2022 DBIR：医療および社会福祉業

サマリーレポート

(NAICS 62)

ベライゾンの15回目のデータ漏洩/侵害調査報告書（DBIR）の医療および社会福祉業のサマリーレポートへようこそ。この報告書の発行開始から15年も経ったとは、本当に信じられない思いです。

DBIRは、一般的なサイバーセキュリティ攻撃を調査し、組織がどのように自らを守ることができるかについてのインサイトを提供しています。今年度は23,896件のインシデントを調査しました。医療および社会福祉業では、このうち849件のインシデントが発生し、そのうち571件でデータの暴露が確認されました。このデータは、Verizon Threat Research Advisory Center （VTRAC）が調査したもの、および世界各地の87の協力組織から提供された実際の漏洩/侵害とインシデントを表しています。

本レポートとそれに含まれる情報を利用して、医療および社会福祉業に対して使用される最も一般的な攻撃の手口に対する認識を高め、組織の態勢にお役立ていただければと願っています。

「医療および社会福祉業」に関するレポートのハイライトをご一読ください。また、このサマリーレポートを同僚の方と共有しいただいても良いですし、2022年の脅威の状況の詳細な分析については、verizon.com/dbirから完全版をダウンロードしてご確認いただくこともできます。

DBIR調査報告書内で被害組織の分類に使われている業種ラベルは、すべて北米産業分類システム（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しています。通常、ベライゾンでは2桁レベル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。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。
census.gov/naics/?58967?yearbck=2012

インシデントの分類パターン

DBIRは、非常に頻繁に発生するインシデントシナリオの有用なツールとして、2014年に初めてインシデント分類パターンを導入しました。昨年、攻撃の種類や脅威の状況の変化により、これまでのパターンの見直しを図り、当初の9パターンから、本レポートに掲載されている8つのパターンに変更しました。

これらのパターンは、洗練された機械学習によるクラスタリングプロセスに基づいており、複雑な相互作用のパターンをより適切に捉えることができ、侵害時に発生する事象に強く焦点を当てたものとなっています。そうしたことから、これらのパターンはデータ管理の推奨にも適しています。

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/侵害させたりする攻撃。

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

- ソーシャルエンジニアリングによる侵害の59%は認証情報への不正アクセスで、31%は窃取した認証情報を使用しています。ソーシャルエンジニアリングによる認証情報への不正アクセスは、他のパターンに比べて3倍以上の割合で発生しています。
- ソーシャルエンジニアリングのパターンでは、「フィッシング」が「なりすまし」の2倍以上の割合で発生しています。
- ソーシャルエンジニアリングによる侵害の動機は、「金銭的目的」が「スパイ行為」の8倍にもなります。

基本Webアプリケーション攻撃

最初のWebアプリケーションの侵害の後、数段のステップまたは追加アクションを伴う単純なWebアプリケーション攻撃

このパターンでは、Webサーバーやメールサーバーなどのインターネットに接続された組織のインフラにアクセスするために、窃取した認証情報を使用する攻撃者が依然として大きな割合を占めています。

- Webアプリケーションに対する攻撃の5件中4件が、窃取した認証情報によるものでした。この調査結果は、パスワードの安全対策の重要性を裏付けています。
- 基本Webアプリケーション攻撃（BWAA：Basic Web Application Attack）による侵害では、他のパターンに比べてスパイ活動の可能性が4倍高く、国家組織が必ずしも複雑な攻撃を行う必要はなく、確立した効果的な攻撃を活用して目的を達成できることを示しています。
- BWAA侵害では、窃取した認証情報の使用が、脆弱性を悪用した攻撃の6倍にものぼります。

システム侵入

システム侵入は、目的を達成するために、ランサムウェアの導入など、マルウェアやハッキングを活用した複雑な攻撃

このパターンは、ソーシャル、マルウェア、ハッキングなど、複数の異なる攻撃の組み合わせを使用した、より複雑な侵入や攻撃で構成されており、今年劇的に増加したサプライチェーンへの侵害やランサムウェアによる攻撃も目立ちます。

- システム侵入の92%は金銭目的を動機としています。
- システム侵入による侵害では、窃取した認証情報の使用が脆弱性の悪用の4倍以上になっています。

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要素を直接的に侵害したインシデント。デバイスの紛失は含まれず、盗難に分類されています。

今年の調査では、すべて従業員によるものであることが示されています。「誤送信」と「設定ミス」が上位2つを占めています。設定ミスは、「セキュリティリサーチャー」という発見方法とよく組み合わされます。

- 誤ってインターネット上に公開されたサーバーの設定ミスや、ユーザが間違った宛先にメールを送信する誤送信が侵害件数全体の13%を占めています。
- 外部のクラウド資産は昨年から83%減少しており、「セキュア・バイ・デフォルト」のアプローチを活用するテクノロジーへのシフトを示唆していると思われます。
- 多種多様なエラーのうち85%がサーバーに関するものでした。

特権の悪用

正規の権限が承認されていない、または悪意を持って使用されることが主な原因となるインシデント

このパターンのインシデントのほとんどは、データ侵害の成功につながります。これらの攻撃者は、依然として金銭的利益を動機としており、収益化が容易であるため、個人データを標的にしています。

- 特権の悪用では、他のパターンに比べ文書の悪用が3倍にものぼります。

資産の紛失・盗難

誤操作や悪意によって情報資産が失われた、あらゆるインシデント

窃盗が多発しているのは、「金銭的動機」によるものです。盗みを働く者の多くは、盗んだ資産を売却してすぐに現金化するために犯行に及んでいると考えられます。

- これらの事件で被害を受けたデータのタイプは、昨年と（ほぼ）同じです。通常、盗みを働く者は外部の人間ですが、従業員は資産の紛失に責任を負います。
- 資産の紛失と盗難のインシデントでは、無関係の攻撃者による関与が他のパターンの14倍にもなります。

サービス拒否（DoS）

ネットワークやシステムの可用性を低下させることを目的とした攻撃。ネットワーク層とアプリケーション層への両方の攻撃が含まれます。

サービス拒否（DoS）インシデントでは、他のパターンに比べて、大企業への攻撃が2倍多く発生しています。これらの攻撃は、広範囲にわたり組織に影響を与える厄介なものですが、一部の組織は、これらの攻撃を定期的に受けており、ビジネスに悪影響を与える可能性があります。

その他全て

この「パターン」は、実際にはパターンとは言えません。他のパターンの枠に収まらない、あらゆるインシデントが含まれます。

医療および社会福祉業

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

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

頻度	849件のインシデント、確認されたデータの暴露571件
上位3つのパターン	「基本Webアプリケーション攻撃」、「多種多様なエラー」、「システム侵入」がデータ漏洩/侵害の76%を占めている
攻撃者	外部（61%）、内部（39%）（漏洩/侵害）
攻撃者の動機	金銭目的（95%）、スパイ活動（4%）、怨恨（1%）（漏洩/侵害）
侵害されたデータ	個人情報（58%）、医療情報（46%）、認証情報（29%）、その他（29%）、（漏洩/侵害）
IG1による優先保護対策	セキュリティ意識およびスキル向上のトレーニングプログラムの実施（CSC 14）、企業資産およびソフトウェアのセキュアな設定（CSC 4）、アクセス制御管理（CSC 6）
昨年との比較	上位3つのパターンは変わらずに、順位が入れ替わっています。 攻撃者の顔ぶれも昨年と全く同じでした（それぞれの占める割合まで）。

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

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

図1は、医療および社会福祉業のデータ漏洩/違反パターンの経時的変化を示しています。2015年当時は「特権の悪用」がトップで、「多種多様なエラー」がそれに続いているパターンでした。

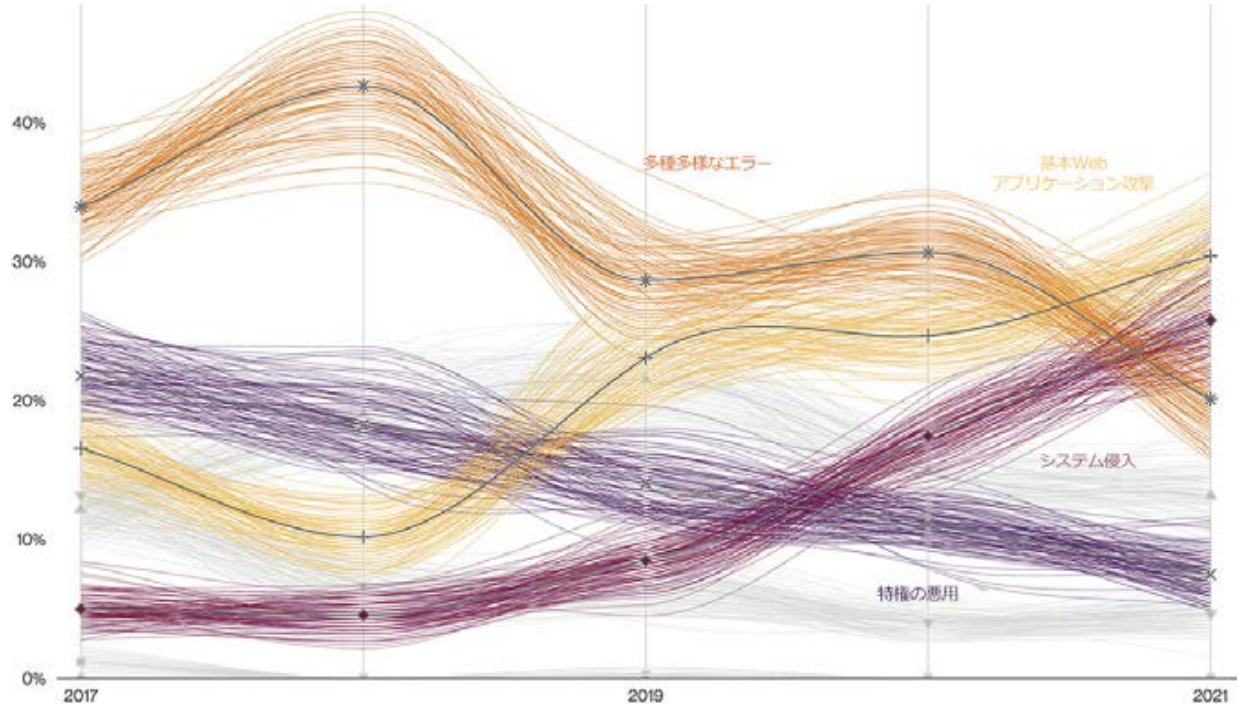

図1. 医療および社会福祉業のデータ漏洩/侵害パターンの経時的変化

「基本Webアプリケーション攻撃」の台頭が見られるようになったのは2019年になってからで、この業種だけでなく、明らかにすべての人にとって深刻な問題になっています。この業種は、ありふれたハッキング攻撃や、よりインパクトのあるランサムウェアキャンペーンの標的となることが増えています（どちらも第3位の「システム侵入」パターンからの攻撃）。ランサムウェアの増加に伴い、「攻撃者による開示」という発見手段も増えています。暗号化された後に身代金のメモが表示され、顧客サービス重視の脅威グループにとって便利な支払い方法を指示された日には、最悪と言わざるをえません（本当に、誰も「お客様」が簡単に支払えるようにしたくないなんて思いませんよね）。

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

自分たちのデータに自信を持つ

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。

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）。

スパゲティチャート、そして比較的新しいピクトグラムのプロット表示は、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、単一の割合表示により適しています。

常に最新の情報を入手して脅威に備える

医療および社会福祉業の組織が今日直面しているサイバー脅威に立ち向かうには、信頼の置ける情報源から提供されるデータが必要です。完全版DBIRにある攻撃者、攻撃とそのパターンに関する情報は、防御の準備や従業員の教育に役立ちます。

2022年DBIRの完全版は、verizon.com/dbirでご覧いただけます。