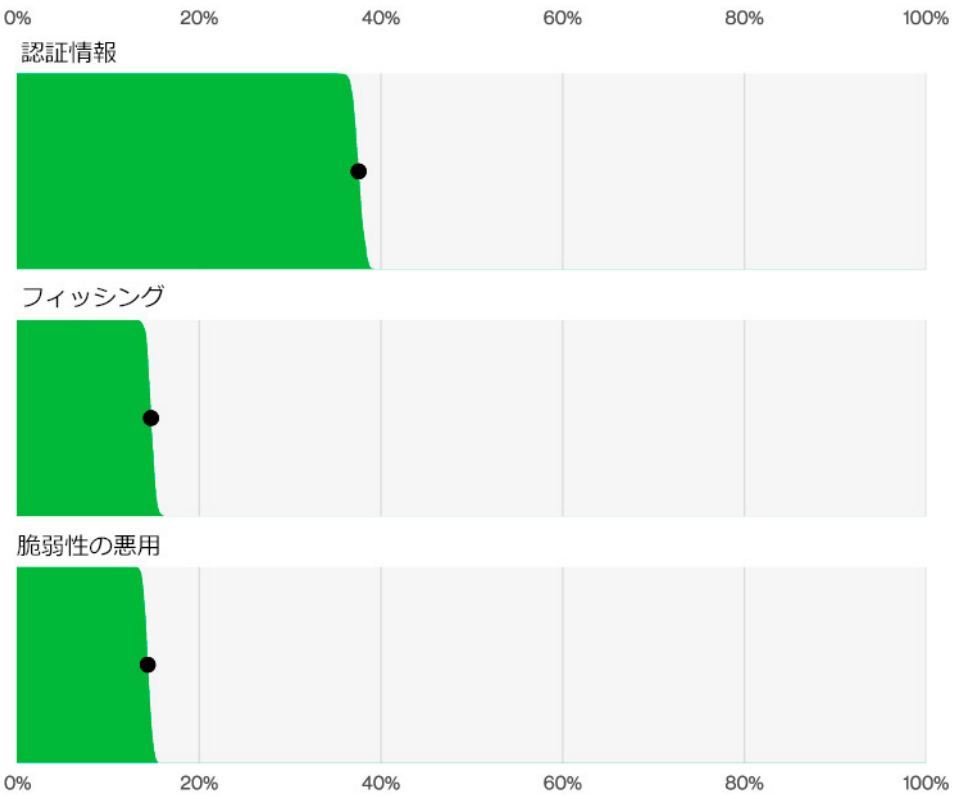


図1. 「エラー」/「（内部）悪用」を除いたデータ漏洩/侵害における上位の主な侵入手段（n=6,963）

侵入経路の分析では、データ漏洩/侵害を開始するためのクリティカルパスとして脆弱性を悪用する攻撃が、前年と比較して大幅に増加していることが確認されています。昨年のほぼ3倍（180%増）もの件数になっていますが、これはMOVEitや同様のゼロデイ脆弱性の影響を調査している人なら驚くことではありません。これらの攻撃は、主に「ランサムウェア」やその他の「脅迫」関連の攻撃者によって利用されました。ご想像のとおり、これらの最初の侵入経路となったのは主にWebアプリケーションでした。

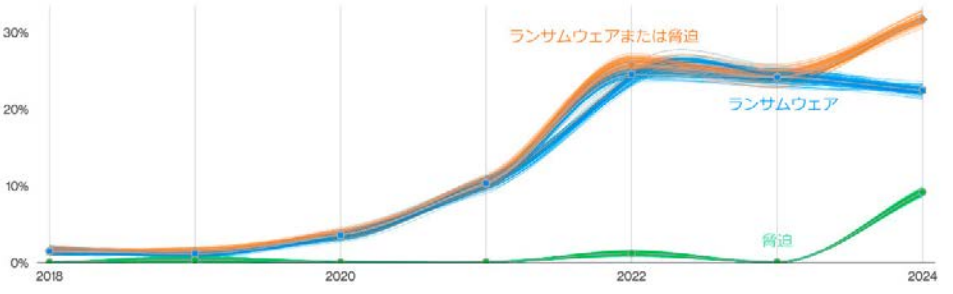


図2. 「ランサムウェア」と「脅迫」によるデータ漏洩/侵害の経時的変化

全侵害のおよそ3分の1が「ランサムウェア」またはその他の「脅迫」手口を使用しています。「脅迫」攻撃だけでもこの1年で増加し、現在では全データ漏洩/侵害の9%を占めています。従来のランサムウェアの攻撃者がこれらの新しい手口に移行した結果、「ランサムウェア」の割合は23%とやや減少しました。しかし、攻撃者が同じであるとしたら、この2つの脅威を合わせるとデータ漏洩/侵害における割合は大きくなり、32%に達します。「ランサムウェア」は全業種の92%に出現し、最大の脅威となっています。

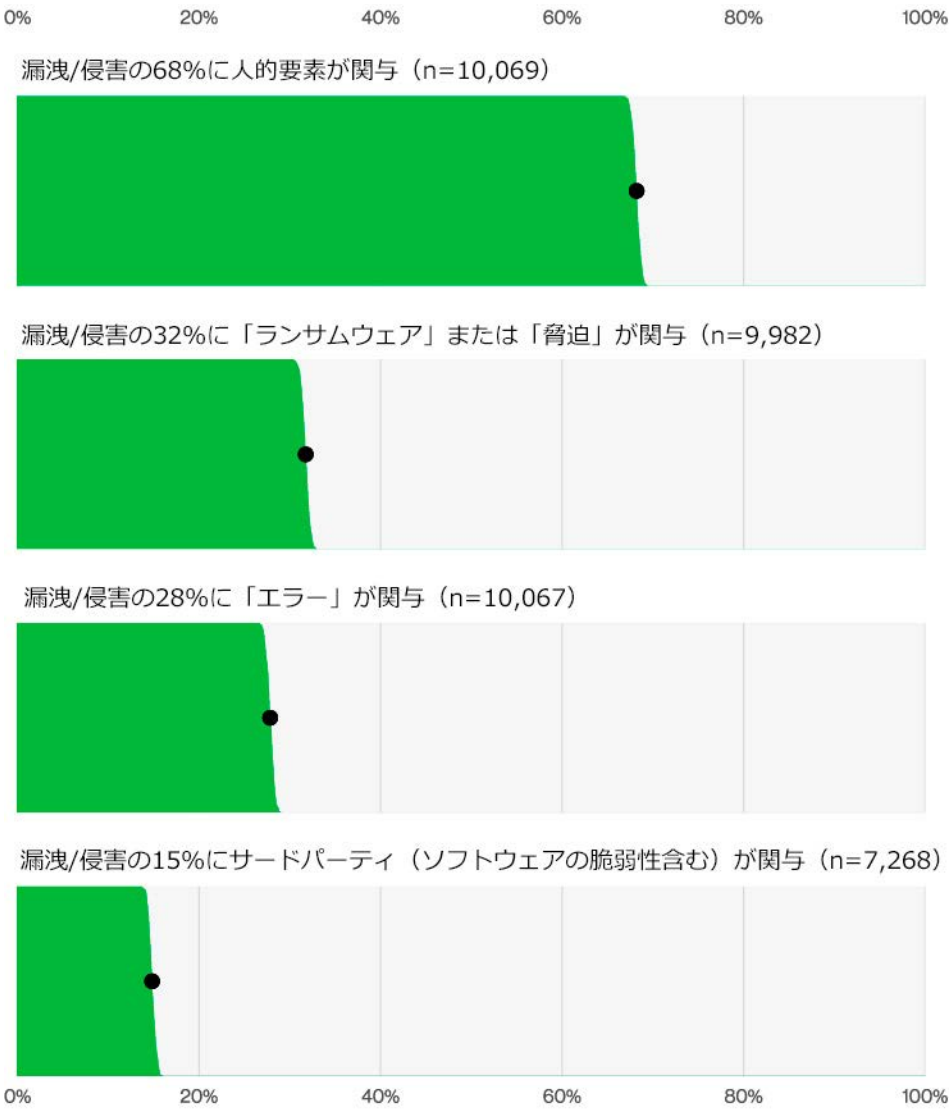


図3. データ漏洩/侵害における上位の主な要因

セキュリティ意識がもたらす影響を明らかにするために、悪意ある「特権の悪用」を除外して、人的要素の関与に関する計算を修正しました。今年のデータセットでは、人的要素がデータ漏洩/侵害の68%に関与しており、これは昨年の分析結果とほぼ同じです。

今年のDBIRでは、サードパーティが関与する侵害の概念を拡大し、パートナーのインフラが影響を受ける場合や、直接的または間接的なソフトウェアにおけるサプライチェーンの問題（サードパーティのソフトウェアの脆弱性によって影響を受ける場合を含む）なども視野に入れました。つまり、サードパーティが関与する侵害とは、組織がより優れたセキュリティ実績を持つベンダーを選択することで、軽減または防御できる可能性のある侵害と考えられます。この数字が今年は15%に達し、前年比68%増となったのは、「ランサムウェア」や「脅迫」攻撃でのゼロデイエクスプロイトの利用が主な原因です。

今年のデータセットでは、「エラー」が関与したデータ漏洩/侵害の件数が増加し、現在では28%に達していますが、これは、新たにデータ漏洩/侵害の通知が義務化された組織を含めることによりデータ提供組織の数が増加したためです。これは、メディアや従来のインシデント対応によるバイアスによって信じ込まされている現状認識以上に、エラーが蔓延しているのではないかという私たちの疑念を裏付けるものです。

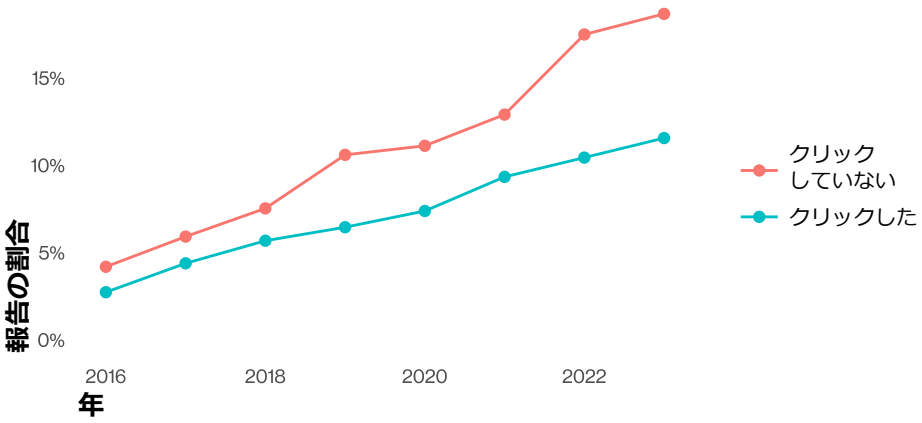


図4. クリック状況別フィッシングメールの報告の割合

フィッシングの報告は全体的にここ数年増加傾向にあります。2023年にパートナーから寄せられたセキュリティ意識向上に関するトレーニングデータでは、フィッシングシミュレーションにおいてユーザの20%がフィッシングを報告し、11%がメールをクリックしたことを報告していますが、一方、メールを開いてから悪意あるリンクをクリックするまでの時間の中央値は21秒で、その後データを入力するまでにさらに28秒しかかからないという事実があります。ここから、ユーザがフィッシングメールに引っかかるまでの時間の中央値は60秒未満という憂慮すべき事実が浮かび上がります。

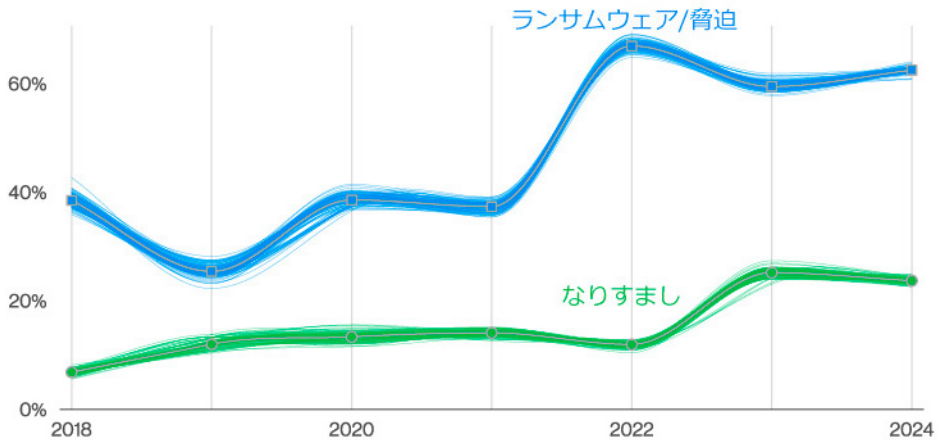


図5. 金銭目的を動機とする主な攻撃の種類の経時的変化

金銭目的を動機とする攻撃者は、通常、投資対効果（ROI）が最も高い攻撃手法に固執します。

過去3年間、「ランサムウェア」とその他の「脅迫」攻撃の組み合わせによるデータ漏洩/侵害は、これらの攻撃のほぼ3分の2（59%～66%の間で変動）を占めています。

FBIのインターネット犯罪苦情センター（IC3）のランサムウェア苦情データによると、これらの攻撃に関連する損失の中央値は46,000ドル（95%のケースで3ドル～1,141,467ドルの間）でした。また、身代金交渉のデータ提供組織からの報告からは、最初に要求された身代金と企業収益の比率の中央値は1.34%でしたが、80%のケースで0.13%～8.30%の幅があることがわかりました。

同様に、過去2年間で「なりすまし」（その大半は「ビジネスメール詐欺（BEC）」）が関与するインシデントが、金銭目的を動機とする攻撃の4分の1（24%～25%）を占めるようになりました。また、FBIのIC3のデータセットによると、BECによる被害金額の中央値は両年とも約5万ドルでした。

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、データ提供組織からの報告、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[1]。

データ提供組織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1つとしました。このような貢献組織の入れ替わりは、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。

本年は、新しいデータ提供組織が大勢加わり、一つの報告書内での分析対象件数が10,000件を超えるという大きな節目を迎えることができました[2]。データを整理し、分析することは途方もない作業ですが、このような結果を皆様に提示できることは、非常に喜ばしい限りです。

このセクションでは、より実践的なものになるよう、VERIS（Vocabulary for Event Recording and Incident Sharing）フレームワークが定義する4A（Actor、Action、Asset、Attribute：攻撃者、攻撃、資産、属性）の固定的な枠組みを超え、過去数年にわたり私たちが強調してきたいくつかの重要な調査結果にまで拡大して、調査結果の概要を説明したいと思います。

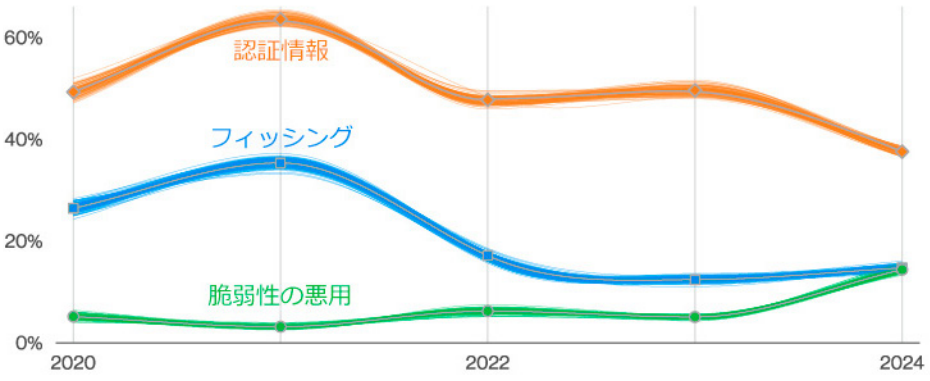


図6. 「エラー」/「（内部）悪用」を除いたデータ漏洩/侵害における上位の主な侵入経路の経時的変化

機密データの心臓部へ侵入する方法

私たちが作成した実用的な視点の1つに侵入経路分析があります。この分析では、データ漏洩/侵害の初期段階を理解することで、それらの攻撃を回避または防御する最善の方法を予測します。調査プロセスや情報開示のパターンがデータ提供組織によって大きく異なるため、データセット全体にはまだ多くの未知の攻撃や攻撃経路が分散していますが[3]、私たちが確実に知っていることに関するこの見解は、長年にわたって安定しており、代表的なものです。

図6は、今年最大の痛手となった問題を明確に示しています。システム侵入の初手となるクリティカルパスの攻撃として脆弱性の悪用が180%増加したことは、MOVEit 脆弱性や、「ランサムウェア」および「脅迫」関連の攻撃者によって悪用されたその他のゼロデイエクスプロイトを調査してきた人であれば、驚くことではありません。

これは、昨年のDBIRでLog4jの脆弱性の影響を分析したときに私たちが予想していた結果です。前回のDBIRの議論で予想された最悪のシナリオは、今年、このあまり知られていないが広く普及している製品で実現してしまいました。MOVEitと脆弱性の悪用の詳細については、「攻撃」と「システム侵入」のセクションで説明します。

1 VERIS Community Database（VCDB）を是非確認してみてください。（https://verisframework.org/vcdb.html）

2 昨年のDBIRで予測したように、累積100万インシデントの節目も通過しましたが、このことは報告書を一層大変なものにしないために脚注で触れているだけで、この不況下で100万件では引退するには不十分であることが非常に残念でした。

3 私たちは批判しているわけではなく、さまざまなタイプの協力組織が、その組織にとって最も関連性の高いことに集中することも当然のことです。

この「攻撃経路」という分析をさらに掘り下げるために、私たちはデータの新たな切り口を提示しています。それは、さまざまなタイプの攻撃とその最も人気のある攻撃経路を重ね合わせることで、攻撃への対応や対策に集中することを可能にします。図7でその結果をご確認ください。

「フィッシング」攻撃のほとんどがメールを媒介にしていることは自明ですが[4]、ここでは、「認証情報の悪用」と「脆弱性の悪用」がどちらも攻撃経路がWebアプリケーションに集中していることに注目したいと思います。「基本Webアプリケーション攻撃」のパターン（クラウドベースのメールやコラボレーションアカウントへの不正アクセス）では、「認証情報の悪用」の占める割合が大きいため、この図に「認証情報の悪用」が含まれていることは驚くことではありません。しかし、最近のバイアスが、脆弱性の悪用の蔓延を疑わせるかもしれません。本報告書は2024年初めに執筆されているため、仮想プライベートネットワーク（VPN）ソフトウェアにおけるゼロデイ（またはゼロデイに近い）脆弱性に焦点を当てています[5]。

当然ながら、2025年のDBIRでは、このような傾向を反映し、VPNを経路とする「脆弱性の悪用」の割合が増加する可能性が高いです。インターネット上の攻撃面を増やすものはすべて標的とされ、外部の脅威者にとって最初の足がかりとなる可能性があります。

今使っているVPNソフトウェアがどうであれ、できるだけ多くのWebアプリケーションをVPNでサポートする方が、夜間に緊急パッチを当てたり、Webアプリケーション自体を動かすその他の依存関係を心配したりするよりも、良い戦略かもしれません。ただし、これは完全にリスクを低減するものではなく、またすべての組織に合っているものでもないでしょう。しかし、最悪の場合、サイバーセキュリティ社会基盤安全保障庁（CISA：Cybersecurity Infrastructure and Security Agency）は、複数のツールをネットワークから切り離すのではなく、1つのツールだけをネットワークから切り離すよう求めるかもしれません。

図7. 「エラー」/「（内部）悪用」を除いたデータ漏洩/侵害おける上位の侵入方法と経路（n=2,770）

いずれにしても、この種の微妙に違う状況によって、デスクトップ共有ソフトウェアがインターネットに直接接続されていることに対するわたしたちの意見が変わることはありません。どうか、早く修正して欲しいところです。

所詮私たちは人間だから。

私たちが数年間調査してきたもう1つの複合的な指標は、データ漏洩/侵害における人的要素に関するものです。完全に自動化された攻撃がいかに組織の一日を台無しにするかに注目が集まっていますが[6]、企業内部の人間がセキュリティの強化にどれだけ貢献できるかは、驚くべきことです。

今年のDBIRでは、人的要素の評価指標に少し手を加え、その影響と対策の機会を明確にしました。DBIRの筆者たち（そして業界全体）がこの指標について議論するとき、その指標とともにセキュリティのトレーニングと意識向上に関する機会の不足の問題も取り上げられていました。完璧ではありませんが、潜在的なデータ漏洩/侵害の3分の2以上の結果を改善できる可能性のある明確な投資対象であれば、少なくとも腰を落ち着けて耳を傾けてくれるかもしれません。

人的要素の指標に含まれるものについての私たちの当初の方程式には、悪意ある内部関係者が関与するケースである「特権の悪用」が組み込まれていることが判明しました。このようなケースと従業員の単純なミスを混在させることは、セキュリティ意識向上トレーニングによってこのようなミスが軽減されることを示す目的からすると、意味のないことでした[7]。

4 そして、「*ishing」の造語マニアには信じがたい残念な結果です。

5 今時点までに、私たちが彼らをネットワークから完全に排除し、狼煙と伝書鳩の通信に戻ることに成功していなければの話ですが...。

6 DBIRチーム内でも、侵入経路としての脆弱性の悪用の増加が話題になっていたところでした。

7 悪意のある内部関係者のための「意識向上トレーニング」がどのようなものになるのか、考えるのも恐ろしいです。

図8は、読者の皆様の今後の参考となるよう、（悪意ある内部関係者を除いた）新たな人的要素の経時的変化を示したものです。2つ前の段落で予告したように、これはデータ漏洩/侵害の3分の2以上、正確には68%に達しています。これは昨年の調査結果の統計に類似しており、ある意味、「多種多様なエラー」（人間中心）とMOVEitの脆弱性（自動化型）の結果で全体的に増加したのは、この指標に関する限り同じような範囲であったことを意味します。

「（内部）悪用」を含めると、その割合は76%となり、統計的には前回の報告書の74%をわずかに上回る程度であったため、人的要素の"本来の姿"を好む方々にとってそれほど失うものはありませんでした。それでも、今後はより明確な定義が望ましいと考え、厄介な内部関係者とその悪事についての分析は「特権の悪用」パターンのセクションに譲ることにします。

相互接続のシステムにおける弱点

最後に、今年、脅威の状況がどのように変化したかという全体像を振り返りながら[8]、今後トラッキングしていく新たな指標を紹介したいと思います。脆弱性の悪用やソフトウェアサプライチェーンへの攻撃の増加により、セキュリティリスクの登録の議論において、これらの攻撃がより一般的になってきているため、私たちは、この条件をできるだけ広義に解釈する新しい第三者評価指標を提案したいと思います[9]。図9をご覧ください。

ここでは、サプライチェーンにおける相互接続が、今回確認されたデータ漏洩/侵害の15%に影響を及ぼしており、昨年の9%から大幅に増加しています。前年比68%増という実に堅調な伸びを示していますが、これはいったい何を意味しているのでしょうか？

発生したデータ漏洩/侵害をサプライチェーン相互接続の指標の一部にするには、ビジネスパートナーが侵害の侵入経路となったか（2013年の標的型攻撃において、今や伝説となった暖房/換気/空調設備（HVAC）会社の侵入経路のように）、あるいはデータ漏洩/侵害がサードパーティのデータ処理業者や管理人サイトで起こった場合（例えばMOVEitの事例で

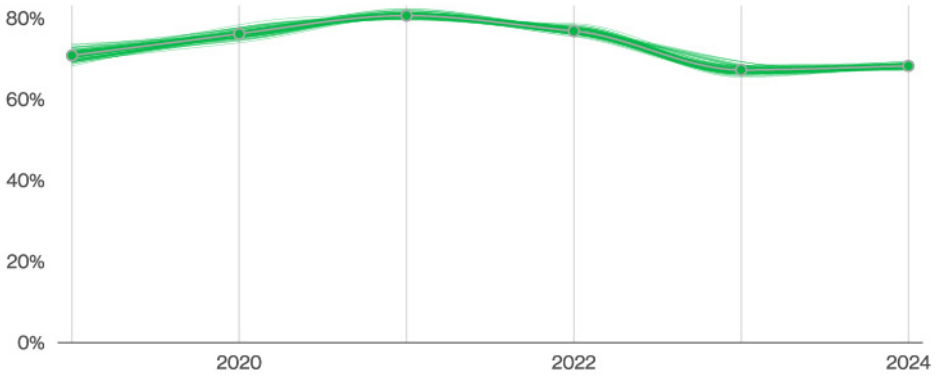


図8. データ漏洩/侵害の主な要因となる人的要素の経時的変化

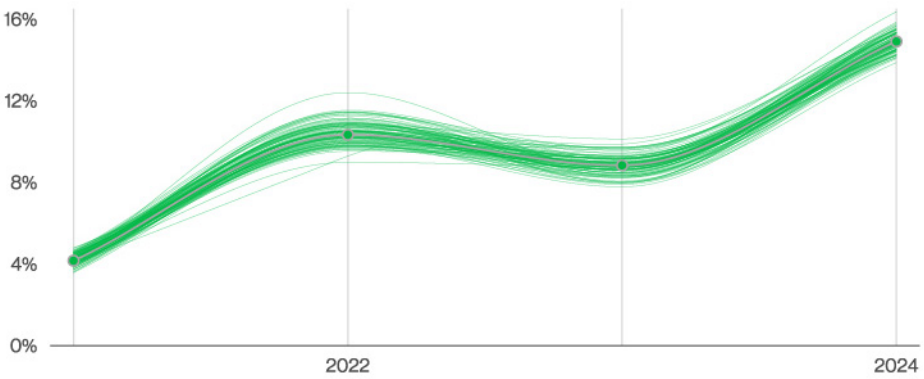


図9. データ漏洩/侵害におけるサプライチェーンの相互接続の経時的変化

8 本報告書で「MOVEit」という用語が言及された数：25件

9 意外な役割交替が起きたのは、私たちが定義づけにおいてしばしば頑ななため

はかなり多く発生）です。DBIRのデータセットではあまり見られませんが、パートナー企業の施設への物理的侵害や組織の施設への侵入を目的に乗っ取られたパートナー企業の車両なども含まれます[10]。

これまでのところ、これはごく標準的なサードパーティによるデータ漏洩/侵害の手段のように思えますが、SolarWinds や 3CXのように、ソフトウェア開発プロセスそのものが乗っ取られ、悪意あるソフトウェアアップデートが顧客に送信されることで、攻撃者による第2段階の攻撃で利用される可能性があるケースも追加されています。これらのデータ漏洩/侵害は、最終的にはソフトウェア開発パートナーにおける最初のインシデントが原因であるため、このタブに追加しています。

さて、議論の的になる部分ですが、「脆弱性の悪用」もこの指標にカウントしています。自分たちのソフトウェアの脆弱性が公開された場合、ソフトウェア開発者も被害者であると主張することは可能ですが（実際、被害者ですが）、この無限に続くと思われるタスクに対応する開発者に対するインセンティブが適切に設定されていない可能性があります。このような品質管理の失敗は、このソフトウェアを使用する顧客に偏った影響を与える可能性があります。私たちは、一握りのゼロデイや不適切に管理されたパッチ適用が、一般的な脅威の状況にどのような重大かつ広範な影響を及ぼしたかを明確に知ることができます。インストール済みソフトウェアの設定ミスを悪用するケースについては、安全でないデフォルトの結果である可能性があるものの、システム管理者は時にかなり独創的な行動を取ることがあるため、ここには追加しないことにしました。

図10は、サプライチェーンに関する指標においてVERISが定義する攻撃の内訳を示しており、予想通り、「ランサムウ ェア」と「脅迫」による攻撃を組織に忍び込ませる「脆弱性の悪用」がこの指標を牽引しています。

この指標は、結局のところ、コミュニティのレジリエンスの欠如と、組織がいかに互いに依存し合っているかという認識の欠如を表しています。組織がパートナー（またはソフトウェアプロバイダー）の選択に失敗するたびに、この指標は上昇します。組織は、相互接続したシステムの弱点による高い代償を払わないように、より良い選択をする方法を検討し始めることを推奨します。データ漏洩/侵害の報告が義務化されつつある今、私たちはようやく、パートナー候補のセキュリティの有効性を測るのに役立つツールと情報を手に入れることができるかもしれません。

私たちはこれを注視し、時間をかけてその定義を改善していくつもりです。皆様のフィードバックや別の角度からの提案を歓迎します。この問題を乗り越える唯一の方法は、犯罪を繰り返す者に責任を負わせ、私たちのビジネスにとって回復力のあるソフトウェアとサービスを高く評価する方法を見つけることだと信じています。

図10. 主な相互接続サプライチェーンでのデータ漏洩/侵害における攻撃の種類（n=1,075）

10 映画「ミッションインポッシブル」をDBIRの執筆シーズン中に見るのは止めるべきですね。

VERIS：攻撃者

今年はどうかこのセクションを読み飛ばないでください。私たちは、時代遅れのポップカルチャーを引用しながら、「あなたのお金を狙っているのはいつも外部の犯罪者だ」と毎年繰り返していることは承知していますが、今年はいくつかの興味深いデータがあります。それは、「外部」の犯罪者が最も多いわけではないということですか？いえ、もちろん彼らが最も多いです。でも、せっかくなので、どうかお読みください。

今年は、データ漏洩/侵害の情報収集プロセスが改善されたうえに[11]、データ漏洩/侵害の報告が義務付けられているデータ提供組織が新たに加わったこともあり、ついに「内部」攻撃者の行為が明らかになったのです。結局のところ、内部に優れた才能を持った人材がいれば、なぜ外部を頼る必要があるのか？ということです。

データ漏洩/侵害のきっかけとなった要因のトップは依然として「外部」の攻撃者が65%を占めていますが、「内部」はなんと35%を占め、昨年の20%から大幅に増加しています。図11に、ここ数年の変化を示します。

ただし、緊急会議を招集し、誰が犯人なのかを突き止めようと互いに指をさし合い始める前に、「内部」犯行による侵害の73%が「多種多様なエラー」に含まれていたことを認識することが重要です[12]。この「エラールネッサンス[13]」については、各パターンのセクションで詳しく説明しますが、大規模なデータ漏洩/侵害の報告を義務付けることで、これらのインシデントの一部がいかに平凡で予防可能なものであるかをよく理解できるようになるのではないかという、DBIRチームの長年の疑念を示すものです。

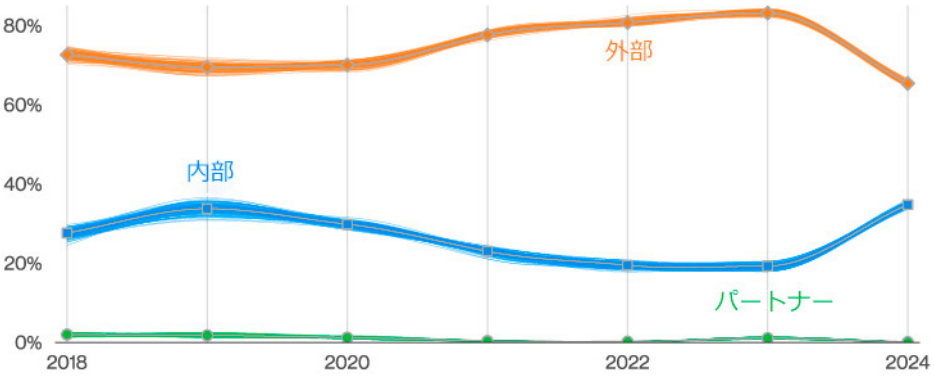


図11. データの漏洩/侵害における攻撃者の経時的変化

そして、情報漏洩について言えば、ランサムウェアの攻撃者が利用する数多くの「脅迫」攻撃は、被害者の内部に侵入し、顧客に侵害を報告させるため、私たちが毎年調査している外部攻撃者によるインシデント件数増加の原因となってきました。世界中で進む情報開示義務化の規制の動向は、誰もが因果関係をこれまでより、よく理解するのに役立つことでしょう[14]。

「攻撃者」セクションの画期的な変更に驚くことになりますが、その前に図12でお知らせするのは、攻撃者の動機ランキングに変化がないことです。「金銭目的」が断然リードを保っているものの、興味深いことに「スパイ活動」が昨年の5%から7%にわずかに増加しています。昨年の報告書と同じく、この動機はほとんど「公務」におけるデータ漏洩/侵害に集中しています。

図12. データ漏洩/侵害における攻撃者の動機（n=5,632）

11 データ漏洩/侵害の分析数を倍増させるのは容易ではありませんでした。それ以上の数を分析しなければならない2025年度版のDBIRの執筆者には、お気の毒としか言いようがありません。

12 不注意や細部への注意が欠けた場合が間違いでなければ。

13 Errorssance（「エラーサンス」エラー+ルネサンスの造語）？

14 これはまた、攻撃者がタレコミ役となって米国証券取引委員会（SEC）のような組織への重大なデータ漏洩/侵害を報告する新たな機会が生まれることになるでしょう。

DBIRが扱っている攻撃者のタイプを考えてみても、同じような結果が予想されます。図13は、私たちの分析が長年示してきたように、「組織犯罪」が「国家支援」よりも優位に立っていることを示しています。誤解しないでいただきたいのは、これは決して、これらの攻撃者の脅威を軽視すべきだという意味ではありません。「国家支援」は異常なほど戦略に優れ、戦術を適応させる能力があります。一般的な組織にとって幸運なことに、彼らは日常的な、通常の犯罪者が行なうほど頻繁には普通の企業を標的にすることはありません。

一方、「エンドユーザ」（VERISの用語では、組織の平均的な「従業員」や「請負業者」）の数は11%から26%へと2倍以上に増加しています。これらは主に「誤送信」が関わっており、上記で説明した「多種多様なエラー」が伸びた要因の1つでした。全体として、世間にいる些細なことまで見逃せない完璧主義者[15]にとっては腹立たしい1年でした。

図13. データ漏洩/侵害における攻撃者のタイプ（n=7,921）

攻撃者のタイプ[16]

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、外部の組織には信頼や特権は当てはまりません。。

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。パートナーが責任当事者とみなされるには、インシデントを起こす必要があります。

15 そういう人の下で働くのはどんな感じか想像してみてください。（編集者注：心外だ！）
16 https://verisframework.org/actors.html

「知能」ではなく「人工」が強調される汎用人工知能（AGI）の脅威状況

サイバーセキュリティコミュニティ内にいる声高な少数派からの圧力にもかかわらず[17]、DBIRチームが2024年にVERISの攻撃者一覧に「悪魔の汎用人工知能（Evil AGI）」[18]を追加することはなさそうです。しかし、これは依然として、世界中のテクノロジーおよびサイバーセキュリティの担当役員の頭を占めている非常にタイムリーなトピックです[19]。

私たちは、攻撃に生成人工知能（生成AI）という新たなテクノロジー分野が活用されている兆候や、それらのテクノロジーがもたらす潜在的な影響に注意を払いましたが、世界中から収集したインシデントデータには具体的な事象を見つけることはできませんでした[20]。

犯罪フォーラムのデータ提供協力者とともにテキスト分析を行った結果、（他のフォーラムと同様に）生成AIへの関心が高まっていることは明らかでしたが、「フィッシング」、「マルウェア」、「脆弱性」、「ランサムウェア」といった伝統的な攻撃の種類や攻撃経路とともに、「生成AI」という言葉が言及されることは驚くほど少なく、過去2年間の累積でかろうじて100を超える程度でした。言及された内容のほとんどは[21]、商業ベースの生成AI製品のアカウント販売や、強姦ポルノをAIで生成するツールに関するものでした。図14にその調査結果を示します。

一般的に理解されている生成AIテクノロジーの用途を広げていくと、高校1年生が学校で読書感想文を書いたり、AIソーシャルメディアの普通のインフルエンサーがナプキンに描いた絵をカメラで撮ってWebサイトを作成するふりをするのとほぼ同じように、フィッシングやマルウェアの開発、新しい脆弱性の発見に使われる可能性があります。

しかし、このようなテクノロジーの力を借りて本当に攻撃を成功させられるのでしょうか？ここ数年の「ソーシャルエンジニアリング」の攻撃パターン数の推移を見ると、「ビジネスメール詐欺（BEC）」のような攻撃が増えていることから、狙いを定めた「フィッシング」や「なりすまし」の攻撃を成功させるために、それほど高度な洗練性は必要はないと主張できます。同様に、特に「ランサムウェア」型のマルウェアも、その有効性が落ちてきているようには思えず、組織への最初の侵入のためのゼロデイ脆弱性が着実に攻撃者に供給されているように思われます。

私たちの見解では、攻撃者たちは、自分たちの課題に生成AIによる解決策を見つけようと実験しているかのように思えます。「コードの書き方を学ぶ」活動で、既知の国家支援型の攻撃者がこのようなテクノロジーを活用している証拠が公表されています[22]。しかし、本格的な普及が間近に迫っているようには見えず、攻撃側の最適化がインシデント対応側で登録される様子もなさそうです。ここでの唯一の例外は、明らかに進歩が見られるディープフェイクのようなテクノロジーに関係しており、報告されている詐欺や偽情報の逸話をすでにかなり生み出しています。

ちなみに、私たちは生成AIツールの1つに、この黎明期のテクノロジーがどのような脅威を増幅させる可能性があるのか質問を投げてみたところ、結局は上記と同じことが示唆されていました[23]。すなわち、ディープフェイクのようなテクノロジーはこれらのテーマにおいてすでに大きな影響力を持っており、「組織は生成AI主導の脅威の洗練度の深化に追いつくために、防衛戦略を適応させなければならない[24]」と思わせました。この小さなテストで、生成AIでさえ効果を狙った誇大表現で自身の経歴を盛る傾向があることを示しているかのようです。

「自然」対「人工」の対立軸のどこに居ようと、誇大宣伝から逃れることは本当に難しいのです。

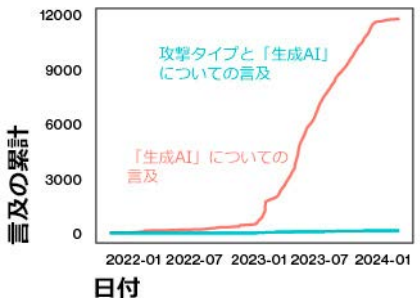


図14. 犯罪フォーラムにおける生成AIの言及の累積合計

17 「unhinged marketing hype（たがの外れたマーケティングの誇大宣伝）」を表す奇妙な綴り。

18 汎用人工知能。HAL9000、Skynet、Cylons、M3GANなど、映画でお馴染みの。

19 ブロックチェーンやメタバースといった、影響力の大きいテクノロジーと同じように。

20 しかし、もし私たちが邪悪なAIテクノロジーに乗っ取られていたら、そう言うでしょう。考えさせられますね。

21 このセクションの執筆中に、Kasperskyが同様の調査を発表しており、これは一見の価値があります。https://usa.kaspersky.com/about/press-releases/2024_new-kaspersky-study-examines-cybercrimes-ai-experimentation-on-the-dark-web

22 https://www.microsoft.com/en-us/security/blog/2024/02/14/staying-ahead-of-threat-actors-in-the-age-of-ai

23 そして、同じ質問を投げ、DBIR風の回答を指定したところ、サーカスや劇場のジョークやダジャレに病的に固執しているような答えが返ってきました。DBIRの文体はそのように受け取られているのでしょうか？

24 これで、次のサイバーセキュリティスタートアップのマーケティングコピーをどこで手に入れるか、よく分かりました。

VERIS：攻撃

かつて「人間とは物事を繰り返す存在である」と言った哲学者[25]がいましたが、このVERISの攻撃のいくつかが毎年上位に現れ続けているそのストイックさに感銘を受けるのではないでしょうか。公平に見て、これは古典的な哲学的原則というよりも、「うまくいっていることに余計なことはしない」という姿勢を実践しているように思えます。しかし、相変わらず、私たち、防衛策を実行する者にとってはやるべきことがたくさんあります。

図15は、データ漏洩/侵害における上位の攻撃の種類を示しています。「はじめに」のセクションで述べたように、今年の大きな変化は、データ漏洩/侵害の初期の攻撃で「盗まれた認証情報の悪用」の占める割合が減少したことです。統計的には、懐かしき2位の「ランサムウェア」の23%をかろうじて上回った24%となり、依然としてトップの座を占めています。

「ランサムウェア」は昨年よりも代表的な脅威ではなくなりましたが、金銭目的の動機に基づくデータ漏洩/侵害という一般的なスタイルが、上位の攻撃の9%を占めるようになった「脅迫」によって補完されつつあります。「ランサムウェア」とランサムウェア攻撃者による「脅迫」を同じデータ漏洩/侵害の攻撃手段の表裏としてカウントすると[26]、合計で32%に達します。

また、「脅迫」はデータ漏洩/侵害の10%を占める「脆弱性の悪用」とも密接に関係しており、この2つのペアの活躍により、「バックドア」や「C2」（コマンド＆コントロール）など、その他のマルウェアやハッキング関連の攻撃の種類とともに、MOVEit（およびその他の類似の脆弱性）の影響力が大きく目立つようになりました。「脅迫」は昨年の脆弱性の悪用の2倍になっており、「はじめに」のセクションで述べたように、明らかに私たちの侵入経路の分析結果に影響を及ぼしています。この驚くべき出来事についての詳細は、「システム侵入」のセクションをご覧ください。

もう1つ注目すべきことは、ソーシャル攻撃において「フィッシング」よりも「なりすまし」のほうが発生率が高くなっている点です。これまで「ビジネスメール詐欺（BEC）」攻撃台頭の経時的変化を追ってきた読者は、収益化の不安を解消しようとする攻撃者にとって、この攻撃が実行可能で規模の拡大/縮小が自在な方法であることはご存じでしょう[27]。

図15. データ漏洩/侵害において上位を占める攻撃の種類（n=9,982）

攻撃の種類[28]

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、またはカづくの故意の脅威。

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。

25 インターネット上の引用はどれも引用元が間違っているため、不特定な哲学者による引用としてしまいましょう。

26 本報告書でこのようにカウントするのは、たまにくどくどと攻撃者の手口や「戦略・技術・手順（TTP）」などを議論してくる人がいるからです。

27 残念ながら、誰もが四半期ごとにノルマを達成しなければならないのです。

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

図16. インシデントにおいて上位を占める攻撃の種類（n=28,625）

図16でインシデントの上位を占める攻撃の種類を見てみましょう。「サービス拒否（DoS）」攻撃がトップであり、確認されたインシデントの59%を占めていますが、長年の読者が驚くことのほどではありません。このトップの座は長年にわたって安定しており、すでに言い尽くされているため、この攻撃タイプについて私たちが言えることはほとんどありません[29]。

「ランサムウェア」についても、データ漏洩/侵害で見られたのと同じ現象が見られます。「ランサムウェア」は全体的に昨年より減少し、インシデントの12%となっていますが、「脅迫」と組み合わせると昨年の「Ramstortion（ランサムウェア＋脅迫）」の15%と同様の割合になります[30]。

図17は、データ漏洩/侵害における攻撃経路を示したもので、「はじめに」と「攻撃者」のセクションで述べたのと同じ結果を示しています。エラーによるデータ漏洩/侵害の増加により「不注意」が大幅に増加し、なりすましの増加により「メール」経由が増加しています。しかし、「Webアプリケーション」は健闘しており、冒頭で説明したように、盗まれた認証情報や脆弱性を悪用して防御壁を突破する手口と密接に関係しています。

図17. データ漏洩/侵害において上位を占める攻撃経路（n=7,248）

29 それでも「サービス拒否（DoS）」のセクションで試みていますが。

30 このペアの組み合わせに名前を付けるとしたら、何が最適でしょう？逆に「Extorware」（脅迫+ランサムウェア）でもいいかもしれませんね？

侵入経路といえば、攻撃の目標と結果を探るのも面白いかもしれません[31]。図18は、「金銭目的の動機」でランサムウェア/脅迫となりすましの攻撃が広く見られることを示しています。たびたび指摘しているように、この2つはデータ漏洩/侵害を収益化する最も成功する方法の1つです。「ランサムウェア」と「脅迫」のコンビは、しばらくの間、3分の2（62%）付近で推移している一方、「なりすまし」は過去2年間、目標を達成した攻撃のほぼ4分の1（24%）を占めています。

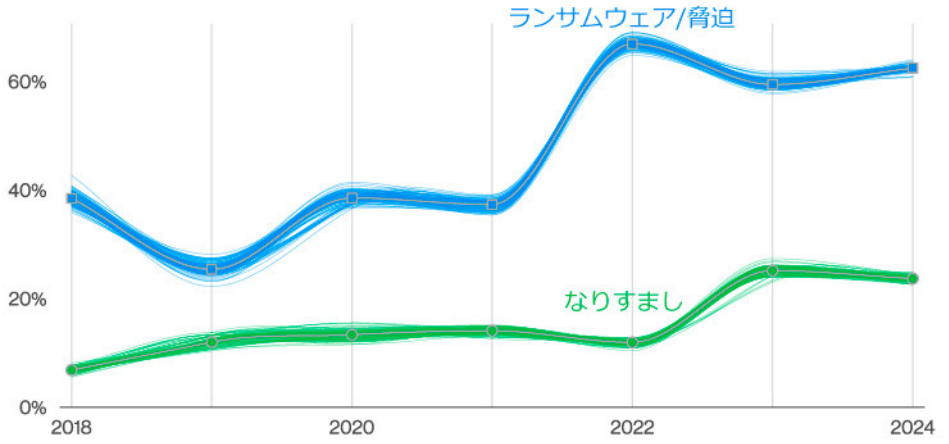


図18. 「金銭目的」の動機において上位を占める攻撃の種類の経時的変化

Jen Easterly氏のメッセージ

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）ディレクター

この1年間、CISAはセキュア・バイ・デザインによるソフトウェア開発革命をリードしてきました。私たちは、外国の諜報機関が何百もの重要なインフラシステムに侵入し、将来の紛争で利用される可能性のある足がかりを築いていることを警告する文書を発行しています。また、イノベーションを犠牲にすることなく、セキュリティを最優先する技術開発文化を確立するために、私たちが何を変えるべきかという青写真も公表してきました。これら2つの取り組みは、同じ問題に対する異なる角度からの必要なアプローチです。

今日、ソフトウェア業界は悪意ある攻撃者とその手口に焦点を当てています。コミュニティ内では、攻撃者の行動の特徴、稼いだ金額、悪用された脆弱性が話題になります。しかし、最後のポイントである悪用された脆弱性については、ほとんど触れられることがありません。ソフトウェアの脆弱性のほとんどは、未知のものでも、ユニークなものでも、目新しいものでもありません。そして、一連のよく知られた脆弱性に分類されてしまうのですが、残念なことに、私たちは何十年もの間、特定されてきたのと同じ種類の脆弱性を見続けています。

CISAの目標は、個々の脆弱性に焦点を当てることから脱却し、代わりに戦略的な観点で問題を検討することです。ソフトウェアの欠陥を何度も発生させる種類に焦点を当てることで、ソフトウェア開発者を鼓舞し、ツール、テクノロジー、プロセスを改善し、ソフトウェアの品質問題に根本から取り組むことができます。攻撃者の侵入手口について深く理解することが、今日から私たちのテクノロジーにおいてセキュア・バイ・デザインを求めるきっかけになることを願っています。

31 「侵入経路（ways-in）」に対して「逃走経路（ways-out）」という言葉遊びの表現は、ここでは意味がありません。逃走用のサイバー車両があれば別ですが。

脅威の中で急速に進む悪用

DBIRは「脆弱性の時代」を迎えています。今年私たちが得た最も重大な発見の1つは、「脆弱性の悪用」の種類の増加です。私たちは数年前から、「認証情報の悪用」は注目すべき大きな問題であり[32]、そして、最も鈍感な人間でも目の前に突きつけられれば、傾向は見抜けると強調してきました。

MOVEitの脆弱性が最初に登場したときに問題があることを私たちは理解し、（非常に漠然とした）データ漏洩/侵害の説明とその発生タイミングを組み合わせることで、MOVEitに関連する1,567件のデータ漏洩/侵害の報告を特定することができました。CISAの報告によると[33]、Cl0pランサムウェアの攻撃チームは、わずかなゼロデイ脆弱性を悪用することで、8,000を超えるグローバル企業のデータを侵害したとのことです[34]。DBIRのインシデントデータセットのサンプルが、攻撃者自身のリークサイトから抽出したデータ漏洩/侵害の報告またはランサムウェア被害者リストのいずれかのすべてではないとしても、この高い数字に言及することは重要です[35]。

ゼロデイ脆弱性とランサムウェアの攻撃者間のこのラブストーリーは、私たち全員を気になる場所に追いやります。脆弱性管理データの生存分析[36]を行い、CISA KEV（Known Exploited Vulnerabilities）カタログ[37]（実際に悪用された脆弱性と対策のデータベース）の脆弱性に焦点を当ててみると（脆弱性管理で優先的に焦点が当てられる領域であることは間違いない）、パッチの公開後にこれらの重大な脆弱性の50%を修復するのに約55日かかることがわかりました。図19が示すように、パッチの適用が開始されるのは公開後30日を過ぎてからであり、1年が経過しても約8%の脆弱性が未解決のままとなっています。

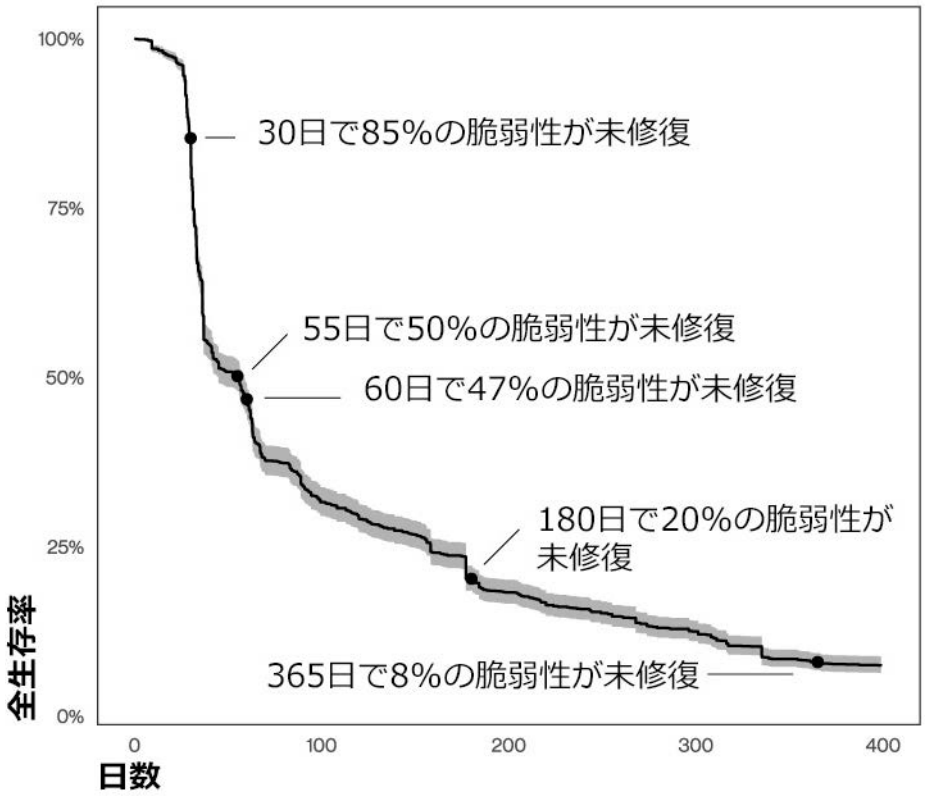


図19. CISA KEVの脆弱性生存分析

しかし、組織が「それはわが社だ。わが社が問題を起こした」と自らを指さし始める前に、優れたリスクベースの分析に従った後[38]、企業のパッチ管理サイクルは通常、実行可能な目標として30日～60日くらいの間に安定し、重大な脆弱性のパッチ適用については15日程度を目標とすることを思い出す必要があります。しかし悲しいことに、この速度では、攻撃者による脆弱性のスキャニングや悪用のスピードの速さに追いついていないように思われます。

32 DBIRは可視化を推進しました。スーパーボウルで青いジャージを着た人たちが「MFA（多要素認証）！MFA！MFA！」と唱えているところを思い描いてください。

33 https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-158a

34 「ドラゴンボール」ベジータのパワースカウターは健在。

35 コンサルタントが「これは場合による 」と言うように、データサイエンティストは「サンプリングバイアスだ」と言うでしょう。

36 方法論についてはCyentiaのJay Jacobs氏に脱帽。https://www.cyentia.com/why-your-mttr-is-probably-bogus

37 https://www.cisa.gov/known-exploited-vulnerabilities-catalog

38 https://www.cisa.gov/sites/default/files/publications/CISAInsights-Cyber-RemediateVulnerabilitiesforInternetAccessibleSystems_S508C.pdfのようなものです。

これだけではリスクを振り払うことはできません。昨年のDBIRで指摘したように、問題の多いLog4jの脆弱性は、そのスキャン活動のほぼ3分の1（32%）が公開から最初の30日間に起こっていました。この業界では、被害を最小限に抑えるため、影響を受けたシステムの被害低減とパッチ適用を非常に効率的に行いました、しかし、ゼロデイであろうとなかろうと、脆弱性が現れるたびに、業界全体がそのような大規模な対応をとることは現実的には期待できません。

実際、図20のインターネットのハニーポットで脆弱性が初めてスキャンされた時期の分布を見ると、CISA KEVに登録されているCVE（共通脆弱性識別子）の場合、その中央値は5日となっています。一方、CISA KEV以外の脆弱性の中央値は68日です。脆弱性がKEVに追加されるのは悪用が横行し始めてからになるため、ここには明らかに「真のスコットランド人論法」（純粋さに訴える論証）による誤った推論が生じます。何に最初にパッチを当てるべきかを導く上で、後知恵の指標としてこれほど有力な指標はほとんどありません[39]。つまり、KEVに入ったら早急に修復せよということです。

この生存分析のチャートは時間が経てば生存率が低くなっているように見えますが、これは楽観主義者の見方です。この統計の対象組織は少なくとも脆弱性管理ベンダーを雇うだけのリソースがある企業であることを忘れてはなりません。それは、彼らがリスクを警戒し、その対策に取り組んでいることを物語っています。しかし、全体的な現実はさらに悪く、ゼロデイや最近の脆弱性を利用するランサムウェア攻撃者が増えてくれば、彼らのリークサイトのリストの空欄に間違いなくあなたの組織名が載ることになるでしょう。

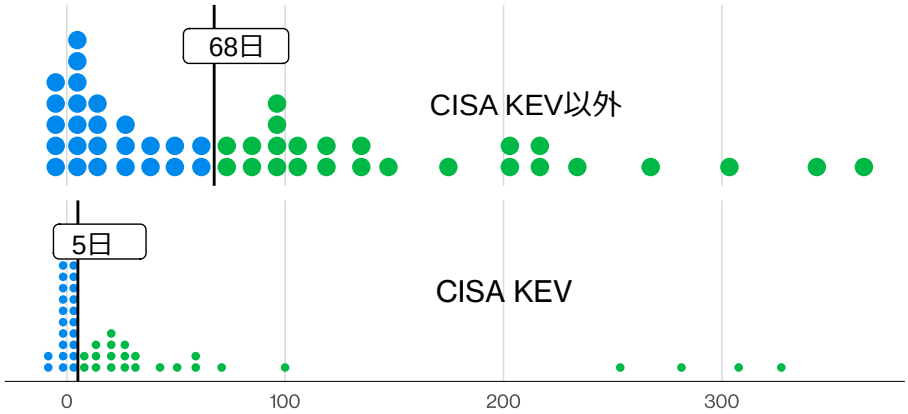


図20. 脆弱性の公表から最初のスキャンが確認されるまでの時間（2020年以降）

脆弱性にパッチをすばやく当てることができないのであれば、論理的な結論として、パッチを当てるべき脆弱性の数を減らすしかないように思われます。このようなことは夢物語であると承知のうえで、少なくとも、企業は、採用したソフトウェアベンダーに自社製品のセキュリティの結果について責任を負わせるべきです（たとえそれらのソフトウェアベンダーに規制当局から改善を求める圧力がないとしても）。DBIRは今後、この点を強調するために第三者によるデータ漏洩/侵害への関与の指標を拡大し、脆弱性の悪用も考慮に入れる予定です[40]。これは、ベンダーを選択する際に、セキュア・バイ・デザインで開発されたソフトウェアが違いを生むことを説明するのに役立ちます。

ソフトウェア開発とソフトウェア調達の双方に携わる方々には、CISAと米国内外の17のパートナーによる「セキュア・バイ・デザイン」レポートの最新版[41]をじっくり検討されることをお勧めします。このレポートでは、優れたセキュリティパフォーマンスを発揮できるソフトウェアを開発できるか、また、バイヤーとしてどの点に注目すべきかが示されています。DBIRは、製品の安全性維持の目標に達していない可能性のあるソフトウェアプロバイダーと疎遠になるつもりはありませんが、増大する脅威に対してこの素晴らしい解決策を優先させると発表する明確なタイミングがあったとすれば、それは今しかありません。私たちは、行動しないことの代償をわかり過ぎるほどによくわかっています。

39 CVSS（共通脆弱性評価システム）は試さないほうが良いかもしれません。
40 「結果と分析」セクションの「概要」のサブセクションを参照してください。
41 https://www.cisa.gov/resources-tools/resources/secure-by-design

VERIS：資産

VERISにおける「資産」の被害状況を分析することで、私たちがずっと言い続けている攻撃がどこに集中しているのかを理解することができます。そして、誰もがこれらの資産を守るための優先順位を決めるのに助けを必要としていることは確かです。この結果は、前述の「VERIS：攻撃」と相関関係があるため、驚くようなものではないかもしれませんが、脅威の状況における経時的変化の傾向を理解することには価値があります。

DBIRでの資産の上位ランキング[42]は、昨年から大きな変化はないものの、図21で指摘するべき変化がいくつか見られます。昨年のDBIRからの順位は変わらず、「サーバー」に集中する攻撃もほぼ同じであるにもかかわらず、「人[43]」と「メディア」の両方の資産の被害が大幅に増加していることがわかります。

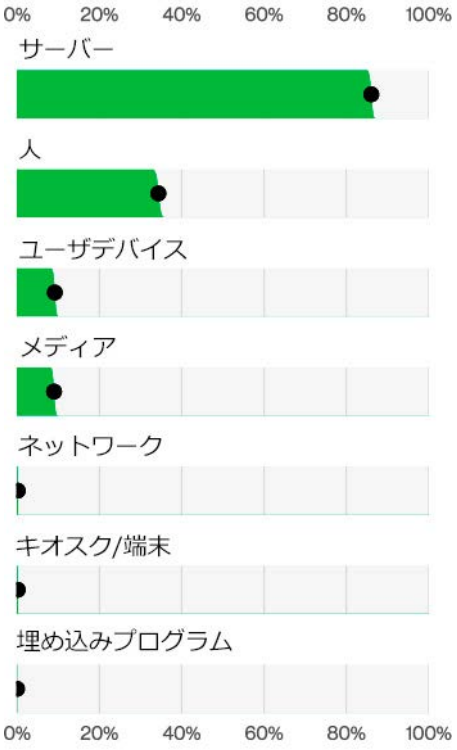


図21. データ漏洩/侵害にあった「資産」（n=8,910）

今年のDBIRで、資産としての「人」の関与が増えたのは、データセット内で純粋な「脅迫」攻撃によるデータ漏洩/侵害が増加したためです。ソーシャル攻撃としての「脅迫」は、直接の被害者として「人」を標的とするため、データセットの「妖精ノーム[44]」たちは躊躇なく従ったということです。ここで興味深いのは、純粋な「脅迫」のスピンオフ元である「ランサムウェア」攻撃に「人的資産」とは関係なく金銭を要求する脅迫の段階があったのを示唆していることです[45]。

したがって、「人」のこのような増加は、こうしたデータ漏洩/侵害の仕組みの本質を表すものとしても納得がいく現象と言えます。従業員は、身代金の要求や脅迫があった場合にどのように対処すべきかを認識し、そのような要求に対処するには、組織で確立された手順に従う必要があります。ちなみに、万が一に備え、文書化[46]した手順を必ず用意しておきましょう。

42 トップ争いで勝つのはメールサーバーか、それとも準備時間のかかるファイルサーバーでしょうか？

43 セラピーを受けるのを忌避して自分のセキュリティ属性を損なう人もいるので、おそらく成熟期ではないでしょう。

44 DBIR執筆者たちのピックルボールチームの名前

45 これは一般の読者にとっては、VERISスタンダードの内部事情として詳しすぎるかもしれないですが、私たちはこんなことですぐに面白がってしまうのです。

46 ファイルサーバーに置いておくだけでいいですよね？（それはどうでしょう）

「メディア」資産の増加は、前述の「多種多様なエラー」の動きと本質的に連動するものです。これらの「誤送信」エラーの中には、紙の文書やファックス[47]を介して発生するものもあり、これはその範囲を限定するものではありますが、規制当局にとってデータ漏洩/侵害としての違いは全くありません。

図22をさらに掘り下げると、「サーバー」資産の内訳がはっきり見えてきます。「Webアプリケーションサーバー」と「メールサーバー」は、そのほとんどが認証情報の盗難によるデータ漏洩/侵害に関係していますが、「ファイルサーバー」は、MOVEitによるデータ漏洩/侵害でほぼ独占されており、データ漏洩/侵害の被害にあった資産の95%以上がサーバーとなっている理由が分かります。

全体として、VERISにおける「資産」においてははごく普通の年でした。これらの資産を安全に保つ方法については、「システム侵入」、「ソーシャルエンジニアリング」、「基本Webアプリケーション攻撃」の各セクションで詳しく説明します。

資産のカテゴリー[48]

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とすれば、それは一部の「サーバー」について「可用性」に影響が出ていることを意味します。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。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。

図22. インシデントにおいて上位を占める「資産」の種類（n=6,606）

47 信じられないかもしれませんが、これは1994年のDBIRではありません。

48 https://verisframework.org/assets.html

VERIS：属性

幼い子供や孫によく言い聞かせる必要があるように、行動には結果が伴うものです[49]。インシデントやデータ漏洩/侵害も同様であり[50]、その結果はデータ漏洩（機密性の問題）、資産の不正変更（完全性の問題）、データへのアクセス喪失（可用性の問題）として現れることが多いのです。

多段階攻撃の過程で、これらすべてで打撃を受けることも少なくありません。図23は、「DBIRのグラフはそれぞれのイベントが独立して成り立っているわけではないので、合計が100%にならない」傾向がこれまでで最も強いグラフの１つで、これら3つの属性が2年間でどのくらい侵害を受けているかを示しています。

今年のDBIRで確認されたインシデントのおよそ3分の1は、データの機密性が侵害されたデータ漏洩/侵害でした。図24は、今年のデータ漏洩/侵害で侵害されたデータの種類の内訳を示したもので、意外にも「個人情報」が上位を占めています。

このように「個人情報」が上位を占め続けているのも、ある意味、当然と言えば当然と言えます。というのも、頻繁に公表されるデータ漏洩/侵害は、被害者への通知が規制で義務付けられている顧客データに関わるものだからです。さらに、顧客データは広く利用され、必要性もなく、適切な管理もされずに蓄積されているため、特にそれ自体を標的にしていないあらゆる種類の攻撃の巻き添えを食うことが多いのです。

社外秘の企業データ（メールやビジネス文書など）やシステム固有のデータが標的にされるのも、その背後にある「決済情報」、「銀行情報」、「医療情報」、「機密情報」などに狙いを定めてのことです。私たちは、「ランサムウェア」（そして今は「脅迫」そのものも含む）によるデータ漏洩/侵害では、どのようなデータを盗んでいるのか攻撃者は関知する必要がないということを何度も説明してきました。その理由は、被害者である組織を常に主な買い手としているからです。ランサムウェア、身代金の金額、脅迫の経済性については、本報告書後半にある「システム侵入」のセクションで詳しく説明します。

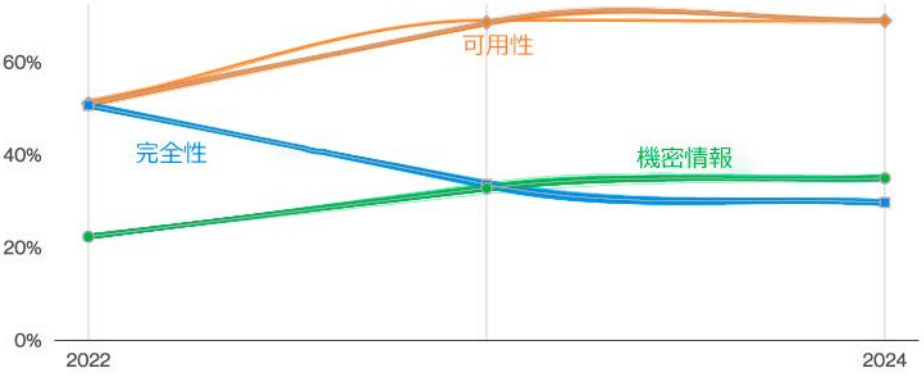


図23. インシデントにおける属性の経時的な変化

図24. データ漏洩/侵害において上位を占める機密データの種類

49 特に悪い行いをした場合。親切な行為はなぜか気づかれないことが多いです。
50 悪さした攻撃者もテレビのない寝室に閉じ込めて、おしおきするべきですね。

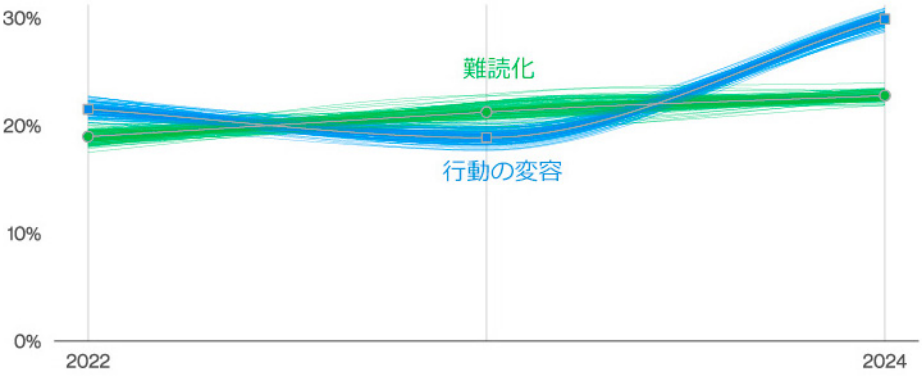


図25. データ漏洩/侵害において上位を占める属性の経時的変化

さらに、割合的には「認証情報」のデータタイプが減少しているのが見られます。これは、クレデンシャルスタッフィングやブルートフォース攻撃で脆弱な認証情報を悪用する外部の攻撃者の減少とは逆に、「エラー」攻撃によるデータ漏洩/侵害の割合が増加しているためです（これもサンプルの結果から）。

最後の興味深い点として、暗号化に拠らない脅迫攻撃の増加のもう1つの副作用として、完全性における「行動の変容」が大幅に増加しています。これは「人」が外部の攻撃者の影響を受けたときに起こる完全性の侵害であり、「フィッシング」や「なりすまし」のソーシャル攻撃の一般的な結果でもあります。

図25で、このように急激に「難読化」（「ランサムウェア」攻撃の通常の結果）を追い越していると見るのは、来るべき事態の前兆かもしれません。その結果、長期的には「システム侵入」の攻撃パターンがより広まることになります。

属性のカテゴリー[51]

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。データが危険にさらされた、危険さらされている、またはその可能性があるということではありません（これらは「所有および管理」の属性に該当）。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、情報の不正挿入、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。

Stephen Bonner氏のメッセージ

英国情報コミッショナーオフィス（ICO）副コミッショナー（規制監督担当）

人々が社会に参加するには、自分の個人情報の安全性が保証される必要があります。そうすることで、サービスを利用したり製品を使用したりする際に安心して自分の個人情報を提供することができます。

本報告書に私たちが提供したセキュリティインシデントのトレンドデータは、サイバー脅威が存在し続けているだけでなく、年々増加していることを示しています。セキュリティに唯一の解決策はないことを忘れてはなりませんが、私たちのガイダンスやツールを利用することで、組織はサイバーセキュリティを強化し、人々の個人情報を安全に保護することができます。

また、サイバーインシデントが発生した際の被害を開示し、早期の支援を求め、情報を共有することで、サイバー脅威の状況を誰もが改善できるようにすることを組織に奨励しています。ICOは、組織がサイバーレジリエンスを継続的に改善できるよう、過去のセキュリティインシデントの評価結果を近く公表する予定です。

51 https://verisframework.org/attributes.html
52 https://en.wikipedia.org/wiki/Parkerian_Hexad

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

パレイドリアとは、自然の中に見つけたパターンから、うさぎのように見える雲や、朝食の皿に乗るトーストの中に見えるこちらを見つめる顔などを連想する知覚現象を指します。本報告書で以前にも述べたように、人の心は、実際にはそこにパターンがなくても、パターンを探してしまうものなのです[53]。人は周囲の世界を理解するためにパターンを必要としますが、サイバーセキュリティの領域も同じです。数年前、私たちは、特定の類似した特徴を持つクラスター内に、あるインシデントが何度も繰り返し発生することに気付きました。このことに気付いてから、私たちはインシデントパターンを考案し、ここ数年間このDBIRで取り上げてきました。

これらのインシデントパターンで、似たようなインシデントを分類することで、パターンを理解しやすく、すぐ思い出せるようにしています。これらはVERISの4つのA（Actor、Action、Asset、Attribute）のカテゴリーに基づいています。その詳細については、本報告書の前のほうにある「結果と分析」のセクションをお読みください[54]。表1にインシデントの分類パターン（8種類）の定義を示し、以下の図26にインシデントにおけるパターンの経時的変化を示します。

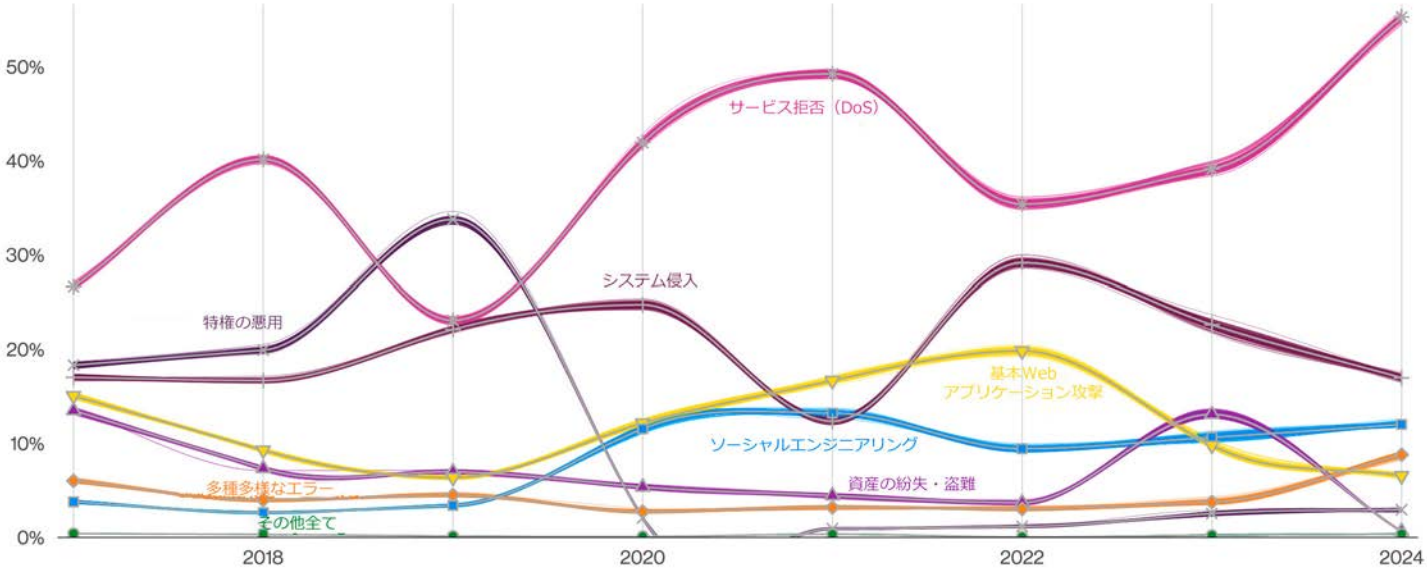


図26. インシデントにおけるパターンの経時的変化

53 トーストの顔は本当だと思いますが…。

54 きちんと読まれましたよね？ざっと流し読みされただけではありませんよね？

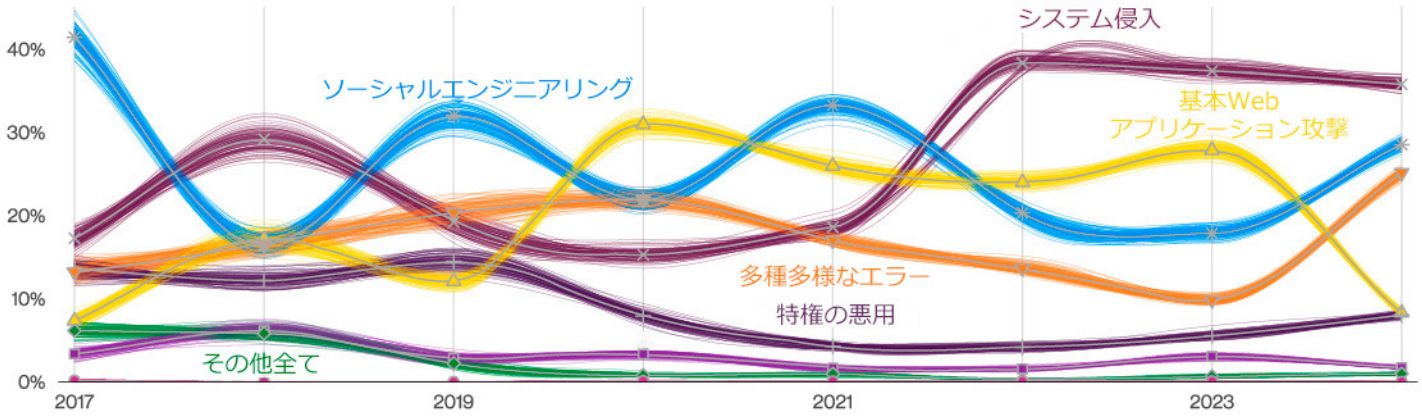


図27. データ漏洩/侵害におけるパターンの経時的変化

今回も、関連するATT&CKテクニック[55]と特定のパターンに関連するCenter for Internet Security（CIS）Critical Security Controls[56]を採用しています。

図27は、過去数年間におけるさまざまなパターンの増減を示しています。おわかりのように、データ漏洩/侵害においては「システム侵入」の攻撃パターンが引き続きトップの座を占めています（「DoS攻撃」が依然としてトップのインシデントとは対照的です）。「ソーシャルエンジニアリング」と「多種多様なエラー」の両パターンについては、特に後者が昨年から大幅に増加しています。逆に、「基本Webアプリケーション攻撃」のパターンは、昨年の順位から劇的に下落しています。これらの変動の理由については、このセクションでさらに詳しく解説していきます。

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。
その他全て	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

55 https://attack.mitre.org
56 https://www.cisecurity.org/controls

システム侵入

サマリー

攻撃者が活用する戦術がシフトしたことにより、上位の攻撃のいくつかが変更されましたが、これらの攻撃者の全体的な影響はあらゆる規模の業種と組織の大部分で引き続き感じられます。

昨年との比較

「ランサムウェア」による攻撃は、全データ漏洩/侵害の23%を占めるようになり、このパターンの拡大を牽引し続けています。

頻度	インシデント5,175件、確認されたデータの漏洩3,803件
攻撃者	外部（100%）（漏洩/侵害）
攻撃者の動機	金銭目的（95%）、スパイ活動（5%）（漏洩/侵害）
侵害されたデータ	個人情報（50%）、その他（34%）、システム情報（26%）、内部情報（22%）（漏洩/侵害）

侵入の手口

攻撃パターンの世界では、今年は競争が激しかった年で、大勢の候補者がMFB（Most Frequent Breach：最も頻繁に発生した漏洩/侵害）の第1位を争いました（もちろんMVPほど栄誉ある賞ではありませんが、とりあえず今あるもので何とか対応します）。「システム侵入」は、3年連続でデータ漏洩/侵害の36%を占め、群を抜いています。攻撃者が何を勝ち取っているか正確にはわかりませんが（かなりの額の賞金だと推測します）、負けたのは誰かと言えば、私たち全員であることは確かです。このパターンの継続的な成功の原動力は何なのかを考察してみましょう。

関連するATT&CKテクニック

脆弱性の悪用（VERIS）

- 一般用アプリケーションの悪用：T1190
- 認証情報アクセスのための不正：T1212
- 防御回避のための不正使用：T1211
- 権限昇格の悪用：T1068
- 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

このパターンを構成する攻撃に大きな変化はありませんが、巧妙さを増した攻撃[57]が見られます。これらの攻撃の大部分は、「ハッキング」の手口と「マルウェア」を組み合わせて被害者の組織に侵入するデータ漏洩/侵害やインシデントであることに変わりはありません（無許可の侵入テストからと想定できるものが多少はあるとしても）。ただし、攻撃者は通常、テストの終了時に有用な報告書を提出するのではなく、「ランサムウェア」を実行し、有用とはかけ離れた脅迫メモを被害者に残します。図28に見られるように、このような「ランサムウェア」攻撃は、「システム侵入」のインシデントの70%を占めています。「システム侵入」パターンのその他の攻撃としては、「脆弱性の悪用」や「バックドア」など、標的の環境へのアクセスを可能にする攻撃がよく見られました。また、この領域でも「脅迫」が見られますが、主に大規模でインパクトのあるイベント（本報告書の後のほうで触れるので、頭に入れておいてください[58]）によるものです。

図28. 「システム侵入」インシデントにおいて上位を占める攻撃の種類

ランサムウェアの侵入経路

攻撃経路（図29）に関しては、「直接インストール」が非常に多く見られました。これは、攻撃者が既に獲得しているシステムへのアクセス権を利用して、「ランサムウェア」や「バックドア」などのマルウェアをインストールするケースです。また、「結果と分析」セクションの侵入経路の分析で取り上げたように、悪用のターゲットとして好まれている「Webアプリケーション」の攻撃経路も頻繁に出現しています。もちろん、「メール」を利用してユーザを攻撃したり、「デスクトップ共有ソフトウェア」を利用してシステムに侵入したりする攻撃者も依然として確認されます。このような攻撃者は多数のツールや手口を使用しているため、このデータはより詳細なものとなっており、そのため比較的多く「その他」がトップ5以内にランクインしています。「その他」のカテゴリーには、VPN、ソフトウェアアップデート、および不明なものが含まれます（明確に報告されていないだけで、上記で説明した手口の間で分けられている可能性が高いというのがDBIRチームの見解です）。したがって、組織の防御の取り組みを優先する際には、「ランサムウェア」に感染する恐れがあるので、マルウェア感染、盗まれた認証情報、パッチが未適用のシステムへの対処を怠らないようにしましょう[59]。

ランサムウェアの標的

まるで山上への岩運びを永遠に繰り返すシジフォス（ギリシャ神話に出てくる人物）のように、終わりのない作業に追われるIT部門の働き者は、進化する「ランサムウェア」の脅威と戦い続けなければならないかのようです。「ランサムウェア」は全インシデントの11%を占め、2番目に多いインシデントのタイプです。「ランサムウェア」（または何らかのタイプの「脅迫」）は、92%の業種で上位を占める脅威の1つになっています。

図29. 「システム侵入」インシデントにおいて上位を占める攻撃経路（n=1,789）

このデータセットから「ランサムウェア」のグループを除外すると[60]、ありふれたタイプの犯罪者が44%、「国家支援型」攻撃者が40%というかなり均等な割合になります。犯罪者が使用する手口は、国のために働く攻撃者が使用する手口と非常に似通っていることが明らかですが、それほど驚くことではありません。

「ランサムウェア」（または何らかの「脅迫」）は、92%の業種で上位を占める脅威の1つになっています。

57 これらの攻撃が人間だとしたら、彼らはレストランで高級ワインを飲み、ヴィンテージについて大声で講釈を垂れ、北欧製の高級車を乗り回している輩でしょう。

58 そして「いいね！」と「購読」ボタンを押していただけるとありがたいです。あ、プラットフォームが違いましたね。

59 当然、皮膚科に行っても治りません。

60 そんなことができたら素晴らしい！考えただけで、気分が良くなります。

その進入経路を使って何をするかという点で、両者に明らかに大きな違いがあります。このパターンの犯罪者でも「ランサムウェア」や「脅迫」を行わないグループは、eコマースサイトから「決済情報」を密かに吸い上げており、盗まれた「ペイメントカード」を含めデータ漏洩/侵害の57%を占めています。一方、「国家支援型」攻撃者は他の種類のデータ[61]を盗むことに注力しています。

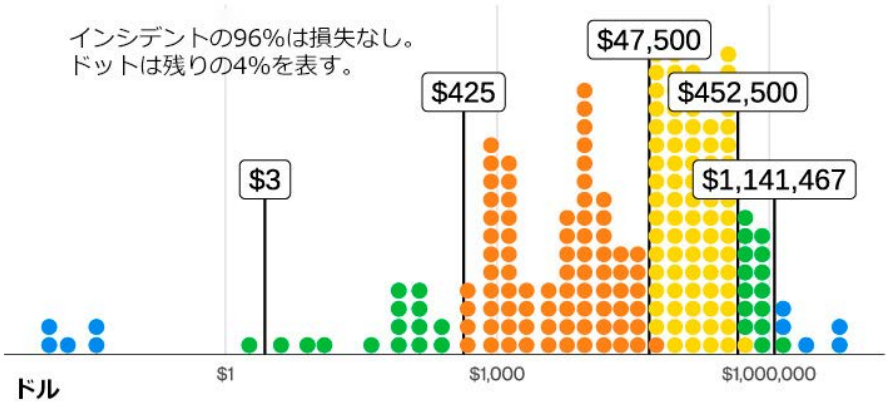


図30. 調整後の「ランサムウェア」インシデントコストの95%および80%信頼区間

ランサムウェアによる被害

「ランサムウェア」に関連するコストを理解することは、風評被害に関連するソフトコストはもちろんのこと、考慮すべき一次コストと二次コストがいくつかあるため、少し複雑です。私たちはこれらのコストを把握するために最善を尽くしていますが、その結果は全体像ではなく、あくまでも私たちの手持ちのデータを使った最善の概算であることをご理解ください。

捕捉しやすいコストの1つは、実際の身代金の支払いに関連する金額です。今年のFBI IC3[62]データセットを分析したところ、図30に示すように、身代金の支払い後の調整損失額（法執行機関が資金回収に努めた後）の中央値は約46,000ドルであることがわかりました。これは前年の中央値26,000ドルから大幅に増加していますが、実際に損失のあった被害申告は、昨年の7%に対して今年はわずか2%であったことも考慮すべきです。

データをスライスするもう1つの方法として、身代金要求額を総収入に対する割合で比較する方法があります[63]。最初の身代金要求額の中央値は、被害組織の総収入の1.34%で、要求額の50%は0.13%～8.30%の範囲でした（図31）。最初の身代金要求額の割合としては、かなり幅があることがわかります。上位10%の中には、総収入の24%に達するケースもいくつかありました。これらの範囲が、ランサムウェア攻撃に関連する潜在的な直接コストを見据えたリスクシナリオを実行する際の一助となれば幸いです。もちろん、他にも考慮すべき要素はたくさんありますが、これは良い出発点と言えるでしょう。

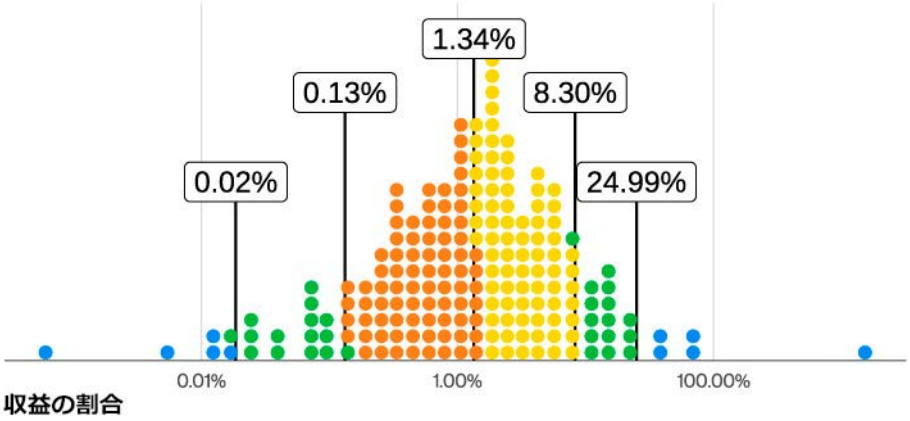


図31. 被害組織の収入に占める身代金の割合の95%および80%信頼区間

61 極秘情報のため、詳細は言えませんが。

62 https://www.ic3.gov

63 このデータのソースはランサムウェアの交渉者であり、自身で選択したサンプルの可能性があることに留意してください。この種のインシデントで交渉人を雇う余裕のある企業は、収益の高い組織である可能性が高いため、より高い身代金要求で狙われる可能性もあります。

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予防策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］

MOVEitか否か。

2023年の夏はずっと、原爆の父（映画『オッペンハイマー』）とプラスティック人形（映画『バービー』）との素晴らしいコラボのアイデアに心をくすぐられたものです。今年の報告書でも、似たようなコラボを紹介しますが、娯楽性には少し欠けるかもしれません。ランサムウェアグループは、彼らの「株主」の関連会社の利益を継続的に増加させることを望み、その戦術を進化させるために驚くべき能力を示してきました。

そのような最近の進化の1つにMOVEitインシデントがあります。攻撃者[64]がファイル管理ソフトウェアのゼロデイ攻撃（それまで知られておらず、パッチが適用されていない脆弱性）を利用し、誰のものでも構わず手当たり次第にデータを横領して人質に取るという、やりたい放題で注目を浴びました。さまざまな業種の組織がこの攻撃の影響を受けましたが、ベライゾンのデータ漏洩/侵害データセットによると、教育機関が圧倒的に大きな影響を受け（図32）、被害に遭った組織の50%以上を占めました。

これは一見、ごく普通のサイバー犯罪のようでしたが、ここで言及しておくに値する攻撃者の戦術の変化でした。まず、このグループは、以前は好んで使っていたにもかかわらず、これらのいずれのケースでも「ランサムウェア」を投入していません。グループが「ランサムウェア」を選ばなかった理由には無数の可能性があり、ここで示唆することは推測に過ぎないかもしれません。

しかし、できたことと言えば、「システム侵入」と「ソーシャルエンジニアリング」のそれぞれのカテゴリーにきちんと当てはまるデータを大量に入れ込むことによって、両パターンの間に存在する違いをわずかに混乱させたことでした。データを盗んだ後、Cl0pグループは、被害者が苦労して稼いだお金を奪う手段として「脅迫」を使いました。

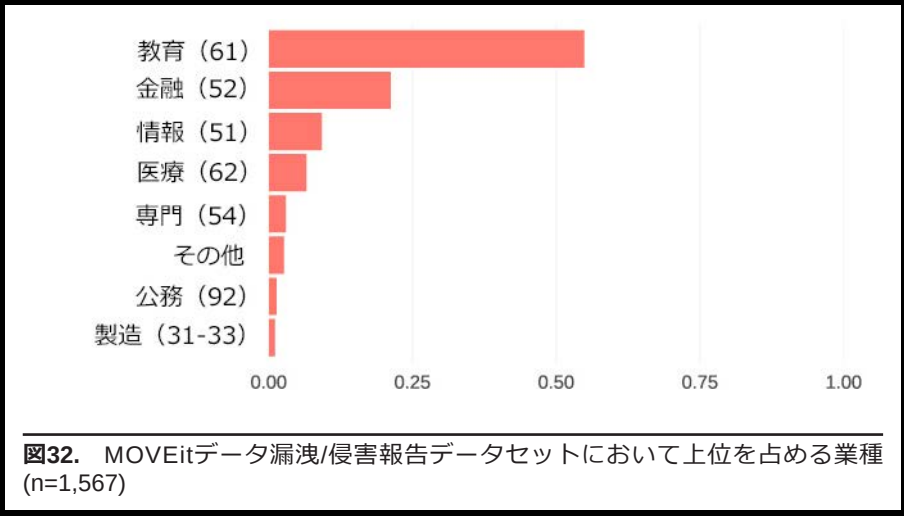


図32. MOVEitデータ漏洩/侵害報告データセットにおいて上位を占める業種 (n=1,567)

64 広くCl0pランサムウェアグループとされています（(https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-158a)）

「ランサムウェア」によるデータ漏洩/侵害の経時的変化を見ると（図33）、件数が減少していることが確認できますが、「脅迫」と組み合わせると、ほぼ同じ傾向線をたどっていることがわかります。このことは、同じ攻撃者が、選んだ進入経路の種類を最大限に活用するために単に戦術を変えているだけなのかもしれないことを示しています。この組み合わせは、「調査結果の概要」の2番目の項目で触れたように、データ漏洩/侵害の一部として大きな伸びを示しています。

DBIRチームはコードではなく数字[65]を見ているので、この報告書はすべての技術的要素を説明するのに最適な場ではありません。とはいえ、この脆弱性が本質的に許してしまったことは、攻撃者が狡猾なSQLインジェクション攻撃を通じてバックドアをアップロードできるようにすることでした。このバックドアによって、攻撃者はデータのダウンロードやアプリケーションの正当なユーザを操るなど、さまざまなタスクを実行することができました。

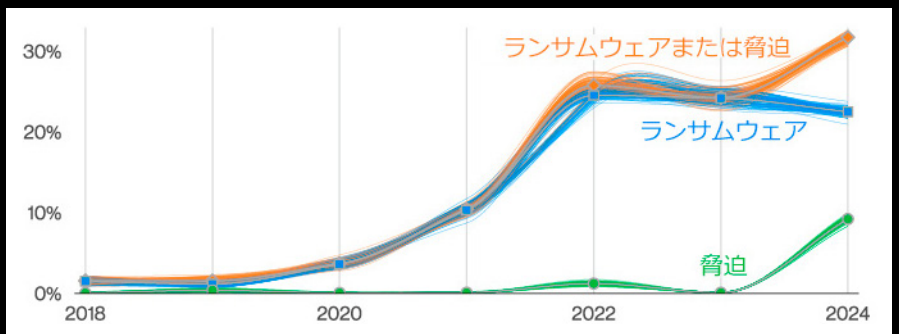


図33. 「ランサムウェア」と「脅迫」によるデータ漏洩/侵害の経時的変化

残念なことに、プラットフォームの性質上、ファイル転送システムはインターネット上に置かれる必要があり、悪用された時点では未知の脆弱性であったため、被害者がこれを防ぐためにできることは何もありませんでした。確かに今回の攻撃は大規模で影響力の大きいものでしたが、前例がなかったわけではありません。実は、そのわずか数か月前の2023年1月にも、同じグループが別のファイルホスティングプラットフォームを標的にし、ランサムウェアの被害が多発した月がありました。

私たちは将来を想定しているので、ランサムウェアグループによってゼロデイ脆弱性が広く活用され続けるとしても、私たちが驚くことはないでしょう。ファイル転送プラットフォームに対する攻撃者の嗜好が続くのであれば[66]、これはこれらのプラットフォームベンダーにとって、一般的な脆弱性がないかコードをよくチェックするようにという警告となるはずです。同様に、読者の皆様の組織がこの種のプラットフォームを利用している場合、あるいはインターネットに公開されているあらゆるものを利用している場合は、これらのベンダーからリリースされるセキュリティパッチに細心の注意を払い、優先順位をつけて適用するようにしてください。

65 それにポップカルチャーの資料

66 そうは言っても、2024年が始まるとVPNとリモートデスクトップ共有ソフトウェアに焦点が当たっているようですが。

ソーシャル エンジニアリング

サマリー

サイバーセキュリティインシデントの主な要因となっているのは、既存のメールチェーンやコンテキストを利用してユーザを狙う「なりすまし」攻撃です。また、大規模なMOVEitインシデントによる「脅迫」も劇的に増加しています。

昨年との比較

メールを使った「フィッシング」と「なりすまし」は、引き続きこの分野におけるインシデントの主な原因であり、データ漏洩/侵害の73%を占めています。

頻度	インシデント3,661件、確認されたデータ漏洩3,032件
攻撃者	外部（100%）（漏洩/侵害）
攻撃者の動機	金銭目的（95%）、スパイ活動（5%）（漏洩/侵害）
侵害されたデータ	認証情報（50%）、個人情報（41%）、内部情報（20%）、その他（14%）（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

風に*かれて（*ishing）

サイバーセキュリティの世界、あるいは「サイバービズ」と呼ばれる世界では、確かにキャッチーな用語がもてはやされます。Whaling（ホエーリング：社会的地位の高い人を狙ったフィッシング）、Smishing（スミッシング：SMSを使ったフィッシング）、Quishing（クイッシング：QRコードを使ったフィッシング）、Tishing（ティッシング：Teamsを使ったフィッシング）、Vishing（ビッシング：音声によるフィッシング）、Wishing（ウィッシング）、Pharming（ファーミング：偽サイトによるフィッシング）、Snowshoeing（スノーシューイング：IPアドレスを悪用したフィッシング）[67]、そして従来のフィッシングなどの用語は、「ソーシャルエンジニアリング」の攻撃パターンでは常に存在します。なぜなら、従業員やエンドユーザを教育する必要がある攻撃経路は数多くあり、さらに5年後にはリストに追加しなければならない新たな攻撃経路が生まれると予想されるからです。

ただし、このような新しい攻撃経路や攻撃の種類が増えたとしても、「なりすまし」や「フィッシング」のような核となるソーシャル攻撃の手口は依然として頻繁に使用される傾向にあります（図34）。インシデントの40%以上に「なりすまし」が、31%に「フィッシング」が関与しています。それ以外のメール、SMS、Webサイトを介した攻撃（図35）などの試行錯誤を経た手口は、必ずしも最高レベルに有効なものではありませんが、セキュリティの専門家であれば、そのキャリアを通じて、何らかの形でこれらの手口を目にしたことがあるでしょう。

図34. 「ソーシャルエンジニアリング」のインシデントにおいて上位を占める攻撃の種類（n=3,647）

組織に侵入するために攻撃者が選ぶ方法はさまざまでも、核となる手口は同じです。攻撃者は、私たちの人間性、信頼や助け合いの気持ちを自分たちの利益のために悪用しようとします。これらの攻撃はすべて共通していますが、手口の規模と普及の点でかなり大きな違いがあります。

まず、今年のDBIRで状況の改善が見られた点を紹介しましょう。昨年のような「なりすまし」の劇的な増加はありませんでした。ただし、減少したわけではなく、「ソーシャルエンジニアリング」インシデントのトップの座を維持している事実も変わりありません。あらためて、「なりすまし」とは、攻撃者が既存のメールチェーンを利用して、被害者に何かをさせる（例えば、関連する銀行口座を更新して入金させるなど）「ビジネスメール詐欺（BEC）」の代替手段として考えるのが一般的です。

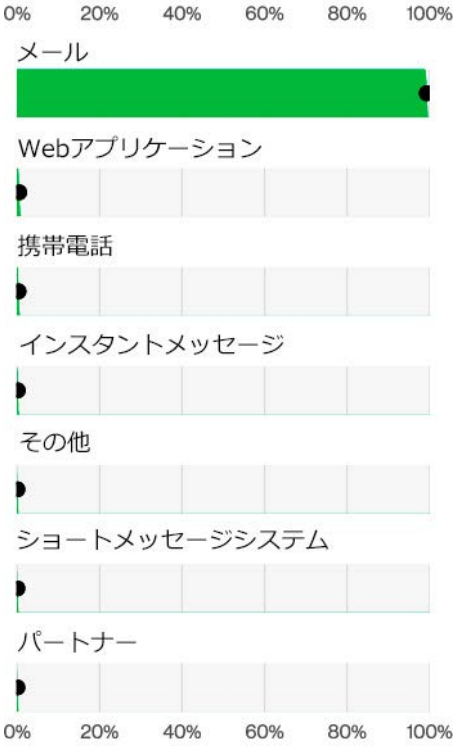


図35. 「ソーシャルエンジニアリング」によるデータ漏洩/侵害において上位を占める攻撃経路（n=2,961）

67　本稿執筆時点では、このうち1つはフェイクでした。

ローテク、高コスト

次は、残念なことに悪化した状況についてです。それは「BEC」が引き続き組織の財務状況に多大な影響を及ぼしているということです。図36は、2018年初頭からの「BEC」に関連したコストの伸びを示しています。上述したように、昨年と比較して今年は伸びてはいませんが、減少もしておらず、詐欺による被害金額の中央値は50,000ドル前後で推移しています。

「BEC」の被害者になったことに気づいたときにできる最善のことの1つは、速やかに法執行機関と連携することです。図37は、FBI IC3[68]のデータ提供組織が担当した事件の結果分布を示しています。半数のケースで、79%以上の損失を回収できています。インシデントの18%を占める幸運に恵まれなかった組織では、何も凍結されず、犯罪者に奪われたものをすべて失う恐れがありました。

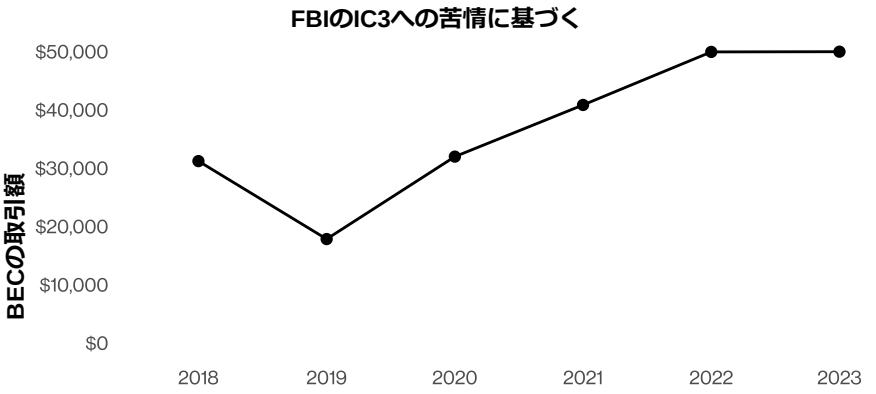


図36. 「ビジネスメール詐欺（BEC）」の取引額の中央値

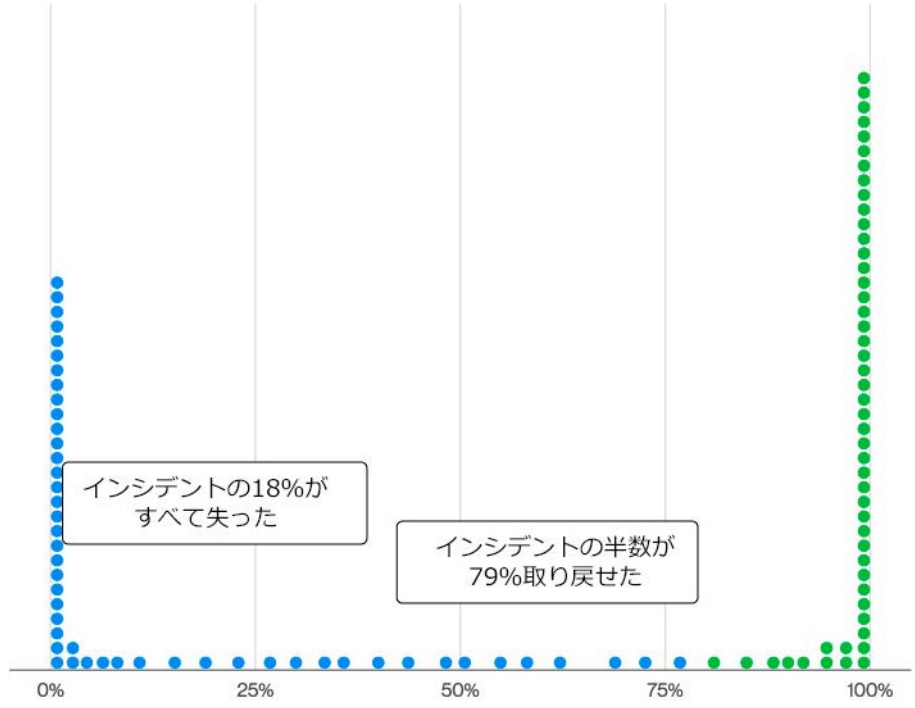


図37. 損失回収のために凍結された損失の割合

68 https://www.ic3.gov

ご機嫌いかがですか。これは脅しです。

内向的な私たちは、ランサムウェアグループによる脅迫型の攻撃がドアを破って「ソーシャルエンジニアリング」パターンに侵入してくる以前から、このようなソーシャルな「やりとり」にはすでにうんざりしていました。「フィッシング」などのソーシャル攻撃は、MGM Resortsやその他のエンターテイメントグループへのALPHVによる侵害に代表されるように、かなり前からランサムウェアを仕込むのに一役買ってきました。しかし、一部のグループによる攻撃手口の変化や、突破口を開く最初の一撃とは対照的な「脅迫」攻撃によるデータ漏洩/侵害の最終的な結果を考慮すると、この一見「システム侵入」的な攻撃は、現在ではこの「ソーシャルエンジニアリング」の攻撃パターンにも現れています。

ただし、「脅迫」はこのパターンでは決して目新しいものではないことにご留意ください。「スマホをハッキングしたところ、どうやらNSFW（職場環境で視聴や閲覧が適切でないとされるコンテンツを指す）なものを見ていましたね」といった口先だけの脅しから、「ちょっと調べていただければ、すぐに分かります。私たちはDDoS攻撃を仕掛ける超スーパーハッカー集団です」のようなある程度信憑性のある脅し、そして「流出させられるデータがここにあります。

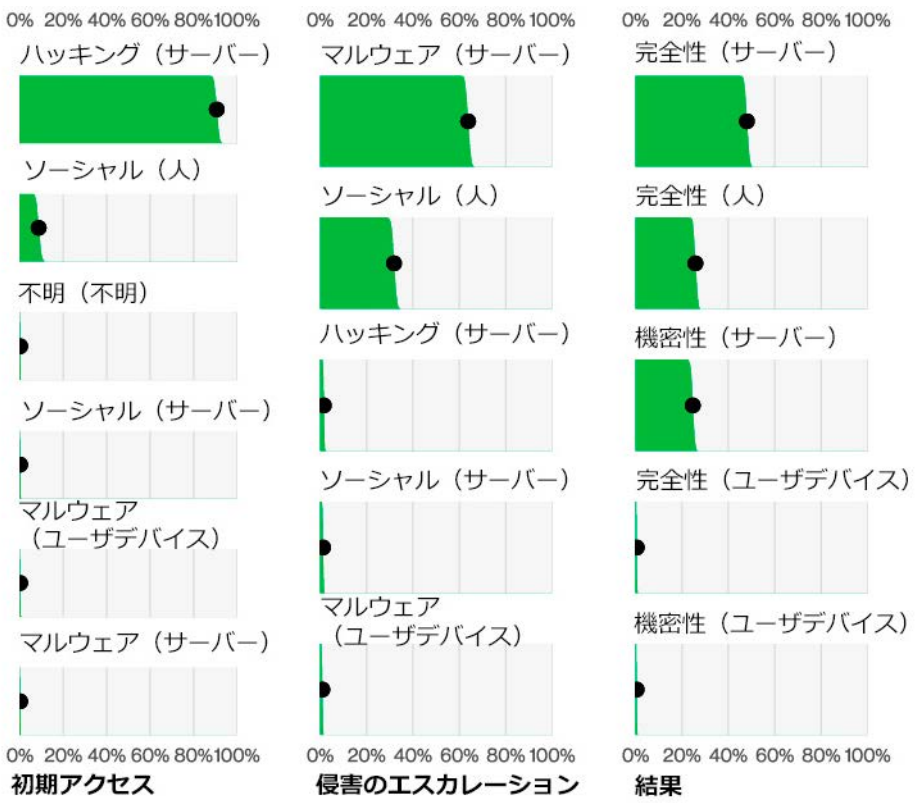


図38. 「ソーシャルエンジニアリング」インシデントのステップ

本物かどうか、どうぞこのサンプルで検証してみてください」といった信憑性の高い脅迫まで、さまざまな段階のバリエーションがありました。ただし、今年はMOVEitによるデータ漏洩/侵害が比較的大規模に、しかも極めて公然の形で組織に影響を及ぼした結果、「脅迫」が大量に発生しました。

このことは、データ漏洩/侵害に至るまでのステップ（図38）をご覧いただければ一目瞭然です。おわかりのように、「ハッキング」によってサーバーを侵害するケースが劇的に増加しています。このような攻撃が蔓延しているため、組織でこのような攻撃が発生した場合にとるべき一連の行動について、経営陣と協議することをお勧めします。

「フィッシング」を学ぶ

これは決まり文句に聞こえるかもしれませんが、私たちは、どのような組織においても、防衛の第一線はシステムを強化する[69]ことではなく、エンドユーザも含めた[70]主要スタッフの教育であると信じています。幸いなことに、これは単に私たちが「ユーザの意識向上」を主張するためにプレゼンテーションをしているということではありません。私たちのスタンスを数値化するためのデータも具体的な数字も用意しています。最初に学ぶべき教訓は、「フィッシング」攻撃はすばやく行なわれるということです。メールを開いてから悪意のあるリンクをクリックするまでの時間の中央値は21秒で、その後にデータ入力するまでにさらに28秒しかかかっていません（図39）。ここから分かるのは、恐ろしいことに、ユーザがフィッシングメールに引っかかるまでの時間の中央値は1分未満という事実です。

今年の良い傾向として、業界内でフィッシングに対するテストの報告に関して改善されつつある様子が見られました。テストメールのやり取りで、メールをクリックした11%のユーザを含んだ20%のユーザがフィッシングを特定し、報告しました。図40が示すように、これもまた目覚しい改善であり、前年度に増加した「フィッシング」と「なりすまし」の状況に対応するためにはどうしても必要なことです。

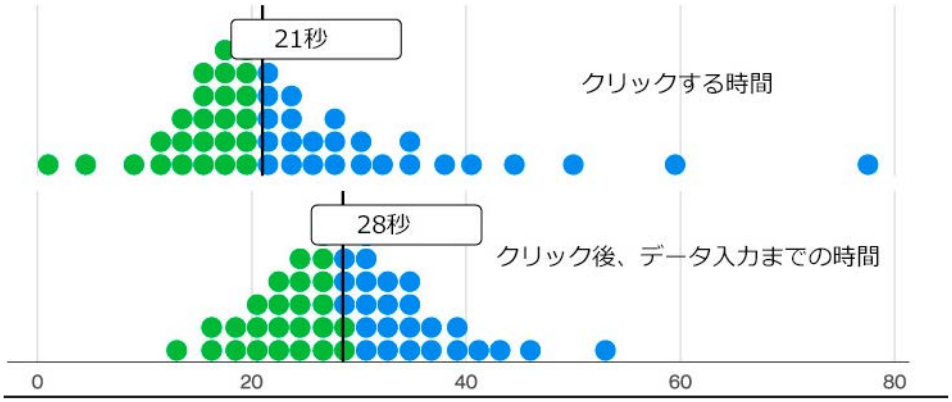


図39. メールをクリックしてからデータ入力が行なわれるまでの時間

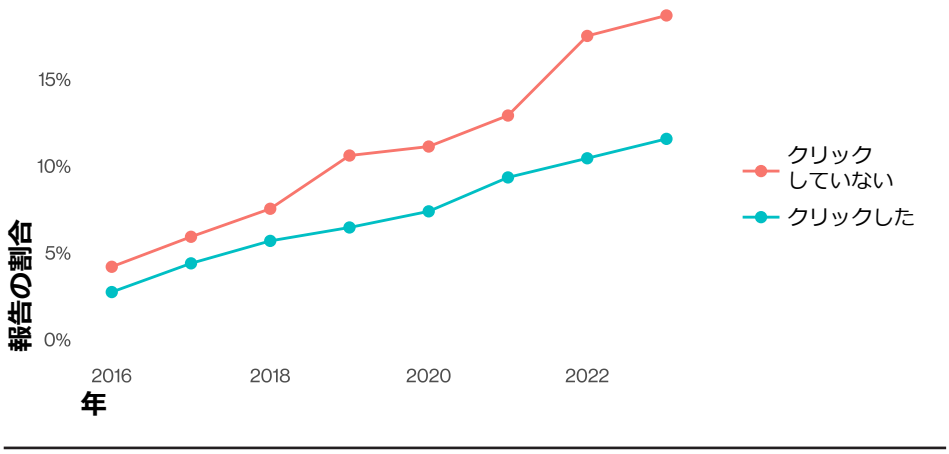


図40. クリック状況で見た「フィッシング」メールの報告の割合

ここから分かるのは、恐ろしいことに、ユーザがフィッシングメールに引っかかるまでの平均時間は1分未満という事実です。

69 ここに非常にわかりやすいマジノ戦線のジョーク（第2次世界大戦時のフランスの対ドイツ要塞線のことですが、道路上に設置した段差のようなものだ、というジョーク）がありますが、読者の見解にお任せします。

70 たぶん「“特に”エンドユーザ」と言うべきかもしれません。

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、フィッシングの罠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。

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］

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

サマリー

攻撃者は、認証情報へのブルートフォース攻撃、情報の購入、または過去の攻撃で得た情報の再利用によって、デフォルトで単純化され、容易に推測可能な認証情報を使用している資産を利用し続けています。

昨年との比較

金銭的な目的を動機とする外部の攻撃者によって引き続き、認証情報と個人情報が狙われています。

頻度	インシデント1,997件、確認されたデータ漏洩881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（85%）、スパイ活動（15%）、（漏洩/侵害）
侵害されたデータ	認証情報（71%）、個人情報（58%）、その他（29%）、内部情報（17%）（漏洩/侵害）

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

おそらく「基本Webアプリケーション攻撃」ほど複雑で、多面的で、率直に言って、読んでいて面白いパターンは他にないと言ったらどう思いますか？やはり読者の皆様をからかっていることになりますよね？このパターンは、基本的にその名の通り、無防備な、あるいは（より多くの場合）保護が不十分なWebアプリケーションに対する単純な攻撃で、犯罪者に組織の環境への侵入の足がかりを与えてしまうものです。「システム侵入」パターンを洗練された銀行強盗[71]になぞらえるなら[72]、この「基本Webアプリケーション攻撃」パターンはオッカムの剃刀（思考節約の原理）を攻撃ではっきり目に見える形にしたものと言えるでしょう。手順が少なく、A点からB点への経路はおそらく最も単純で最短の距離をとっています。あまり複雑でない多くのものがそうであるように、それは非常にうまく機能しています。

昨年、この種の攻撃は全データ漏洩/侵害の4分の1を占めていましたが、今年のデータセットでは、「基本Webアプリケーション攻撃」パターンによるデータ漏洩/侵害は8%強にとどまっています。この攻撃パターンではいつもそうですが、攻撃者は「盗まれた認証情報の悪用」（77%）、「ブルートフォース（通常は推測が容易なパスワード）」（21%）、または「脆弱性の悪用」（13%）によるハッキングによってアクセス権を獲得します（図41）。

図41. 「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「ハッキング」攻撃（n=713）

暗号を扱う開発者に注意。

興味深いことに、このパターンのマルウェアの約20%は、暗号通貨をマイニングする「マルウェア」で構成されています。さらに詳しく調べてみたところ、既知の脆弱性と暗号通貨をマイニングするマルウェア（および「ランサムウェア」）を活用して、自国のために小銭稼ぎをしている国家レベルの小さな攻撃者グループが見つかりました。特に画期的なことはありませんが、10年以上も前の手口が今でも通用するのを見るのはいつも興味深く思います。

フリーサイズのガソリンスタンドの野球帽（「Keep on Truckin'ワッペンを付けたような」）のように、どの組織も「基本Webアプリケーション攻撃」のパターンに当てはめることができますが、あまり似合うのも困りものです。「金融および保険業」（18%）、「情報産業」（14%）、「専門的・科学的・技術的サービス業」（13%）が、「基本Webアプリケーション攻撃」の影響を受ける上位3つの業種にランキングされていますが、その他のほとんどの業種でもこのような攻撃が見られます。また、「基本Webアプリケーション攻撃」のパターンでは、大規模組織（55%）と小規模組織（47%）の間に大きな差はありません。

盗まれた認証情報による攻撃

これまでの読者の方は[73]、もうお気づきかもしれませんが、DBIRのデータセットには盗まれた認証情報を悪用したインシデントが非常に多く含まれています。過去10年間で、盗まれた認証情報はデータ漏洩/侵害のほぼ3分の1（31%）に出現しています（図42）。つまり、認証情報は組織を危険にさらす中核的な要素なのです。しかし、これが事実であることは承知していても、盗まれた認証情報については分からないことだらけです。これらの認証情報はどこから来たのか、どのようにしてここまで来たのか、そしてその全貌を知ることはできるでしょうか[74]？

図42. 2013年以降の上位を占める攻撃の種類（n=35,970）

71 銀行強盗については、「業種別ハイライト」セクションの「金融および保険業」をご覧ください。

72 「オーシャンズ11」や「大列車強盗」などの映画には触れないほうがいいでしょう。著作権料を要求されることになるかもしれませんから。

73 そうであってほしいです。

74 それとも、私たちの日常生活に謎のスパイスを与え続けるだけなのでしょうか？

盗まれた認証情報の出どころを理解するには、さまざまなタイプのクレデンシャル攻撃が存在することを考慮する必要があります。当然のことながら、「フィッシング」はDBIRのデータセットに見られる最も一般的な認証情報に関連する攻撃であり、「認証情報」に関わるデータ漏洩/侵害の14%を占めています。「ソーシャルエンジニアリング」は、システムではなく個人を標的にするため、極めて一般的であり、効果も非常に高いものです。「ソーシャルエンジニアリング」のセクションで説明したように、システムを強化するのは個人を強化するよりもはるかに容易です[75]。クレデンシャル攻撃のもう1つの基本タイプは「ブルートフォース」（すべてのパスワードを推測する）で、これは攻撃者の懐にある効果的なツールですが、今年の侵害ではわずか2%しか確認されていません。この手法が最も成功するのは、個人やアプリケーションが推測可能な脆弱な認証情報、あるいはもっと悪いことに認証情報を初期状態のまま使用している場合です。ここでの光明と言えば、「ブルートフォース」攻撃がログインオプションが存在する限り存在するため、許しがたいほど複雑、あるいは許せる程度の長いパスワードの入力をユーザに強制したり、ログインの試みが可能な時間の長さと回数を制限するなど、さまざまな攻撃緩和策が一般に利用可能であるということです。

古い認証情報ではもうやっていけない

「クレデンシャルスタッフィング」は、「ブルートフォース」のいかした従妹[76]のような存在です。両者には多くの共通点がありますが、クレデンシャルスタッフィングのほうが成功の可能性が高いといえます。なぜなら、クレデンシャルスタッフィング攻撃は、可能なユーザ名/メールアドレスとパスワードの組み合わせを総当たりで試すのではなく、過去のデータ侵害で取得した既知の組み合わせを利用するからです。最近では、攻撃者がこの手口で極めて個人的なユーザデータにアクセスする事件が多発しています。

この種の攻撃は、さまざまなアカウントやIPアドレスに分散させるため巧妙さが増しており、攻撃を防ぐことは困難です。もし多くの顧客、特に消費者向けのWebアプリケーションやアプリケーションプログラミングインターフェイス（API）を運用されている場合は、攻撃者がツールや無料で入手したプロキシリストを使って、チャットサイトで見つけた組み合わせを試みる前に、強固な防御体制の構築を検討することをお勧めします。

APIといえば、APIファイアウォールのデータ協力組織から提供された検出データのサンプル（図43）から、それらの攻撃の種類の割合を調べることができます。予想通り、クレデンシャルスタッフィング攻撃は最もよく検出されていますが、ブルートフォースと混同されることが多いということもあります。このデータセットから得られたもう1つの興味深い結果は、認証情報の不正使用のような攻撃の普及度は攻撃全体のわずか15%に過ぎず、インシデントデータセットで見られた「盗まれた認証情報の悪用」の半分以下であったことです。この結果が妥当に思えるのは、API上で悪用しようとするものは認証情報だけではないからです。

しかし、消費者向けのWebアプリケーションやAPIがない場合はどうでしょうか？24文字のパスワードを毎月更新するなど、厳格なパスワードポリシーをすでに実施していたらどうでしょうか？悲惨な運命に見舞われることはないでしょうか？残念ながら、それでもパスワード窃盗犯はあなたのデータを盗むことができます。DBIRのデータセットでは、パスワードダンパーはあまり見かけませんが（データ漏洩/侵害の2%）、報告書に載っているのは視認できたものだけであること、そしてこの種の「マルウェア」はほとんど目につかない場所[77]（仕事関係ではなく個人のコンピューターなど）に潜むことを念頭に置くことが重要です。

この問題がどの程度浸透しているかを知るために、これらのパスワード窃盗団から集めた認証情報とCookieの販売と転売を専門にしている市場を見てみました。サンプルの対象としたのは1つの市場でたった2日間だけでしたが、それでも1日あたり1000件以上の認証情報が平均10ドルで売りに出されていました。

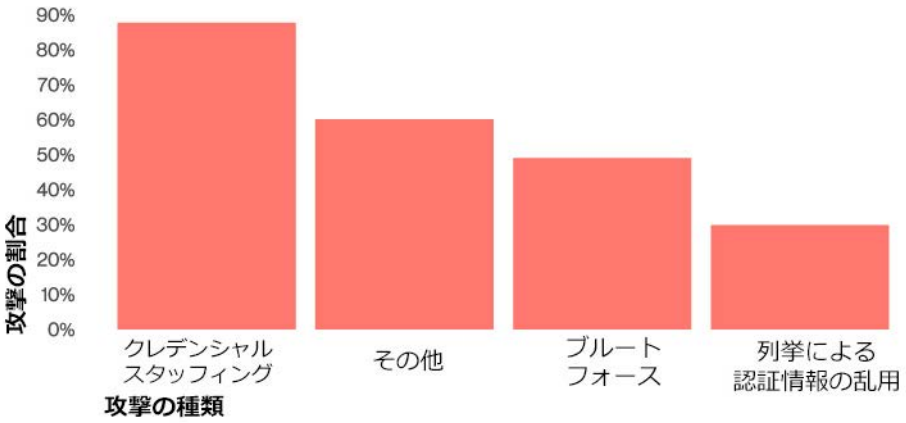


図43. Webアプリケーションの攻撃タイプの割合

75 前者は安全性が強化され、後者は単純に食傷気味ということです。

76 パイロットサングラスが決め手。

77 Bigfoot（未確認動物）が住んでいるようなところとは違います（少なくとも1つはSasquatch（Bigfootと同一視されるアメリカインディアンに伝わる巨人）に関する言及がなければDBIRは完成しない）。

これらの売り出し投稿を調査した結果、認証情報の65%が、収集されてから1日も経たないうちに売りに出されていることがわかりました[78]。ほとんどは攻撃者が購入し、従業員個人やその雇用主の企業に対する別の攻撃の足がかりに利用されています。多くの場合、売りに出されるこれらの商品には有用な認証情報やCookieのリストだけでなく、それぞれに関連する地域の情報も含まれています。私たちは、これらの認証情報が組織で管理された資産から来たものなのか、個人のコンピューターから来たものなのかを特定したいと考えました。平均して30%以上の投稿には、ソーシャルメディアの認証情報は記載されていませんでした。これは、システムの多くが個人用のものではないということなのかもしれません。図44は、インフォスティーラーグループ名別に、ソーシャルメディアアカウントが記載されていない投稿の割合を示しています。

パスワードスティーラーのもう1つの発生源は、公開リポジトリに投稿されたライブラリです。開発者以外の世界中の人々にとってコードを書くことは信じられないほど面倒なことであり、現代の「簡単でなければやらない」社会では「pip install library-of-my-choice」とか「install.packages ('library-of-my-choice')」[79]と入力するだけでインポートできるライブラリを開発者の誰かが作成し、投稿されたライブラリをダウンロードできるようなしくみが作られています。言うまでもありませんが、現実問題としてこの方法はかなりリスクが高く、ダウンロードするライブラリがマルウェアに感染していないことを信じる他ありません。人間というものの性質からして、感染しているライブラリは多く、マルウェア配布の恰好の手段にされています。幸いなことに、アップロードされたライブラリを積極的にスキャンし、マルウェアの存在を特定する会社が数多く存在します。悪意のあるパッケージが発見された場合、それらは大抵、インフォスティーラー（ショッカー）で構成されています。

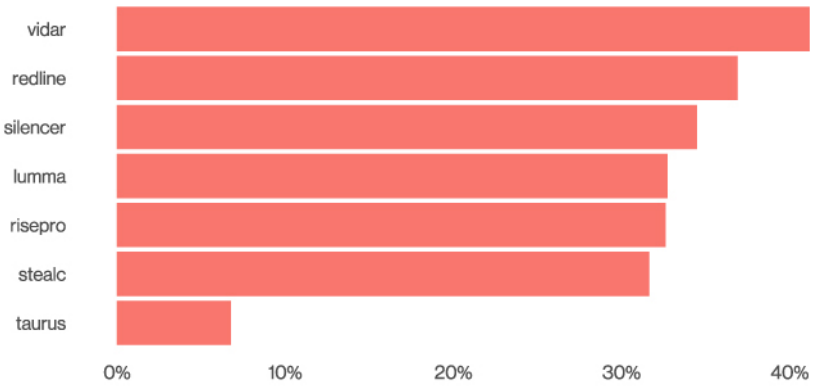


図44. 大手のソーシャルメディアアカウントの記載がないインフォスティーラーによる投稿の割合

もちろん、単にパッケージをアップロードするだけでは十分ではなく、誰かにそれをダウンロードしてもらう必要があります[80]。図45は、npmリポジトリで見られるよくあるアプローチのいくつかを示したものです[81]。JavaScriptのエコシステムで最もよく見られたのは、無料のビデオゲーム通貨ジェネレーターであることを宣伝しているような悪意あるパッケージでした。このようなパッケージは、コードのインストールやダウンロード方法の知識がある賢い人たちをターゲットにしていますが、そのパッケージが良すぎて本物とは思えないような場合、通常はそういうものなのですが、彼らはそのことに気づくほど賢くはありません[82]。

さらに、タイポスクワッティング（URLの入力ミスを利用し、詐欺サイトへ誘導する攻撃）を利用した悪意のあるパッケージも存在します。これは、マルウェアの開発者が、誰かが正規のパッケージをインストールしようとして、誤ってパッケージ名をタイプミスをすることを狙って、人気のあるパッケージと似た名前のパッケージを投稿することです。スペルチェックツールが無かったらチームごと失業したかもしれないDBIRの著者たちの目から見ると、これは比較的効果的な戦術であると考えられます。

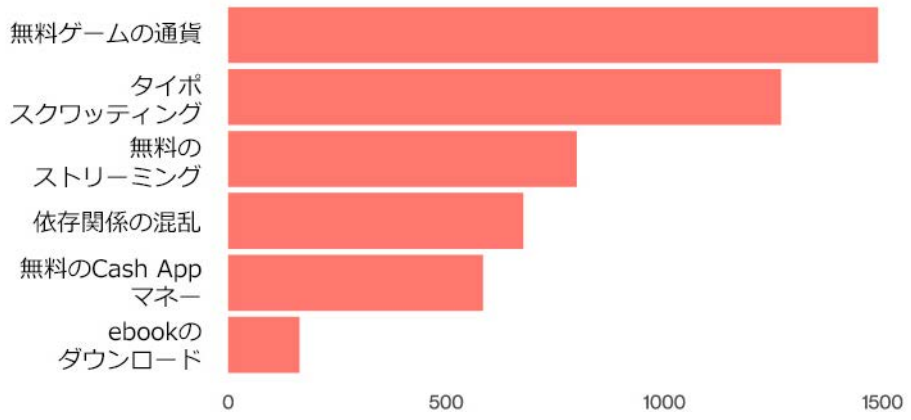


図45. ソーシャルエンジニアリング手法による悪意のあるnpmパッケージ

78 もしこれらの認証情報がドーナツだったら、「できたてのホヤホヤ」のシールがまだついていることでしょう。

79 DBIRチームがどのようなコーディング環境を使用しているか、おそらく誰も想像つかないことでしょう。:p

80 この報告書と同じです。このPDFまたは印刷されたものを友人からもらった人は、verizon.com/dbirにアクセスして自分用のコピーをダウンロードしてください。

81 https://www.npmjs.com/about

82 残念ながら、お金を得るためのチートコードはありません。オンラインゲームのマイクロトランザクションの場合はその逆で機能します。

最後に、私たち（＋私たちよりも賢い数人）が依存関係攪乱攻撃だと考えているものを目的にしたパッケージもありました。これは、あるツールがプライベートなリポジトリをチェックする前にパブリックリポジトリのパッケージをチェックすることを利用するタイプの攻撃です。たとえば、組織が社内のプライベートリポジトリに格納されているライブラリ「super-cool-internal-library」を使用していることが分かれば、攻撃者は公開リポジトリ上に「super-cool-internal-library」というライブラリを作成することができます。そうすれば、ツールにプライベートリポジトリをチェックする前にまずパブリックリポジトリをチェックさせることができます。幸いなことに、このような脅威から組織を保護してくれる素晴らしい会社もあれば、攻撃を軽減するのに役立つさまざまなプログラミングのベストプラクティスもあります。

このセクションを読み終えたら、一息つきましょう。あなたの組織をクレデンシャル攻撃から守るために避けなければならない地雷がたくさん埋まっているようです。これは新しいことではありません。私たちは（そして他の多くの人たちも）このことを、多要素認証（MFA）がこの種の攻撃を軽減する解決策となるずっと前から言ってきました。この問題に関して、子供たちに会社のコンピューターを使わせて、オンラインゲームで使える通貨V-Bucksを無料で稼ぐ方法を探させないようにすることも大事です[83]。セキュリティに関連するものは何でもそうですが、最も効果的な管理策は、技術的なリソースとともに人的要素を改善することです。

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/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］

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］

83 DBIRのバトルパスからカスタムカバースキンをアンロックするには、レポートの全セクションを必ずお読みください。

多種多様なエラー

サマリー

「エラー」は今年大幅に増加しており、おそらく「ケアレスミス」の増加と思われますが、新しいデータ提供組織によって攻撃データの漏洩件数が増えたことを反映している可能性もあります。エラーの50%以上が「誤送信」によるもので、昨年に引き続きこの傾向が続いています。一方、「廃棄」などその他のエラーは減少傾向にあります。「エンドユーザ」がエラーの87%を占めるようになり、業種を超えた万能なエラー捕捉管理の必要性が高まっています。

昨年との比較

私たちは、人がミスを犯すことを常に当たり前のこととして考えます。ミスのカテゴリーは毎年変わらないまま、いくつかの「エラー」の種類は減りましたが、頻度のランキングは変わっていません。

頻度	インシデント2,679件、確認されたデータ漏洩2,671件
攻撃者	内部（100%）（漏洩/侵害）
侵害されたデータ	個人情報（94%）、内部情報（34%）、銀行情報（14%）、その他（12%）（漏洩/侵害）

図46. 「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=2,586）

自分が何をしているのかよく分かっているよ。

忙しく慌ただしいときは、時折ミスを犯しがちです。重要なのは、そのようなミスの発生を押さえ、習慣にならないように心がけることです。今年の報告書で「エラー」関連のデータ漏洩/侵害件数が昨年の約5倍になったことを考えると、従業員のミスは習慣化に近づきつつあるのかもしれません。これだけ大幅な増加となったのは、細部への意識が足りないことや不注意が増えているからでしょうか[84]？おそらくそうかもしれませんが、本報告書の冒頭で述べたように、私たちのデータ提供パートナーの積極的な協力を示すものでもあります。調査するデータ漏洩/侵害の件数が増えれば増えるほど、この割合は高くなります。図46に示すように、昨年のエラーの50%以上は「誤送信」（送信の宛先を間違えること）が原因です。これは昨年の報告書でも第1位でした。

次に多い「設定ミス」は、データ漏洩/侵害の約10%となっています。「設定ミス」は過去3年間、減少傾向にあり[85]、これにはいくつかの理由が考えられます。最も大きな理由は、（ありがたいことに）多くのシステムでデフォルト設定の安全性が強化されており、マニュアルを読まずに新しいテクノロジーを立ち上げられ、推奨される設定でよりリスクが低くなっているということです。他の要因としては、風に煽られてバタバタする網戸のような危ないシステムを見つけ出すのに、セキュリティ研究者がそれほど時間を奪われていないことがあります。そ

84 同僚たちを見回してから、最善の判断でこの質問にお答えください。
85 大半の文明と同じように

して最後に、このようなエラーを発見するために研究者がこれまで使用してきたのと同じツールを犯罪者も使用し、それを悪用してデータを盗んでいる可能性があり、 その結果、これらの攻撃は「エラー」ではなく「ハッキング」のカテゴリーに入れられるようになったのではないかと推測されます。

「分類エラー」、「公開エラー」、「失言（口が滑ること）」は、この順番で比較的きっちりと並んでいます。「廃棄ミス」は（ここ数年の一般的傾向として）わずかながら減少を続けており、このパターンでは1%強を占めています。この件に関しては以前より注意が払われるようになったのか、それとも単に従業員が駐車場のドラム缶の中で記録文書を燃やすのがうまくなったのかは不明です。

図47は、このパターンの攻撃者についてかなり劇的な変化を示しており、「エンドユーザ」によるエラーは、昨年の報告書の20%から87%に増加し、「システム管理者」によるエラーは、昨年の46%からわずか11%に減少しています。この割合の減少は、エンドユーザの「誤送信」の増加によるところが大きいです。「設定ミス」は「システム管理者」でなければ起きようがありませんが、「エンドユーザ」はベテランでも誤送信する可能性があります。人々にどうか力を！

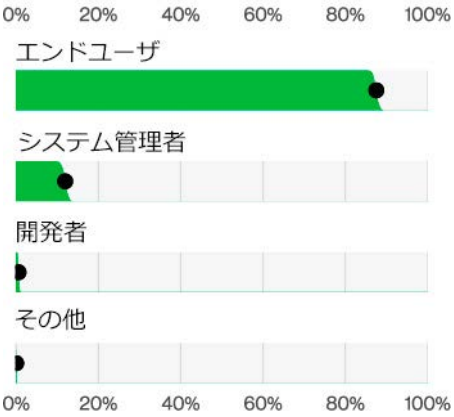


図47. 「多種多様なエラー」のデータ漏洩/侵害において上位を占める攻撃者（n=2,260）

図48. 「多種多様なエラー」のデータ漏洩/侵害において上位を占める業種(n=2,671)

最後に、「多種多様なエラー」パターンの業種は比較的多様で（図48）、「医療」と「公務」が上位を占め（規制の報告要件を考慮すれば当然）、「金融および保険業」、「教育サービス業」、「専門的・科学的・技術的サービス業」などの他の業種も相応の結果を示しています。このことは、不注意はやや普遍的な特徴であるという重要な事実を示しており、どの業種の雇用主も、この種のエラーを早期に発見できる管理体制を構築することが推奨されます。

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］

サービス拒否（DoS）

サマリー

「サービス拒否（DoS）」攻撃はインフラのさまざまな箇所を標的にすることができ、組織が対処するために準備する必要があるいくつかの形態で現れます。

頻度	インシデント16,843件、確認されたデータ漏洩3件
攻撃者	外部（100%）（インシデント）

昨年との比較

「サービス拒否（DoS）」攻撃は各所で発生し続け、インシデントパターンの最上位を示しています。

図49. インシデントのパターン（n=30,458）

今年もまた「サービス拒否（DoS）」がチャンピオンの座を維持しました。図49は、分析された今年のインシデントの50%以上がこの攻撃であったことを示しています[86]。このパターンは、ここ数年、最も多く見られるパターンであり、その理由は難しく考える必要はありません。比較的安価に実行できる「サービス拒否（DoS）」攻撃は、少なくとも攻撃を軽減するために組織の防御体制が敷かれるまでは成功率のかなり高い攻撃です[87]。

コンテンツデリバリーネットワーク（CDN）が監視しているWebアプリケーションに特化した「サービス拒否（DoS）」攻撃の継続的な分析によると、攻撃規模の中央値は2.2Gbpsから1.6Gbpsにわずかに減少しているにもかかわらず、これらの攻撃の97.5パーセンタイル地点ある攻撃[88]は、過去の最高値であった124 Gbpsから170Gbpsに増加しています。図50は、このデータと、より現実的で根拠のある90パーセンタイルなどの他のパーセンタイルのブレイクポイントを示しています。この攻撃タイプは通常、短時間に大量の攻撃を行うもので、その50%は5分以内に収束しています。

しかし、今年はこれまでとは違う分析を試したいと思います。高精度の標的型攻撃は非常に量が多く、一般的な分散型DoS（DDoS）フィルタリングがインターネットサービスプロバイダー（ISP）レベルに与える影響と対照的であるのは興味深い点です。DDoSフィルタリングの場合は、より広範な種類の攻撃を軽減する必要があり、大量攻撃の巻き添えになりやすい性質があります。

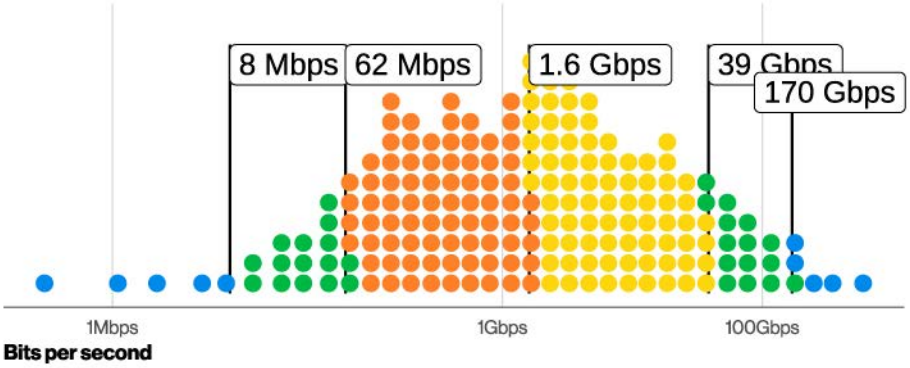


図50. CDNの分析によるDDoSインシデントにおける1秒あたりのビット数（n=10,713）

86 この「サービス拒否（DoS）」攻撃パターンの増加が観察された間は、電動歯ブラシに被害はありませんでした。
87 ある程度無視できる成功ですが。
88 あるいは、「データ分析を台無しにするような奇妙な異常値ではない、統計的に最悪のシナリオ」と呼びたいところです。

図51と52は、それぞれ世界全体のISPレベルの間接攻撃の1秒あたりのビット数と1秒あたりのパケット数の両方の分布を表しています[89]。このデータセットに含まれた攻撃対象は、ISP自体、ISPによるDDoS防御サービスの料金を支払っている企業、さらにはブロードバンド、モバイル、ワイヤレス、衛星を利用する個人ユーザのグループに分けられます[90]。個人ユーザの多様なグループへの攻撃は、企業への攻撃ほど大きくする必要がないため、規模がはるかに小さいことは明らかです。また、これらの攻撃は攻撃時間が長いことも特徴で、攻撃時間の中央値は約9分です[91]。全体として、このクラスの「サービス拒否（DoS）」攻撃は、電子商取引ではない、あるいはエクストラネットサービスを重視する組織が直面する可能性のある課題をよく表しているかもしれません。

さらに、DBIRにご協力いただいてる専門家（SME）の方々は、ドメインネームシステム（DNS）のようなインタラクションの多いサービスに対する執拗な小規模攻撃の増加を報告し続けています。インターネットから誰かを排除したい場合、ジャガイモの皮をむく方法は1つではないように方法はいくつかあります[92]。

結局のところ、私たちが推奨する対策はこれまでと変わりありません。DoS攻撃の防御に必要な体制の構築は比較的最小限で済むため、組織はこれらの攻撃を軽減するために、自動化または半自動化型の保護システムの導入を検討すべきです。インターネットへのユーザアクセスを一定時間妨害したいと考える攻撃者が現れる可能性に備えること以上に、なすべきことは多くありません。そうでないと考えるのは、”拒否”する人生を歩むことです。

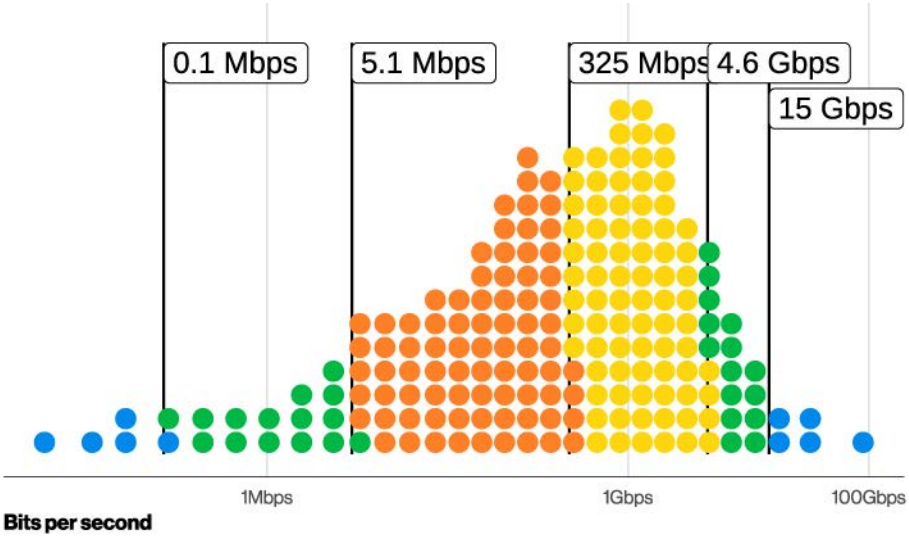


図51. ISPレベルのDDoSインシデントにおけるビット/秒（n=800,155）

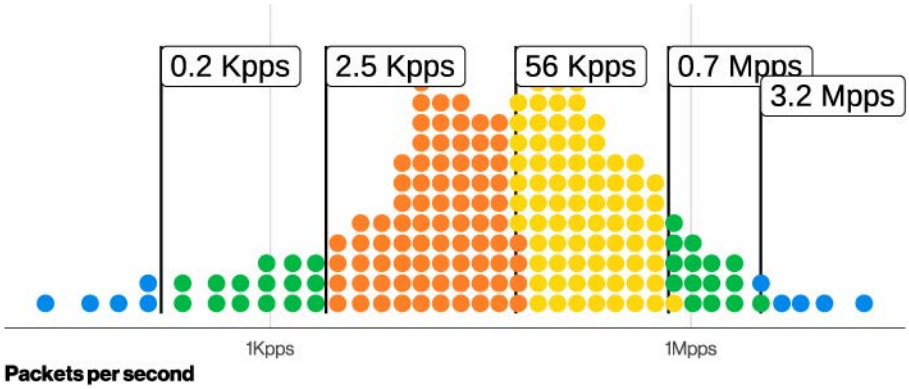


図52. ISPレベルのDDoSインシデントにおける1秒あたりのパケット数（n=800,155）

89 このサンプル数（n）のサイズを見てください！

90 おっと！Verizon Consumer Groupの縄張りに足を踏み入れたことはご内密にお願いします。

91 オンラインポーカーの対戦を台無しにするには十分すぎる時間。

92 DBIRはペットに優しいので、言葉のあやとして「猫の皮を剥ぐ（skin a cat）」ことを非難しています（“There’s more than one way to skin a cat.”という「方法は別にある」という意味の慣用句に対するジョーク）。

資産の紛失・盗難

サマリー

今年は、このパターンでのデータ漏洩/侵害が確認されるケースの割合が増加しました。

昨年との比較

デバイスは依然として盗難よりも紛失の方がはるかに多く、特にノートパソコンは依然と紛失のリスクとなっています。

頻度	インシデント199件、確認されたデータ漏洩181件
攻撃者	内部（88%）、外部（12%）（漏洩/侵害）
攻撃者の動機	金銭目的（92%～100%）、利便性/スパイ活動/恐怖/愉快/怨恨/イデオロギー/その他/二次的動機（各0%～8%）（漏洩/侵害）
侵害されたデータ	個人情報（97%）、内部情報（42%）、銀行情報（25%）、その他（17%）（漏洩/侵害）

あれ、どこに置いたっけ？

空港のセキュリティ検査で、電子機器を外し、靴を脱ぎ、飲みかけの水を捨てなければならない列に並んだことがある人なら、「追加のセキュリティ検査」の引き金にならないよう、不安な気持ちを隠しながら待つことがストレスフルな体験であることを知っているでしょう。人がいつもの環境から離れ、気をそらしているような間に物を失くすのも不思議なことではありません。ストレージ容量が十分多く、サイズもますます小さくなっているにもかかわらず、悪意であれ不注意であれ、紛失する可能性が最も高いのは「ユーザデバイス」です。その最たるものがどこでも使用できるノートパソコンです。図53に示すように、2022年には一時的に減少していたものの、今年は増加しています。

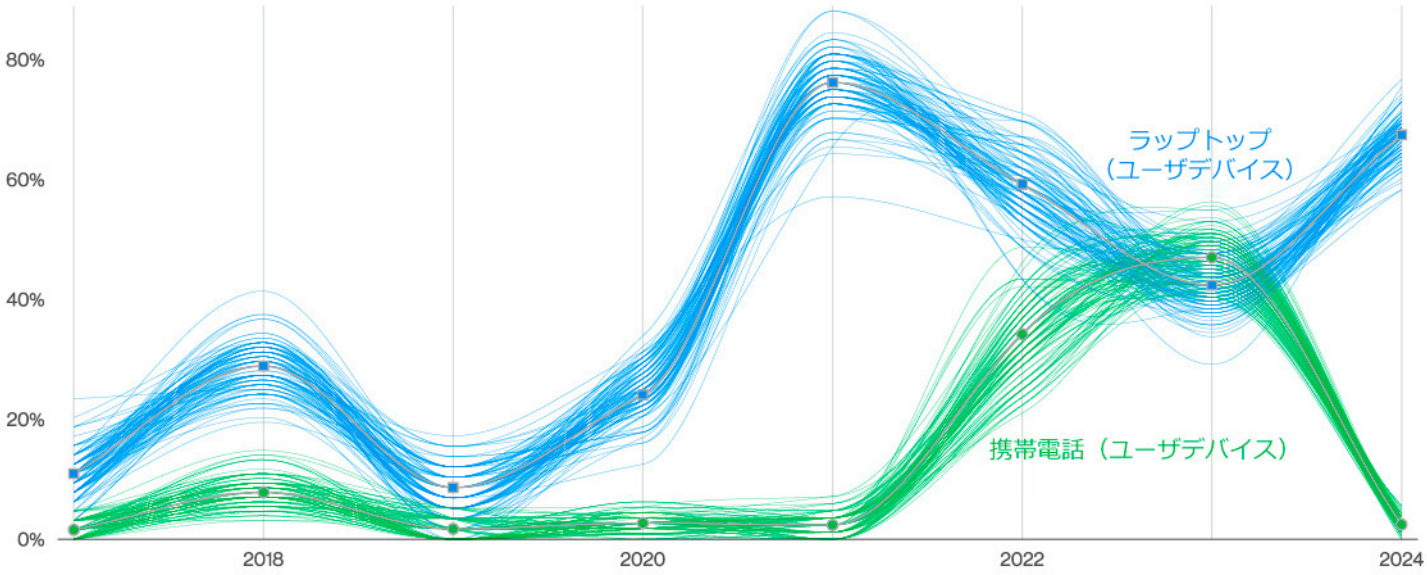


図53. 「資産の紛失」・「盗難」において上位を占める「資産」の種類の経時的変化

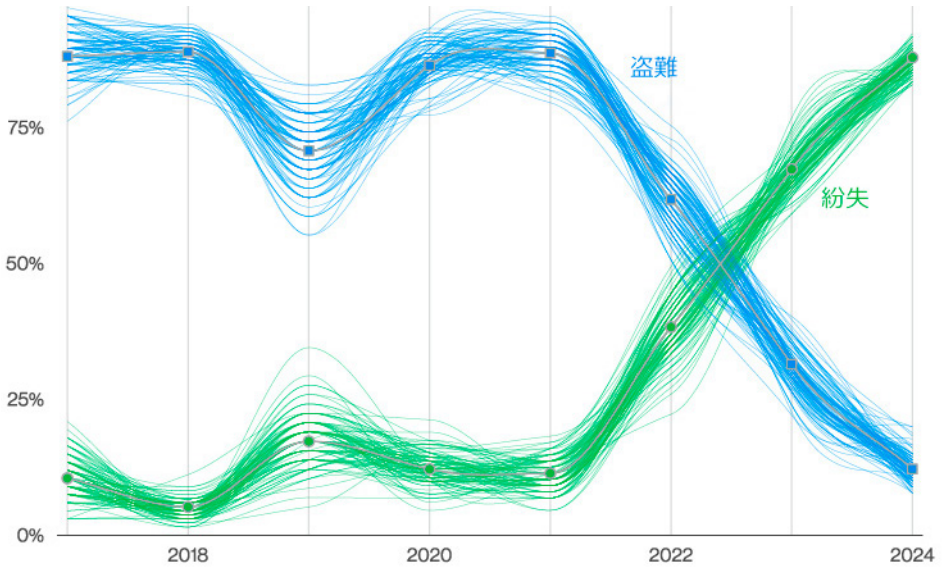


図54. 「資産の紛失」・「盗難」において上位を占める攻撃の種類

DBIRのデータセットでこれまでも見られたように、資産は盗まれるよりも紛失する可能性の方が圧倒的に多いです。しかし、図54は、これが常にそうであったわけではないことを示しています。2021年までは、資産が盗難に遭うことが多かったのですが、新型コロナウイルス感染症流行によって人々が外で会う機会が減ったため、盗難件数が減ったのかもしれません。とはいえ、ほとんどの企業が元の対面式の職場環境に戻っているにもかかわらず、この傾向は続いています。

今年は、このパターンで「資産」に関わるインシデントの割合が高く、昨年は約8%だったデータ漏洩/侵害が、今年はなんと91%にも達しています。

重要なのは、紛失や盗難に遭ったデバイスが報告義務のあるデータ漏洩/障害に発展しないよう、可能な限り資産に保護を施すことです。このパターンの攻撃が多いことを考えると、誰かがその注意書きを紛失したようです。

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

従業員が個人的な利益のためにデータを盗み、時には「外部」の攻撃者と共謀するため、従業員の背任は重大な脅威となります。「機密情報」とともに、「個人情報」は主要な標的となっています。昨年は「不正取引」が急増しましたが、また横ばいとなり、懸念は小さくなっています。

昨年との比較

このパターンでは、またもや「内部」の攻撃者が単独で行動しています。「金銭目的」の動機が依然として主要であり、「スパイ活動」はその次です。「個人情報」が依然として主な標的となっています。

頻度	インシデント897件、確認されたデータ漏洩854件
攻撃者	内部（100%）、 外部（1%） 複数（1%） （漏洩/侵害）
攻撃者の動機	金銭目的（88%）、 スパイ活動（46%）、 怨恨（6%）、 イデオロギー（2%）、 その他（2%） （漏洩/侵害）
侵害されたデータ	個人情報（83%）、 内部情報（46%）、 その他（22%）、 銀行情報（14%） （漏洩/侵害）

一度騙してみるがいい。

企業は従業員を信頼しています。自分に与えられた仕事をこなし、注意を払うべき問題を提起し、一般的に組織の最大の利益を念頭に置いているものと信頼しています。そして完璧な組織の世界では誰もがこのシナリオに従うでしょう。しかしこの攻撃パターンでは、必ずしもそうではないことがわかります。時には、従業員が自分だけの利益を求め、会社に不利益をもたらすことがあります[93]。また、人間関係がうまくいかない従業員が、転職を成功させるために次の雇用主にとって価値のあるデータを持ち出す権利があると考えることもあります。このような行為の結果として、このパターンで見られるデータ漏洩/侵害の分析を提供することができるのです[94]。誰も従業員が背任行為をするとは信じたくないでしょうが、もしそうなった場合、あなたの組織にそれを検知する方法があるでしょうか？あなたの組織だけのことではありませんが、検知する方法がないのであれば、すでに背任行為が行なわれているかもしれません。

恥を知れ。

従業員がデータを盗む動機は何でしょうか？私たちの経験では、それは主に「金銭目的」です。データを使って金銭を得る犯罪を犯すつもりだろうと、単に新しい就職先で有利になるためだろうと、直接的には自分だけの利益のために行なう傾向があります。また、従業員が不正に得たデータを競合他社に持ち込んだり、あるいは競合会社を立ち上げるために利用したりする「スパイ活動」的な動機も見られます。そして、それらの仕事をいつも一人で行なっているわけではありません。

93 「ブルータス、お前もか？」

94 ということは、それほど悪いニュースばかりではないということですよね？

昨年のDBIRでは、共謀（複数の関係者が協力してデータ漏洩/侵害の目的を達成すること）は7%でしたが、これは2019年の最高値には遠く及ばないものの、やはり驚きの結果でした。今年は、事態は正常に戻ったようで、共謀はデータ漏洩/侵害の1%未満に低下しています。これは良い状況と言えます。なぜなら、従業員が会社のデータを持ち逃げし始めるのも十分に悪質ですが、外部の攻撃者と手を組むことで混乱が生じるからです。

図55に示されているように、従業員が持ち出すのは主に「個人情報」です。これはおそらく顧客に関するもので、名前、連絡先、その他の情報は新しい競合会社を立ち上げたり、金銭を奪う犯罪を犯したりするのに大いに役立つ可能性があるからです。「内部情報」も今年は若干急増しましたが、これには機密性の高い企業計画や知的財産が含まれており、「スパイ活動」を動機とする従業員を惹きつけています。最後に、「銀行情報」は標的にされるデータの種類として長期的にほぼ安定しています。

昨年は「不正取引」が急増したため、今年はそれがトレンドの始まりなのかどうかを見極めたいと考えていました。これは一般的に「ビジネスメール詐欺（BEC）」攻撃の最終手段であり、攻撃者がソーシャルエンジニアリングによって被害者に現金を電子送金させるものです。「内部」の攻撃者はそうした機能を含む既存のシステムにアクセスすることができ、昨年はそれがよく利用されていましたが、この傾向が続いていないことは喜ばしいことです。昨年のデータセットでは15%近くまで急増したにもかかわらず、今年は3%と平穏な状態に戻っています。

検討すべきCISコントロール

アクセスの管理

企業資産とソフトウェアのセキュアな設定［4］
– 安全な設定プロセスを確立し維持する［4.1］
– 企業資産とソフトウェアのデフォルトアカウントを管理する［4.7］

アカウント管理［5］
– 休止アカウントを無効にする［5.3］
– 管理者権限を専用の管理者アカウントに限定する［5.4］

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］

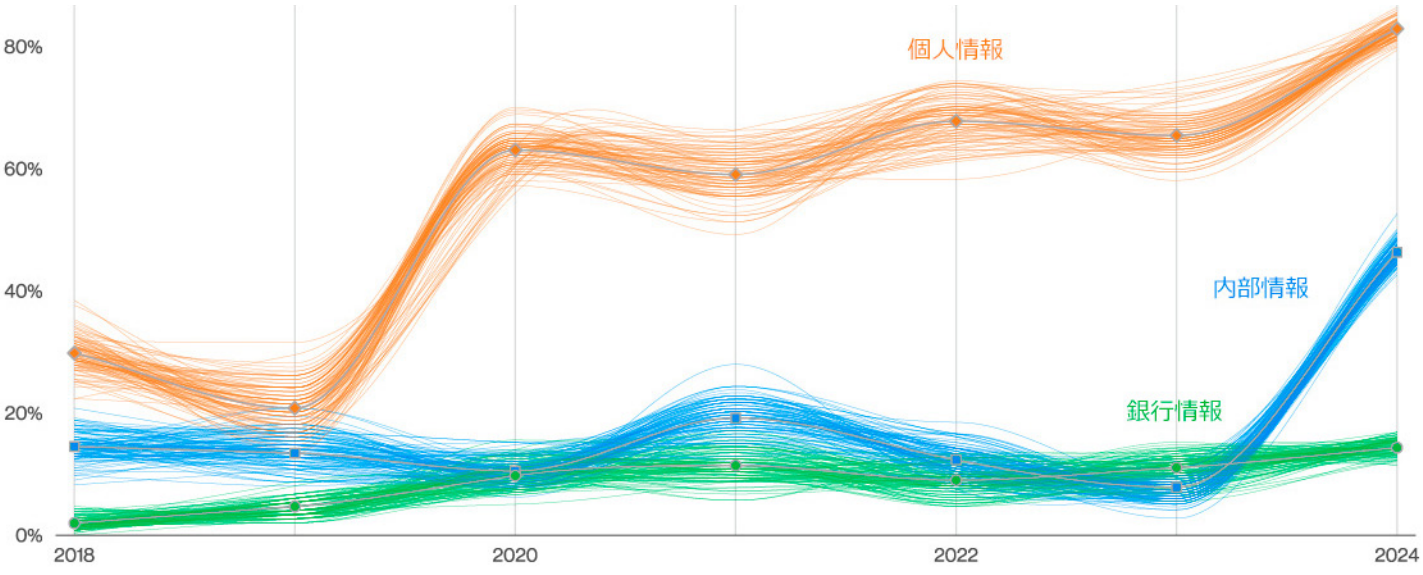


図55. 「特権の悪用」において上位を占める機密データ種類の経時的変化

4
業種別のハイライト

各業種のハイライト：概要

DBIRのこのセクションを今回初めてお読みになる方は、まずこの「概要」に目を通してください。過去のDBIRからご愛読されている方は、この説明はすでにお馴染の内容ですので、気軽に先へお進みください。

前述したように、本報告書では30,458件のインシデントを調査し、そのうちデータ漏洩/侵害が10,626件確認されています。以降のセクションでは、インシデントとデータ漏洩/侵害の2つのカテゴリーについて、さまざまな業種や地域での発生状況や被害状況をより詳しく解説します。これまでのDBIRでも述べたように、ある業種では夜も眠れないほど深刻であっても、別の業種ではレーダーにかすりもしません。それは、サイバー犯罪の格好の餌食となる「攻撃対象領域」に集約されるからです。特定のタイプの攻撃者の特徴、各業種を支えるテクノロジー基盤、組織が扱い保持するデータの種類、そのデータへのアクセスと運用などを考慮して、セキュリティ上の複雑な要素を混ぜ合わせた強力なカクテルができあがります。

例えば、モバイルデバイスとそれぞれのアプリを導入し、デジタル環境を整備しているハイテク大企業を考えてみましょう。そのリスクの特徴は、ベンダーがサポートするPOSシステムやシンプルなeコマースプラットフォームに依存する小規模なファッション小売業とは明らかに異なります。さらに、これらの調査結果は報告要件にも影響されるため、業種によってその観点からの精査のレベルが異なる可能性があります。最後に、業種によってはサンプルサイズが小さいことも、統計分析に関わる重要な要因となります（サンプルサイズが小さいと、統計的な信頼性も低くなります）。したがって、読者の皆様には、インシデントレポートの結果のみに基づいて業種のセキュリティ態勢について結論を急がないようお願いします。

各業種に特化したインサイトが必要な場合は、時間をかけて各業種の上位を占める攻撃パターンを確認し、本報告書の関連するパターンのセクションの説明を読み込むことをお勧めします。念のためお伝えしておきますが、DBIRの業種の分類は北米産業分類システム（NAICS）に基づいています。この分類についての詳細は付録Aをご覧ください。

	インシデント				データ漏洩/侵害			
業種	合計	中小企業（1～1,000人）	大企業（1,000人以上）	不明	合計	中小企業（1～1,000人）	大企業（1,000人以上）	不明
合計	30,458	919	1,298	28,241	10,626	617	986	9,023
宿泊および飲食業（72）	220	16	9	195	106	16	9	81
管理・支援及び廃棄物処理並びに除去サービス業（56）	28	7	7	14	21	6	4	11
農業（11）	79	5	0	74	56	4	0	52
建設業（23）	249	17	6	226	220	12	5	203
教育サービス業（61）	1,780	82	630	1,068	1,537	56	618	863
芸術、娯楽、およびレクリエーション業（71）	447	16	2	429	306	10	1	295
金融および保険業（52）	3,348	75	122	3,151	1,115	54	87	974
医療および社会福祉業（62）	1,378	54	21	1,303	1,220	41	18	1,161
情報産業（51）	1,367	79	62	1,226	602	49	19	534
事業経営業（55）	22	4	1	17	19	4	1	14
製造業（31-33）	2,305	102	81	2,122	849	62	49	738
鉱業、採石業、石油・ガス採掘業（21）	30	1	2	27	20	1	1	18
その他のサービス（81）	462	13	5	444	417	8	5	404
専門的・科学的・技術的サービス業（54）	2,599	205	102	2,292	1,314	124	73	1,117
公務（92）	12,217	56	115	12,046	1,085	39	27	1,019
不動産業、レンタル及びリース業（53）	432	35	5	392	399	29	2	368
小売業（44-45）	725	90	47	588	369	55	32	282
運輸および倉庫業（48-49）	260	21	38	201	138	17	12	109
公益事業（22）	191	17	11	163	130	12	6	112
卸売業（42）	76	22	21	33	54	17	14	23
不明	2,243	2	11	2,230	649	1	3	645
合計	30,458	919	1,298	28,241	10,626	617	986	9,023

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

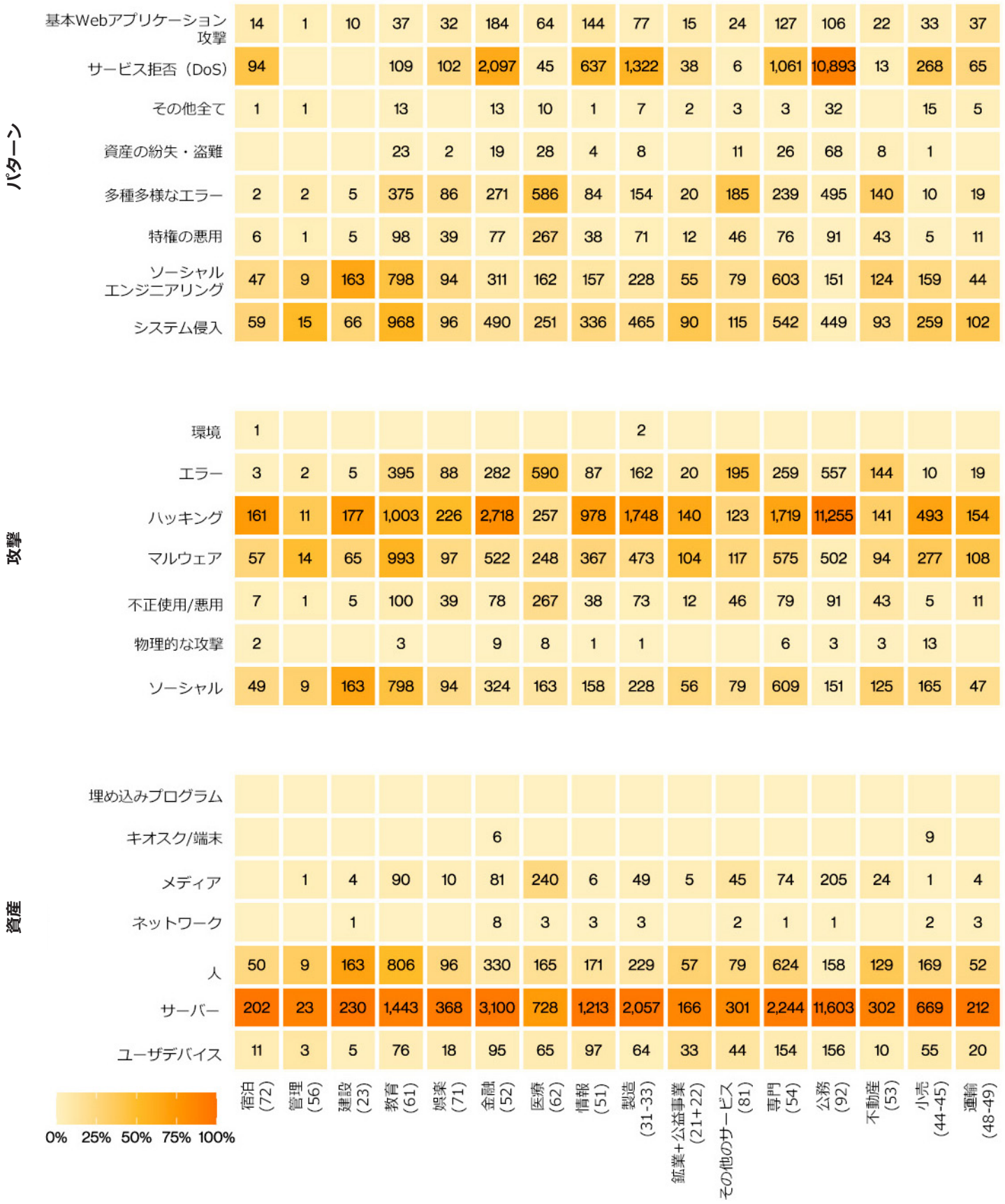


図56. 業種別インシデント

データ漏洩/侵害

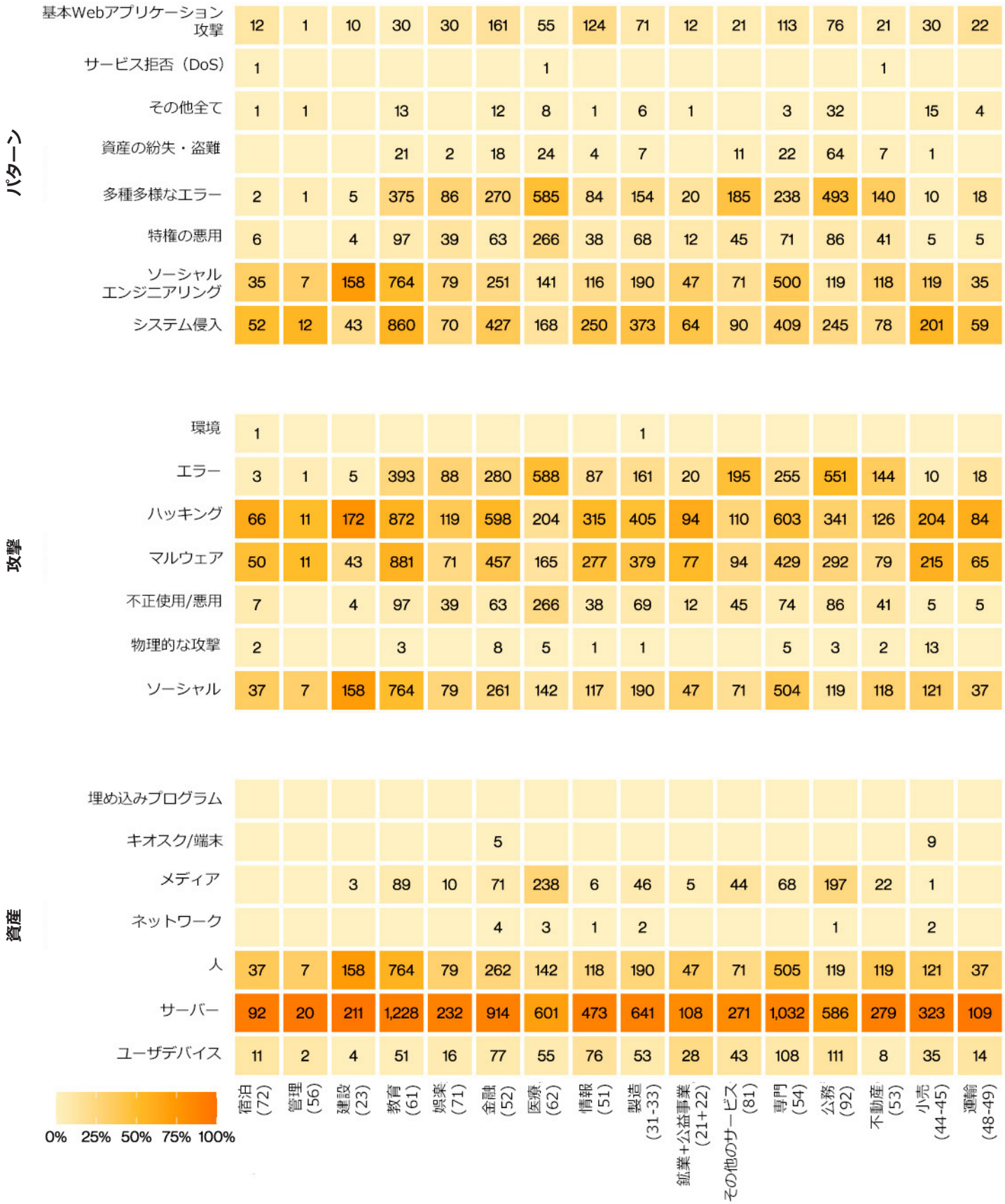


図57. 業種別データ漏洩/侵害

宿泊および飲食業 NAICS 72

頻度	インシデント220件、確認されたデータ漏洩106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（92%）、内部（9%）複数（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	認証情報（50%）、個人情報（28%）、決済情報（19%）、システム情報（19%）、その他（16%）（漏洩/侵害）
昨年との比較	ランサムウェアとソーシャル攻撃は、この業種では依然として根強い問題であり、インシデントの35%を占めています。

サマリー

「ソーシャルエンジニアリング」が劇的に増加しており、現在ではこの業種におけるインシデントの25%を占めています。そのうち「なりすまし」は昨年の2倍以上に増加し、インシデント全体でも20%を占めています。

データの流出

「第二の我が家」と呼べる地元の喫茶店は、いつも居心地の良さと安らぎを与えてくれますが、攻撃者にとっても同様に居心地が良い場所です。宿泊および飲食業は、「システム侵入」、「ソーシャルエンジニアリング」、「基本Webアプリケーション攻撃」を筆頭に、以前と同様に主要な脅威に直面しています。図58に見られるように、「ソーシャルエンジニアリング」攻撃は昨年から顕著に増加しています。これは主に「なりすまし」の増加によるもので、昨年に比べて2倍以上に増え、現在ではインシデント全体の20%を占めています。

苦労して稼いだお金をうっかり犯罪者に渡してしまったことがまるで被害とは言えなかったかのように、この業種は、限りなく無礼な客である「ランサムウェア」の攻撃者とも戦わなければならないのです。「ランサムウェア」は、ここ3年間ずっとトップクラスの攻撃です。ただし、状況の改善を挙げるとすれば、今年は増加がなく、全インシデントの16%で変化していないことだけです。

その他の状況については、「ペイメントカード」のデータ漏洩/侵害が過去最低となり、2023年には41%であったのが、今年は19%程度にとどまっています。この減少は、さまざまな業種において「ペイメントカード」データが狙われる件数の全体的な減少とよく一致しており、ICチップテクノロジーの採用により、攻撃者が他のアプローチに力を注ぐようになっていることを示しているのかもしれません。カプチーノをゆっくり味わえる良いニュースです。

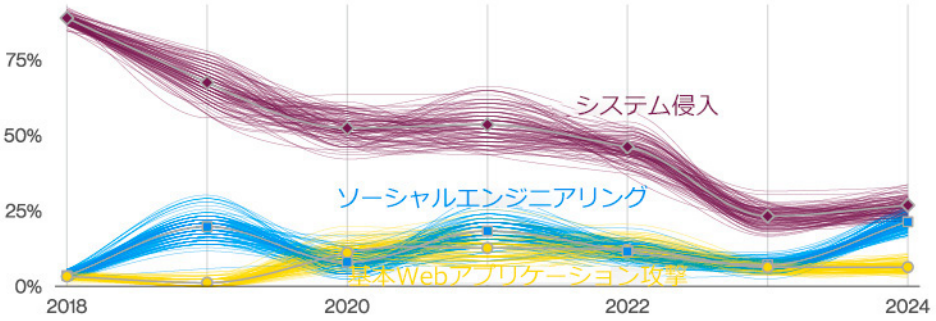


図58. 宿泊および飲食業におけるインシデントの上位を占めるパターン

教育サービス業 NAICS 61

頻度	インシデント1,780件、確認されたデータ漏洩1,537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」、「多種多様なエラー」が侵害の90%を占める
攻撃者	外部（68%）、内部（32%）（漏洩/侵害）
攻撃者の動機	金銭目的（98%）、スパイ活動（2%）（漏洩/侵害）
侵害されたデータ	個人情報（83%）、内部情報（20%）、その他（18%）、認証情報（9%）（漏洩/侵害）
昨年との比較	この業種では昨年と同じ3つのパターンが大半を占めています。個人情報を盗む「外部」の攻撃者がデータ漏洩/侵害の大半を占めています。

サマリー

内部攻撃者の犯行による「多種多様なエラー」と「外部」攻撃者者による「脅迫」が、引き続きこの業種の"カリキュラム"を構成しています。

失敗から学ぶ。

教育サービス業には、誇るべきものが数多くあります。最終的にはインターネットの誕生に重要な役割を果たし、誰もが知っている教科書業界を作り上げ、そしてもちろん、休み時間も作り上げたのは間違いなく最大の功績です。とはいえ、このような成功にもかかわらず問題がないわけではありません。Advanced Placement（米国における高校生の早期履修プログラム）レベルのデータ漏洩/侵害の調査結果に入る前に、まず改善の可能性が高い「エラー」セクションを取り上げます。図59によると、教育サービス業では、過去2年間「多種多様なエラー」パターンが増加傾向にあります。他の業種とは異なり「誤送信」がエラーの56%を占め、最前線で中心的な役割を果たしています。「紛失」（19%）と「分類ミス」（10%）がエラーの上位3つを占めています。

搾取されている気分だ。

さて「エラー」の話はここまでにして、次にこの業種における懸念事項の実態についてお話ししましょう。マルウェア（「バックドア」57%）、ハッキング（「脆弱性の悪用」56%）、ソーシャル（「脅迫」50%）攻撃の種類は、ほぼ同じ割合で存在しています。これはもちろん、「教育サービス業」にも例外なく、MOVEit（昨年多くの人々を悩ませた有名なファイル転送ソフトウェアの悪用）が"履修登録"されていたことを示しています。ご記憶にあるとおり、昨年の報告書では「ランサムウェア」がこの業種を席捲していましたが、「ランサムウェア」の最終段階は「脅迫」です。MOVEitの脆弱性を悪用した攻撃は、同じく「脅迫」を目標とする、巧妙さを増した[95]別の手口に過ぎません。MOVEitの悪用がこれほど多用されたために、「バックドア」が増加するのとは逆に「ランサムウェア」が減少しました。しかし、「教育サービス業」にとっての最終結果は同じでした。つまり、そのおかげで犯罪者は学生ローンを短期間で完済することができたということです。

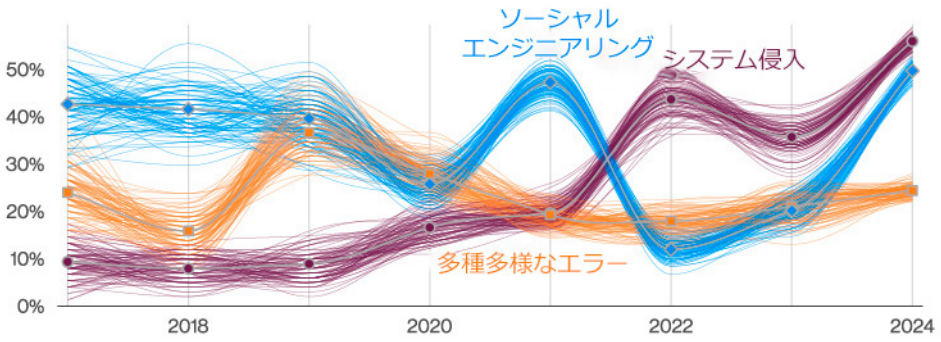


図59. 「教育サービス業」におけるデータ漏洩/侵害の上位３つのパターン

95 確かに、暗号化を見送った方が計算量は少なくて済みますが、攻撃者が環境に気を配っているとは誰が知っていたでしょうか？

金融および保険業 NAICS 52

頻度	インシデント3,348件、確認されたデータ漏洩1,115件
上位3つのパターン	「システム侵入」、「多種多様なエラー」、「ソーシャルエンジニアリング」が侵害の78%を占める
攻撃者	外部（69%）、内部（31%）（漏洩/侵害）
攻撃者の動機	金銭目的（95%）、スパイ活動（5%）（漏洩/侵害）
侵害されたデータ	個人情報（75%）、その他（30%）、銀行情報（27%）、認証情報（22%）（漏洩/侵害）
昨年との比較	「多種多様なエラー」は、この業種を悩ませ続けています。昨年同様、「誤送信」はこの業種にとって目の前の課題となっています。

サマリー

今年の「金融および保険業」においてトップの脅威は、「多種多様なエラー」と「基本Webアプリケーション攻撃」を抜いて「システム侵入」となり、「ソーシャルエンジニアリング」の増加とともに、より複雑な攻撃へシフトしていることを示しています。また、欧州・中東・アフリカ（EMEA）地域の状況把握が進んだため、「ランサムウェア」攻撃が同地区で健在であることが明らかになりました。

ジョージアの松のように高く

DBIRのデータセットが何らかの指標となるならば、「金融および保険業」で上昇しているのは金利と保険料だけではありません。一般的に複雑な攻撃が多い「システム侵入」パターンは、昨年の3位から今年は1位に上昇しています（図60）。複雑さが増す攻撃を代表する「ソーシャルエンジニアリング」パターンも同じく上位3つのパターンにランクインしている一方で、単純な「基本Webアプリケーション攻撃」（昨年は第1位）は、ランキングから完全に転落しています。これは、この業種では攻撃者が多大な労力をかけずに企業データにアクセスしていると指摘した昨年の調査結果と比較すると、まったく対照的な結果です。これらの変化は、この業種を侵害するために攻撃者が少し努力せざるを得なくなっていることを示しているかのようです。もちろん、攻撃者を除けば、誰にとっても朗報です。

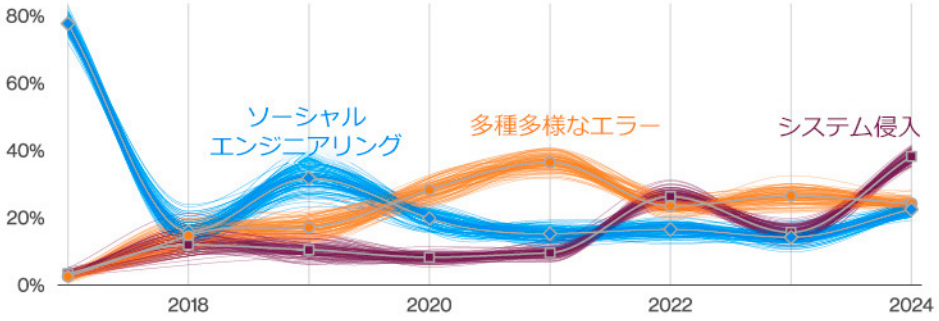


図60. 「金融および保険業」におけるデータ漏洩/侵害の上位３つのパターン

犯罪者を手助けするかのように、この業種は一貫して「エラー」を犯し続けています。今年はほぼ例外なく見られたように、「誤送信」が非常に目立ち（図61）、「設定ミス」、「紛失」とともに、この業種におけるエラーの大半を占めています。

対応策は取られているのか？

「攻撃」の種類に関しては、比較的明確にパターンが存在しています。「ランサムウェア」と「盗まれた認証情報の悪用」は「システム侵入」パターンの糧であり、この業種では非常に一般的です（そして「金銭目的の動機」95%を後押ししています）。これらの盗まれた認証情報はすべてどこからか入手しなければならず、それは主に「フィッシング」や「なりすまし」のようなソーシャル攻撃によるものです。もちろん、認証情報は、ブルートフォース攻撃（ハッキング攻撃のリストではかなり低いでしたが）、または単に別のデータ漏洩/侵害から入手して再利用するなど、他の多数のソースから取得されることもあります。

最後に、この業種をターゲットにしたインシデントデータセットのうち8%のケースがMOVEit絡みのデータ漏洩/侵害の渦中にあったことは特筆に値しますが、サプライチェーンへの侵害がいかに広範囲に及んでいるかを示しています。

図61. 「金融および保険業」のデータ漏洩/侵害において上位を占める「エラー」の種類（n=250）

医療および社会福祉業 NAICS 62

頻度	インシデント1,378件、確認されたデータ漏洩1,220件
上位3つのパターン	「多種多様なエラー」、「特権の悪用」、「システム侵入」が侵害の83%を占める
攻撃者	内部（70%）、外部（30%）（漏洩/侵害）
攻撃者の動機	金銭目的（98%）、スパイ活動（1%）（漏洩/侵害）
侵害されたデータ	個人情報（75%）、内部情報（51%）、その他（25%）、認証情報（13%）（漏洩/侵害）
昨年との比較	「システム侵入」によるデータ漏洩/侵害が、依然として攻撃パターンの上位3つに入っています。

サマリー

今年の「医療および社会福祉業」では、例年と比べて大きな変化が見られました。内部関係者が意図的に引き起こすデータ漏洩/侵害は、2018年以降着実に減少していましたが、再び2位に急浮上しています。興味深いことに、攻撃者が好む標的として「個人情報」が「医療情報」を上回っています。

業種の"容態"が急変している

もっとも、今年の「医療および社会福祉業」の変化を診断するのにレントゲン検査は必要ありませんでした。昨年と今年とでは健康状態に異なる点がたくさんあるので、詳しく診察していきましょう。2018年以降、この業種では悪意ある内部関係者による脅威が減少する傾向にありました（図62）。しかし、昨年はその傾向がいくぶん逆転し始めている様子が見られました。その後も内部関係者は失地回復を続け、今年は2位の座を占めています。昨年は「特権の悪用」が上位の3つにも入っていなかったことを考えると、これはさらに特筆に値する状況です。

その結果、「内部」の攻撃者はこの業種で主導的立場を取り戻したということです。「特権の悪用」という悪意ある犯行であれ、罪のない単なるミスであれ、今年のランキングでは「多種多様なエラー」がトップに躍り出る結果となり、内部関係者は業種内で鮮やかな復活を遂げつつあります。DBIRの他のほぼすべての業種と同様、最も犯しがちなエラーは「誤送信」（電子的、物理的手段を問わず、情報の送り先を間違うこと）です（図63）。「紛失」は第2位で、主な要因は紙文書の置き忘れですが、これは組織にも環境にも優しくありません。「失言」（DBIRチーム内でもよく起こる）は、口がすべって機密情報が他人の耳に入ってしまうことです。

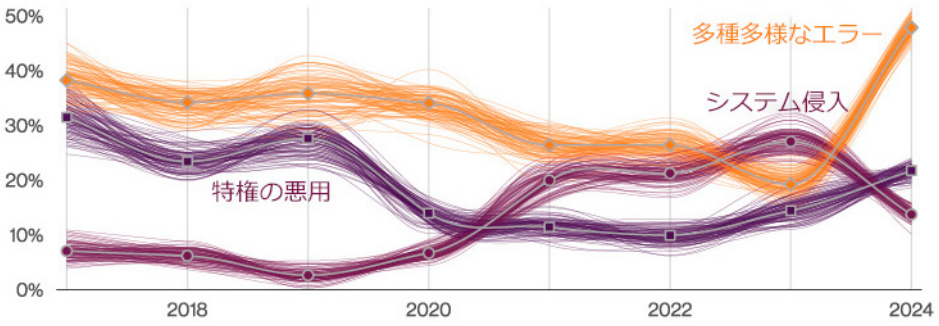


図62. 「医療および社会福祉業」におけるデータ漏洩/侵害の上位３つのパターン

最後に、DBIRチームにとって特に興味深かったのは、通常この業種で最もよく盗まれる「医療情報」が一顧だにされていないことです（図64）。攻撃者にとって、今年の流行は「個人情報」であり、バーサおばさんの外反母趾には関心がないようです。

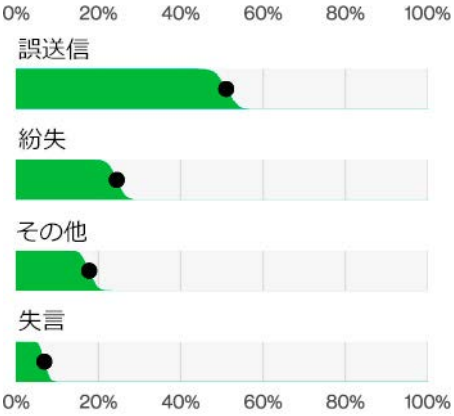


図63. 「医療および社会福祉業」におけるデータ漏洩/侵害の上位 3 つのエラーの種類（n=568）

図64. 「医療および社会福祉業」におけるデータ漏洩/侵害の上位 3 つの属性（n=1,102）

情報産業 NAICS 51

頻度	インシデント1,367件、確認されたデータ漏洩602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」が侵害の79%を占める
攻撃者	外部（79%）、内部（21%）、複数（1%）（漏洩/侵害）
攻撃者の動機	金銭目的（87%）、スパイ活動（14%）（漏洩/侵害）
侵害されたデータ	その他（46%）、個人情報（45%）、認証情報（27%）、内部情報（22%）（漏洩/侵害）
昨年との比較	上位3つの攻撃パターンは昨年と同じで、順位も変わっていません。昨年よりもデータ漏洩/侵害の件数が増加していることを考えると、少し興味深い結果です。

サマリー

データセット全体でデータ漏洩/侵害のサンプル数は昨年より増加していますが、この業種で発生したインシデントは大幅に減少しています。「システム侵入」のパターンでは、「ランサムウェア」と「盗まれた認証情報の悪用」が引き続き大半を占めていますが、「ソーシャルエンジニアリング」のパターンでは、「フィッシング」攻撃がわずかに減少し、「なりすまし」が増加しています。また、この業種を標的にした「スパイ活動」や、国家の支援を受けた攻撃者も若干増加しており、検知機能を強化する必要性が増しています。

本報告書の他の部分でも触れているように、データ漏洩/侵害のサンプル数は全体的に昨年よりも増加しました。ただし、「情報産業」で発生したインシデントは、今年は741件減少しました。一方、データ漏洩/侵害の件数は大幅に増加しました。この業種の上位３つのパターンは変わらず、その順位も同じです（図65）。

「ランサムウェア」と「盗まれた認証情報の悪用」（「システム侵入」のパターンの多くを構成する組み合わせ）も、予想どおり、依然として攻撃の種類の上位にランキングされています。「ソーシャルエンジニアリング」パターンのデータ漏洩/侵害に関しては、「フィッシング」攻撃が若干減少し、逆に「なりすまし」が増加しています。これは、攻撃者が標的に対してより巧妙な手口を使わざるを得なくなっていることを示す1つの指標かもしれません。

今年、特にEMEA地域ではこの業種のデータセットが大半を占め、北米地域の97件とは対照的に、243件のデータ漏洩/侵害が確認されています。これらのインシデントは、この地域で新設された法執行機関や規制機関のいくつかによってもたらされました。これこそ、データ保護規制が堅固であることの証です。

最後に、「スパイ活動」が若干増加しました（2023年の報告書の8%から14%に増加）。また、「国家機関」または「国家関連」の攻撃者も昨年の12%から15%へと増加しています。これは統計的には有意な数値ではありませんが、（たとえわずかであっても）自分の業種がより手口の巧妙な攻撃者にますます狙われるようになっていることは決して良い兆候とは言えません。とはいえ、標的にされた場合に早期に警告を出せるよう、検知機能を確実に整えるように注意喚起を促す数字ではあります。

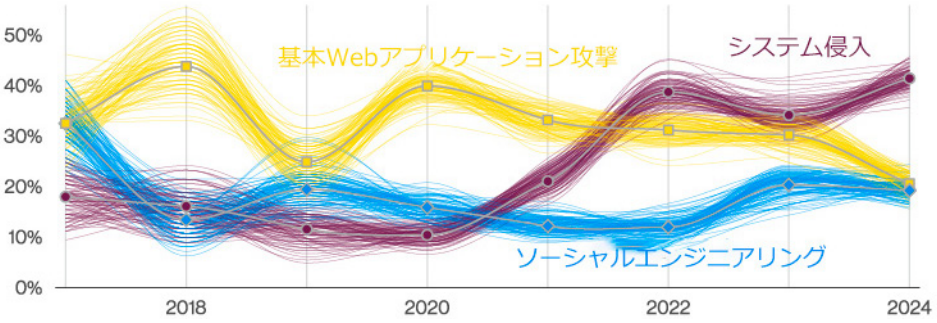


図65. 「情報産業」におけるデータ漏洩/侵害の上位３つのパターン

製造業 NAICS 31–33

頻度	インシデント2,305件、確認されたデータ漏洩849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」、「多種多様なエラー」が侵害の83%を占める
攻撃者	外部（73%）、内部（27%）（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	個人情報（58%）、その他（40%）、認証情報（28%）、内部情報（25%）（漏洩/侵害）
昨年との比較	昨年の上位3つのパターンのうちの2つがまだ残っており、「金銭目的」の動機がほとんどの攻撃の原動力となっています。

サマリー

「製造業」では「エラー」絡みのデータ漏洩/侵害が増加しています。「盗まれた認証情報を悪用」してハッキングした後に、マルウェアをインストールする手口がある程度普及しています。

今年のモデル

今年の「製造業」における"新機種"には、新しく改良された機能が搭載されています。それは、「エラー」です。他のほとんどの業種と同様、「誤送信」はまさにエラーの中のエラーであり、エラー絡みのデータ漏洩/侵害のほぼ半分（48%）を占めています。別のセクションで述べたように、これはデータ提供組織によって異なる部分もあるとはいえ、間違った宛先に物を送ることは業種に関係なくある程度広まっているようです。「紛失」と「設定ミス」は上位3つのエラーのうち、それぞれ約20%と18%を占めています。

「製造業」では「システム侵入」が引き続きトップの座を維持しています。これはおそらく、環境にアクセスするために「盗まれた認証情報を悪用」するハッキング（製造業におけるデータ漏洩/侵害の25%に見られます）と、「ランサムウェア」の豊富なアプリケーション（この業種におけるデータ漏洩/侵害の35%に見られます）という、依然として非常に効果的な組み合わせに関連しています。データが完全にロックされ、他の誰かが鍵を握っていれば、組立ラインから製品を生産し続けることは難しいです。

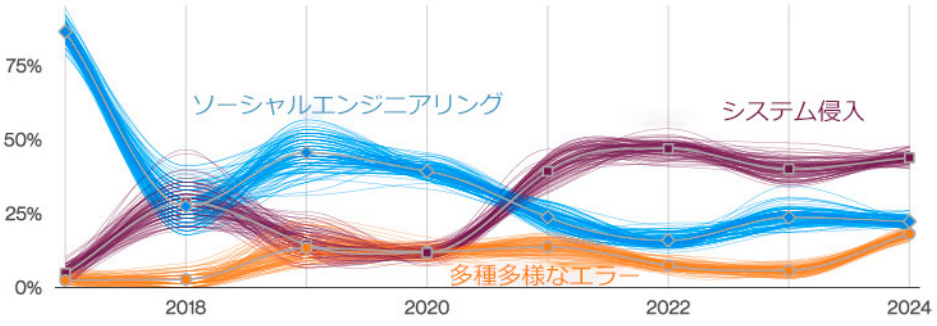


図66. 「製造業」におけるデータ漏洩/侵害の上位３つのパターン

（製造）ライン上にあるあなたの資産。

「ソーシャルエンジニアリング」は、「フィッシング」（55%）や「なりすまし」（42%）といった攻撃の多様性により、この業種におけるデータ漏洩/侵害の原因として安定しています。どうやら、消費者からのクレームで「基本Webアプリケーション攻撃」パターンがいかにも2022年ぽいという烙印を押されたようで、現在では「特権の悪用」のようなパターンとともに、パターンランキングの下位に甘んじています。実際、「Webアプリケーション（サーバー）」の攻撃は、やや減少傾向にあります。図67は、この減少を示すとともに、それに代わる「メール（サーバー）」の増加も示しています。上述のように製造業では「フィッシング」が依然として蔓延していることを考慮すると、この傾向は理にかなっています。もちろん、主にフィッシングによって入手される認証情報は、犯罪者が被害者のメールアカウントを使って組織に侵入する足がかりとなります。

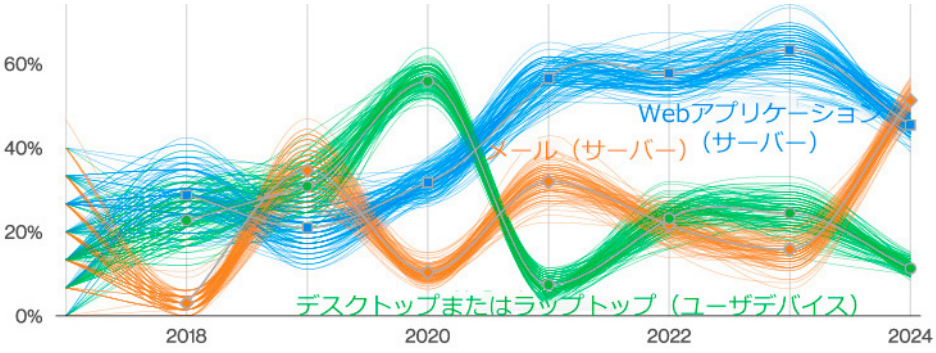


図68. 「製造業」におけるデータ漏洩/侵害の上位を占める「資産」の種類の経時的変化

図67. 「製造業」におけるデータ漏洩/侵害の上位を占める攻撃の種類

専門的・科学的・技術的サービス業 NAICS 54

頻度	インシデント2,599件、確認されたデータ漏洩1,314件
上位3つのパターン	「ソーシャルエンジニアリング」、「システム侵入」、「多種多様なエラー」が侵害の85%を占める
攻撃者	外部（75%）、内部（25%）（漏洩/侵害）
攻撃者の動機	金銭目的（95%）、スパイ活動（6%）（漏洩/侵害）
侵害されたデータ	個人情報（40%）、認証情報（38%）、その他（33%）、内部情報23%）（漏洩/侵害）
昨年との比較	この業種では、「個人情報」「認証情報」が依然として上位を占めています。

サマリー

「ソーシャルエンジニアリング」は、この業種が直面している最大の脅威の1つであり、データ漏洩/侵害の40%を占めています。また、「誤送信」などのエラーも増加しています。

広く網を張る

NAICSコードを使用するのは良いのですが、似たような業種をまとめるのに必ずしも理想的な方法ではないことは認識しています。この業種は特に、インテリアデザイナーからナノテク企業まで、多様な会社を網羅しているからです。この業種は、意図的であれ偶発的であれ、ほとんどの業種に影響を与えるタイプのデータ漏洩/侵害を示しています。では、内訳を詳しく見てみましょう。多くの業種と同様に「ソーシャルエンジニアリング」と「システム侵入」が上位に上がっていますが、図69に見られるように「多種多様なエラー」も含まれています。

意図的なデータ漏洩/侵害に関しては、その大部分が2つの攻撃パターンに仕訳けられます。「ランサムウェア」が24%、「ビジネスメール詐欺（BEC）」が20%です。「ランサムウェア」が上位3に入るのは今回が初めてではありませんが、「なりすまし」攻撃がこれほど躍進したのは初めてのことです。これらは昨年から大幅に増加しており、現在ではデータ漏洩/侵害の40%を占めています。最後に、組織がデータへのアクセスを守り続ける必要があるのは、データ漏洩/侵害の34%に「認証情報」が含まれているからです。

これらの認証情報は犯罪者にとってシステム侵入の足がかりとなる貴重なものですが、意図的でない（あるいはまれに悪意のある）内部関係者の存在も忘れるわけにはいきません。データ漏洩/侵害の25%が組織の内部関係者絡みによるものであったとしても、その大半は「誤送信」（12%）であり、個人の「特権を悪用」したもの（5%）はほんの一握りです。つまり、悪意のある人間よりも、不器用な人間の方が多いということを覚えておきましょう。

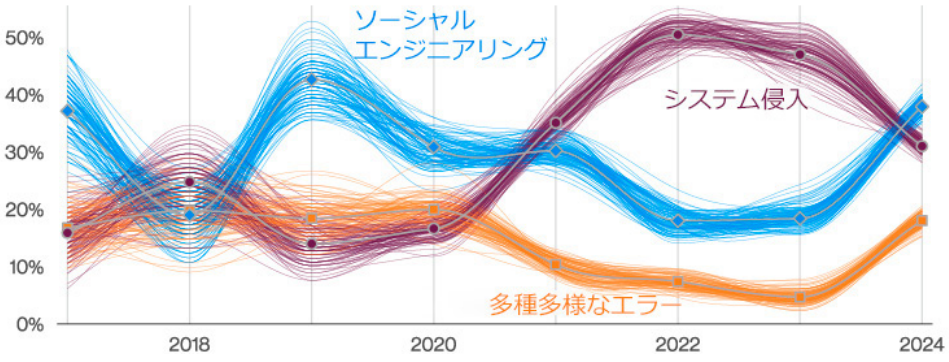


図69. 「専門・科学・技術サービス業」におけるデータ漏洩/侵害の上位３つを占めるパターンの経時的変化

公務 NAICS 92

頻度	インシデント12,217件、確認されたデータ漏洩1,085件
上位3つのパターン	「多種多様なエラー」、「システム侵入」、「ソーシャルエンジニアリング」が侵害の78%を占める
攻撃者	内部（59%）、外部（41%）（漏洩/侵害）
攻撃者の動機	金銭目的（71%）、スパイ活動（29%）（漏洩/侵害）
侵害されたデータ	個人情報（72%）、内部情報（37%）、その他（31%）、認証情報（17%）（漏洩/侵害）
昨年との比較	「システム侵入」と「ソーシャルエンジニアリング」の攻撃パターンが、依然としてこの業種の上位3つに入っています。

サマリー

この業種では「多種多様なエラー」、特に「誤送信」が急上昇しており、データ漏洩/侵害につながるミスの共通性を反映しています。「システム侵入」が第2位、「ソーシャルエンジニアリング」がそれに続きます。内部関係者による要因が圧倒的に多いことは、従業員の不注意がもたらす潜在的な結果を浮き彫りにしており、「エラー」がデータ漏洩/侵害の大半を占めています。

ミスを公表する義務

新しいデータ提供組織の中にはデータ漏洩/侵害開示の義務に従って報告する組織があったため、この業種では「多種多様なエラー」の攻撃パターンがトップに躍り出ました[96]（図70）。「公務」で最も多かったエラーは、デジタルデータまたは紙の書類形式を問わず、情報の送信先を誤った「誤送信」でした。頻繁に起こるのはメールの送受信ですが、印刷された文書や、奇妙なことにファックスでもよく発生します。昨年第2位の「紛失・盗難」は、「紛失」がかなり多い印象だったにもかかわらず、上位の3つには入っていません。

選挙公約よりも行動がものを言う

他の業種と同じく、「システム侵入」と「ソーシャルエンジニアリング」のインシデント件数は依然として多く、どちらもこの業種の2位、3位のパターンになっています。ハッキングは「公務」のデータ漏洩/侵害の31%にしか現れていませんが、攻撃者は依然として明らかに「盗まれた認証情報の悪用」に”投票”しており、ハッキング関連のデータ漏洩/侵害の83%に関与し、そのほとんどがWebアプリケーションへの攻撃でした。

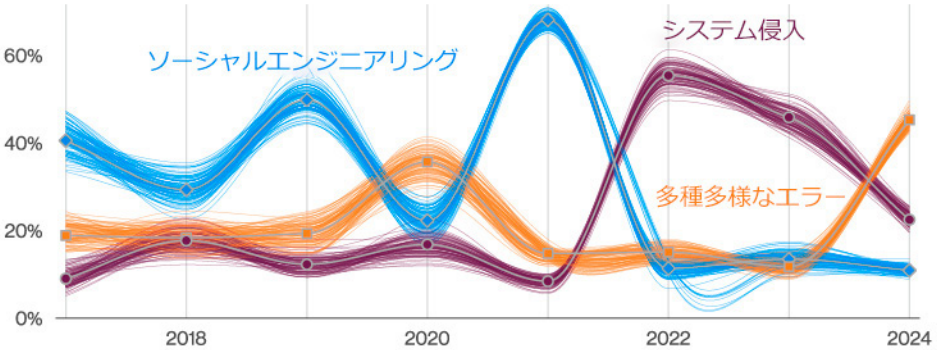


図70. 「公務」におけるデータ漏洩/侵害の上位３つを占めるパターンの経時的変化

96 「結果と分析」の「攻撃者」のセクションで、データ漏洩/侵害の報告が義務化されたことが、真に普及している漏洩/侵害の原因を理解する上で、どのように役立っているかを論じています。

今年の「公務」のデータ漏洩/侵害の27%は「マルウェア」によるものでした。他の多くの業種と同様、マルウェアの種類では「ランサムウェア」がトップとなり、マルウェア関連のデータ漏洩/侵害の61%を占めています。次に「バックドア」が38%を占め、さらに数種類のマルウェアが拮抗して3位の座を争っています（図71）。

「公務」への侵入を図る「ソーシャルエンジニアリング」による攻撃は、「フィッシング」（66%）と「なりすまし」（23%）がデータ漏洩/侵害の大半を占めています。気になる点は少なくありませんが、他の調査結果との関連では注目すべきほどのものではありません。

図72. 「公務」でのデータ漏洩/侵害におけるマルウェアの種類（n=243）

素行が悪い攻撃者

今年の一番の脅威が「内部」からの攻撃によるものという事実は、最も善意のある従業員であっても、注意を怠るだけでデータ漏洩/侵害を引き起こす可能性があるという事実を浮き彫りにしました。すべての攻撃者について、「エラー」が全データ漏洩/侵害の51%を占めているのに対し、悪意ある内部関係者は8%にすぎません。図73は、データ漏洩/侵害への道がいかに"善意"で舗装されているかを示しています。

エラー絡みのデータ漏洩/侵害とそれを引き起こした「エンドユーザ」を除いて、この公務に最もよく登場した外部攻撃者は「組織犯罪」（主に「ランサムウェア」攻撃）が67%と、「国家関連」の攻撃者（29%）でした。また、「スパイ活動」を企む攻撃者にはほとんど変化が見られませんでしたが、金銭目的を動機とする攻撃はわずかに増加しました。

図73. 「公務」のデータ漏洩/侵害において上位3つを占める攻撃の種類（n=1,088）

図71. 「公務」におけるデータ漏洩/侵害の上位3つを占める外部攻撃者（n=305）

小売業 NAICS 44–45

頻度	インシデント725件、確認されたデータ漏洩369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」が侵害の92%を占める
攻撃者	外部（96%）、内部（4%）（漏洩/侵害）
攻撃者の動機	金銭目的（99%）、スパイ活動（1%）（漏洩/侵害）
侵害されたデータ	認証情報（38%）、その他（31%）、決済情報（25%）、システム情報（20%）（漏洩/侵害）
昨年との比較	上位3つの攻撃パターンは変化がないだけでなく、順位も昨年と同じです。「金銭目的」を動機とする攻撃者によって依然と標的にされています。

サマリー

この業種では通常、「ペイメントカード」の情報が盗まれることが多いですが、攻撃者の焦点は「認証情報」に移りつつあります。「フィッシング」が減少する一方で、「なりすまし」が増加しています。「サービス拒否（DoS）」攻撃は、「小売業」にとって依然として悩みの種であり、顧客へのサービス提供や商品の販売に支障をきたしています。

「小売業」では「Magecart（マゲカート）」と呼ばれる攻撃者をよく見かけます。彼らは特に、小売企業のネットショップのサイトに悪意のあるコードを埋め込み、（通常は）顧客の「ペイメントカード」情報を吸い上げることに長けています。この種の攻撃は、今年も昨年とほぼ同じ割合で見られました（図74）。しかし、侵害されたデータの種類には驚くべき変化が見られました。

「認証情報」が昨年の35%に非常に近い38%でありながら、「ペイメントカード」のデータが37%から25%に下がったのは予想外でした。一般的な攻撃者にとって、「認証情報」がいかに魅力的で有用なものであるかは理解できますが、手っ取り早い詐欺行為に極めて有用な「ペイメントカード」のデータがこれほど急激に減少したことには驚きました（図75）。以前にも指摘したように、「何の」データが変化したかはわかっても、その変化の「理由」が明らかになるとは限りません。これは、ペイメントカード情報の収益化に関する対策が厳しくなり、犯罪者が盗んだ情報を使用することが難しくなった結果なのでしょうか？それとも、単に認証情報のほうが盗みやすくなっただけなのでしょうか？いずれにせよ、こうした状況が判明したのは一過性に過ぎないのか、それともトレンドが実際に始まっているのか、注目したいところです。

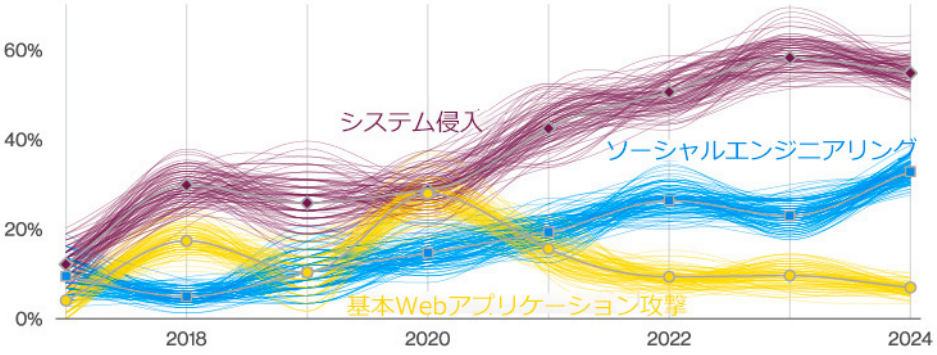


図74. 「小売業」のデータ漏洩/侵害において上位3つを占める攻撃パターンの経時的変化

図75. 「小売業」のデータ漏洩/侵害において上位 3 つを占めるデータの種類（n=341）

データ漏洩/侵害のソーシャル攻撃の種類では、「なりすまし」が「フィッシング」を抑えてトップとなりました。狙った標的に効果的な打撃を与えるために、攻撃者が方法を工夫せざるを得なかったことは評価できることです。人々へのセキュリティ教育が行きわたり、ありふれたフィッシングに抵抗できるようになったためと言えるでしょうか？不審なユーザコミュニティこそ、十分に保護されたユーザコミュニティです。

インシデントに関しては「サービス拒否（DoS）」が依然と深刻な問題となっています。この種の攻撃においてデータ漏洩が確認されることはほとんどありませんが、ビジネスを運営している組織の機能が著しく損なわれる可能性があります。また、「ランサムウェア」が関係するインシデントは2021年以降、減少を続けています。

5
地域別

地域別の分析

このセクションでは、改めて各地域のサイバー犯罪をマクロ的観点から考察します。世界のサイバー犯罪のトレンドが地域によってどのように異なり、またどのような共通性を持っているのか、読者の皆様が迅速かつ簡単に知るための一助となれば幸いです。いつものように、各地の情報開示規制、ベライゾンのデータセット、データ提供協力組織が事業を展開している場所など、さまざまな要因によって、それぞれの地域についての可視性は変動します。以下のページに記載されていない地域にお住まいの方やお仕事をされている方で、データ提供組織になることを希望される場合は、ベライゾンまでお問い合わせください。 また、あなたの地域の他の組織にも同じことを勧めてください。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不十分なことが主な要因であることをご了承ください。

世界の地域は、国連のM49基準[97]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）

NA（北アメリカ）：北アメリカ（021）。主に米国とカナダのデータ漏洩/侵害

読者の多くは、各主要セクションの上部に掲載されている「早見表」をご存じでしょう。下の表は、インシデントの発生頻度や上位のパターンなどに関して、各地域が他の地域と比較してどのような違いがあるのかを簡単にご確認いただけるようにまとめたものです。

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2,130件、確認されたデータ漏洩523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」が侵害の95%を占める	外部（98%）、内部（2%）（漏洩/侵害）	金銭目的（75%）、スパイ活動（25%）（漏洩/侵害）	認証情報（69%）、内部情報（37%）、機密情報（24%）、その他（17%）（漏洩/侵害）
欧州、中東、アフリカ（EMEA）	インシデント8,302件、確認されたデータ漏洩6,005件	「多種多様なエラー」、「システム侵入」、「ソーシャルエンジニアリング」が侵害の87%を占める	外部（51%）、内部（49%）、（漏洩/侵害）	金銭目的（94%）、スパイ活動（6%）（漏洩/侵害）	個人情報（64%）、その他（36%）、内部情報（33%）、認証情報（20%）（漏洩/侵害）
北アメリカ（NA）	インシデント16,619件、確認されたデータ漏洩1,877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」が侵害の91%を占める	外部（93%）、内部（8%）（漏洩/侵害）	金銭目的（97%）、スパイ活動（4%）（漏洩/侵害）	個人情報（50%）、認証情報（26%）、内部情報（19%）、その他（16%）（漏洩/侵害）

表3. 各地域の状況

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

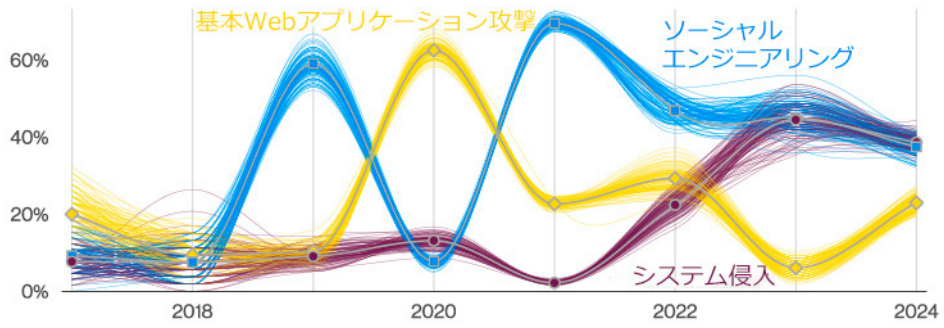


図76. APACにおけるデータ漏洩/侵害の上位3つを占めるパターンの経時的変化

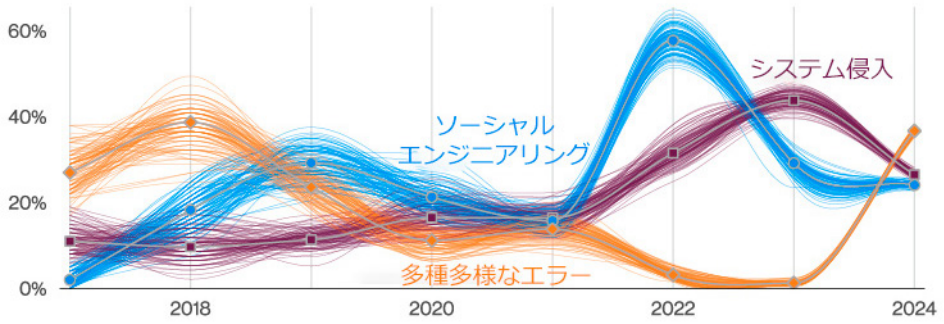


図77. EMEAにおけるデータ漏洩/侵害の上位3つを占めるパターンの経時的変化

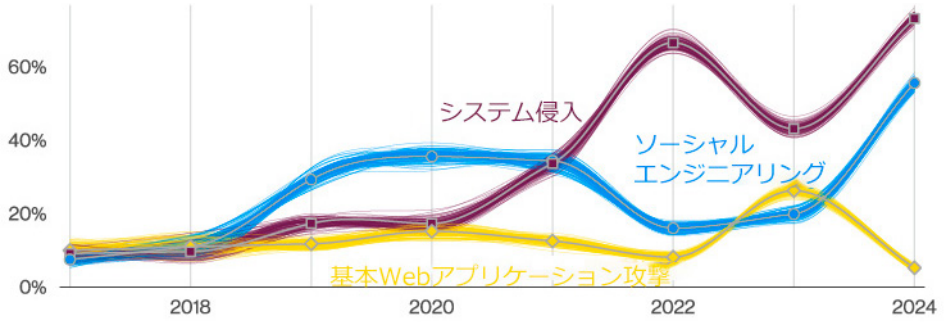


図78. NAにおけるデータ漏洩/侵害の上位3つを占めるパターンの経時的変化

4つのパラグラフで世界を表現

今年は、EMEAから新たなデータ提供組織が加わるという幸運に恵まれました。同地域の報告要件に加え、データ提供機関の性質上、「多種多様なエラー」のパターンが大幅に増加しました。現在EMEAで第1位の攻撃パターンとなるほどの増加を示しています。大きなデータセットを持っていたり、特定の攻撃タイプ（この場合はエラー） を報告する傾向がある協力組織が増えると、予想されるようなデータの歪みが生じます。おそらく来年になれば、この「多種多様なエラー」の急増が続くのか、それとも他の攻撃パターンと一致するように平準化されるのか、判断できるようになるでしょう。

「エラー」の多いデータセットを脇に置いて各地域を見てみると、「システム侵入」の攻撃パターンが依然として全地域でトップであることがわかります。いつものように、「システム侵入」のパターンで見られる2つの主な攻撃タイプは、「盗まれた認証情報の悪用」によるハッキングと「ランサムウェア」の形をとるマルウェア（これが最も多い）です。また、エラーを除外したデータセットでは、「システム侵入」のパターンが大きな上昇や下降は見せずに、昨年から比較的直線的な軌道を描いています[98]。

一方、「ソーシャルエンジニアリング」は、データセット全体で見ると、29%から45%へと大幅に増加しています（主に北米によるもので、データ漏洩/侵害の56%を占めています）。北米におけるこの増加の最大の要因は「脅迫」であり、データ漏洩/侵害全体の46%を占めています。その他の「ソーシャルエンジニアリング」については、北米での被害は低調を示し、「フィッシング」は13%、「なりすまし」は 4%でした。

98　金利とは違います。

攻撃者については、金銭目的を動機とする外部の者が依然としてサイバー犯罪の大半を占めています。特筆すべき例外はAPACで、この地域では90%以上の攻撃が金銭目的を動機とする一方で、「スパイ活動」という動機が他の地域よりも大きく、データ漏洩/侵害の25%も占めています（他の地域では4%～6%）。その結果、APACでは侵害されたデータのうち、「内部情報」が37%を占め、「機密情報」は24%となっています。

この種類のデータは、他の地域では通常、上位3位に入って来ることはありません。一方、APACでは「認証情報」が侵害されたデータの69%を占めています。昨年のDBIRで述べたように、私たちはどのような種類のデータが盗まれたかを頻繁に確認してはいますが、その理由を正確に説明する事情を常に詳しく把握しているわけではありません。

地域によって規制要件が異なり、その結果、データの種類によっては入手が難しいものがあることは十分承知しています。しかし、サイバー犯罪にとって「認証情報」と「個人情報」が重要な標的になっているのは一定の地域に限ったことではないのは明らかです。

Cyber Security Agency of Singapore（CSA）からのメッセージ

信頼性の高い回復力のあるサイバースペースを構築するには、政府と産業界の双方の力を結集した取り組みとパートナーシップが必要です。私たちは、すべてのユーザのためにサイバースペースの安全を確保するという責任を共有しています。サイバーセキュリティを多面的に強化するには、強力な官民のパートナーシップの構築が必要です。これには、可視性を高めるための脅威情報の共有、高度なサイバー脅威に対抗するための共同作戦の実施、あるいは必要とされる能力の開発への共同投資などが含まれます。

Cyber Security Agency of Singapore（CSA）が産業界との深いパートナーシップの構築に取り組んでいるのはこのためです。CSAは、当面のサイバーセキュリティ問題に官民共同で取り組むために、重要な業界のパートナーとの間でさまざまな覚書を交わしています。これらの覚書により、世界的な悪意のあるサイバー攻撃やプロパガンダキャンペーンの検知、シンガポールのユーザを一般的なマルウェア攻撃から確実に保護するためのモバイルセキュリティ対策の共同開発などに、力を合わせて取り組むことができます。たとえば、CSAはGoogleと提携し、マルウェアを利用した詐欺からアンドロイドのモバイルユーザを確実に守るために、Google Play Protectに強化された新しい保護機能を試験的に導入しました。この強化された保護機能は、金融詐欺や詐欺に頻繁に使用される機密性の高い権限の使用が必要なサイドローディングされたインターネットソース（ブラウザ、メッセージングアプリ、ファイルマネージャ）からのアプリのインストールを分析し、自動的にブロックするものです。

こうした協力関係は政策分野にも及んでいます。今年、CSAはシンガポールのサイバーセキュリティに関する法律を改定しました。今回の改定は、各業界のパートナーやその他の利害関係者と協議して実施されたものです。サイバー空間における新たな課題を理解するとともに、シンガポールでの規制の取り組みが政策意図を満たし、かつ実用的で、さまざまな主要サービス部門やデジタルインフラ/サービスにおいて顕著なサイバーセキュリティのリスクに見合ったものであることを確認にする方法について意見を求めたのです。

CSAは、産業界は協力して築くサイバーセキュリティにおいて重要な役割を担っており、自社の製品やサービスを設計や初期設定による保護から始めることができると固く信じています。この取り組みは、社会で最も脆弱なグループにとって特に重要です。このため、CSAはアプリ開発者やプロバイダーがモバイルアプリのセキュリティを強化できるよう、「Safe App Standard」を開発しました。DBIRの読者の皆様には、CSAのWebサイトからこれらのガイドラインなどにアクセスされることをお勧めします[99]。

CSAは、サイバースペースのセキュリティをさらに向上させるために、産業界とのパートナ ーシップを深めていきたいと考えています。

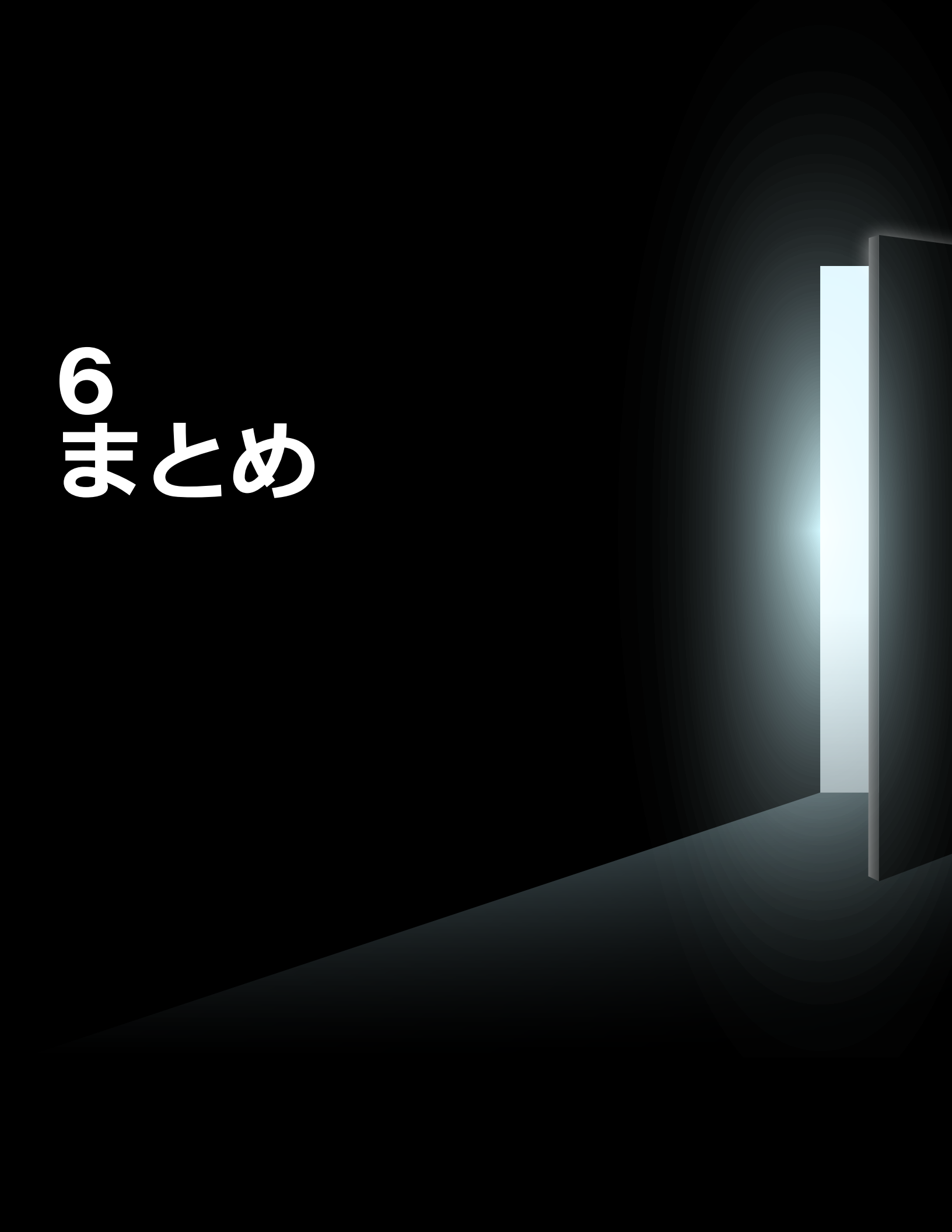
99 https://www.csa.gov.sg

図79. 地域別のインシデントとデータ漏洩/侵害

次に、図79のヒートマップに注目してください。「モナリザ」の絵画ほど魅惑的ではないかもしれませんが、少なくとも企業にとっては有用な図です。この図は、地域によって攻撃がどのように異なる（または類似している）かを示しています（「早見表」セクションのようなものですが、情報量は多くなっています）。ヒートマップは、インシデントとデータ漏洩/侵害について、上位３つの攻撃パターン、攻撃の種類、侵害された資産の種類に分類して表示しています。これは、地域における潜在的な問題領域を見つけるのに役立つ非常に便利な図です。

特に、業種や組織の規模など、本報告書に掲載されている他のデータと組み合わせることで、自分の組織が受けやすい攻撃を知る参考として、防御戦略の立案のお役に立てていただければ幸いです。

6
まとめ



今年のDBIRは以上で終了です。この情報が読者の皆様のお役に立ち、サイバー攻撃対策の参考にしていただけることを願っています。

人生は予測不可能なことが多くありますが、あらゆる事態に備えて可能な限り備えておくことが最も安全な道であることをDBIRは改めて示してくれます。本報告書が、どのような脅威がお客様の組織に影響を及ぼす可能性が最も高いかを予測し、リソースを適切に配備するための一助となれば幸いです。本報告書の作成にご協力いただいたデータ提供組織の方々に心より感謝申し上げます。そしてもちろん、読者の皆様には、時間を割いて本報告書をお読みいただくとともに、有益なご指摘をいただき、DBIRの改善に毎年多大なご協力をいただいていることに感謝いたします。

DBIRチーム一同、本年も皆様にとって安全で豊かな一年でありますよう、お祈り申し上げますとともに、2025年に再びお会いできることを楽しみにしております。

年間総括

VTRAC Monthly Intelligence Briefingsの月次報告のスナップショットです。さらに詳しい情報をご覧になりたい方は、お気軽にVTRACチーム（Intel.Briefing@verizon.com）までご連絡ください。

1月

1月にVTRACが収集したサイバーインテリジェンスでは、2023年の残りの期間を通じて繰り返し観測される情報セキュリティ（InfoSec）リスク問題のほとんどが反映されていました。ランサムウェアは変わりなくあらゆる業種を悩ませていました。例えば、LockBitの攻撃者は1月11日にRoyal Mailを攻撃してから6週間以上、英国の郵便業務を中断させました。メリーランド州ベルリンのAtlantic General Hospitalが、ランサムウェアに襲われた最初の医療機関でした。FortiOSのセキュアソケットレイヤー（SSL）VPN製品の脆弱性が中国のAPT（Advanced Persistent Threat）攻撃者に悪用され、政府系のネットワークとアフリカのマネージドサービスプロバイダーが攻撃を受けました。ロシアのAPT攻撃者がウクライナへの攻撃を続けていました。スピアフィッシングや偽装ログインページを使用して、COLDRIVERがブルックヘブン、アルゴンヌ、ローレンス・リバモアの国立研究所への侵入を試みました。パッチのリリース前に悪用された注目すべきゼロデイ脆弱性として、WindowsのAdvanced Local Procedure Call（ALPC）の特権昇格の脆弱性であるCVE-2023-21674と、SugarCRMのメールテンプレートのリモートコード実行の脆弱性であるCVE-2023-22952が含まれていました。月末には、Hiveランサムウェアの攻撃者を打破するために2022年7月に始まり、1,000人以上の被害者に復号鍵を提供していた多国籍作戦のニュースがもたらされました。

2月

Fortra社のGoAnywhere MFT（マネージドファイル転送）ソリューションにおける認証前コマンドインジェクションの脆弱性（CVE-2023-0669）は、月の第1週に発見されたゼロデイ脆弱性でした。数日のうちに、GoAnywhere MFTが絡んだ、Community Health Systemの100万件を超える患者の医療データが流出したことが判明しました。Cl0pランサムウェアグループは、1月18日からGoAnywhereを悪用して100社以上からデータを盗み出しました。この脆弱性はデータ漏洩/侵害に数か月間悪用されたましが、6月に別のマネージドファイル転送ソリューションであるProgress Software社のMOVEitに新たなゼロデイ脆弱性が発見され、これに取って代わられました。Microsoft社のパッチチューズデーには3件のゼロデイ脆弱性に対するパッチが含まれ、Apple社もWebKitのゼロデイパッチを適用しました。北朝鮮のAPTであるLazarus Groupは、医療研究、ヘルスケア、化学工学、エネルギー、防衛の各分野の組織や主要研究大学から100GB以上のデータを流出させた「No Pineapple！」攻撃を展開しました。カリフォルニア州オークランド市は、ランサムウェアへの感染により市のほとんどのサービスが停止したことを受け、非常事態宣言を発令しました。これに対し、PlayとLockBitの両方の攻撃者が成果を主張しました。

3月

3CX社はVoice over Internet Protocol（VoIP）のPBXソフトウェア開発会社で、その3CX Phone Systemは世界中で35万人以上の顧客に使用され、1,200万人以上のユーザが毎日利用してきました。デジタル署名され、トロイの木馬に汚染されたバージョンの3CX VoIPデスクトップクライアントが、進行中のサプライチェーン攻撃で同社の顧客を標的にするために使用されました。Lazarus Groupによると、最終的なペイロードはバックドア型トロイの木馬Gopuramでした。攻撃者は外科医のような精密な手際でGopuramを使用しました。Gopuramは10社に満たない標的にインストールされ、そのすべてが暗号通貨企業でした。3CX絡みの攻撃は、北朝鮮のAPT攻撃者によるかなり高度な能力を示していました。そして月末近く、北朝鮮の新たなAPT、APT43が出現しました。当初の報告によると、APT43はサイバー犯罪を利用してサイバースパイ攻撃の資金を調達していました。Winter Vivernは、ロシア/ベラルーシの国家安全保障上の利害と一致するAPTで、悪意のある文書を使用して認証情報を収集し、脆弱なZimbraコラボレーションサーバーを悪用していました。Winter Vivernの標的は、ウクライナを支援する国々の政府、軍事、外交機関などでした。3月のゼロデイ脆弱性には、Outlook、Microsoft Defender SmartScreen、Adobe ColdFusionなどがあり、パッチ管理チームが多忙でした。

4月

この月は、Apple社製品における2件のゼロデイ脆弱性の悪用で始まりました。Google社は、ChromeブラウザのV8JavaScriptエンジンのゼロデイ脆弱性を軽減し、その4日後にはSkiaグラフィックスエンジンのゼロデイ脆弱性を軽減する新バージョンをリリースしました。そしてMicrosoft社は、同社のCommon Log File Systemドライバーに今年2つ目のゼロデイパッチを適用しました。もう1つのゼロデイ脆弱性であるCVE-2022-27926は、Zimbraコラボレーションサーバーに影響をおよぼしました。この脆弱性は、パッチのリリースが発表される前に、Winter VivernというAPT攻撃者によって発見され悪用されていたのはほぼ確実でした。CERT Polskaは、ロシアのAPT29が、北大西洋条約機構（NATO）加盟国を中心に、多くの国の外交標的を積極的に追っていると警告しました。APT28は、世界中の脆弱なCiscoルータを攻撃していました。ネットワークインフラの4年前の脆弱性を悪用するというTTP（サイバー攻撃の戦術・技術・手順）は、革新的であると同時に、多くの攻撃者が採用し適応するのに十分なほど単純なものでした。GRUのSandstormハッカー集団が、ロシアのウクライナ侵攻の支援に引き続き注力していました。複数のトップクラスのサイバー犯罪者は、引き続きPaperCutとFortra GoAnywhere MFTシステムを侵害し、Cl0p、LockBit、BlackCat/ALPHVランサムウェアをインストールし、被害者のネットワークからデータを頻繁に流出させました。Microsoft社は、イランの攻撃者に起因するサイバー攻撃のペースが早くなり、攻撃範囲が広がっていることを指摘しました。たとえば、Mint Sandstorm（Charming Kitten）は、一般的な企業アプリケーションのN-day脆弱性を迅速に武器化し、高度に標的化されたフィッシング攻撃を実施し、関心のある環境に迅速かつ首尾よくアクセスしました。Mint Sandstorm APTは、概念実証（PoC）が公開されたのと同じ2023年1月19日に、Zoho ManageEngineのCVE-2022-47966の悪用を開始していました。

5月

Camaro Dragonという名の中国の国家支援型APTグループが、TP-Linkのルータに悪意のあるファームウェアを感染させ、攻撃者が検出を回避しながら感染したデバイスを完全に制御し、侵害されたネットワークにアクセスできるようにしていることが判明しました。このグループは、以前Mustang Pandaによる犯行とされた活動とも重なる部分があります。また、Mustang Pandaは、欧州の企業に対してフィッシング攻撃を実施していることも確認されています。また、他のフィッシングメールは、騙されたマシンにマルウェアをダウンロードする偽の「公式」ウクライナ政府報告書を配信していました。Mustang Pandaが最も多く使用していたのは、PlugXと呼ばれるトロイの木馬プログラムで、同グループが好んでスパイツールとして使用し続けていました。2021年半ば以降、グアムや米国内の重要インフラ組織を標的としていることが確認され、中国と連携する新たなAPT攻撃者としてVolt Typhoonが特定されました。Barracudaは5月19日、同社のメールセキュリティゲートウェイ（ESG）機器にゼロデイ脆弱性（CVE-2023-2868）を発見しました。この脆弱性を解消するセキュリティパッチは、5月20日に世界中のすべてのESG機器に適用されました。Microsoft社のパッチチューズデーには、2件のゼロデイ脆弱性が含まれていました。Apple社は、WebKitに影響する3件のゼロデイ脆弱性を含む、30件以上の脆弱性を緩和するセキュリティ勧告とパッチをリリースしました。5月31日、Progress Software社 は、マネージドファイル転送ソフトウェアMOVEit のSQLインジェクションの脆弱性を修復するパッチをリリースしました。CVE-2023-34362とラベル付けされ、5月27日に悪用が始まったことが後に判明しました。

6月

MOVEitの悪用が拡大し始めました。VTRACは多数の被害報告を受けるようになり、2024年2月に本報告書が発行された時点でも被害報告を受け続けていました。（MOVEitは1年を通して大混乱を引き起こし続け、複数のサイバーセキュリティ専門家が、被害を受けた組織や個人の数が増加していると報告しています）[100、101、102、103]。Cl0pランサムウェア攻撃者が2021年にMOVEitの不正プログラムをテストしていた形跡がありました。少なくとも1,000の組織が被害者となり、少なくとも1億人の「個人を特定できる情報（PII）」が漏洩しました。ロシアのAPTであるGamaredon Groupが、PowerShellベースの情報窃取ツールをマルウェアが仕込まれたUSBメモリで配布し、ウクライナを攻撃しました。Google社は、すでに悪用されていたV8 JavaScriptエンジンの脆弱性を軽減するため、Chromeブラウザの新バージョンをリリースしました。FortinetのFortiOSおよびFortiProxyのSSL-VPN事前認証に存在するゼロデイ脆弱性が悪用されていました。CVE-2023-2868に関する5月の警告発表の後、6月6日にBarracudaは、侵害されたESGアプライアンスはサービスを停止して廃棄する必要があると発表しました。Kaspersky社のセキュリティアーキテクチャによって、複数のiOSベースの携帯電話から発信された不審なアクティビティが検出されました。同社は「Operation Triangulation」と呼ばれる標的型APT攻撃を発見しました。ターゲットのiOSデバイスが、不正プログラムが埋め込まれた添付ファイル付きのゼロクリックメッセージをiMessageサービス経由で受信しました。このメッセージはユーザによる操作を必要とせず、コード実行につながる脆弱性を誘発しました。APTペイロードのインストール後、メッセージは削除されました。6月21日、Apple社はiOSカーネルとWebKitのゼロデイ脆弱性「Operation Triangulation」にパッチを適用しました。

100 7月：https://techcrunch.com/2023/07/27/us-government-contractor-says-moveit-hackers-accessed-health-data-of-at-least-8-million-individuals

101 8月：https://techcrunch.com/2023/08/25/moveit-mass-hack-by-the-numbers

102 11月：https://www.cpomagazine.com/cyber-security/more-fallout-from-moveit-data-breach-documented-632000-emails-from-us-departments-of-defense-and-justice-accessed-by-russian-hackers

103 12月：https://www.techradar.com/pro/security/the-moveit-breach-may-well-have-been-the-biggest-cyberattack-of-the-year

7月

ランサムウェア攻撃者のトップ3にとって素晴らしい7月でした。したがって、InfoSec実務担当者はLockBit、Cl0p、ALPHVによる攻撃を回避し続けるために7月の1か月を費やしました。7月4日（月）、日本の名古屋港がLockBit 3.0に襲われました。Cl0pは、MOVEitにパッチが適用される前の5月と6月に侵入した130以上の組織を引き続き利用していました。ALPHV（BlackCat）は、検索エンジン最適化（SEO）ポイズニングと不正広告を利用してユーザを誘い、トロイの木馬化されたWinSCP（Windows Secure Copy Protocol）をダウンロードさせ、広範囲な悪用、データ窃取、ランサムウェア感染を引き起こしました。Storm-0558と名付けられた中国のAPTは、一連の判別困難な抜け穴を利用して、Microsoft社のエンジニアのシステムからMicrosoftアカウント（MSA）のコンシューマーキーを取得しました。このキーにより、OutlookおよびOutlook Web Access（OWA）アカウントへのアクセスが可能となり、政府機関を含む約25の組織に影響を与えました。Microsoft社のパッチチューズデーでは、5件のゼロデイ脆弱性が修復されました。Zimbra Collaboration Suiteには、データの機密性と完全性に影響を与えるクロスサイトスクリプティングのゼロデイ脆弱性が含まれていました。Adobe社は、パッチチューズデーにColdFusionのアップデートをリリースしました。その3日後、Adobe社はColdFusionのデシリアライゼーションに関するゼロデイ脆弱性について、緊急でセキュリティ情報をリリースしました。Ivanti Endpoint Manager Mobileの新たなゼロデイ脆弱性2件が悪用され、ノルウェーの12省庁のITシステムが侵害されました。Citrix社は、NetScaler（旧Citrix）のアプリケーションデリバリコントローラ（ADC）とNetScaler Gatewayの脆弱性3件に対するセキュリティアドバイザリとパッチをリリースしました。CISAは、6月にNetScalerの脆弱性が1件悪用され、米国の重要インフラ組織のネットワークが侵害されたことを報告しました。8月2日には、640台のNetScalerサーバーが正体不明の攻撃者によってバックドア化され、China ChopperのWebシェルがインストールされていたことが判明しました。

8月

複数の情報源から、20%～33%の範囲でのランサムウェア攻撃の減少が報告されました。台湾の数十の組織を標的とした継続的なスパイ活動が発見されました。研究者は、この活動は「Flax Typhoon」という名の新しい中国のAPTグループによるものであるとしています。このAPTグループは、カスタムマルウェアの使用を最小限に抑え、代わりに被害者のオペレーティングシステムに存在する正規のツールを使用して（Living off the land：現地調達で）スパイ活動を行なっています。VTRACは、Carderbeeという別の新しいAPTの情報を収集しました。このAPTは、中国のセキュリティ企業の更新プログラムを悪用しサプライチェーン攻撃を行い、PlugXバックドアのコード署名バージョンをインストールして、主に香港にある約100台のコンピューターを攻撃しました。北朝鮮の Lazarus Groupは、新たなリモートアクセス型トロイの木馬（RAT）であるQuiteRATとCollectionRATを実戦投入し、Lazarus Groupが「現地調達した」TTPに移行している痕跡を残しました。FBIは、Qbot（別名Qakbot）に対する国際的なセキュリティ対策活動を発表しました。FBIが主導するこの「Duck Hunt」作戦では、ボットネットを掌握し、感染したデバイスからマルウェアを駆除し、影響を受けたシステムの相当数を特定しました。多くのマルウェア駆除と同様、中心的なサイバー犯罪者は逮捕も拘束もされなかったため、Qbotは12月に再び活動を開始することになります。Microsoft社のパッチチューズデーには、悪用された2つのゼロデイ脆弱性の軽減、CVE-2023-38180（パッチ適用済み）とCVE-2023-36884（パッチ未適用）が含まれていました。

9月

Caesars Entertainment社は9月7日、ALPHVランサムウェア攻撃者が、外注のITサポートベンダーを標的としたソーシャルエンジニアリング攻撃を行い、Caesars社のネットワークと、多くの顧客の運転免許証番号と社会保障番号を保存しているロイヤルティプログラムのデータベースに侵入したことを発見しました。Caesars社はデータ復旧のため、3,000万ドルの身代金の約半分を支払うことを選択しました。9月11日、MGM Resorts International社は、ALPHVランサムウェア攻撃者がソーシャルエンジニアリングを活用してMGMのネットワークに侵入し、機密データを盗み出し、さらに100台以上のESXiハイパーバイザーを暗号化したことを公表しました。MGMは、このサイバー攻撃により1億ドルの損害を被ったとSECに報告しました。Akiraランサムウェア攻撃者は、組織に侵入するためにMFAが設定されていないCisco VPNを標的としていました。Cisco社は、Cisco Adaptive Security Appliance（ASA）SoftwareおよびCisco Firepower Threat Defense（FTD）のリモートアクセスVPN機能に脆弱性があり、リモートの認証されていない攻撃者が有効なユーザ名とパスワードの組み合わせを特定しようとブルートフォース攻撃を行う可能性があるとして、セキュリティアドバイザリを公開しました。Cisco社は、すでに8月に、この脆弱性を悪用しようとする動きがあることに気づいていました。トロント大学のCitizen Labは、iOSのゼロデイ脆弱性が悪用され、NSOグループの商用スパイウェア「Pegasus」がインストールされたことを報告しました。Microsoft社のパッチチューズデーには、2つのゼロデイ脆弱性が含まれていました。WebPコーデックは数えきれないほど多くのアプリケーションやWebサイトで使用されており、ゼロデイ脆弱性が攻撃されたことをApple社とGoogle社から報告されました。Adobe社は、Adobe AcrobatとReaderに存在するゼロデイリモートコード実行の脆弱性を軽減するために、緊急でセキュリティアドバイザリとパッチをリリースしました。

10月

Okta社は、10月19日に非公開の顧客に対して送信したセキュリティアドバイザリで、「盗まれた認証情報の悪用によりOktaのサポートケース管理システムにアクセスする敵対的行為を確認した」と発表しました。Okta社の広報担当者によると、同社は1PasswordやCloudflareを含む顧客ベース（170以下の顧客）の約1%に通知したとのこでした。10月7日、ハマスがイスラエルに侵攻し、大きな動揺を引き起こしました。1時間経たぬうちに、ロシア系グループAnonymous Sudanが、ミサイル攻撃を市民に警告するイスラエルの民間アプリを無効にした可能性があるとして犯行を主張しました。それぞれの紛争当事者に属するハッカーたちは、ハック＆リークや改竄だけでなく、DoS攻撃も行い始めました。ほとんどの場合、国家と連携したAPT攻撃者は、ハマスやイスラエルを攻撃の標的としたサイバー紛争活動は限定的か、あるいはまったく行っていませんでした。Atlassian社のConfluence Data Centerと Confluence Serverを使用している組織から侵害の報告がありました。Atlassian社は、ゼロデイアクセス制御の脆弱性CVE-2023-22515が悪用されていると判断しました。Apple社はiOSとiPadOSのアップデートをリリースし、さらに2つのゼロデイ脆弱性に対処しました。Microsoft社のパッチチューズデーでは、104件のセキュリティアップデートの中に3件のゼロデイ脆弱性が含まれていました。Cisco社と複数の情報ソースは、Cisco IOS XEソフトウェアの2つのゼロデイ脆弱性を悪用した攻撃（アカウントを新規作成し、マルウェアを遠隔操作で埋め込む）を追跡しています。

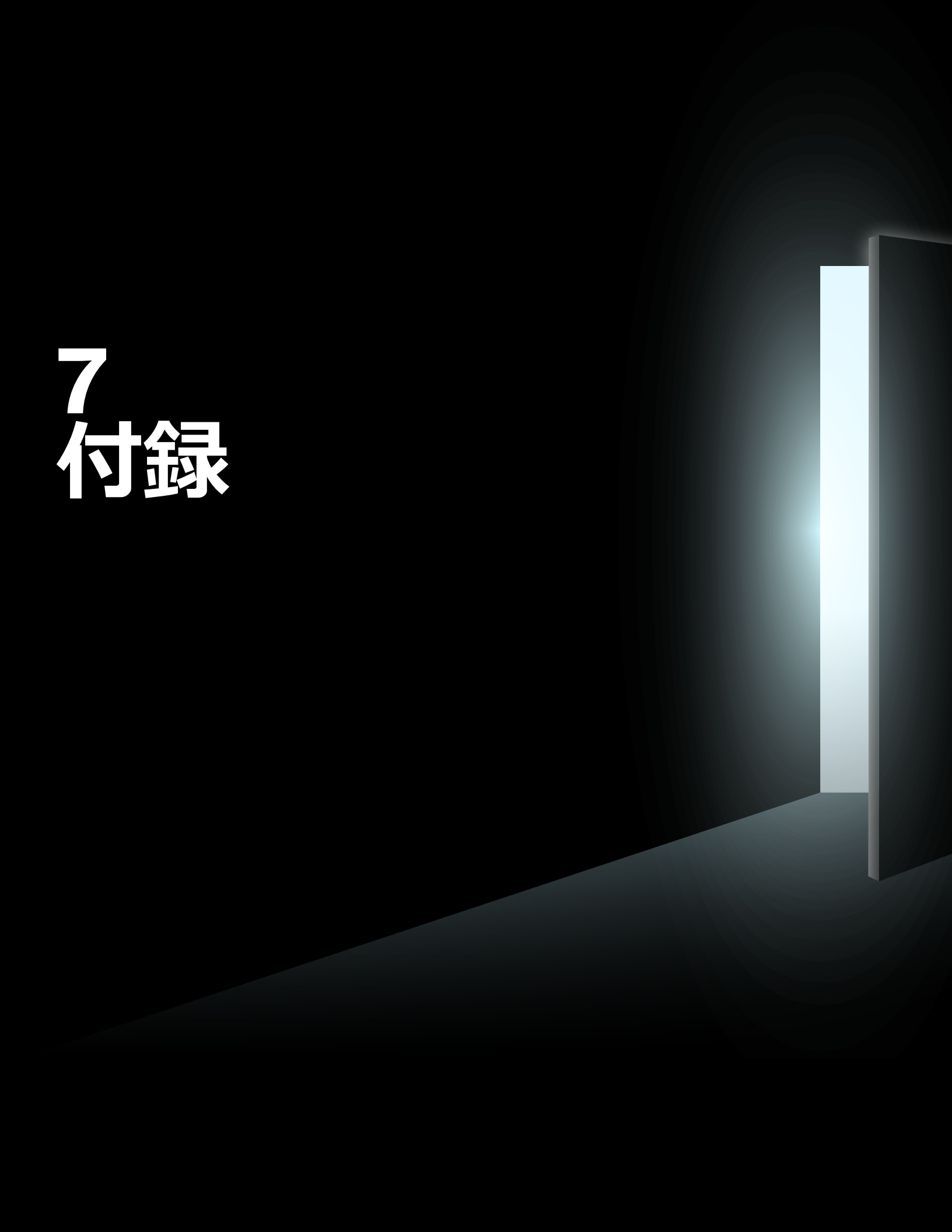
11月

9月と10月に観測されたランサムウェア攻撃の件数が大幅に減少した後、11月にはその件数が予想以上に再び上昇しました。有名な金融系マルウェアであるCarbanakが、APT級のサイバー犯罪者であるFIN7によってコントロールされ、比較的注目されていない状態から復活しました。複数の情報源は、FIN7をCarbanak、Cl0p、ALPHVランサムウェアの攻撃者と結びつけていました。HelloKittyランサムウェアは、人気のあるオープンソースのマルチプロトコルメッセージブローカーであるApache ActiveMQのゼロデイ脆弱性を攻撃していました。Cl0pランサムウェアは、ITサービス管理ソフトウェアSysAidのゼロデイ脆弱性を悪用していました。ロシアのAPT Sandwormグループが、デンマークの22の重要インフラ組織に対する攻撃に関与していました。11月のパッチチューズデーは77件のMicrosoft社パッチに対応し、そのうち、悪用されていた新らしい3件のゼロデイ脆弱性のためにMicrosoft社がリリースしたパッチが含まれていました。F5 Big IPの脆弱性2件が、セキュリティ勧告とパッチのリリースから5日以内に攻撃されていました。Chromeブラウザと複数のApple製品にゼロデイ脆弱性のパッチが適用されました。中国のAPT「Mustang Panda」が、フィリピンと環太平洋西部地域の組織を標的としたサイバースパイ活動を実行しました。

12月

イスラム革命防衛隊（IRGC）に所属するハッカー攻撃者「Cyber Av3ngers」が、ペンシルバニア州アリキッパ市水道局のワークステーションを改竄しました。この攻撃者は、ユニトロニクスのPLC機器を標的として、米国内の複数の水道事業会社を攻撃したと報じられました。ウクライナ最大の移動体通信事業者であるKyivstar社が、サイバー攻撃を受けて同社のシステムインフラに甚大な損害が生じ、数日間にわたって操業不能に陥りました。以前から悪名高いSandwormグループとつながっていたSoIntsepek攻撃者が、1日後に攻撃を行なうと宣言し、1万台のコンピューター、4000台以上のサーバー、すべてのクラウドストレージ、バックアップシステムを破壊した攻撃成果を主張しました。Google社のChromeブラウザ、QNAP社のネットワークビデオレコーダーVioStor、Future X Communicationsの無線LANルーターAE1021PEとAE1021はそれぞれ、すでに出回って悪用されていた新たな脆弱性にパッチを適用しました。Barracuda社のESG機器には、ゼロデイ脆弱性があり、中国の攻撃者によって悪用されていました。月の中旬に、Microsofts社は、Qbot（Qakbot）が国税庁職員からのメールを装ったフィッシング攻撃で再び配布されていると警告しました。

7
付録



付録A：
本書の凡例と定義

2024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付録をお読みいただくことをお勧めします。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、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/2024**—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

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80～図83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）。

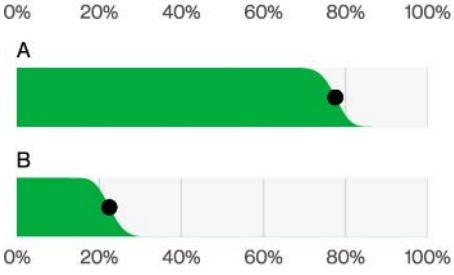


図81. 斜めカットの棒グラフの例（n=205）

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。

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

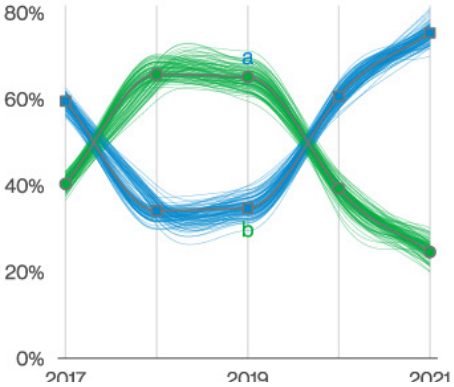


図80. スパゲッティチャートの例

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。

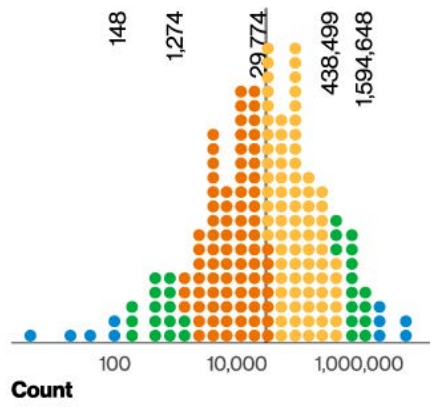


図82. ドットプロットの例（n=672）。各ドットは組織の0.5%を表す。オレンジ：80%の下半分。黄色：80%の上半分。緑：80%–95%。青：異常値。組織の95%：148–1,594,648。80%：1,274–438,499。中央値：29,774（対数スケール）

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。

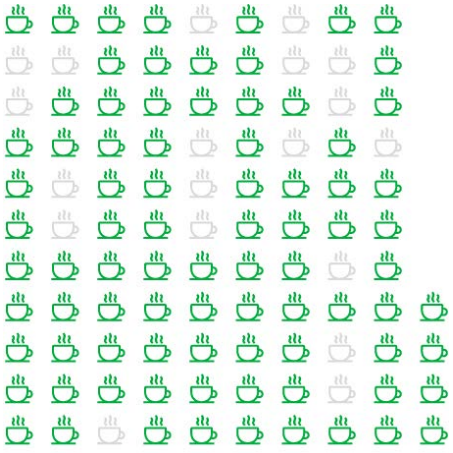


図83. ピクトグラムプロットの例（n=4,110）。それぞれ図柄は40のデータ漏洩/侵害

付録B：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1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、私たち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、私たちは間違いを犯します。コラムが入れ替わっていたり、数字が更新されていなかったりなど、修正すべき点がいくつか見つかるかもしれません。その際にはその都度、以下の修正ページにリストアップします。https://verizon.com/business/resources/reports/dbir/2024/corrections.

次に、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。ただし、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、このことに関する私たちの自信は、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

私たちの全般的な手法はここ数年ほとんど変わっていません[104]。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。

104 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。私たちは、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（サンプルには未報告のデータも含まれます）。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84～87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、データ提供組織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組織間で、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

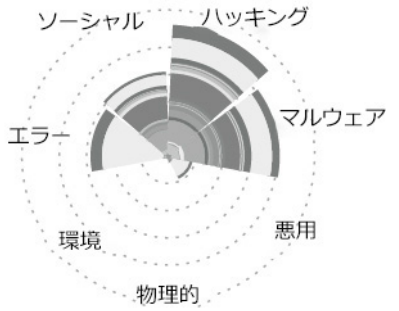


図85. 攻撃別の各貢献度

データ漏洩/侵害

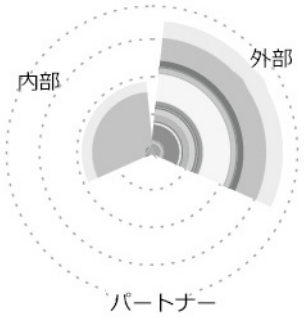


図84. 攻撃者別の各貢献度

データ漏洩/侵害

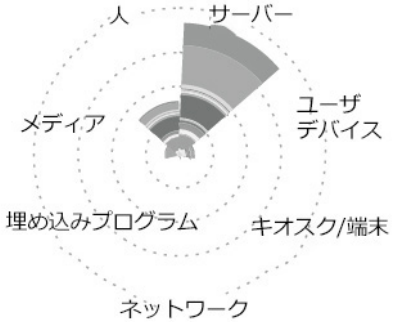


図86. 資産別の各貢献度

データ漏洩/侵害

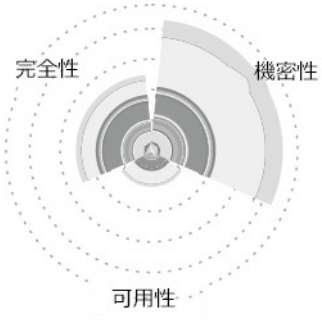


図87. 属性別の各貢献度

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組織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組織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）[105]。

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。

105 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C：米国シークレットサービス

米国シークレットサービス、アシスタントディレクター Brian Lambert氏および特別捜査官補Krzysztof Bossowski氏

技術革新の中でのサイバー犯罪対策

米国シークレットサービスは、2023年、新たなテクノロジーによって引き起こされる新たな脅威を特定しつつ、従来の手法で詐欺対策に取り組みました。ランサムウェアは引き続き、米国企業に影響を与えるデータ漏洩/侵害において際立っていました。一方、国際的なサイバー犯罪者はますます、詐欺を可能にする画期的な方法を見出すことに成功していました。人工知能（AI）は世界の注目と想像力を惹きつけ、サイバー犯罪者はいち早くこれを活用しています。シークレットサービスでは、詐欺を実行するためにこれらの新しい生成ツールを試している多数のサイバー犯罪者を調査しました。結果、これらの詐欺師が詐欺のために利用しているのと同じテクノロジー企業と提携しました。これは、詐欺を発見し、悪質な攻撃者に責任を負わせるための貴重な戦略であることが証明されたのです。

シークレットサービスは、米国の金融システムの完全性を守るという基盤の上に成り立っています。私たちの機関は、南北戦争後に急増した偽造に対処するため1865年に創設され、今日では、コンピューター詐欺や不正使用、銀行詐欺、ペイメントカード詐欺、個人情報窃盗、金融恐喝、電信詐欺などにも対応しながら、偽造と闘い続けています。この他に、地元の法執行機関や、全米行方不明/被搾取児童センター（NCMEC）への捜査支援なども行っています。シークレットサービスの捜査任務の継続的な成功は、法執行機関や民間部門の専門家との連携にかかっています。シークレットサービスは、パートナーとのこのような交流を促進するサイバー詐欺タスクフォース（CFTF）のネットワークを全国で展開しています。長期的なパートナーシップは、サイバー犯罪を防止、軽減する最良の仕組みです。

企業に対するランサムウェアの悪用もまた、大規模なデータ漏洩/侵害において中心的な役割を果たしました。これらの攻撃の背後にある犯罪組織は、盗んだデータを公開すると脅すなど、crime-as-a-service（犯罪のサービス化）のビジネスモデルを大いに活用していました。シークレットサービスは、法執行機関や民間部門のパートナーとともに、これらの犯罪者に立ち向かいました。このチームでのアプローチにより、複数のランサムウェア攻撃が阻止され、標的となった多くの米国企業や組織が保護されました。また、捜査官がこれらの犯罪組織に潜入し、IT担当者の役に立つ具体的な情報を提供しました。これにより、企業のITチームは自社のインフラを保護するための対策を講じることができ、データの漏洩/侵害や金銭的損失を大幅に削減することができました。ランサムウェアに関する業界レポートによると、2023年におけるランサムウェア詐欺の流行と収益性の傾向は一律ではないとのことです。シークレットサービスでは、このような詐欺の収益性をなくす努力を続けています。

生成AIは依然としてホットな話題です。ChatGPTは2023年1月に技術的な成功を納め、1億人のアクティブユーザが登録しました。正規のユーザは、論文の作成や質問の回答にAIツールを利用しました。しかし、数週間のうちに、犯罪者もAIツールを詐欺や恐喝の犯罪に活用し始めました。シークレットサービスの捜査によってAI翻訳ツールを利用した個人グループが逮捕された例もあります。彼らは英語を話せず、高度なコンピューター技術も持っていませんでした。しかし、悪知恵の働くこれらの攻撃者は、最新のツールを使って国境を越えたロマンスや恐喝計画を立て、被害者から数百万ドルをだまし取りました。これらの事件の被害者は、翻訳が使われていることも、外国の誰かとやりとりしていることさえも気が付きませんでした。

犯罪の先手を打つため、シークレットサービスはテクノロジー企業との提携を増やし、新しいテクノロジーが犯罪を可能にするのではなく、犯罪を未然に防ぐ手助けになるように努めています。これには、企業がそのツールの悪用を検出するために実施できる対策や、これらのテクノロジーが捜査を適切に支援する方法を探ることも含まれます。たとえば、私たちの調査チームや調査担当者は、大規模なデジタルデータの分析が次第に困難になってきています。しかし、新しいデータ分析テクノロジーによって、不正な活動を検知し対処する能力を大幅に向上させることができます。カリフォルニア州に影響を与えた大規模な詐欺犯罪の捜査には、このような最新テクノロジーが用いられ、成功を収めました。この事件では、調査担当者が数週間のうちに詐欺犯罪のパターンを特定し、その結果、シークレットサービスの捜査官が、カリフォルニア州在住の電子給付金送金（EBT）カードの利用者から盗んだ情報を使ってATMから数万ドルを引き出した5人の犯罪者を逮捕しました[106]。この事件によって、新しいデータ分析ツールが役に立ち、官民の両方で犯罪を迅速に検出して対処できる可能性が実証されました。

シークレットサービスは、ランサムウェアやクレジットカード詐欺と戦う場合も、インターネットを利用する児童略取者の手から未成年者を守る場合も、常に最先端テクノロジーに取り組んでいます。新しいテクノロジーは、犯罪者にも捜査官にも同じように役立つものです。私たちが推進する民間部門と法執行機関とのパートナーシップは、犯罪を検出し、防止するための鍵となります。私たちのサイバー詐欺タスクフォースのネットワークは、アメリカの経済的利益を保護するという重要な目標を掲げ、サイバー犯罪の防止と軽減を促進するために、パートナーとの定期的な交流を深めていきます。協力し合うことで、犯罪を防止するためにテクノロジーの効果的な使用方法を特定し、実行していくことができるのです。

106 https://www.secretservice.gov/newsroom/releases/2023/06/five-charged-theft-california-benefits-low-income-families

付録D：VERIS Community Database（VCDB）を利用したリスクの推定

HALOCK Security Labs社およびCenter for Internet Security （CIS）

VCDBはインシデントの情報共有において飛躍的な進歩を遂げました。CISとHALOCK社にとっては、リスク分析のための強固な基盤となっています。リスク評価を行う上での最大の課題の1つは、インシデントが発生する可能性を推定することです。VCDBには構造化されたインシデントデータがたくさん含まれているので、これを使えば何とかこの課題を解決できると確信していました。

私たちが共にVCDBの検討を始めたとき、そこには約7500件のインシデントレコードがあり、それぞれに約2500のデータポイントが存在し、各インシデントがどのように発生したかを教えてくれていました。しかし、これはほぼ1,900万データポイントに相当するものです。CISコミュニティがリスクを推定するのに役立つように、そのデータをどのような形にすればいいのでしょうか？

私たちはテストを繰り返し、記録された大量のインシデントに形と意味をもたらす多くの有用な集計を見つけ出しました。レコードセットに含まれる攻撃の種類に注目することで、特定の攻撃がどの程度一般的に（または、まれに）使用されているかを確認することができました。また、攻撃経路や脆弱性に注目することで、特定の弱点がどのようにインシデントの要因になったかを理解することができました。業種に基づいて（NAICSコードにしたがって）データを集計すると、攻撃手法が組織の種類に共通する資産の分布とどのように相関しているかがわかりました。

どの業種がどのような攻撃を受けやすいか、あるいは受けにくいか、あるいはどの攻撃手法がどの資産クラスに最もよく使われるか、あるいはあまり使われないかなどの複雑な質問に答えるために、データを集計できることが理解できました。忍耐強くスキルを身に付ければ、どのような種類の攻撃が前年比で多いか少ないかの傾向や、どの資産とどの攻撃方法が最もよく関係しているかを調べることもできます。

前の段落を読んで心拍数が上がった方は、私たちと同類です。しかし私たちは、楽しんでいるのと同じくらい、「最もシンプルな方法で、最も広い母集団に対するリスク確率をモデル化する方法を見つける」という、私たちの目的に集中しなければなりませんでした。

ある資産クラスが攻撃でよく悪用されることに気づいたとき、私たちはVCDBデータとCISコントロールのシンプルな相関関係を見出すことができました。CISコントロールのセーフガードは資産クラスに関連付けられ、VCDBは各インシデントに関係した資産を示しているため、VCDBのインシデントとCISのセーフガードを結びつけることで、攻撃の種類を防ぐことができました。そして、それをリスク評価手法であるCIS RAM107に組み込むことで、企業がリスク分析の中の可能性のある部分を推定するのに役立てることができました。インシデントのレコードによく登場する資産であればあるほど、それに対応するセーフガードが強力でない限り、最終的なインシデントの原因となる可能性が高くなります。このインサイトが、リスクの可能性を自動的に推定するための「期待値」スコアとなりました。

この2つの図は、期待値の相関関係を示しています。図88は、VCDBにおける資産の共通性と、その資産を保護するCISコントロールのセーフガードの成熟度との相関関係を示しています。資産における低い共通性と高い管理成熟度がマッチすると、期待値スコアは低くなります（この図では「5」のうちの「2」）。

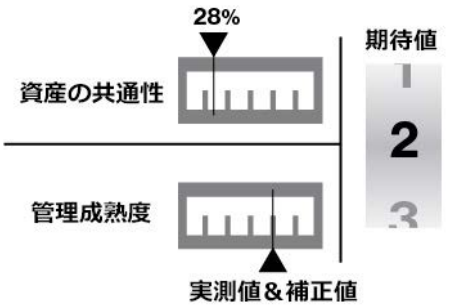


図88. 資産の共通性が低く、管理成熟度が高い

逆に、図89は、資産の共通性が高く、管理成熟度が低い場合に、期待値スコアが高くなることを示しています。

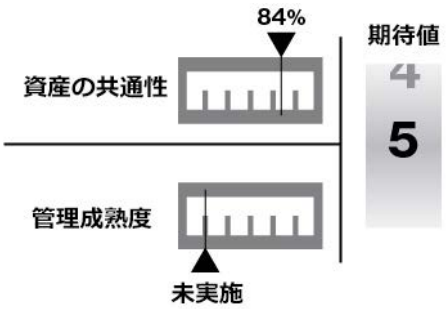


図89. 資産の共通性が高く、管理成熟度が低い

この相関関係を平易な言葉で表現すれば、一般的にある資産が侵害されればされるほど、その資産に対する管理能力が高くなるはずだということになります。

しかし、インシデントの影響も考慮しなければ、リスク分析は完了しません。CIS RAMは、企業が影響度スコアを推定するのに役立つ手法をさらに追加しているため、「期待値」スコアと組み合わせることで、エビデンスに基づくリスク分析が可能になります。そして、VCDBコミュニティの精神に則り、CIS RAMは必要とする人にその分析を自由に提供することができます。

リスクアナリストは、私たちが「可能性（likelihood ）」や「確率（probability）」ではなく「期待値（expectancy）」という用語を使っていることに疑問を持つかもしれませんが、これはVCDBが示唆してくれるものによって慎重に選択された用語です。

「確率 」という言葉は、ある期間内に計算された割合の範囲や値（たとえば、「12%～22%の見込み」や「1年以内に12%の確率」など）を示す統計分析に最適です。「可能性」は通常、より口語的に、またはより厳密でない推定プロセス（「非常に可能性が高い」、「可能性が低い」など）に使用されますが、これもまた期間や頻度を意味します。

しかし、「期待値」スコアは時間枠を考慮しません。これは、何らかの事故が発生することを受け入れるというものであり、「期待値」スコアが高いほど、その資産と管理が関係していることを期待しているということです。「期待値」スコアが低いほど、その資産や管理が関係する可能性は低くなります。

これは、各企業がリスクを最も低減できるセーフガードの改善に優先順位をつけるのに役立ちます。

組織が攻撃の可能性を推定するためにVCDBを利用できるのは、この相関関係だけではありません。CISとHALOCK社でさえ、それぞれの目的を考慮し、ベライゾンが独自に集計したデータを使用しています。もし、あなたの業種でどのような攻撃手法が最も一般的なのか、あるいはどのような攻撃手法がどのような資産に対応しているのか、あるいは時間の経過とともにどのような攻撃手法が増加傾向にあるのかを知っているとすれば、どのようにサイバーセキュリティプログラムを管理するかを考えてみてください。

時間をかけてVCDBのリスク分析の使い方を調べてみてください。きっと何か発見があるはずです。

VERIS Community Database
https://verisframework.org/vcdb.html

107 https://learn.cisecurity.org/cis-ram

付録E：協力企業

A

Akamai Technologies

Ankura

Apura Cyber Intelligence

B

Balbix

bit-x-bit

Bitsight

BlackBerry

C

Censys, Inc.

Center for Internet Security (CIS)

Cequence Security

CERT Division of Carnegie Mellon University's Software Engineering Institute

CERT – European Union (CERT-EU)

CERT Polska

Chubb

Coalition

Coveware

Cowbell Cyber Inc.

CrowdStrike

Cyber Security Agency of Singapore

Cybersixgill

CYBIR

Cyentia Institute

D

DomainTools

E

Edgescan

Emergence Insurance

EUROCONTROL

EVIDEN

G

Global Resilience Federation

GreyNoise

H

Halcyon

HALOCK Security Labs

I

Ivanti

J

JPCERT/CC

K

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

KnowBe4

KordaMentha

L

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

M

Maritime Transportation System ISAC (MTS-ISAC)

Mimecast

mnemonic

N

National Cyber-Forensics & Training Alliance (NCFTA)

National Fraud Intelligence Bureau

NetDiligence®

NETSCOUT

O

Okta

OpenText Cybersecurity

Q

Qualys

R

Recorded Future, Inc.

Resilience

ReversingLabs

S

S21sec by Thales

Securin, Inc.

SecurityTrails, a Recorded Future Company

Shadowserver Foundation

Shodan

Sistemas Aplicativos

Sophos

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

Z

Zscaler

あ

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

アメリカ合衆国サイバーセキュリティ・社会基盤安全保障庁（CISA）

英国家犯罪対策庁（NCA）

ウォッチガード・テクノロジー

か

カスペルスキー

国防防諜・安全保障局（DCSA）

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）

情報コミッショナーオフィス（ICO）

た

チェック・ポイント・ソフトウェア・テクノロジーズ

は

パロアルトネットワークス

米国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）

ら

ロンドン市警察


Akamai

ankura

apura

Balbix

bit-x-bit
SM

BITSIGHT

BlackBerry

censys

CIS
Center for Internet Security

CEQUENCE

Carnegie
Mellon
University
Software
Engineering
Institute

CERT-EU

NASK
CERT.PL

CHECK POINT

CHUBB

CITY OF LONDON
POLICE

Coalition

COVEWARE

COWBELL™
CYBER

CROWDSTRIKE

CSA
SINGAPORE

CISA

CyberSecurity
MALAYSIA

cybersixgill

CYBIR

Cyentia
INSTITUTE


DomainTools

edgescan

emergence

EUROCONTROL

EVIDEN


GLOBAL
RESILIENCE
FEDERATION

GREYNOISE

halcyon

HALOCK

ico.

IRISS
Irish Reporting and
Information Security Service

ivanti

JPCERT CC®

K12 SIX

kaspersky

KnowBe4
Human error. Conquered.

KordaMentha

LEGAL SERVICES ISAO	Maritime Transportation System Information Sharing and Analysis Center	mimecast	mnemonic	NCA National Crime Agency
NCFTA	National Fraud Intelligence Bureau	NetDiligence	NETSCOUT	okta
opentext™	paloalto NETWORKS	Qualys. Continuous Security	Recorded Future®	resilience
REVERSINGLABS	S21SEC Cyber Solutions by Thales	Securin	SecurityTrails A Recorded Future® Company	SHADOWSERVER
SHODAN	SISAP Sistemas Aplicativos	SOPHOS	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	zscaler™	

verizon business