2017年度
データ漏洩/侵害
調査報告書

第10版

verizon

この報告書を最大限ご活用いただくためのヒント

2009年度の弊社レポートでは、下記のとおり報告しております。

「これらの調査結果は、アタックやインパクト、一般的なセキュリティインシデントやリスクではなく、データ漏洩を引き起こすセキュリティ侵害の発生（もしくは可能性）について具体的に説明しています。」

それ以来、この調査はデータ漏洩に加えて、セキュリティインシデントが含まれるまでに発展しましたが、その他の考察は今日でもそのまま当てはまります。これらの情報がお客様にとって適切なものとなるように、業界別、動機別など、様々なフィルタを通しています。いわば、情報セキュリティというパズルの1つのピースです。それは出発点となり得る有効な角のピースですが、あくまで1つのピースにすぎません。残りを埋めるのはお客様です。お客様それぞれの業界で最も一般的に行われている攻撃行為の威力を弱めるために、ご自身が現在実施している、または実施していない対策をご存知のはずです。また、お客様の環境において機密データが保管されている資産とデータフローについてもご存知のはずです。もしご存知でないようでしたら、急いでご準備ください。さらに、ご自身のインシデントやデータ紛失の履歴についてもご存知でしょう。お客様の知識とこの報告書から得たデータを組み合わせてご活用ください。これら2つは互いに補完しあいます。

初めてお読みになる方へ

この報告書はこれまでと同様、実際のデータ漏洩とセキュリティインシデントから構成されており、いずれもベライゾンによる調査もしくは優れた協力企業・組織より提供された情報に基づくものです。

本書に記述されている内容は、インシデント報告書または様々なセキュリティベンダーから提供されたインシデント以外のデータに基づいています。

我々は、調査や複数の情報源から類似データを収集するのではなく、このようなタイプのデータを使用することによって、偏りに対処しています。すなわち、インシデント以外のデータセットの分析結果を利用して、インシデントとデータ漏洩に関する調査結果の質を高め、裏付けています。とはいえ、どのようなセキュリティ報告書にも言えることですが、ある程度の偏りは残ります。これについては、付録Dでご説明します。

インシデントとデータ漏洩の違い

本書におけるインシデントとデータ漏洩の定義は以下のとおりです。

インシデント：情報資産の完全性、機密性、または可用性を侵害するセキュリティイベント。

データ漏洩：結果的に、関係者以外へのデータの流出（単なる露呈の可能性ではなく）が確認されたインシデント。

VERISのリソース

VERIS（Vocabulary for Event Recording and Incident Sharing）は無料でご利用いただけます。お客様がすでに導入されているインシデントレスポンス報告機能に統合いただくか、または少なくとも、簡単に内容をご確認いただくことをお勧めします。

veriscommunity.netには、フレームワーク情報とともに、例や分類一覧があります。

github.com/vz-risk/verisには、VERISのスキーマのすべてがあります。

github.com/vz-risk/vcdbでは、公開されているデータ漏洩に関するベライゾンのデータベース、VERISコミュニティデータベースをご利用いただけます。

サイバー犯罪のケーススタディ

この報告書では、個々の事件・事故に重点を置いていません。実際のデータ漏洩のシナリオを掘り下げるには、「ベライゾンデータ漏洩/侵害ダイジェスト」[1]に集められている、サイバー犯罪のケーススタディをご覧ください。これは実際のインシデント調査に基づき、データ漏洩対応に関わった様々な関係者の観点から集めた体験談です。

今すぐ読む ›

[1] http://www.verizonenterprise.com/verizon-insights-lab/data-breach-digest/2017/

目次

はじめに

> 希望こそが世界を支える柱である
>
> — 大プリニウス

10周年を迎えたデータ漏洩/侵害調査報告書（DBIR）にようこそ。セキュリティの世界における無法行為と悪意に満ちた破壊行為がこの10年で最高潮に達しましたが、情報セキュリティの謎を解き明かす機会をいただき、心より感謝いたします。2016年は米国でも海外でも、実に騒々しい年でした。対立を深めた大統領選挙、英国のEU離脱（ブレグジット）など、大勢の血圧を上昇させた政治的出来事の一方で、ソーシャルメディアでは一年中インターネット・ミームが溢れかえっていました。大混乱と怒号にかかわらず、サイバー犯罪は1年中発生し、公表された多数のデータ漏洩は疑念を強めるだけです。「悪い評判も良い宣伝」はセキュリティの世界では成り立ちません。

ではなぜ冒頭で「希望」という言葉を使ったと思いますか？ 本書は憂鬱な悪い運命と、何かがうまくいかなかった時に起こり得る最悪の事態ばかりを書いたものだとお考えでしたか？ 本書をそのように見ることも確かに可能です。降参して我々（リスク管理と情報セキュリティのコミュニティ）に「敗者」のレッテルを張りますか？ 我々は、この報告書や、同業者による類似した報告書に対し、現実的なアプローチを取り、よりよい対応が可能であることを認識しなければなりません。我々には希望を唱える大きな理由があると確信しています。

「100%安全なんてことはありえない」または「完璧は充分の敵である」という決まり文句のとおり、確かにDBIRが空白になることはありません。また、DBIRの性質上、すべてが成功談にはならないということも、確かに認めざるを得ません。なぜなら、本書は実際にあったデータ漏洩に関する報告書だということが根底にあるからです。とはいえ、その中にも、多数の成功談があります。必ずしも善人のための悪いニュースばかりではありません。我々の希望は、この調査結果を10年間続けて公表することができた、という事実に由来します。また、この報告書をたった1つの組織から65のソースにまたがる協力企業・組織が含まれるまでに成長させ、学習できるセキュリティインシデントやデータ漏洩に関する確かなサンプル集を提供するに至った、ということにも由来します。

加えて、この報告書で、「状況はより好転しているのか」というマクロレベルの問いに明確に答えることはできないにしても、お客様が結集された成果（データ収集にご協力いただいた企業・組織に改めて感謝いたします）を活用できる、ということにも由来します。この調査結果をベースにして、攻撃者が用いる戦術に対する意識を高め、お客様とその業界に最も関係がありそうな脅威について理解し、情報セキュリティ戦略を広め、支持を得るための手段にしてください。

さて、2017年度の報告書で目新しいことはなんでしょう？ これまでのDBIRを通して我々が発展させたものの1つに、9種類のインシデント分類パターンに定義し、それを業界ごとにマッピングする、ということが挙げられます。我々は、これによりDBIRの実用性が大いに高まったと考えております。今年の報告書はさらに一歩進んで、主要な業界に特化したセクションが含まれています。これらのセクションでは、誰がどの業界をターゲットとしているか、目的を果たすためどのように取り組んでいるかを掘り下げ、ある種の攻撃の実行者が特定の業界に照準を合わせている目的を解説します。何が業界ごとにユニークであるか、それがデータセットに見られる結果にどのように影響しているかを検証します。こうした業界に対応するセクションがセキュリティの専門家の共感を呼び、お客様にとって、有益なデータを見つけるための一助となることができればと考えます。

したがって、報告書は次のような流れに沿っています。まずは本年度のデータから得られた知見からなるエグゼクティブサマリーから始まります。他の報告書と同様、これまでの経緯を振り返り、この間に何が変わったか、また、何が変わらなかったかについて解説します。次に、業界別のセクションに進み、情報セキュリティにおける人的要素と、今や誰もが口にするランサムウェアを重点的に取り上げます。例年どおり、9つのインシデント分類パターンを取り上げ、2016年の良かったこと、悪かったこと、厄介なことを検証して、これらをまとめます。

エグゼクティブサマリー

データ漏洩の背後に誰がいるか？

75%
外部者の犯行の割合。

25%
内部者が犯行に関与した割合。

18%
国家の支援を受けた実行者による犯行の割合。

3%
複数の関係者を特徴とする割合。

2%
パートナーが犯行に関与した割合。

51%
組織的な犯罪グループが関与した割合。

どのような戦術が用いられているか？

62%
ハッキングを特徴とするデータ漏洩の割合。

51%
データ漏洩の過半数にマルウェアが関係。

81%
ハッキングに関連するデータ漏洩で、盗んだパスワード、セキュリティ強度が弱いパスワード、またはその両方が利用されている割合。

43%
ソーシャル攻撃の割合。

14%
データ漏洩の14%が偶発的なミスによるものでした。特権の不正利用を伴った割合も同じです。

8%
データ漏洩の8%で、物理的な行為が存在しました。

誰が犠牲になったか？

24%
データ漏洩が金融機関に影響を与えた割合。

15%
医療組織が関係したデータ漏洩の割合。

12%
公的機関はデータ漏洩の犠牲者数の多さで第3位であり、その割合は12%です。

15%
小売業とホテル業を合わせると、データ漏洩件数の15%を占めます。

その他、何が一般的か？

66%
不正な電子メールの添付ファイルによって、マルウェアがインストールされた割合。

73%
金銭を動機とするデータ漏洩の割合。

21%
スパイ活動に関連したデータ漏洩の割合。

27%
第三者が発見したデータ漏洩の割合。

データ漏洩の動向

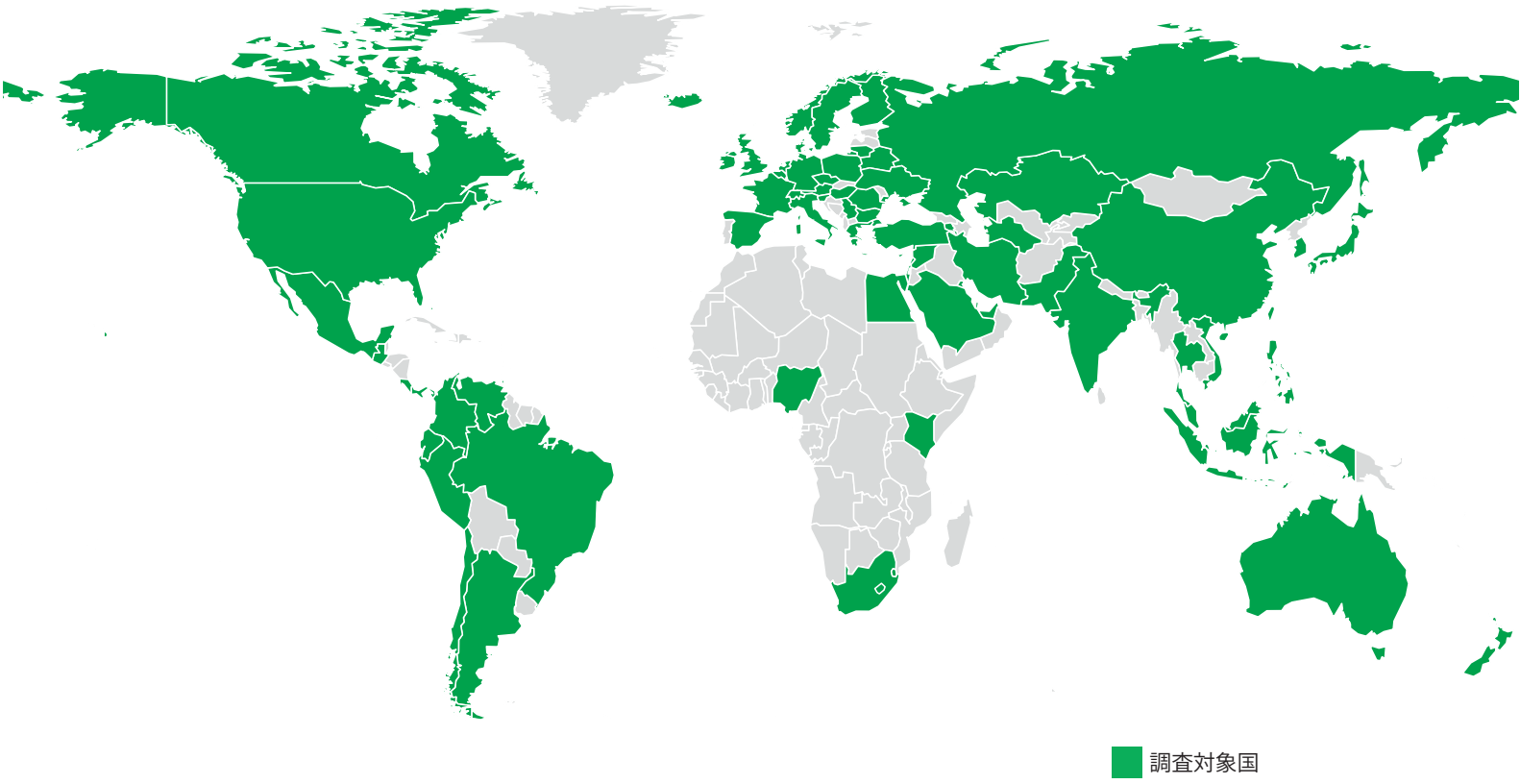


図1：調査対象国の合計件数

2014年、我々は「データソースが年々増大し続け、多様になっていることから現状維持が難しく、我々の分析視点にも変化があることから、データを視覚化し、結果をまとめる方式も年々進化している」と指摘しました。年ごとにデータを提供いただく企業・組織には変化があります（コミュニティで調査するインシデントのタイプにも変化があります）。これらは、攻撃実行者の行動における変化ほどではないにしろ、調査結果に影響する可能性があります。

対象の変化や調査結果が前者の産物である場合は、それを明らかにします。たとえば、特定の分類におけるスパイクは昨年の報告書に見られる、Dridexボットネットによるデータ漏洩に関連して受信されたデータのスパイクが原因でした。今年は、多くが過去の年のレベルに下がっています。

その一方で、2014年には、「差分の測定には価値があり、読者は複数のレポートの間にある程度の継続性を望んでいることを承知しています」とも述べました。したがって、このセクションではそれを試みます。

図2は、外部者が犯行に関与したデータ漏洩の割合の低下を示しています。これは、内部者の犯行によるデータ漏洩の増加が原因です。しかし、絶対数で見ると、内部関係者によるデータ漏洩は比較的一定であり、12%前後の増加です。

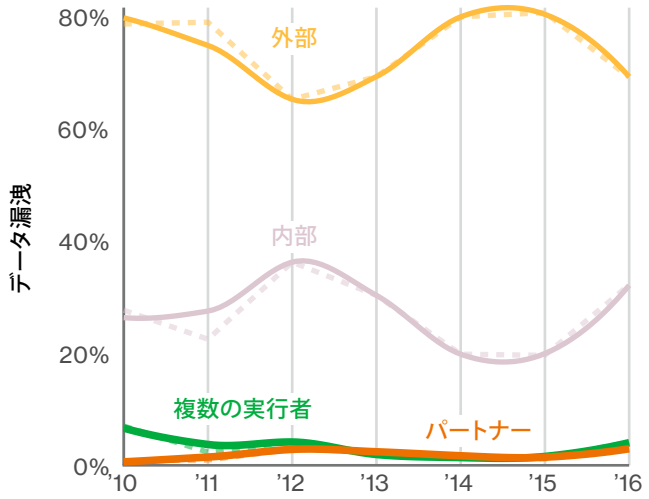


図2：攻撃実行者のカテゴリーの経時変化

言い換えると、上昇傾向の内部脅威については言及しませんし、この線は今後も上昇傾向が続くという説にすべてを賭けるつもりはありません。この2本の線が2016年に収束するのは、攻撃者対被害者の比率の高さが一般的な特徴である、2種類の外部攻撃、すなわちパスワード窃取ボットネットと日和見的POSへの侵入が低下したことが原因です。複数の関係者、ビジネスパートナー[2]が関与するデータ漏洩は存在するものの、発生頻度ははるかに少なく、毎年、下位を保っています。

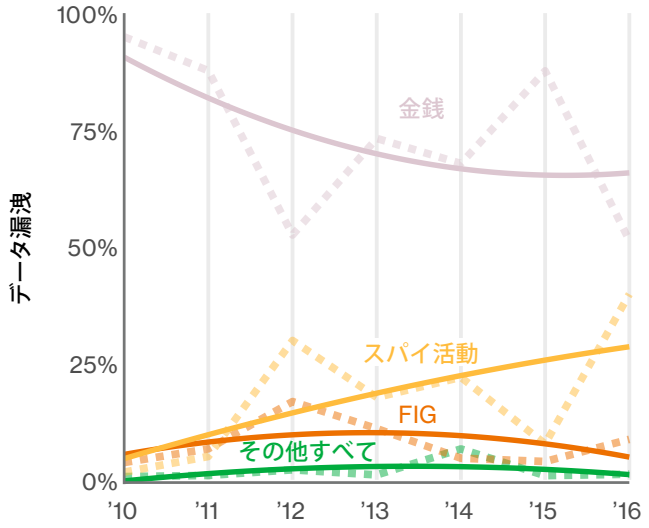


図3：攻撃実行者の動機の経時変化

2016年も引き続き、金銭とスパイ活動が動機のトップ2であり、その2つでデータ漏洩の93%を占めます。図3では、愉快犯（Fun）、イデオロギー（Ideology）、悪意（Grudge）という3つの動機を合わせて、FIGとして示しています。この報告書の他のグラフも同様です。スパイ活動が上昇した理由は、単に、今年のデータセットでこれらのデータ漏洩を重視したということもありますが、すでに述べた、銀行業のトロイの木馬ボットネットとPOSの減少も理由です。組織的な犯罪グループは引き続き、ランサムウェアを利用して犠牲者から金銭を巻き上げていますが、これらのインシデントでは、データ漏洩が確認されないことがよくあるため、図3には反映されていません。

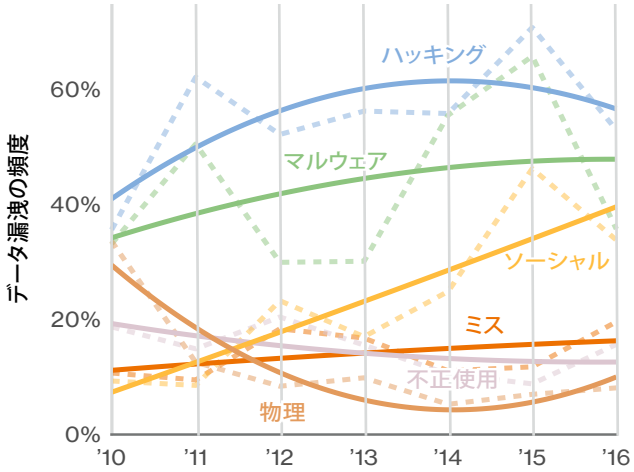


図4：攻撃行為のカテゴリー別に示したデータ漏洩の割合の経時変化

2016年は我々にとって、現在起こっている出来事について論じるよう求められるのが怖く、ディナーの誘いすら受けたくないほどの年でした。世界規模での大混乱や激変がありすぎて、理解に苦しみます。そのため、上記の図4を見て、妙に安心するほどです。ハッキング、マルウェア、ソーシャルという三つ巴の脅威がここ数年、トップに君臨し、上昇傾向にありました。今後もすぐに消え去ることはなさそうです。これはサイバー攻撃の強力な組み合わせで、誰もが納得できるものです。今年のデータセットでは、この3つの攻撃の件数が減少しました。（ここでも、やはり）POSとボットネット駆動型のデータ漏洩が減ったことが原因です。

[2] 注：パートナーを攻撃実行者として選ぶには、偶発的にデータ漏洩となった行為の背後にそのパートナーがいなければなりません。ビジネスパートナーがハッキング攻撃を受け、連鎖の上位組織がその影響を受けた場合も、ハッキングを支援している関係者に実行者のタグを与えます。

実行される行為と侵害される資産は、実行者とその動機に大きく左右されます。図5では、動機別にとられるアクションの種類の違いが一目瞭然です（金銭的な動機を持つ実行者がキーロガーのマルウェアを使用しているなど）。

このレポートを通して実行者とその動機、手口の関連性、業界別に特徴のあるインシデントパターンが理解できます。図5に示されている具体的な実行者と動機は次のとおりです。FIG（愉快犯、イデオロギー、悪意を動機とするか、または活動家グループの攻撃実行者）、ESP（スパイ活動が動機であるか、または国家の支援を受けた実行者）、FIN（金銭的な動機を持つか、または組織犯罪グループの実行者）。

		種類		
		ESP	FIG	FIN
盗んだ認証情報の使用	（ハッキング）	27	6	598
バックドア/C2の使用	（ハッキング）	121		557
窃取	（物理）			39
改ざん	（物理）			27
監視	（物理）			21
SQLインジェクション	（ハッキング）			14
スパイウェア/キーロガー	（マルウェア）	38		557
スキミング	（物理）			60
ランサムウェア	（マルウェア）			14
RAMスクレーパー	（マルウェア）			191
特権の不正使用	（不正使用）	17	37	74
なりすまし	（ソーシャル）			39
所有権の不正使用	（不正使用）	6	9	29
フィッシング	（ソーシャル）	163		490
知識の不正使用	（不正使用）	7		12
フットプリント	（ハッキング）	18		
データのエクスポート	（マルウェア）	49		451
脆弱性の悪用	（マルウェア）	6		
ダウンローダ	（マルウェア）	38		5
制御不能	（物理）			23
不正なデータ処理	（不正使用）	16	5	22
保管データの取得	（マルウェア）	49		
アプリケーションデータの取得	（マルウェア）			8
C2	（マルウェア）	119		559
ブルートフォース	（ハッキング）			73
贈収賄	（ソーシャル）			8
バックドア	（マルウェア）	112		21
アドミンウェア	（マルウェア）	53		

		種類		
		ESP	FIG	FIN
Webサイト	（ソーシャル）	19		
Web経由	（マルウェア）	26		
Webアプリケーション	（ハッキング）	5	23	507
被害者の職場	（物理）			16
被害者の公共区域	（物理）			39
被害者の敷地	（物理）			31
リモートアクセス	（不正使用）		7	7
公共施設	（物理）			6
物理アクセス	（不正使用）	8	11	34
電話	（ソーシャル）			5
自家用車	（物理）			7
パートナーの施設	（物理）			5
パートナー	（ハッキング）			108
LANアクセス	（不正使用）	19	31	68
対面	（ソーシャル）			5
未知の電子メール	（マルウェア）	9		
電子メールリンク	（マルウェア）	23		
電子メール添付ファイル	（マルウェア）	110		452
電子メール	（ソーシャル）	156		523
マルウェアによるダウンロード	（マルウェア）	33		
直接インストール	（マルウェア）			184
デスクトップ共有	（ハッキング）			74
バックドアまたはC2	（ハッキング）	123		557

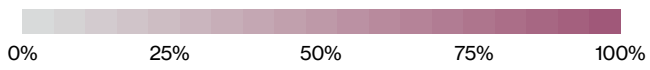


図5：データ漏洩における実行者/動機別に見たアクションの種類と経路

漏洩したレコード数が1億4,400万から400万に下がった2011年度のDBIRをご記憶でしょうか。[3] 以前の報告書で中心だったPCIデータの大規模な漏洩がその年はなく、派手に再登場したのは2年後でした。その間、我々は一般公開されている漏洩に関するデータを含め、データソースの拡大に着手し、100万単位のデータ漏洩がなくなっていないことに気づきました。2012年度の報告書では、活動家がWebサイトやデータベースから入手し、Pastebinなどのサイトに放出した個人情報が盗まれたレコードの中で多くを占めると同時に、今後の兆候を示していました。下の図6の数字は、実際のインシデント発生日と一致しており、多くは最初のデータ漏洩から何年もたつまで、DBIRに反映されませんでした（データ漏洩の発見は即座に判明するものではないため）。

現在まで早送りします。図6では、大量に保存されるデータは、巨大で、個人データと認証情報の合計は数年で数十億件になると想定されます。一部の認証情報はハッシュ化され、また、一部はSaltを利用して強固な暗号化を施されるかもしれませんが、膨大なレコードであることには変わりません。

今年、データ漏洩の観点から見た大物は、NAICS 51（北米産業分類システム）のなかでも情報産業です。この分類には、オンラインショッピングではないWebポータルやサイトも含まれます。消費者は一要素認証で多数のWebサイトにログインし、登録プロセスの中で、名前や住所を提供します。何百万人もが、あるWebサイトの会員になっていて、サイトでデータ漏洩が発生したと聞かされたときには、「報道価値」という言葉が浮かびました[4]。

皆さんを当てもなく苛立たせるために、こうした派手な数字を持ち出しているのではありません。少なくとも、このようなデータ漏洩に注意しなければならない理由は、いくつもあります。お客様の企業・組織に、顧客または会員からの外部ログインがある場合、詳細情報を盗んで金儲けすることを狙う外部勢力の手に、その認証情報が渡ることは好ましくないはずです。お客様のデータが漏洩しなかったとしても、何百万（または何十億）という認証情報を持つボットネット軍団が他のサイトでそれらの認証情報を再利用しようとします。つまり、認証に関する被害がお客様のところでなかったとしても、それに関わる情報の漏洩が発生しなかったということではありません。繰り返しますが、他のデータ漏洩から得たパスワードの再利用、または顧客デバイスに感染したマルウェアがあることを考えれば、ユーザー名/メールアドレスとパスワードに頼るのは、一か八かの勝負をするのと同じことです。この2点について、心配することがないようにしなくてはなりません。

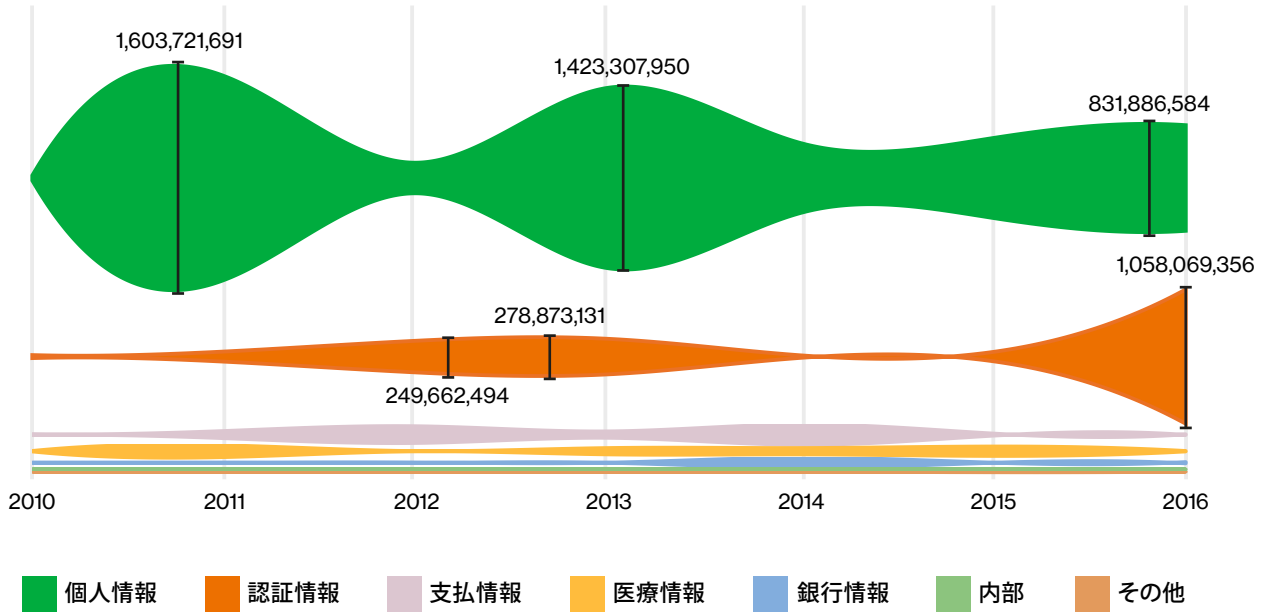


図6：データの種類別に見たレコード数の経時変化

[3] Pepperidge Farmが覚えています。

[4] 詳細を知りたい場合は、VERIS（Vocabulary for Event Recording and Incident Sharing）コミュニティデータベースで、未加工のパブリックデータをご参照ください（https://github.com/vz-risk/VCDB/tree/master/data）。個々のデータ漏洩について、詳細をご覧いただくことができます。用いられた戦術と手口については、情報産業およびWebアプリケーション攻撃パターンのセクションをご参照ください。

データ漏洩が発見された方法はもっとも変化の大きい指標の1つです。図7は、Dridexボットネットの被害の法執行機関による公開で、2015年のスパイクが2016年に大きく修正されたことを示しています。また、カードスキミングとPOS犯罪の騒動が減ったことは、法執行機関と不正検知による発見の大幅な低下に影響しています。内部での発見は2年連続で、従業員による通報が最も一般的でしたが、ビジネスメール詐欺（BEC）に関連した、内部会計監査による発見も増加しました。被害を受けた顧客、得意になって被害者をゆすった攻撃者が増加したため、第三者の指摘による発見が上昇しています。

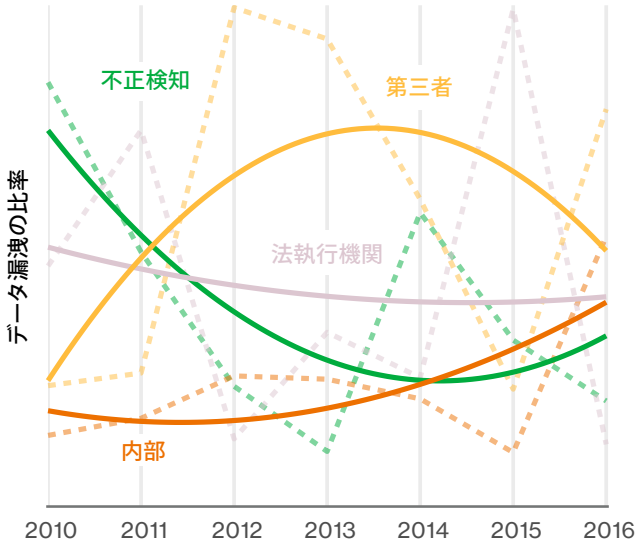


図7：データ漏洩発見方法の経時変化

図8では、データ漏洩の傾向について時系列で検証します。ボットネットとPOSのデータ漏洩が減少した結果、数秒または数分かかる侵害の件数が減少しています。それでも、数分以内に侵害されるケース[5]が全体の98%を占めています。

長年の読者であるお客様は、「侵害発生から発見されるまでの時間的差異」を示した図がどこにいったのかと疑問に思っているかも知れません。この図は、侵害に要した時間の割合と、発見に要した時間の割合を比較したものでした。検討を重ねた結果、**確認されたデータ漏洩を見るかぎり**、侵害に要した時間と発見に要した時間を比較しても、何ら改善は見られそうにないと判断しました。理由は2つあります。まず、侵害に要する時間に私たちが影響を与えることはできません。一般的な侵害の手口が有効であれば、短時間の間に漏洩は発生し、手口が有効でない場合は漏洩が発生することはないからです。次に、迅速に発見された場合（C2サーバーに戻ってきたアウトバウンドトラフィックが識別されてブロックされるなど）、そのイベントはデータ漏洩ではなく、インシデントとして定義される可能性がはるかに高いため、当てはまらないからです。

数分、数時間、または数日で発見されたデータ漏洩の増加については、その3分の2ほどが「人的エラー」または「物理的窃取および紛失」のパターンに結び付いていることに留意する必要があります。今年のデータセットで、発見に数か月以上を要するデータ漏洩は、POSへの侵入、特権の不正使用、またはサイバースパイ活動でした。

この憂鬱な話をアクションのきっかけに変えるためにも、組織内でこれらの事実を確認してください。盗み出すのに要する時間を長引かせ、発見に要する時間を短縮することに重点を置いてください。そうすることによって、インシデントがデータ漏洩になることを阻止できるはずです。

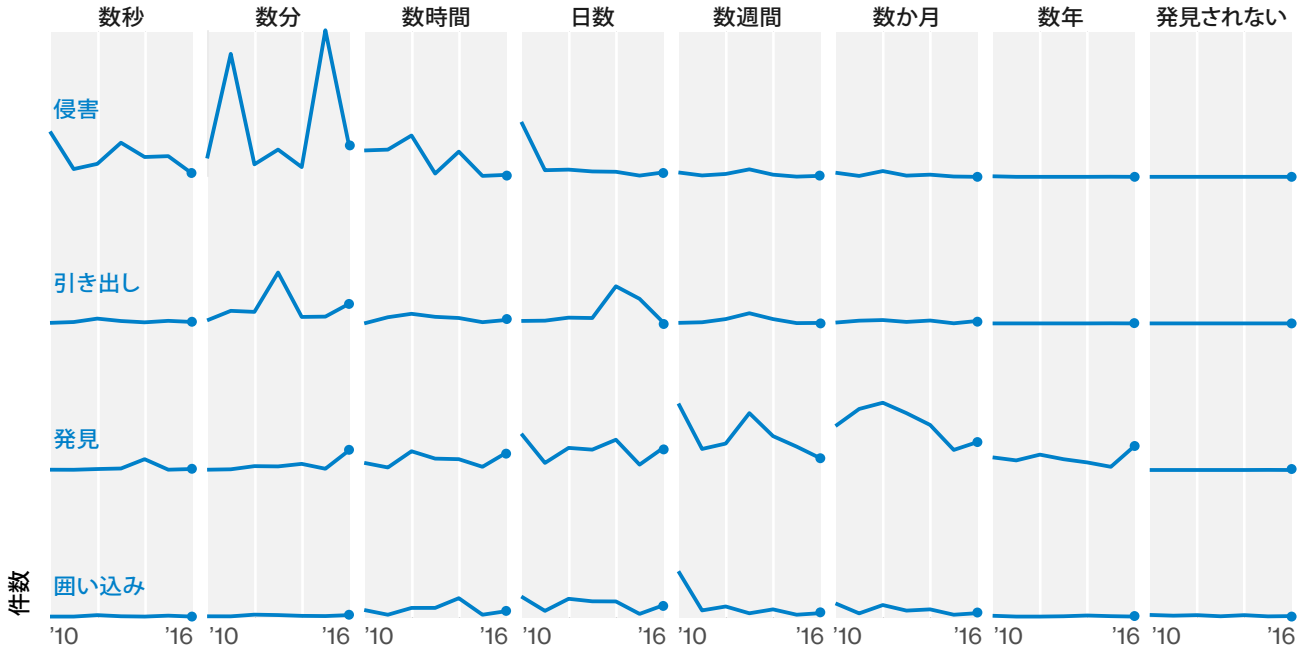


図8：データ漏洩イベントの期間に見られる経時変化

[5] インシデントにデバイスの紛失または特権の不正使用が関連する場合は、侵害に要する時間を記録していません。

業種別の概要

我々は、過去数年にわたり、主要な産業ごとに別々の報告書を発表してきました。「はじめに」で述べたとおり、今年はこの本体の報告書で、業界固有の調査結果をこれまで以上に重視することにしました。このセクション全体で、個々の業界を掘り下げ、業界別に調査結果の差異を検証します。

これから数ページにわたって、業種別の概要を紹介し、その後、個々のセクションで差異を詳しく検証します。読者の関心と統計上の有用性に基づいて、重点を置く業界をいくつか選択しました[6]。

表1の合計は、今年の調査におけるサンプルの大きさを示しています。ある業界が他の業界より安全である、または安全でないことを示すものではありません。協力企業・組織により提供されたデータが各業界をどれほど適切に代表しているかを示しています[7]。例えば大規模な建設会社で、記録されたデータ漏洩が1件しかない場合、そこからは何も結論を引き出せそうにないでしょう。しかし、金融業の場合のように、471件のデータ漏洩がある場合は、統計的に興味深い、確かなサンプルサイズといえます。

表1は、冷蔵庫を開けて料理に使える材料には何があるかを確認するようなもので、「パンを膨らませる」のに十分な業界があるか、と考えてください。

	インシデント				データ漏洩			
	合計	小規模の企業・組織	大規模の企業・組織	不明	合計	小規模	大規模	不明
合計	42,068	606	22,273	19,189	1,935	433	278	1,224
ホテル業(72)	215	131	17	67	201	128	12	61
管理サービス業(56)	42	6	5	31	27	3	3	21
農業(11)	11	1	1	9	1	0	1	0
建設業(23)	6	3	1	2	2	1	0	1
教育サービス業(61)	455	37	41	377	73	15	15	43
芸術/娯楽業(71)	5,534	7	3	5,524	11	5	3	3
金融業(52)	998	58	97	843	471	39	30	402
医療業(62)	458	92	108	258	296	57	68	171
情報産業(51)	717	57	44	616	113	42	21	50
マネジメントサービス(55)	8	2	3	3	3	2	1	0
製造業(31~33)	620	6	24	590	124	3	11	110
鉱業(21)	6	1	1	4	3	0	1	2
その他のサービス(81)	69	22	5	42	50	14	5	31
専門サービス業(54)	3,016	51	21	2,944	109	37	8	64
公的機関(92)	21,239	46	20,751	442	239	30	59	150
不動産業(53)	13	2	0	11	11	2	0	9
小売業(44~45)	326	70	36	220	93	46	14	33
貿易/通商業(42)	20	4	10	6	10	3	6	1
運輸業(48~49)	63	5	11	47	14	3	4	7
公益事業(22)	32	2	5	25	16	1	1	14
不明	8,220	3	1,089	7,128	68	2	15	51
合計	42,068	606	22,273	19,189	1,935	433	278	1,224

表1:被害にあった企業・組織の業界別および規模別セキュリティインシデント件数、2016年度のデータセット

[6] 関心のある業界が記載されていない場合は、dbir@verizon.comにご連絡ください。お手伝いいたします。
[7] 2015年度の報告書を引用すると、「公的機関のインシデント数の多さに惑わされないでください。この報告書の作成には多くの政府機関のCSIRT(コンピュータセキュリティインシデントレスポンスチーム)にご協力をいただいており、これらの機関では膨大なインシデントを扱っています。」

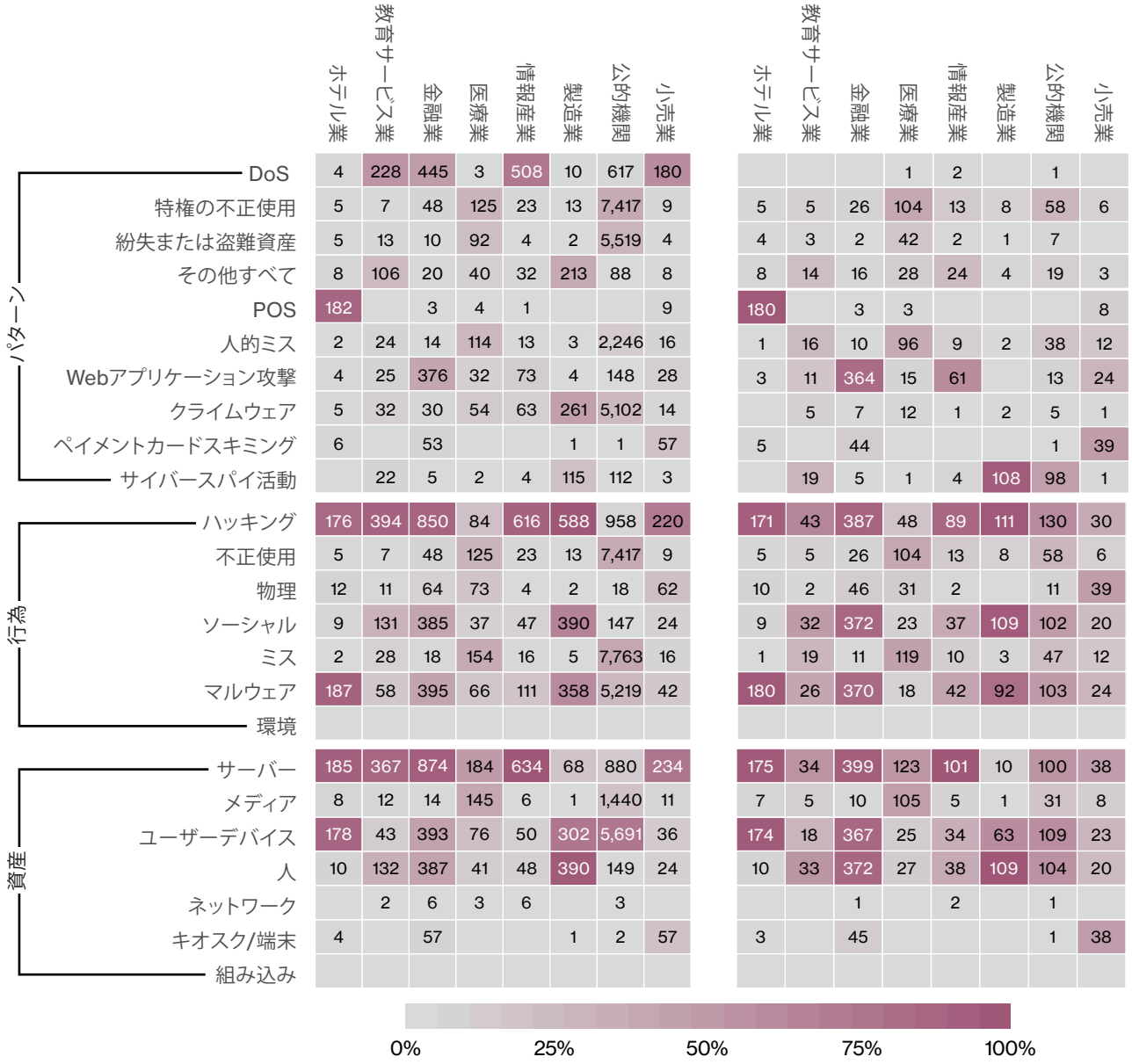


図9：業界別の比較（左：すべてのセキュリティインシデント、右：データ漏洩のみ）

図9は業界の比較に大変役立ちます。数字が雄弁に物語っているように、お客様の業界では何が頻発しているかを確認してください。詳しくは各業界のセクションで説明します。

我々のインシデントデータに加え、インシデント以外のデータから抽出した多くの有用な情報も、各業界の焦点に加えることができます。上図が冷蔵庫の中の食材を使った料理だとすると、次頁の図はスパイスラックと言えます。

業界別のDDoS

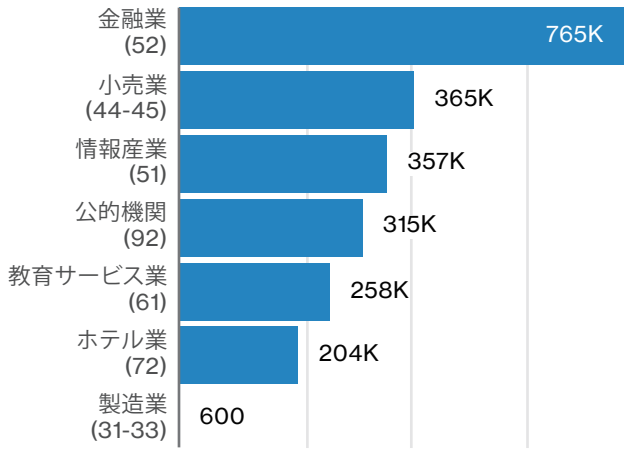


図10：業界別DDoSの平均的な規模（pps）（N=2,133）

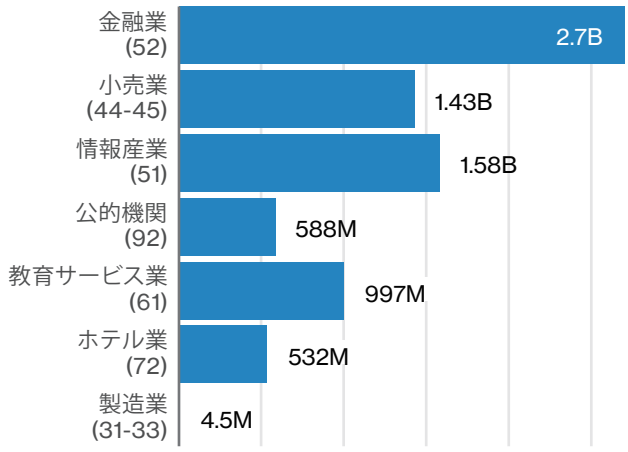


図11：業界別DDoSの平均的な規模（bps）（N=2,133）

図10および図11から、ビジネスやコミュニケーションをインターネットに依存している業界ほど、大規模なDDoS攻撃を受けやすいことがわかります。我々のインシデントデータセットでは、DoSが最も目立つパターンだという業界が非常に多いです。

製造業のように、当てはまらない場合でも、耐性があるというわけではなく、単に我々のデータに示されていないだけです。DoSパターンを確認して、このような攻撃のライフサイクルと可用性の関係に関する概要全体を把握してください。

業界別のフィッシング

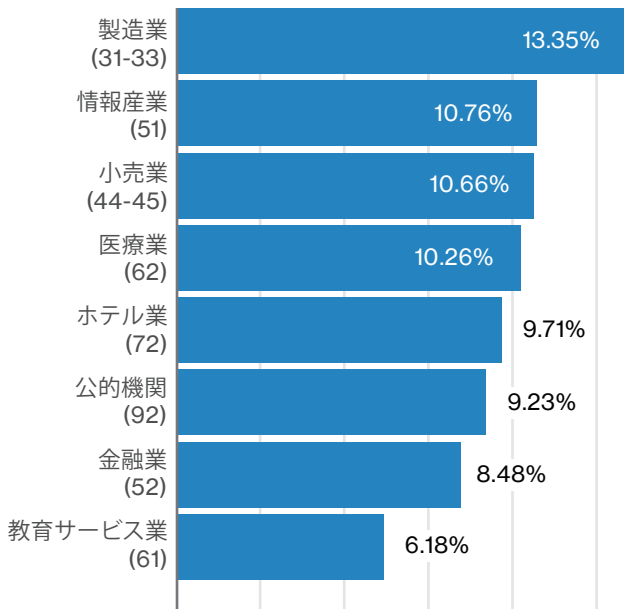


図12：業界別のキャンペーンごとの平均クリックレート（N=7,153）

図12から、各業界がどの程度、フィッシング攻撃を受けやすいかがわかります。セキュリティ意識向上トレーニングの実施結果から、完全にゼロの業界はないということと、大部分の業界で、フィッシングのリンクや添付ファイルをクリックするユーザーの割合に、大きな違いはないことがわかっています。フィッシングの詳細については、「対人攻撃」のセクションをご参照ください。

業界別のマルウェア

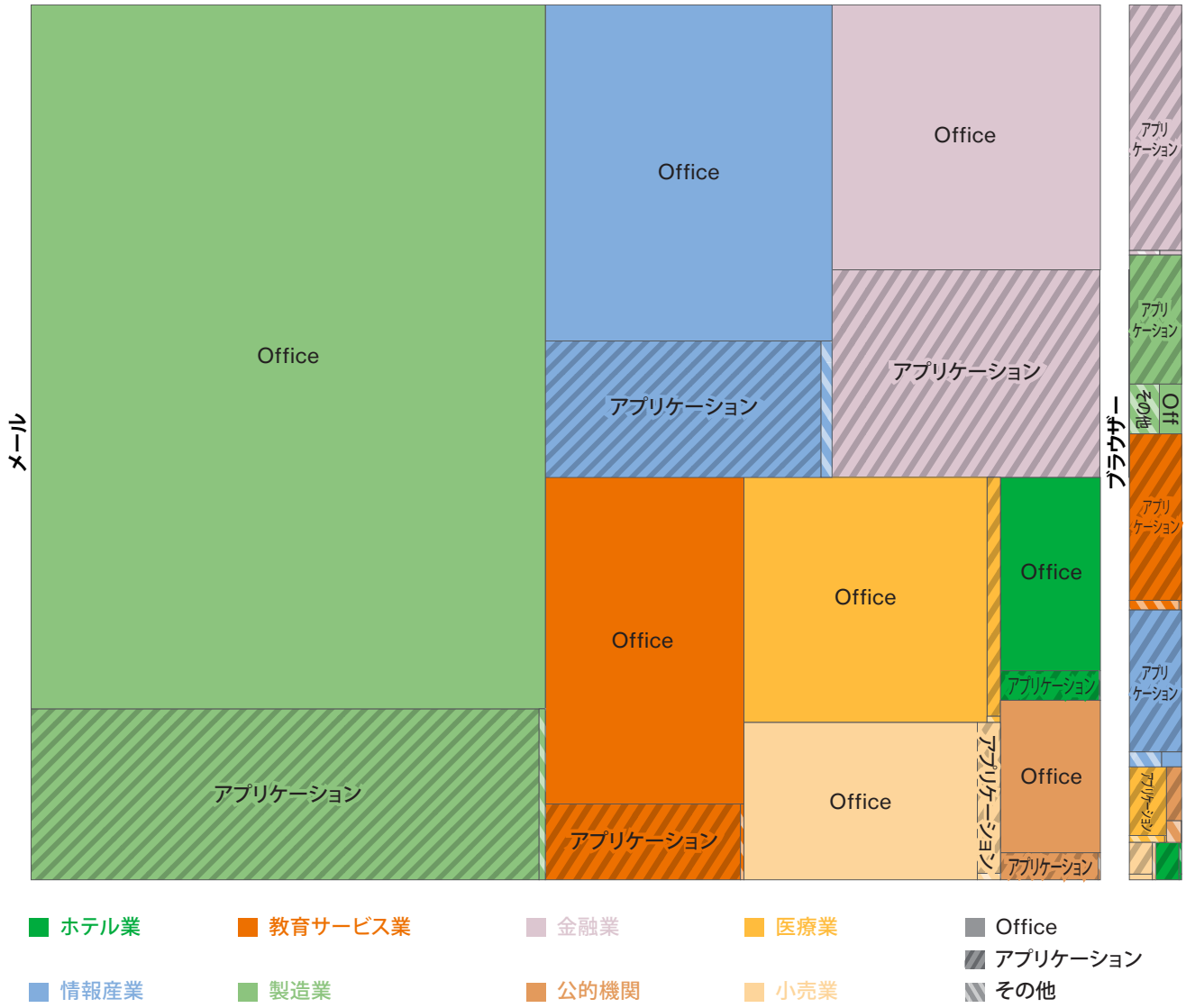


図13：業界別マルウェア検知の詳細（N=42,821,799）

図13では、オンザワイヤ検知[8]に基づく5千万件から、マルウェアを比較しています。サンプルにおける個々の業界の企業・組織数によって影響を受けることがないように、データを標準化・正規化しました。スペースの大きさは、業界の各カテゴリーにおけるマルウェア除去の件数を表します。このデータセットは、インシデントの報告書に含まれていませんが、マルウェアのインストール経路は、我々の実世界のデータと一致しています。

たとえば、製造業の企業・組織が電子メールベースのマルウェアの宛先として、しばしば想定されているという調査結果は、その業界のセクションで説明するインシデントデータを裏付けているとともに、図12のクリックレートとも結びついています。すべての業界にわたって、企業・組織にマルウェアを配布するために、最も利用されている手段は電子メールです。メールとWebブラウザという経路はさらに、Office文書、実行可能なアプリケーション、または「その他」に組み込まれたマルウェアに分けられます。

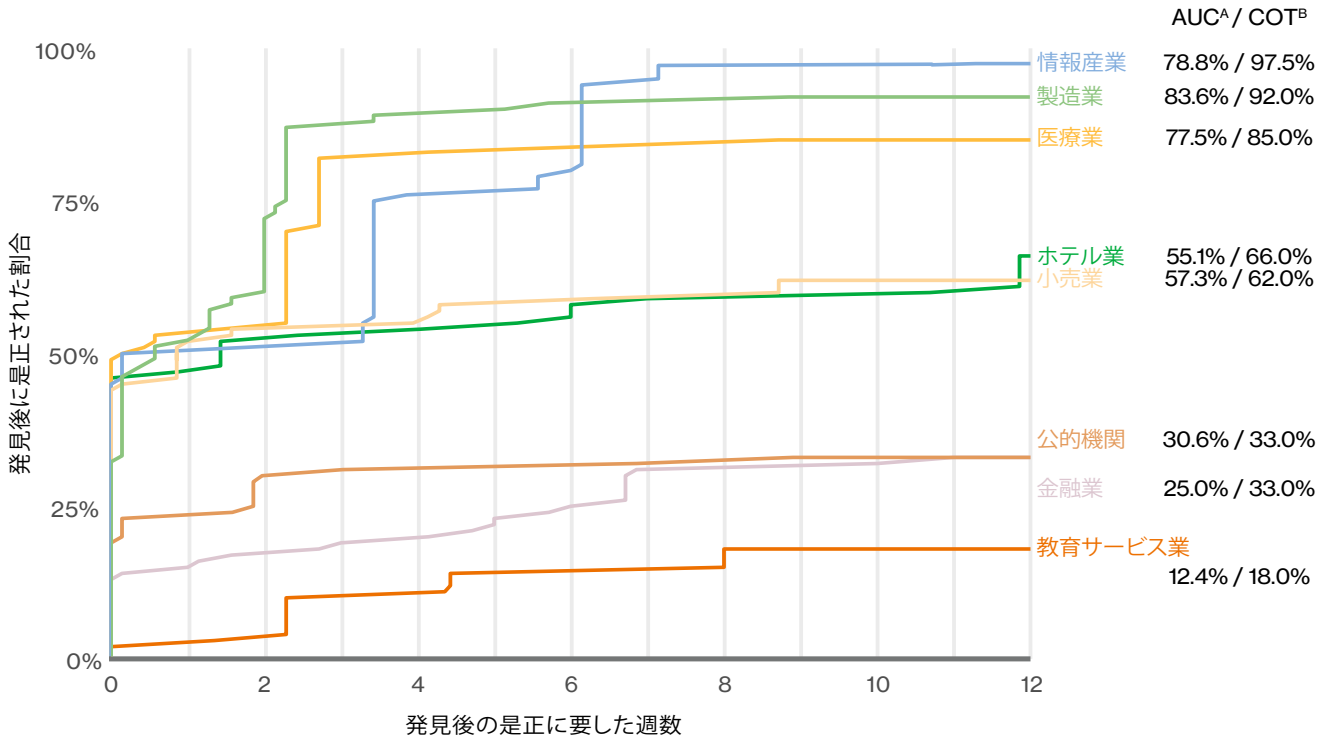
[8] JavaScriptのマルウェアは、クライムウェアのパターンで突出しています。しかしながら、5千万のサンプル、データセットを使用して図13が作成されていますが、JavaScriptのマルウェアは測定していません。

業界別のパッチ

我々はありがたいことに、6つの企業・組織から脆弱性スキャンデータを受け取りました。結合されたデータセットで、面白そうな話題を見つけようと、意気込んで取り掛かりました。我々の調査は、パッチに要する時間と未対応の調査結果がどれぐらいあるかに焦点をあてています。付録B:「パッチプロセスの積み残し」にマニアックな統計上の結果がありますが、ここでは、業界別にパッチを比較することによって、予習しておいていただきたいと考えます。いきなり下の図に飛びつく前に、物事をはっきりさせましょう。

お客様の環境には、発見された特定の脆弱性と対象となる資産に応じて、長い・短いといったパッチサイクルがあるはずです。脆弱性は下の図表では「イコール」として扱われ、企業・組織は脅威レートと潜在的な影響の係数を特定して、COT[B] を見直す、独自のパッチに要する期間を設定する必要があります。

さて、図14に基づくと、情報産業がトップで、教育サービス業が最下位ということでよいでしょうか。そうとは限りません。事前調査によると、脆弱性は最初のサイクルの間にパッチが適用されるか、長期間放置されがちになるかのいずれかです。この現象にはいくつか妥当な理由があり、脆弱性の調査は継続していく価値がありそうです。有力な仮説は、他のコントロールがすでにある、悪用できるような脆弱性ではない、または誤判定です。しかし、業界によって、大急ぎで対応するところもあれば、ゆっくり着実に進めるところもあり、興味深いです。放置されるものが何であるかを理解することが重要です。付録Bで、このように放置される脆弱性について再び扱います。デバイスタイプと資産タイプの間で、どのような関連があるのか、じっくり検証しましょう。



A. AUC（曲線下面積）
通常のパッチプロセスを待たず、潜在的脆弱性にどの程度、対処したかを測定したものです[9]。分かりやすく言うと、多くの脆弱性に即座にパッチを適用した場合、80日後に対処した場合に比べて、AUCは高くなります。

B. COT（定時完了）
通常のパッチサイクルのどこかで対処した調査結果の割合を示します。「積み残し」は、パッチサイクル終了後のスキャンでも存在する脆弱性を指します。上の図では、すべての業界が第12週になると安定してきます。したがって、この場合は12週間を「定時」の長さにしました。

図14：業界別パッチサイクルの比較

[9] データ専門家への注意：ベライゾンにおける曲線下面積の使い方は、ROC曲線下面積と同じではありません

ホテル業
および外食産業

頻度	外部96%、内部4%（データ漏洩）
上位3パターン	POSへの侵入、その他すべて、および特権の不正使用がホテル業におけるデータ漏洩全体の96%です。
攻撃実行者	外部96%、内部4%（データ漏洩）
実行者の動機	金銭目的99%、悪意1%未満（データ漏洩）
漏洩したデータ	支払情報96%、個人情報2%、認証情報1%
要約	この業界はPOSへの侵入が優勢でした。その大部分は日和見的であり、金銭が動機であり、マルウェアやハッキングといった攻撃行為を伴います。。侵害に要する時間はわずかですが、発見して囲い込むまでの時間は、いまだに何か月にも及びます。過去の年度と比べて、不正の発見件数が増えています。

いらっしゃいませ

サービス業は少なくともPOSへの侵入に関してはよい「おもてなし」がされていません。POSへの侵入は不断に続いており、コンチネンタルブレックファストと同様に満足することはありません。真っ先に浮かぶのはホテルでしょうが、レストランもこの業界に含まれ、被害者の大部分を占めています。外食産業の被害者は、IT部門、CISOなどを持たない、小規模なところが多く、ペイメントカードを受け付けているので、日和見的攻撃の標的になっています。

では、ホテル業と最もつながりの深いインシデントパターンから見てみましょう。図15が示しているとおり、POSの傾向は2年前に比べて低下したものの、いまだにトップです。一方、「その他すべて」と「特権の不正使用」のパターンは、どちらも増加していますが、ごくわずかです。したがって、POSへの侵入に重点を置きます。

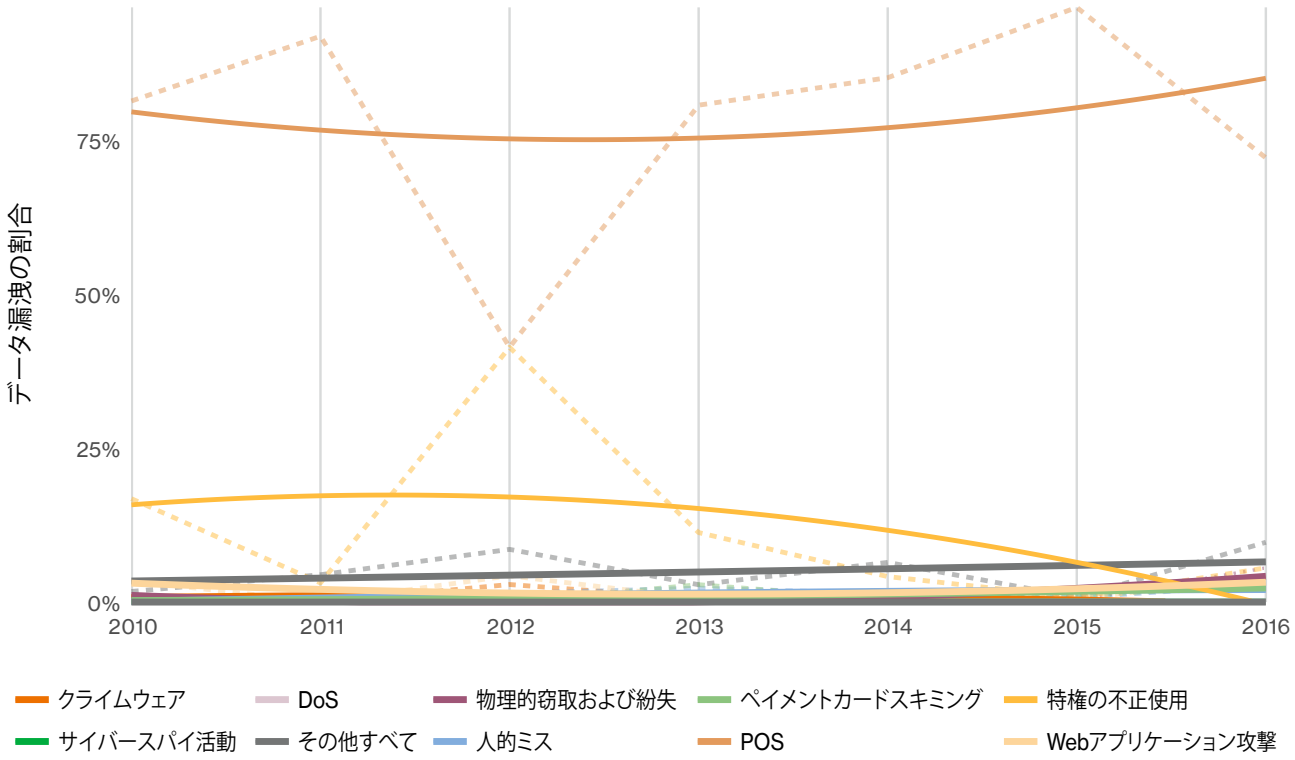


図15：ホテル業界のデータ漏洩におけるインシデント分類パターンの頻度に見る経時変化

すでに指摘したとおり、データ漏洩の96%は、外部実行者が関係していました。金銭的な動機で、機会に乗じて標的を攻撃し、ペイメントカードデータを侵害する、組織犯罪グループによる攻撃がほとんどです。マルウェアおよびハッキングという攻撃行為のカテゴリーは、この業界に対する攻撃に一般的に見られます。そして第三者が管理するPOSデバイス（端末とコントローラーの両方）が侵害された資産の大部分を占めていました。

図16に示した具体的な攻撃行為の種類は、シェフのスペシャルである、『放し飼いのRAMスクレーパー・ソテーC2添え』です。バルサミコ風味のブルートフォースソースで、キーロガーと認証情報の上にのせてご提供いたします[10]。

[10] グルテンフリーのキーロガーについては、ご利用のサーバーにお問合せください。

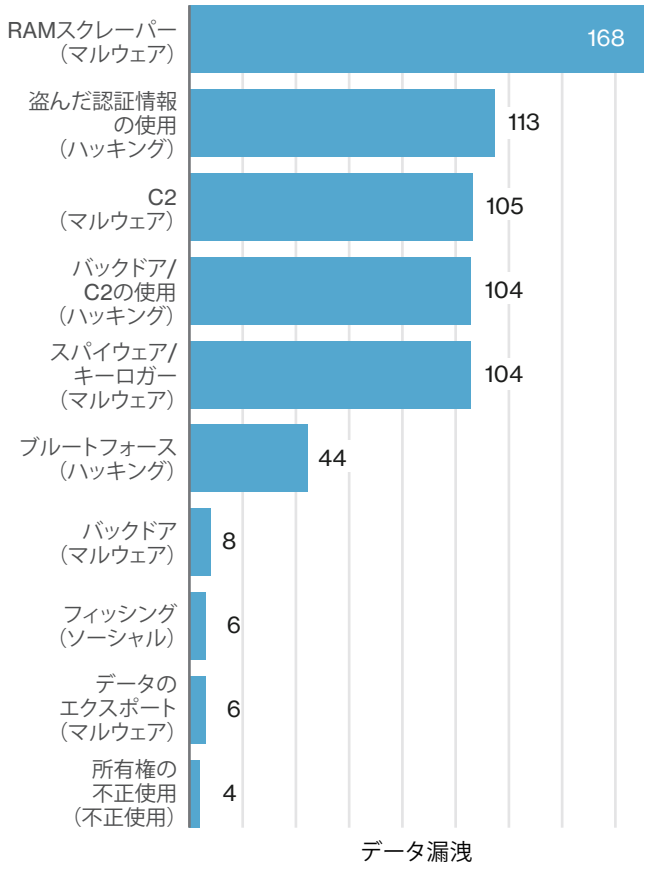


図16：ホテル業界のデータ漏洩で上位の攻撃行為（N=197）

マルウェア関連のデータ漏洩に関するかぎり、96%をRAMスクレーパーが占めている一方、60%がC2およびスパイウェア/キーロガーを備えていました。いずれも、最初のアクセス成功後にインストールされていました。これら上位3つのマルウェアが含まれている170件のデータ漏洩のうち102件で、データ漏洩に3種類がすべて含まれていました。これは、（少なくとも、3種類のうち1つが含まれた）データ漏洩の過半数は、C2機能を備えた、POSマルウェアの多次元亜種・変種の産物であることを意味します。ここで明確にしておかなければならないのは、これは特定のタイプのPOS侵害に特徴的であり、必ずしも全面的な傾向ではありません（我々は単に、データによる物語を伝えているだけです）。

盗んだ認証情報とバックドア/C2の使用が、最も有力なハッキングタイプであり（データ漏洩の過半数に相当）、ブルートフォースが3位に続いています。このような攻撃の多くに、有効なパートナーの認証情報とバックドアを使用している実行者が関与していました。また、その3分の1は、ハッキングの経路としてデスクトップ共有を示していました。

> **いつでも好きな時にチェックアウトはできますが、決して外へ出て行くことはできません**

明らかに、イーグルス（ロックグループ）が名曲ホテル・カリフォルニアから抜け出せないように同じパターンが続いています。ハッカーは今後も無限にチェックインし続けます。データ漏洩のタイムラインはむしろ、憂鬱な状況を示し続けています。侵害に要する時間はわずか数秒になり、盗み出すのに要する時間は数日、発見と囲い込みに要する時間は数か月の長丁場です。驚くことではありませんが、不正検知が最も有力な発見方法であり、すべてのデータ漏洩の85%を占めていました。その次は法執行機関の発見（4%）によるものです。

そろそろまとめに入ります。この業界は、POSに対する攻撃が蔓延しています。今年のデータでは、ホテル業界がPOSへの侵入のトップであり、そのパターンのなかでは87%に達しました。さらに詳細を知るには、ご遠慮なく、そのインシデントパターンのセクションにお進みください。

考慮事項：

Killing me softly with malware — この業界で発生しているソフトウェアインストールのレベルを引き下げる必要があります。この種の完全性に対する侵害が今年のデータ漏洩の94%を占めているからです。

ご使用前にこのタブを外してください — デフォルトのパスワードを使用してはなりません。犯罪者の仕事がものすごく簡単になるからです。

ここからあそこへはたどり着けない — POSネットワークへのリモートアクセス権をフィルタリングします。ホワイトリスト化されたIPアドレスからの接続に限り、許可してください。

時代に遅れない — 迅速に、一貫性のある形でパッチを適用し、すべての端末とサーバーで最新バージョンのソフトウェアが稼働しているか、よく確認してください。

教育
サービス業

頻度	455件のインシデント、73件でデータ漏洩を確認
上位3パターン	サイバースパイ活動、人的ミス、およびその他すべてが教育サービス業における全データ漏洩の67%を占めています
攻撃実行者	外部71%、内部30%、パートナー3%（データ漏洩）
実行者の動機	金銭目的45%、スパイ活動43%、愉快犯9%（データ漏洩）
漏洩したデータ	個人情報56%、機密情報27%、認証情報8%
要約	このセクションでは、確認されたデータ漏洩に重点を置きますが、教育サービス業は今なお常に、DoS攻撃の標的でもあります。2016年は、スパイ活動に関連するデータ漏洩件数が大幅に増えているという結果がでました。

取り組みは「A評価」でよいでしょうか？

スパイ活動と人的ミスは確かにこの1年、教育サービス業において頭の痛い問題でした。サイバースパイ活動はデータ漏洩の26%に存在し、人的ミスでは、それに迫る22%でした。昨年は教育サービス業において、サイバースパイ活動パターンは、データ漏洩の5%未満で、Webアプリケーション攻撃が支配的でした。図17は、スパイ活動がどれほど増加したかを時系列で示しています。国家の支援を受けた集団から見れば、大学は単にピザとテールゲートパーティーの場ではなく、無数の分野にわたって調査研究が行われている場と映ります。

ベライゾンのデータ漏洩に関する調査結果は、学生と職員の双方について、過半数が保管された個人情報の侵害と漏洩に関係していたことを示していますが、一方、知的財産の漏洩は4分の1余りでした。機密情報を安全に保管しようとすると、この業界特有のさまざまな課題に直面します。特に、この業界の本質であり、常につきまとうのは、根底にある自由で開放的な意見/情報交換です。さらに、専門能力も好奇心もさまざまなレベルの学生/ユーザーの分布を考慮する必要があります。言うまでもなく、データ主体としての彼らの役割はもとより、PII（個人の特定が可能な情報）およびその他の情報を保護する必要があります。セキュリティコントロールを実施しながら、開放性という文化を維持するというのは、事実上、MITのコース番号16.512です。

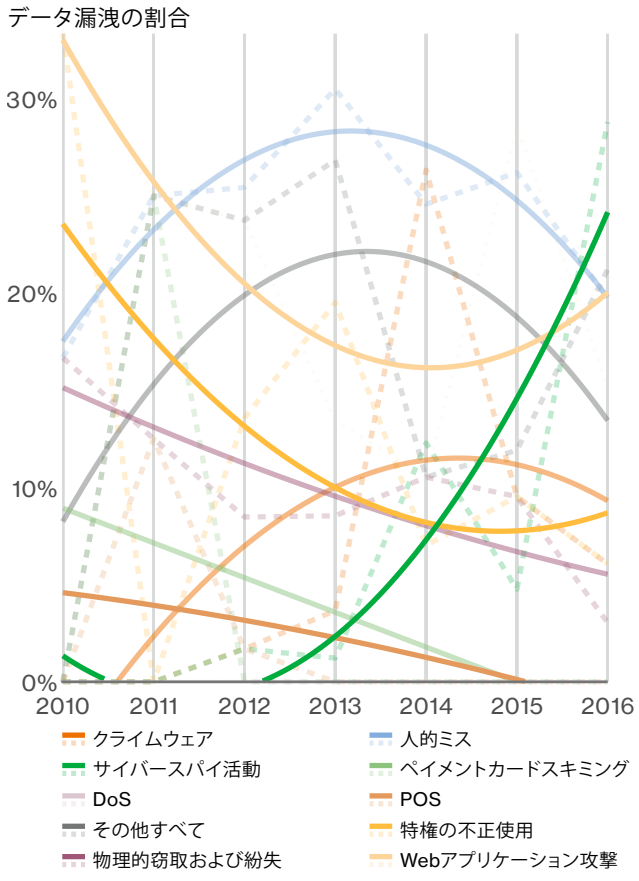


図17：教育サービス業のデータ漏洩におけるインシデント分類パターン別に見た頻度の経時変化

今度は次のように問われるかもしれません。「誰がこのようなデータ漏洩の背後にいるのですか？ 本質的に標的型なのでしょうか、それとも日和見的なのでしょうか？」良い質問です。星3つ、差し上げましょう。データは、国家の支援を受けた実行者（データ漏洩の過半数に関与）がこのような教育機関を標的にしていたことを物語っています。金銭目当てに組織犯罪グループが関係したデータ漏洩も、わずかながらありました。内部実行者が関係したデータ漏洩は、ほとんどが悪意ではなく、人的ミス、特に機密データの誤配や公開ミスが原因でした。

「何を」と「誰が」を話したところで、今度は「どうやって」を簡単に説明しましょう。

上で指摘したパターンの中で、本当にトラブルメーカーだった脅威のカテゴリーは、ハッキング、ソーシャル、それにマルウェアです。昨年と比較して、ソーシャルとマルウェア攻撃を伴うデータ漏洩が増えています。ソーシャルはデータ漏洩のほぼ44%に相当し、マルウェアは3分の1強で見られました。ソーシャル攻撃では、電子メール経由のフィッシングが最も流行していた種類ですが、Webアプリケーションに対して盗んだ認証情報を使用することが、ハッキング行為で最も利用された戦術でした。上位3つの行為（ハッキング、ソーシャル、マルウェア）間に明確な結びつきがあった、代表的なデータ漏洩を検証しようと考えました。攻撃行為が重複しうることは確実なので、これら3つのカテゴリーのうち、2つ以上があるデータ漏洩は、どの程度の頻度で発生しているのかということに、興味を持ちました。図18で確認できるように、ソーシャルメディアに投稿されたデータ漏洩の3分の1余りは、「関係しあって」おり、多面的な攻撃の手口を示しています。

このセクションではデータ漏洩に重点を置きましたが、教育機関にとって、DDoS攻撃が重大な脅威であり、すべてのセキュリティインシデントの半分を占めているということも事実です。これらの攻撃は30ページの研究論文に取り掛かる際、怠慢に打ち勝ち素晴らしいものを次々に生み出すのにまだ1週間の猶予があると思っていたとき、実は締め切りが翌朝であったことに気付いてしまった状況と類似しています。パニックが始まり、思考停止に陥り、隅の暗がりに逃げ込み、膝を抱え丸くなります。この悪夢はまさに、可用性低下であり、この業界に対するDDoSインシデントも同様です。

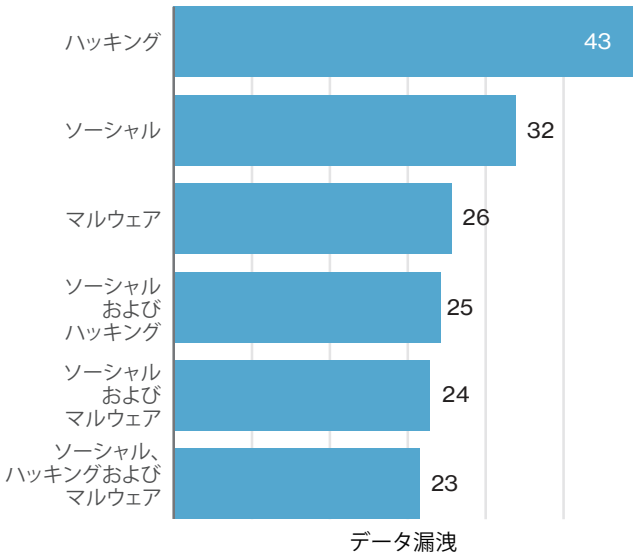


図18：教育サービス業のデータ漏洩における手口間の関係（N=73）

考慮事項

「All aboarded」— セキュリティ意識の向上に関して、お客様の従業員と学生を教育し、フィッシングの可能性、なりすましなど、疑わしい活動を報告するように促し、労います。

Classes are cancelled — 必ず、対応計画を作成し、災害復旧計画を毎年または1年おきに実践して、異常に高いトラフィックへの備えが万全であることを確認します。

金融業
および保険業

頻度	998件のインシデント、471件でデータ漏洩を確認
上位3パターン	DoS、Webアプリケーション攻撃、およびペイメントカードスキミングが金融業の全セキュリティインシデントの88%を占めています
攻撃実行者	外部94%、内部6%、パートナー1%未満（全インシデント）
実行者の動機	金銭目的96%、スパイ活動1%（全インシデント）
漏洩したデータ	認証情報71%、支払情報12%、個人情報9%
要約	DoS攻撃が最も一般的なインシデントタイプでした。 確認されたデータ漏洩は、ATMスキミング操作とともに、顧客のパスワードを盗んで再利用する、銀行を狙ったトロイの木馬としばしば結びついていました。

我々のデータセットに従来の銀行強盗はありませんが、上の要約セクションが、外部の関係者がいまだに正当（不正）な稼ぎを期待していることを物語っています。

金融業界全体は、多数のサブセクターからなり、攻撃実行者の戦術は必ずしも類似していません。例えば、パーカーとスエットをまとった人物がATMにスキミング機器やカメラを取り受けないか、心配しなければならないのは、民間銀行または信用金庫の現実ですが、保険業者や投資銀行にこれは当てはまりません。後に登場する図表では、ニッチな攻撃は除外されています。詳細をつきつめると独自のパターンが得られる程、それぞれユニークだからです。一方、DoSは誰もが標的になり得る攻撃の手口でありながら、やはり後ろの図表からは除外されます。これは、業界における確認された（ATMスキミング以外の）データ漏洩により注視できるようにするためです。

ここまで来ると大掃除のような気分ですが、もう一度、確認しましょう。銀行を狙ったトロイの木馬は存在しますが、放置されて莫大な数となったデータ漏洩は、沈黙の誓いで知られるトラピスト修道院に電話を掛けるテレマーケターのように会話を独占してしまいます。より興味深い調査結果が明らかになるように、これらも除外しています。

ボットネットについて

ボットネットは今なお、金銭的利益を得るために組織犯罪グループが作成し（貸し出す、または自ら）利用している強力なツールです。ゾンビマシン群による金融機関への攻撃の1つは、DoSボットネットの利用です。これは、数の力を生かして、被害者のインフラストラクチャに対して望ましくないトラフィックを大量に放出します。2012年には、米国の銀行に対するイデオロギー型の攻撃で、全国の注目を集めました。もう1つ、注目すべきは、銀行を狙ったトロイの木馬に感染した消費者向けデバイスです。銀行を狙ったトロイの木馬は、サイバー犯罪の世界で決して新しいものではありませんが、いまだに偏在し、まだまだ進化を続けています。金融機関にとって難しいのは、不正な行為、VERIS用語の「攻撃行為」の多くが内部で管理している機器ではなく、顧客に向けられることです。

一連の事象は次のとおりです。

1. 消費者に不正な添付ファイルを送付します。
2. 消費者の機器にマルウェアがインストールされ、いつ銀行取引サイトにアクセスしているかが特定されます。

3a. キーロガーがユーザーの認証情報を取得し、不正に再利用します。または

3b. ユーザーのWebリクエストが偽サイトに転送され、そこで入力された認証情報が捕捉されます。

4. 攻撃実行者はSMSの第2要素認証コードの生成を誘因するよう顧客のふりをしてアプリケーションの正当な認証情報を発行します。
5. 第2要素認証コードが偽のWebサイトに伝えられ、ステップ4が繰り返されます。
6. 口座残高が減ります。

2016年7月、米国標準技術局（NIST）は上記のシナリオと、SMSで配信された第2要素を取得するように設計された、モバイルエンドポイントの不正なコードを記載し、第2認証要素としてコードをテキストで送信しないように勧めました。SMS経由で2要素認証を使用するのは、オオカミの攻撃を軽減するためにわらではなく、小枝で家を建てるようなものだとは思いませんが、敵について考える機会になります。多要素認証を破ると、再利用するために両方の要素を取得する手段を現実的な方法で編み出します。

ATMスキミング、DoS、およびボットネットを除外し明らかになったもの：

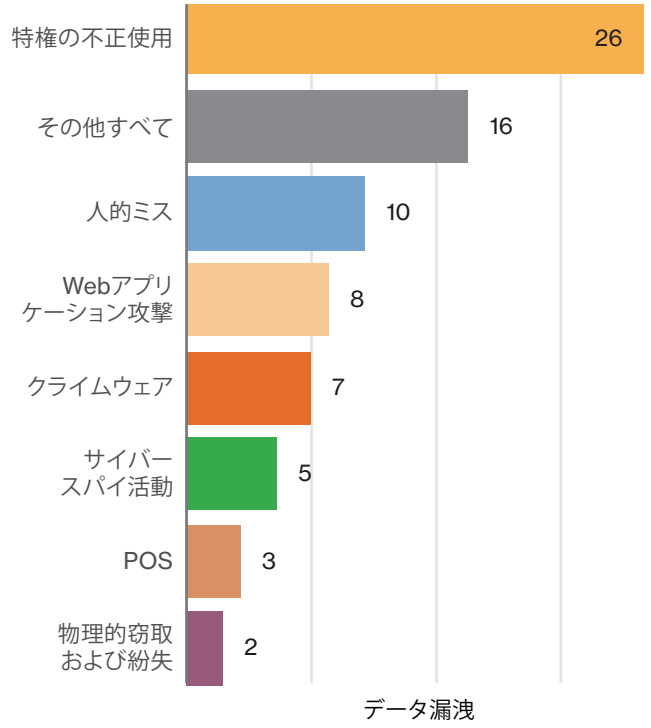


図19：特定の金融業界のデータ漏洩におけるインシデントの分類パターン（N=71）

銀行の従業員は普段から勤務中に、自分が得るに値すると思えるボーナスを稼ぐ手段としてのデータにアクセスできます。不正送金のためにシステムにアクセスする、またはアイデンティティ窃盗を目的に、顧客の個人情報を使用するというのが、金銭を動機とする不正使用の代表的パターンです。興味深いことに、銀行口座情報より個人情報の方が好まれています。恐らく、送金したときに、痕跡が後に残ることを警戒し、個人情報を利用して新たに与信枠を取得する、または自分の職場以外で不正を働く方を好むのでしょう。

「自分の職場では不正を働くな」という格言がありますが、捕まるリスクがあるため、これを守っているのかもしれません。

不正送金のためにシステムにアクセスする、またはアイデンティティ窃盗を目的に、顧客の個人情報を使用するというのが、金銭を動機とする不正使用の代表的パターンです。

金融業界は、換金が容易なデータを保護しなければならないだけではありません。投資銀行およびその他の非営利機関は、投資戦略、吸収合併、市場影響要因など、スパイ活動を動機とする実行者が追い求めるような情報を保有しています。このような動機に関連する戦術の詳細については、サイバースパイ活動のパターンをご参照ください。

「その他すべて」のカテゴリーの多くはすぐ結論に結び付く記述子がない、または9パターンに分類できないハッキングやフィッシング攻撃を特徴としています。

考慮事項

Taunt them a second — すべてのWebアプリケーションを守るために2要素またはマルチ要素認証を使用してください。

Make a new plan, Stan — この業界はDoS攻撃の標的になりやすいです。DoS保護/緩和サービスを導入するとともに、プロバイダーとの契約詳細をきちんと把握してください。

It's not that I don't trust you, but… — 従業員から目を離さず、彼らの活動を定期的に監視してください。職務に不要な権限を与えないでください。また、解雇および自発的な辞職後は必ず、ただちにアカウントを無効にしてください。

サイバー詐欺に取り組むもう1つのソリューション

– 法律事務所 Mishcon de Reya

現在、不正の大半はオンラインで行われ、警察は犯罪発生率と規模に追いつけません。公的機関は人手不足のため、盗まれた金銭を取り返せることはめったになく、サイバー犯罪が処罰されることはありません。サイバー犯罪はますます巧妙になっており、この種の犯罪が落ち着く兆しはありません。

現在、英国のロンドン市警察が試験的に運用している、独創的なソリューションがあります。法執行機関がMishcon de Reyaおよびその他の民間企業と協力して、刑法ではなく、通常の民法の修正で、資産を特定し、取得し、犯罪者から回復するための2年がかりの新たな取り組みがあります。

これにより陪審団が犯罪の被害者が他の方法では損失の回収が困難な場合、詐欺師の資産から損失を回収できるようにすることが期待されます。主張が金銭的かつ法的に合法な場合、陪審団は被害者に訴訟の機会を提供し、警察の証拠を資産回収のために利用します。

警察と民間企業間で情報を共有することで、法執行機関が刑事/民事運営委員会のもとで刑事的手段に加え、民事的手段も念頭に共同指示書の作成が可能であることを、同じ加害者を持つ被害者グループに知らせることができるようになります。被害者グループはこの場合、犯罪者の追跡、資産凍結し、証拠を押さえるための第三者開示命令、英国では捜索命令および資産凍結命令、またはその他の国では類似した命令により加害者に民事的制裁を与えます。この民事的手段を使うと、プロセスのスピードアップが可能になり、被害者は損失を回復する最良の機会を得ることができます。

サイバー犯罪が刑事法廷と同様に民事法廷でも追及されるため、いずれこの共同戦略は将来の法執行に多大な影響を与える可能性があります。サイバー詐欺に免疫のある企業・組織や個人などいない世の中では、素早く犯罪者を特定し、迅速に資産のコントロールを取り戻す能力が極めて重要です。

医療業

頻度	458件のインシデント、296件でデータの漏洩を確認
上位3パターン	特権の不正使用、人的ミス、物理的窃取および紛失が医療業界におけるデータ漏洩の80%を占めています
攻撃実行者	外部32%、内部68%、パートナー6%（データ漏洩）
実行者の動機	金銭目的64%、愉快犯23%、悪意7%（データ漏洩）
漏洩したデータ	医療情報69%、個人情報33%、支払情報4%
要約	医療業には、大量の個人情報および医療情報を保護することと、医療従事者がそれらの情報に迅速にアクセスできるようにすることのバランスを追及するという、やっかいな仕事がつきものです。内部実行者の典型は、好奇心から患者データにアクセスするか、アイデンティティ詐欺を働く職員です。

「たやすい」からはほど遠い

医療業の企業・組織で情報セキュリティ担当でいるというのは、決して容易ではありません。電子的に（集中データベース、ラップトップ同様）保存された、膨大な医療記録を扱わなければなりませんし、いまだに紙媒体のものもあるでしょう。このような記録には、個人情報（氏名、住所、社会保障番号）が伴っていることもよくあります。患者ケアの必要上、この情報を迅速に利用できなければならないので、厳格なアクセス制御方式は、メリットよりデメリットが大きくなる場合もあります。「医療業界のCISOにとってストレスになるもの」リストに追加される項目がもう1つあります。この業界に対する開示要件です。

医療業界では、内部者の不正使用が大きな問題です。実際、従業員がデータ漏洩の主たる攻撃実行者になっている、唯一の業界です。図20を見ると、興味深いことに、内部者の動機として、金銭目的と愉快犯がほぼ同率です[11]。これは、大勢のスタッフメンバーがアクセスできる大量の機密データの産物と言えます。こうした機密データには、アイデンティティの窃取に最適なPIIや（知りたいという）好奇心を掻き立てる（時として友人や親戚の）医療履歴が含まれます。

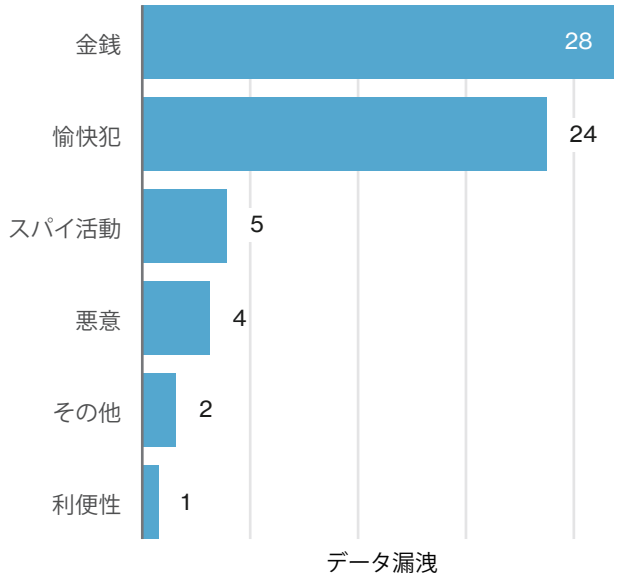


図20：医療業界のデータ漏洩に見る内部実行者の動機（N=64）

[11] あとで説明しますが、ミスに動機は無縁です。

間違いの喜劇

医師がラップトップを紛失する、レントゲン写真をうっかりごみ処理場に出してしまう、従業員がAさんの退院許可をBさんに出してしまうといったような人的ミスが今年も上位3パターンにとどまっています。図21のデータ漏洩件数から、誤配、廃棄ミス、紛失資産の合計が医療業界におけるデータ漏洩全体の約30%であることがわかります。これは、懸念すべき対象は悪意のある内部者だけではないことを物語っています。

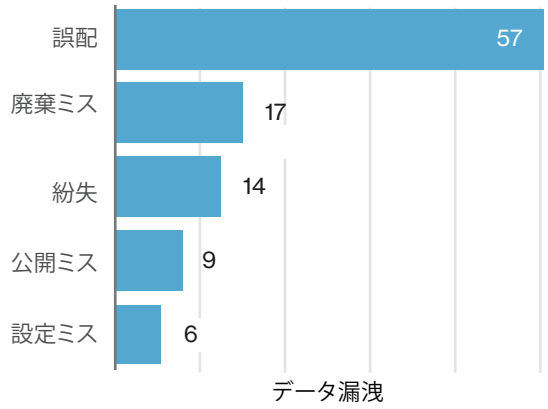


図21:医療業界のデータ漏洩で上位を占めているミス (N=113)

トール、ダーク、ランサム

我々のデータセットにおいて、ランサムウェア攻撃はデータ漏洩とみなされていません。通常、データの機密性が侵害されたことを確認できないからです。しかし、米国保健社会福祉省 (HHS) は、報告目的でランサムウェアインシデントをデータ漏洩として扱うようにと指導しています[12]。今年、ランサムウェアは医療業界におけるマルウェアインシデントの72%を占めています。

タイムライン

医療業界の発見タイムライン (図22) は、データセット全体より健全に見えます。残念ながら、(数日以内に発見されたデータ漏洩を検証することによって) 戻ってきた調査結果から、大部分は情報の誤配や盗まれた資産に関連するデータ漏洩であることが判明しました。今後、確認した記録とその従業員が直接担当した患者の相関関係に基づいて、医療記録の不正アクセスを迅速に特定する事例が増えることを期待しています。

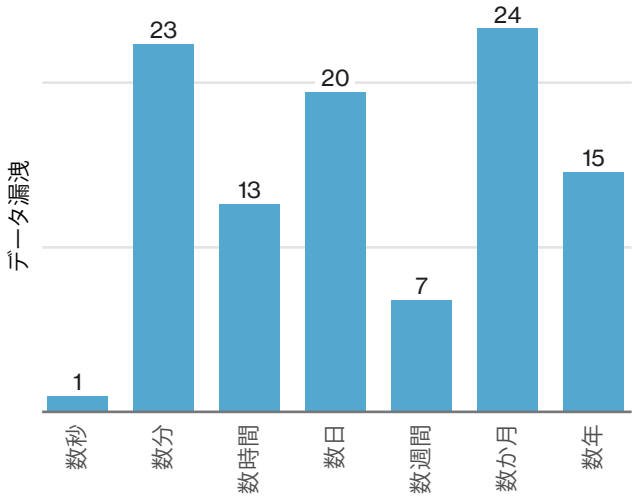


図22:医療業界でデータ漏洩の発見に要する時間 (N=103)

考慮事項

Achtung, baby – 自分の行いに注意を払ってください。医療業における問題の多くは、防ぐことのできたミスです。公開ミスを避けるために、オンライン変更には別の人による承認を義務付けるプロセスを設けてください。PIIの破棄について、ポリシーを策定し、それが遵守されていることを確認してください。すべてのモバイルデバイスを暗号化し、デバイスの紛失または盗難による影響が限定されるようにしてください。

I love it when a backup plan comes together – ここでは詳しく説明しませんが、ランサムウェアは医療業界でますます猛威を振るっています。定型業務としてすべてのシステムをバックアップし、この種の攻撃を受けた場合に、即座に代替が効くようにしてください。

See a doctor and get rid of it – 不正使用が非常に多いため、従業員の行動を定型業務としてチェックし、業務上の必要性がない情報を表示、ダウンロード、または印刷していないか確認してください。警告バナーを使用し、監視を実施しており、詮索する価値がないことを明示してください。

Token of my appreciation – 機密情報 (社会保障番号など) は記録の識別にのみ使用し、従業員にとって請求またはケアに必要だというのでなければ、可能な限り、トークン化してください。

[12] https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf

情報産業

頻度	717件のインシデント、113件でデータの漏洩を確認
上位3パターン	DoS、Webアプリケーション攻撃、クライムウェアが情報産業におけるインシデント全体の90%を占めています
攻撃実行者	外部97%、内部3%（全インシデント）
実行者の動機	金銭目的75%、愉快犯/イデオロギー/悪意18%、スパイ活動6%（全インシデント）
漏洩したデータ	認証情報56%、個人情報45%、内部情報6%
要約	情報産業におけるインシデントとデータ漏洩はどちらも、インターネットに接続するWebサーバーと強い結びつきがあります。

情報過多

情報産業（NAICS 51）には、ソフトウェア発行者から通信事業者、クラウドプロバイダーからソーシャルメディアサイト、オンラインギャンブルまで、あらゆるものが含まれます。ギャンブルといえば、パターンブレークアウトによって得られた証拠から、情報産業の企業・組織は保安官、ジェームズ「ワイルド・ビル」ヒコックとそっくりで、可用性に関する重大な問題（必ずしも、「死者の手」を持っているときとは限らない）を抱えていることが明らかです。歴史的な言及はさておき、結果がハッキング、特にDoSに偏っている（全インシデントの71%）という事実は、常識的な結果であり、大部分のインシデントがWebベースサイト/アプリケーションへのアクセス停止に基づいていることを示しています。

セキュリティインシデントから確認されたデータ漏洩までに状況が発展すると、ほとんどの場合、認証情報や個人情報がWebアプリケーション経由で収集され、影響を受けるメンバーの数は百万単位になることもよくあります。我々のデータは、データ漏洩の約60%に、影響を受けた資産、影響を受けた資産への経路、またはその両方として、Webアプリケーションが関係していることを示しています[13]。このようなデータ漏洩に的を絞ると[14]、この業界の企業・組織において、どのような戦術が使用され、どのような固有の問題が結果に影響するのでしょうか？

[13] Webアプリケーションが経路および影響を受ける資産として特徴づけられることは、大いにあり得ますし、実際よくあります。

[14] 資産の種類またはハッキング経路がWebアプリケーションの場合。

図23は企業・組織に潜り込むための認証情報を取得したり、データを盗み出したりする目的で、C2およびキーロガーソフトのインストールを含む強力な上位6種類の攻撃行為を示しており、フィッシング詐欺被害者がよく使われる経路を経由していることが分かります。このグループに続くのが、不明のハッキング（図に記載なし）とSQLインジェクション（SQLi）です。ということは、アプリケーションコードに対する攻撃は健在であり、実数はさらに大きい可能性があります。

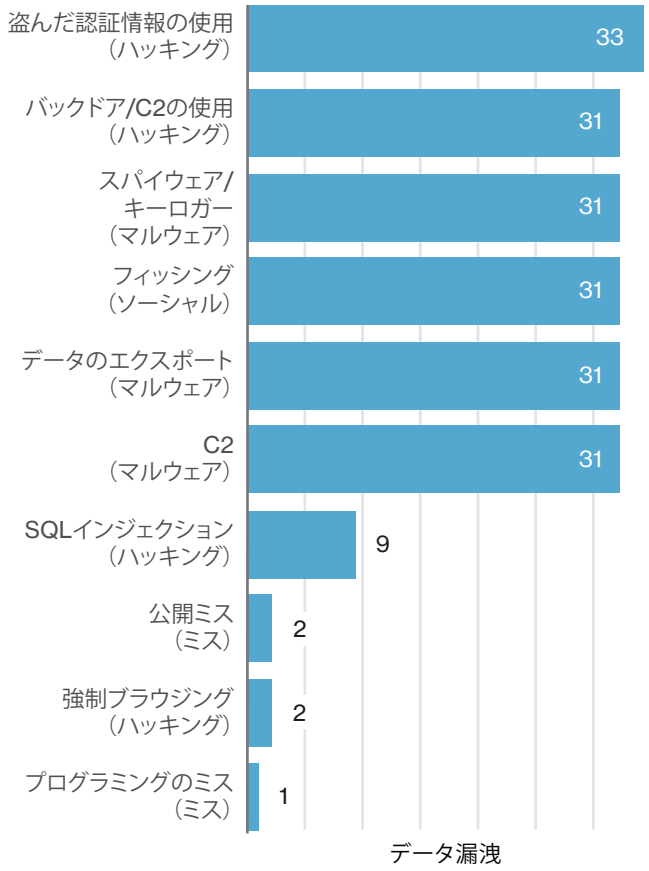


図23：情報産業において、Webアプリケーションが関係する、攻撃行為によるデータ漏洩の上位（N=48）

十分な情報により被害者のNAICSコードを6桁の数字に振り分けると、3分の1以上がカテゴリー519130（インターネット出版/放送およびWeb検索ポータル）に当てはまります。これは、小売業以外のWeb関連企業・組織を分類する、包括的カテゴリーです。Webプレゼンスがビジネス上重要であり、データを収集するための侵害の主な標的はWebアプリケーションで、データはユーザー名、パスワード（暗号化されたものもあれば、そうでないものもある）、および電子メールアドレスの組み合わせになることが多いです。

つまり、ユーザー情報を保存しているWeb関連企業であるため、ハッカーはユーザー情報を入手しようと、Webアプリケーションを追い求めます。もう1つの共通性は組織の規模であり、被害にあった企業・組織の4分の3以上が小規模で、専任のセキュリティ担当者やプロセスがありません。データ漏洩件数は膨大ですが、一般に規制された種類のデータ（ペイメントカード情報、保護すべき医療情報など）に比べ、機密性は低いと考えられます。サイト管理者がユーザー名/パスワードの漏洩をそこまで懸念していない場合もあるため、2要素認証を導入する、侵入テストを実行する、またはコンテンツ管理プラットフォームを最新の状態で維持するより、パスワード変更を通知して強制的に実行させる方が容易かもしれません。

「まあ、古いWordPressでマクラメレース編みの掲示板を運営しているわけではないし」とでも、おっしゃるのでしょうか。ごもっともです。Webアプリケーションが関係したデータ漏洩を除外すると、結果は多岐に渡ります。「その他すべて」のパターンがトップに躍り出て、さらに調査を進めたところ、データベースがハッキングされていた侵害が発見されましたが、補足データが不足しているため、それ以上分類できません。Webアプリケーションが関係していたことはほぼ確実ですが、むやみに信じるわけにはいきません。

考慮事項：

認証情報の設定 — Webアプリケーションおよびデータが保管されているその他のデバイスに管理者としてアクセスする場合、2要素認証を導入します。メンバーまたは顧客情報にアクセスするために再利用される盗まれた認証情報の有効性を低下させます。可能であれば、強力な認証の使用をユーザー層まで拡大します。

Don't be denied — DDoSレスポンスプランを策定し、事業継続/災害復旧のリーダーと連携します。ネットワークの使用状況を監視し、トラフィックが通常の正当な利用より増えた場合のスパイクに備えます。

すべてのシステム管理者は職場に戻る前に、サーバーソフトウェアを更新しなければならない — 打ち鳴らし続けられ軽視されるようになった警鐘：セキュリティの予防策。サーバーソフトウェア（OS、Webアプリケーション、プラグイン）を最新の状態で維持する行為、さらにセキュリティの脆弱性が公開され、パッチが利用可能になった場合に、それを認識する方法は、驚くようなことではありません。しかし、Shodan（検索サイトhttps://www.shodan.io/）の検索結果は、この不完全な社会に今なお、不適切な設定のサーバーが大量に存在していることを物語っています。

製造業

頻度	620件のインシデント、124件でデータの漏洩を確認
上位3パターン	サイバースパイ活動、特権の不正使用、その他すべてが製造業におけるデータ漏洩の96%を占めます
攻撃実行者	外部93%、内部7%（データ漏洩）
実行者の動機	スパイ活動94%、金銭目的6%（データ漏洩）
漏洩したデータ	企業秘密91%、内部情報4%、個人情報4%
要約	スパイ活動に関連する行為で戦略的優位性を獲得することが、この業界におけるデータ漏洩の大半を占めます。大部分は国家の支援を受けた実行者によって行われますが、内部のスパイ活動によって企業秘密が盗まれる事例もあります。

Spies like us

我々がまだ駆け出しの頃、報告書について受けた主な苦情の1つに、次のようなものがあります。「銀行業や飲食業、小売業であれば素晴らしい報告書だけど、私の企業秘密を狙っているのはAPTなので何の役にも立ちません」何年も前になりますが、我々の情報漏洩のデータは、盗まれたペイメントカード情報から、セキュリティ上重要である知的財産を保護する企業・組織が経験する、一般的な問題まで拡大されました。製造業に対応するNAICSコードは、「原料、材料、または成分を機械的、物理的、または化学的に変化させ、新製品にすることを目的とする民間企業・組織」から構成されます。[15] 要するに、モノ作りです。モノを作る場合、品質の向上を目指したり、より安価になるようにしようとする競合者が必ずいます。安く仕上げる最良の方法は、研究開発の一切合切を誰かに負担させ、その成果である知的財産を単純に盗むことです。それを念頭に置いて図24を参照すると、製造業では、データ漏洩に結び付いたパターンとして、サイバースパイ活動が他と比較しても圧倒的であることに納得するはずです。

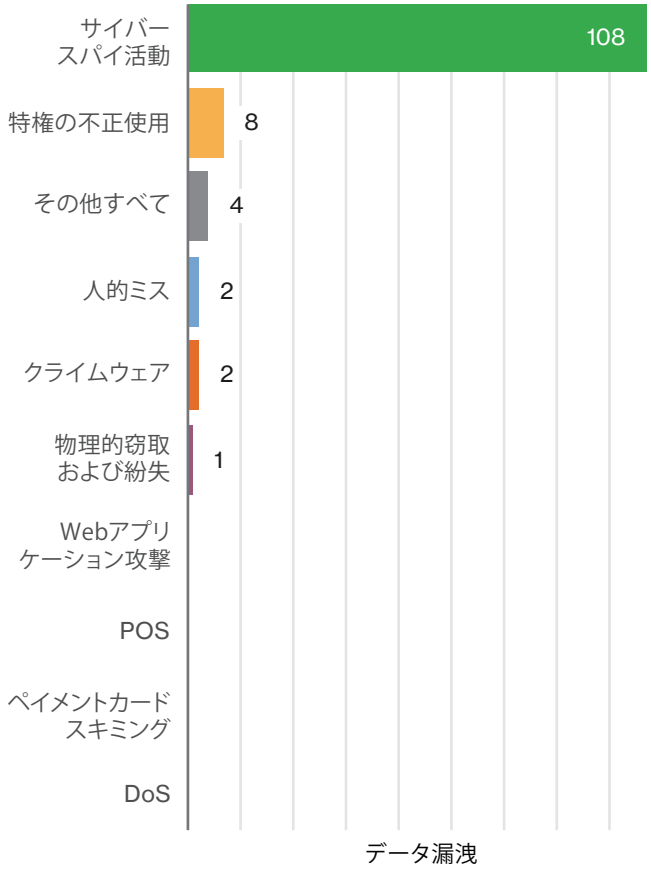


図24：製造業のデータ漏洩に見るインシデント分類パターンの発生頻度（N=124）

[15] https://www.bls.gov/iag/tgs/iag31-33.htm

秘密を守れますか?

「3人のうち2人が死ねば、秘密を守れる」と、ベンジャミン・フランクリンは言いました。もしお客様が製造業に携わっている場合、企業秘密を守ることについて、間違いなく心配するでしょう。製造業では実に90%もの盗まれたデータが「企業秘密」です。図25も、まったく気休めにはなりません。

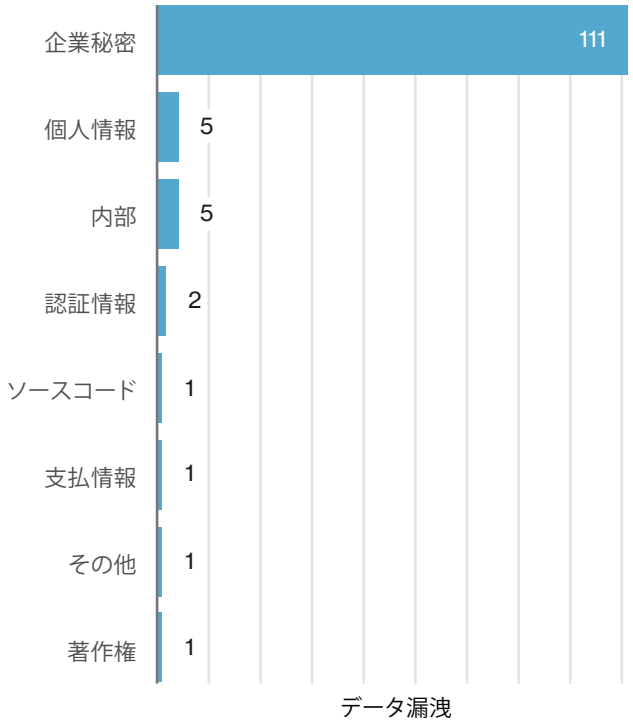


図25:製造業で漏洩したデータの種類 (N=122)

製造業にとって、所有する知的財産こそ、何より重要です。例えそれが秘密のレシピ、創造的な新しいコンセプトまたは製品を安く作る方法であろうと、窃盗犯にとって魅力的な標的になります。他の業界に見られる、もっとありふれた「略奪して逃走する」攻撃と異なり、スパイ活動という攻撃は一般に、より長期的な成果を狙います。犯人はネットワークに侵入し、企業秘密の保管場所を突き止め、できるだけ長く居座って、蜜をゆっくり搾り取ろうとします。このような攻撃は多くの場合、まず第8層 (つまり、ユーザー) に対して開始されます。企業・組織の従業員にフィッシングメールが送付され、従業員が不正なリンクまたは組み込まれた添付ファイルをクリックします。バックドアまたはC2の形でマルウェアがインストールされ、攻撃者が都合の良いときに戻ってきて、ネットワークに入り込み、必要なものを窃取します。実際、このようなデータ漏洩の73%で、ソーシャルエンジニアリングとマルウェアを組み合わせた攻撃が発生しています。

国家の支援を受けた実行者が関与した場合、作戦は日和見的攻撃ではなく標的型攻撃になります。言い換えると、犯人は特定の目的を持って、特定の企業・組織を相手に直接攻撃します。

次に一般的なインシデントパターンである特権の不正使用は (サンプル数がごくわずかですが)、上で説明した外部のスパイ活動によるデータ漏洩とある意味、類似しています。不満を抱えた従業員が抑圧にうんざりして、どこかよそで一旗揚げようと考え、できるだけ多く情報を持ち出そうとしたときにしばしば発生します。

考慮すべき事項:

分けて保管する — 非常に機密性の高い情報がある場合は、そのデータを分けて保管し、職務を果たすためにその情報を必要とする人に限定して、アクセスを許可します。

汝、クリックすることなかれ。しからば汝らも欺かれざらん。— この業界に対する攻撃の多くは、フィッシングメールが発端になっています。フィッシングについて従業員を教育し、疑わしい電子メールを迅速かつ簡単に報告できる手段を提供します。

自分自身を見直す — ネットワーク、デバイス、アプリケーションの内部監視が不可欠です。アカウント監視、監査ログ監視、およびネットワーク/IDS監視の実施を試みます。

餞別はなし — 情報漏洩防止 (DLP) コントロールを導入し、従業員による不適切なデータ転送を特定して阻止します。

公的機関

頻度	21,239件のインシデント、239件でデータ漏洩を確認
上位3パターン	サイバースパイ活動、特権の不正使用、人的ミスが公的機関におけるデータ漏洩の81%を占めています
攻撃実行者	外部62%、内部40%、複数の関係者4%、パートナー2%（データ漏洩）
実行者の動機	スパイ活動64%、金銭目的20%、愉快犯/イデオロギー/悪意13%（データ漏洩）
漏洩したデータ	個人情報41%、機密情報41%、認証情報14%、医療情報9%
要約	確認されたデータ漏洩に至った攻撃の約半数が国家の支援を受けています。データ漏洩の50%が発見されるまでに「数年」かかっています。

最初にすべてのインシデントをつぶす...

この報告書の最初に指摘したとおり、我々のデータは協力企業・組織が行った調査や、直面したこと、そして提供してくださったリソースなどに大きく依存しています。一部の協力企業・組織は、特定のタイプのデータを提供してくださる傾向があり、公的機関では特にそれが顕著です。行政機関は、多くの企業・組織で見逃されているインシデントについてでさえ、上層部に報告する必要があります。同時に機関が非常に大規模であるため、引き続きインシデントの数の多さが公的機関の特徴となっています。その多くは「未確認」のイベントや漠然とした「ポリシー違反」でした。

したがって、これらを突き詰めて検証することに、ほとんど価値はありません。推測では、ポリシー違反とはWebコンテンツフィルターからの不適切なWeb利用のレポートや有効ではあるものの未承認の業務手段を使用している従業員などが問題のほとんどでしょうが、憶測は求められていないので、これらの検証はいたしません。また、多くの紛失や盗難資産が報告されていますが、これについては物理的窃取および紛失のセクションで、すでに十分説明しているので（そして実際に情報漏洩が発生したか、単にその危険があるだけなのか証明できないので）、もう少しはっきりしていることに話を進めましょう。具体的には確認された239件のデータ漏洩につながった事例についてです。

公的機関のデータ漏洩パターンの調査結果は、過去数年間比較的一定であり、通常はサイバースパイ活動、特権の不正使用、人的ミスが上位3パターンです。この業界では、データ漏洩の約41%がスパイ活動に関連していますが、どこの政府も、宇宙人やミステリーサークル、コンウェイ大統領顧問が発言した（監視）カメラになる電子レンジなどの重要問題について米国政府がどのように考えているかを知りたいわけですから、当然かもしれません。外部によるスパイ活動が行われる場合、一般的には図26が示しているように、実行者の区分別比率は国家支援の個人・団体に大きく偏ります。

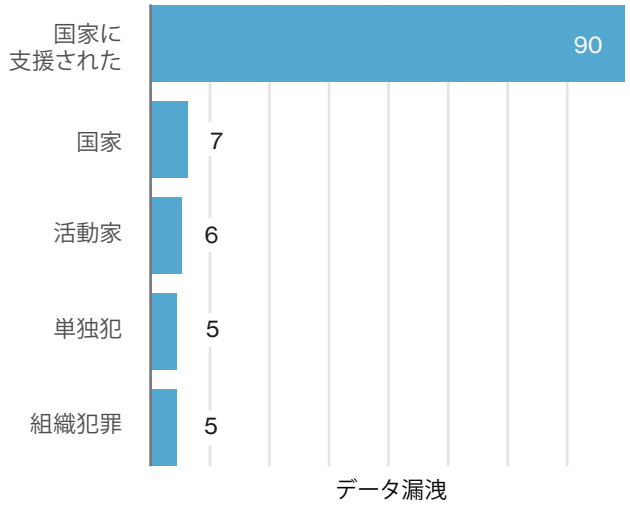


図26：公的機関のデータ漏洩における外部実行者の種類（N=113）

ここで読者は「製造業の話をまた読んでいるのだろうか？」と思うかもしれません。いいえ、そんなことはありませんが、この両者には非常に明らかな類似点があります。どちらも機密情報を扱い、特定の犯罪者にとって魅力的であり、非常に似通った戦術が使われがちです。

類似点の次は、興味深い相違点について話しましょう。製造業の場合、実行者の93%が外部者であり、91%の確率で企業機密が狙われました。公的機関では、内部実行者の比率が高くなり、40%にもなります[16]。データの種類は企業機密と個人情報の比率がほぼ同じです。多くの場合、犯罪者データベースに不正アクセスする警察官などがここで見られる内部実行者であり、愉快犯/好奇心を動機とするデータ漏洩の13%を説明しています。

内部のデータ漏洩を発見

原則的に、公的機関が急ぐのは、貸しを返してもらうときだけです。つまり、彼らは精度の高い仕事をするかもしれませんが、とても時間がかかります。データ漏洩の発見についても、まさにそのとおりです。図27「公的機関でデータ漏洩の発見に要する時間」の約60%の事例で、データ漏洩を認識するまでに何年もかかっています。これは、被害者のネットワークに潜り込み、長期間潜伏しようとするスパイ活動関連の攻撃件数が非常に多いことに起因しているかもしれません。それ以上にありそうな可能性としては、小規模な行政機関が人手不足で問題を迅速に発見できないということです。いずれにしても、我々市民にとっては困った話です。

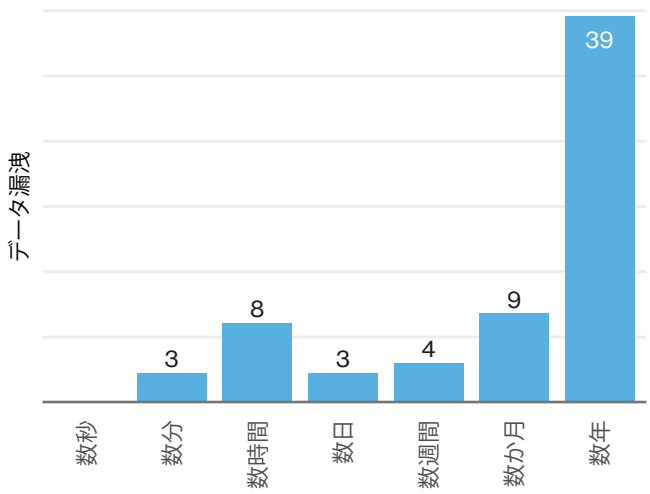


図27：公的機関でデータ漏洩の発見に要する時間（N=66）

考慮事項：

データを知る — 自分のデータ、特に機密性が高いデータをきちんと把握する必要があります。データの所在とアクセス可能な人、そして実際にアクセスしている人は誰かを把握します。

Exits are located above the wings — 企業・組織 データの出口を監視する手段を講じ、データが企業・組織から流出することを防ぎます。データが外に出ていく場合は、その事実を認識し、行先を知る必要があります。

敵を知る — 公的機関には、国の安全保障を担う組織から、地域の土地利用に関する委員会まで、あらゆるものが含まれます。自分の部門に最も関係しそうな攻撃実行者のタイプを理解する必要があります。

[16] 内部実行者の40%は、すべてが悪意による活動ではありません。内部者によるデータ漏洩の約半数は、ミスが原因です。

小売業

頻度	326件のインシデント、93件でデータの漏洩を確認
上位3パターン	DoS、Webアプリケーション攻撃、およびペイメントカードスキミングが小売業の全セキュリティインシデントの81%を占めています
攻撃実行者	外部92%、内部7%、パートナー1%未満（インシデント）
実行者の動機	金銭目的96%、スパイ活動2%、好奇心2%（インシデント）
漏洩したデータ	支払情報57%、個人情報27%、認証情報17%
要約	オンライン小売業者は常にDoS攻撃の標的であり、POS環境は金銭目的のセキュリティ侵害を受け続けています。

Ye olde e-commerce shoppe

この報告書において、小売業界は従来の小売業者とオンラインショッピングにはっきりと分かれています（両方に当てはまる小売業者が存在することは承知しています）。Webアプリケーションが関係したインシデントを分析すると、DoS攻撃がインシデントの80%以上を占め、図28に示した209件のハッキングインシデントでは、その大部分の背後にDoS攻撃があります。電子商取引サイトに関連するデータ漏洩は非常に分かり易く、概ねWebアプリケーションのハッキングを伴います。興味深いのは、多種多様のハッキングが関係していることです。フィッシング攻撃の一部として、顧客から盗んだ認証情報がWebアプリケーションのデータ漏洩手口として圧倒的です。世界中の小売業者がすべての入力バリデーションの脆弱性を解消したと確信はしていませんが、我々の総合データセットでは著しい数字にはなっていません。

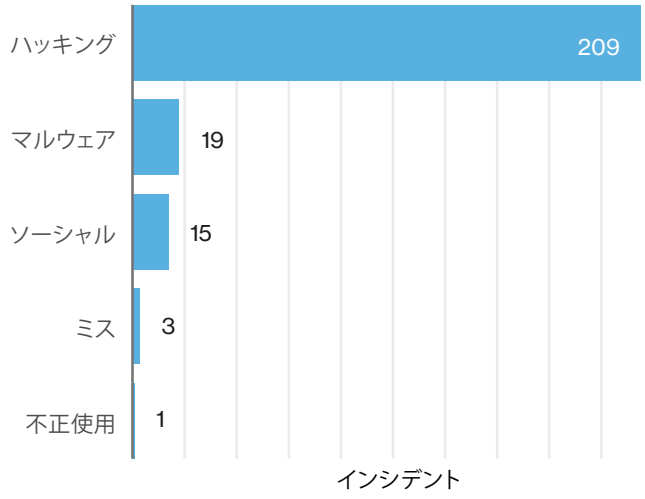


図28：Webアプリケーションが関係する小売業のインシデントにおける攻撃行為のカテゴリー別発生頻度（N=214）

Are you being served?

従来の店舗型小売業者の場合は、攻撃の様相がまったく異なります。ガソリン給油機やATMにスキミング機器が取り付けられた件数は、電子商取引以外の小売業者におけるデータ漏洩の約60%を占めています。図29を見て、特に小売業でPOSへの侵害が少ないことに驚きました。これについては、納得のいく説明がまだできないので、今後も注視していきます。

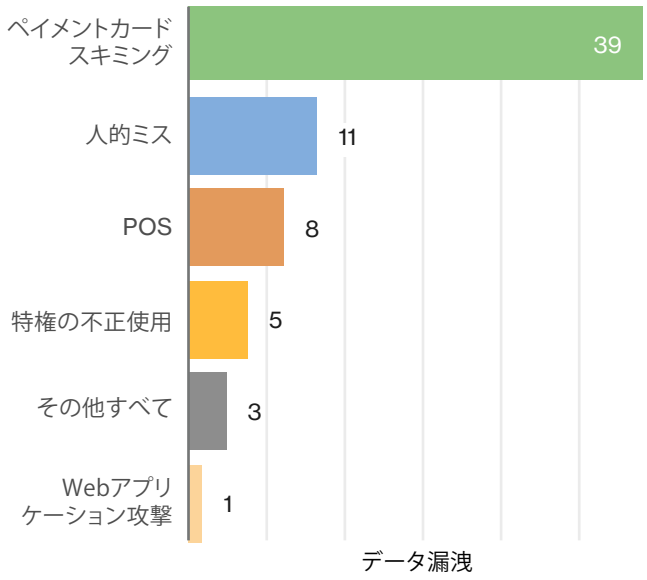


図29：Webアプリケーションが関与しない小売業のデータ漏洩におけるインシデント分類パターン別発生頻度（N=67）

規模は問題にならないのか？

小規模な小売業者はこれまで、POSへの侵入パターンで目立っていました。2013年度のDBIRでは、インターネットに接続するPOSシステムへの、拡張性のある自動攻撃を「スマッシュ アンド グラブ」作戦と名付けました。ありがたいことに、大規模な小売業者はデフォルトパスワードの使用によりPOS資産をインターネット全体へ広範囲にさらすという被害は受けていませんでした。2014年度のDBIRでは、POS攻撃に関連した相当な規模のデータ漏洩が明らかになり始めた大手小売業者に注目しました。そしてこれらの多くの場合で、推測されたのではなく、盗難された認証情報が使われました。今年は、「POSへの侵入」パターンに大手小売業者が含まれていません。教訓が活かされ、改善につながった表れであればいいと考えます。小規模な小売業者に関しても同様に教訓を活かしているのか、またはデータ漏洩の規模が小さく、我々のデータセットまで到達していないのか解明していくつもりです。

考慮事項：

何がほしいのか？ 稼働時間 いつほしいのか？ 今すぐ — 必ず、DoS軽減プランを策定し、攻撃が発生した場合に備えて、保護の限界とプロバイダーとの契約の詳細をきちんと把握しておいてください。

人は独りでは生きていけない — しかし、お客様の資産はそうあるべきです。重要資産は別個のネットワーク回線（セグメント）で保管してください。単純なネットワークほど最初の足がかりから目的の地までの到達を容易にします。デフォルトや簡単に推測できるパスワードを使用することは、現代の基準を満たしません。全社的にマルチ要素認証を導入してください。とりわけ、ペイメントカード処理ネットワークへのリモートアクセスには、これが必須です。

対人攻撃

頻度	1,616件のインシデント、828件のデータ漏洩を確認
上位3パターン	Webアプリケーション攻撃、サイバースパイ活動、およびその他すべてがソーシャル攻撃を伴うすべての漏洩の96%を占めています
攻撃実行者	外部99%、内部1%、パートナー1%未満（データ漏洩）
実行者の動機	金銭目的66%、スパイ活動33%、悪意1%未満（データ漏洩）
漏洩したデータ	認証情報61%、企業機密32%、個人情報8%
要約	今年のデータセットでは、データ漏洩全体の43%でソーシャル攻撃が利用されていました。データ漏洩に至ったほぼすべてのフィッシング攻撃は、何らかのマルウェアが後に続き、フィッシングによるデータ漏洩の28%が標的型でした。我々のデータセットでは、フィッシングが最も一般的なソーシャル戦術です（ソーシャルインシデントの93%）。

詐欺師とカモ

熱意、不注意、好奇心、不安。これらのすべてが人間を行動に駆り立てる要因であり、その1つ以上を利用して、情報を開示させたり、リンクをクリックさせたり、または「ベンダー」の口座に送金させたりします。ソーシャルエンジニアリング攻撃にはさまざまな種類がありますが、ここでは「フィッシング」と「なりすまし」を重点的に取り上げます。この2つがソーシャルエンジニアリング攻撃に向けた活動を伴ったインシデントとデータ漏洩の両方で約98%を占めています。具体的にはビジネスメール詐欺（BEC）に関連するので、金銭目的の「なりすまし」について検証します。さらに、セキュリティ意識向上トレーニング演習から得られた、インシデント以外のデータより見出された調査結果について議論し、コンテキストを追加します。

Wings of reason

まず、一歩下がって全体像を検証しましょう。今年の報告書では、1,600件余りのインシデントと800件を超えるデータ漏洩で、ソーシャルエンジニアリング行為が見られました（すべて外部の実行者が主導）。フィッシングが再びトップとなり、インシデントとデータ漏洩の両方で90%を超えています。フィッシングに成功すると、ソフトウェアのインストール、機密データ漏洩の誘発、悪用目的としたアセットの改ざんなど、さまざまな事象が発生する可能性があります。昨年の報告書では遠隔からのデータ漏洩の大半が、フィッシングのマルウェア経由で足がかりを確保し、盗んだ認証情報を利用して足がかりを軸に展開するという一連の事象から始まっていると説明しました。今年も、データ漏洩に至ったフィッシング攻撃の95%はその後、何らかの形でソフトウェアがインストールされています。

フィッシングによるデータ漏洩の大部分を占める、実行者と動機の組み合わせは、2つのカテゴリーに当てはまります。4分の3は金銭目的の組織犯罪グループであり、4分の1は国家の支援を受けてスパイ活動を行う実行者でした。金銭目的によるフィッシングの相当数は、銀行を狙ったトロイの木馬ボットネットと結びついていました。図30および31では、ボットネット駆動型フィッシングのサブセットを取り除き、被害にあった企業・組織の人的ターゲットに焦点を当てています。

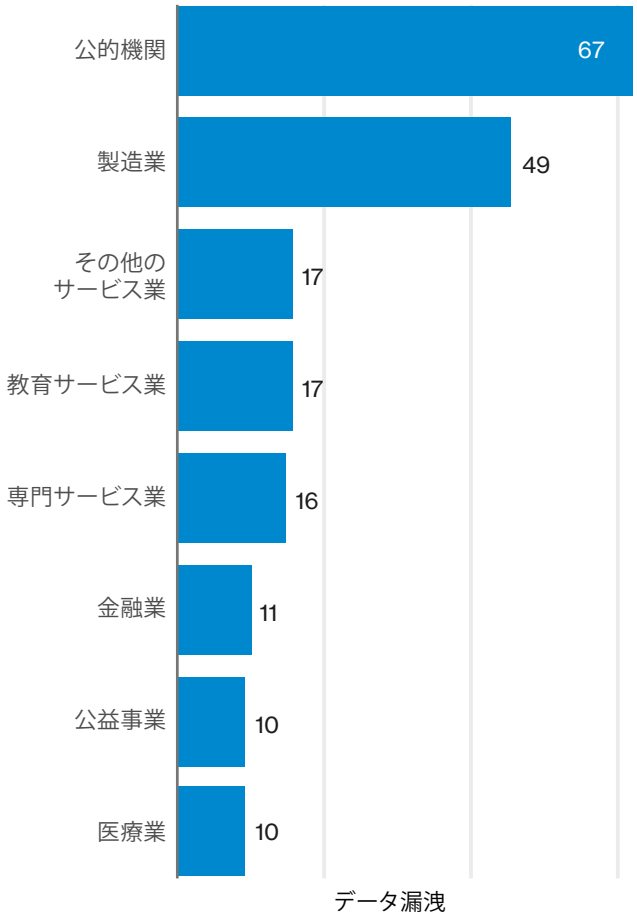


図30：ソーシャルエンジニアリングを伴うデータ漏洩の被害にあった上位の業界（ボットネット駆動のキャンペーンは除外）（N=216）

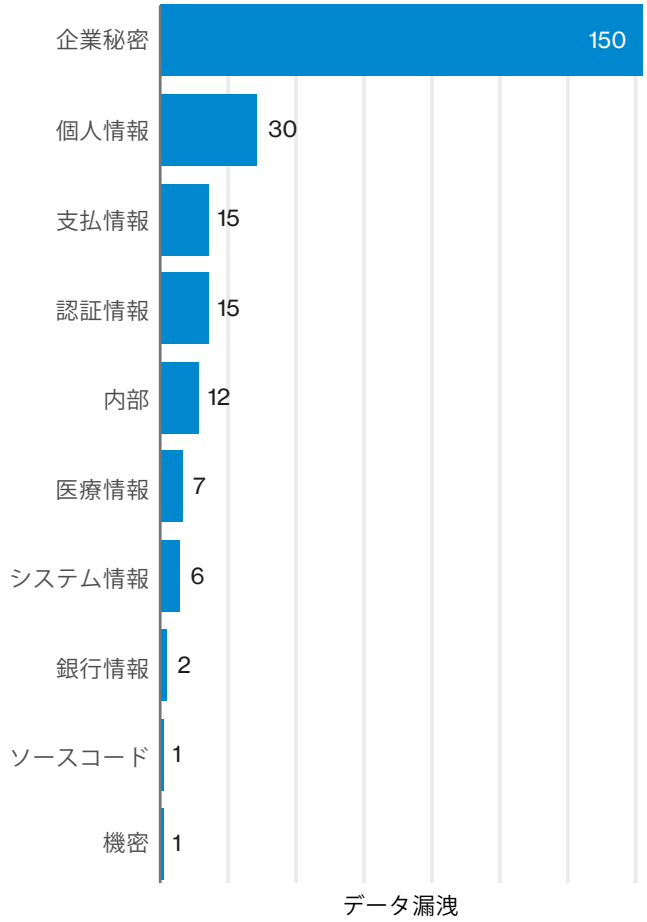


図31：フィッシングによって漏洩したデータの種類（ボットネット駆動のキャンペーンは除外）（N=211）

公的機関と製造業で、このデータのサブセットにおける被害者の過半数を占めていますが、すでにこれらの業界別のセクションをお読みになっているので、予測できていたかもしれません。しかしこれはサイバースパイ活動とフィッシングの強い結びつきを表すもう1つの例です。図31でさらに補足しており、標的になったデータの種類は、企業機密がトップで、個人情報がそれに続いています。

教育によるセキュリティ強化

この報告書の主な焦点は、これまでも、そしてこれからも、データ漏洩です。とはいえ、真価の点から得られるものを収集するだけではなく、データ漏洩の報告書にふさわしいコンテキストを提供するために、インシデント以外のデータセットに基づく調査結果も検証します。我々のインシデント以外のフィッシングデータは、730万件のレコード（ユーザーレベルまで下げたキャンペーンデータ）となり、2,280の組織にまたがる14,000以上のキャンペーンと300万以上のユニークユーザー数を示しています。

クリック

複数のデータ提供企業・組織において、7.3%のユーザーがリンクまたは添付ファイルを開くことによって、見事にフィッシングに引っかかっています。そこで、「どれぐらいのユーザーが1年間に複数回、被害にあっているのだろう」という疑問が生じます。実は、一般的な企業（従業員30人以上）では、一度被害にあったユニークユーザー全体の15%が2度目もおとりに引っかかっています。全ユニークユーザーの3%は2回以上クリックしていますが、3回を超えてクリックしたのは1%未満です。

報告

フィッシングに引っ掛かったユーザー数と、繰り返し引っ掛かったユーザー数が分かったところで、どの程度の人がその出来事を報告したかを見てみましょう。つまり、「何かを見て、何かを語った」人々です。これが何より重要です。フィッシングメールを受信して、誰かがクリックしてしまうことを完全にゼロにはできないかもしれませんが、発見して処理する適切なプロセスが用意されていれば、組織への影響を軽減できる可能性があります。フィッシング対応キャンペーンの一部（全部ではない）では、フィッシングメールを報告する仕組みをユーザーに提供しました。記録された報告事例のうち、実際に報告したユーザーの割合は20%でした。したがって、善意ある人々の5人に1人が何か変だと気付き、ポリシーに従って報告しました。報告は、電子メールのフィルターをすり抜けたフィッシングの実効性を限定するために重要です。上記のキャンペーンの一部で報告された割合がクリックしてしまった全体的な割合より高くてよかったのですが、これは将来確実に増えてほしい数字です[17]。

嘘でできた王座に座る

なりすましは、標的をそそのかすシナリオ、すなわちもっともらしい話の作成に特化した、ソーシャルエンジニアリングの1つの形です。いささか、高校生のデートのようですが、より「サイバーチック」です。本物のプロは、でまかせを使いこなして金銭を奪い取る、組織犯罪グループのようです。なりすましはフィッシングほど一般的ではありませんが、注目すべき重要な点がいくつかあります。ほぼ必ず、本質的には標的型です。従ってターゲットの過半数が経理部門担当者です。つまり、実行者は調査して適切な従業員を特定し、もっともらしい話をでっち上げます。

今年のデータでは、幹部役員になりすまして従業員をだまし、会社の口座から時には億単位にも及ぶ送金を指示するというインシデントが多く見られます。このようななりすましのインシデントの多くは、内部の会計監査で発見されており、不正検知によって発見されたものはわずかです。この場合、内部監査で不正が発見されるのは「馬が馬小屋から出たあと」ですので、送金を阻止するという意味では通常外部の不正検知のほうがより好ましいです。通信媒体のトップは電子メールで、金銭的なりすましインシデントの88%を占めます[18]。電話によるやり取りが第2位で、10%未満です。

注目すべき領域

データは、フィッシングのシミュレーションが重要であることを物語っていますが、シミュレーションをもってしてでもクリックする人は必ず出てきてしまいます。単に防止するだけではなく、発見と報告に重点を置いてください。次のように、フィッシングレスポンスプランを導入してテストしてください。

- 「フィッシング」の可能性があるメールを通告するように、ユーザーに徹底させます。
- フィッシングの受信者を突き止め、メールを回収します。
- リンクをクリック、または添付ファイルを開いてしまった、フィッシングの受信者を突き止めます。
- 侵害されたホストからアクセスした認証情報を無効にします。
- 感染ホストからの、クリック後の通信を調査します。
- マルウェアが拡散しないように、システムを隔離します。
- マルウェアを突き止めて削除します。
- アプリケーションのサンドボックス機能を有するオペレーティングシステムなど、サンドボックステクノロジーの利用を検討します。ユーザーデバイスからのメールやOffice文書に対してサンドボックスを実行するクラウドアプリケーションについても、前もって考慮しておきます。

外部からのメールには、件名見出しに[External（外部）]、[E]、または[Not from the CEO!（CEOからではない）]を前に付加して、重要人物からだと主張するなりすましメッセージを見破れるようにします。しかし一部のBEC（ビジネスメール詐欺）では、ハッキングしたメールアカウントを使用するのでそれでも十分ではありません。つまり、幹部役員から送られたメールではないのに、その役員本人のメールアドレスから送付されてくるのです。支払を承認するプロセスに、電子メール以外の連絡手段を組み込んでください。送金処理を開始できる従業員に対して、文書化された承認ポリシーから外れて、メールで送金を依頼することは絶対にないと、指導してください。金融機関と協力して、高額または異常な送金を阻止し、厳戒態勢を取ってください。

[17] 1つ以上の追跡された報告事例があるキャンペーンから。大部分のキャンペーンには、報告されたフィッシングが含まれていませんでした。追跡可能なレポーティングツールが組み込まれていないか、または顧客が実装しなかったことが理由として考えられます。またユーザーが報告しなかったからという可能性もあります。いずれも確実とは言えませんが、報告が追跡されなかった事例の楽観的な推論です。

[18] 「おとり」としてリンクまたは添付ファイルの形で特別なフックを仕掛けて、電子メールにフィッシングを使用するのに対して、プリテキスト（なりすまし）には、人物とともに、実行者と被害者間の対話が必要です。

身代金要求の手紙は最も儲かる

ランサムウェアは最新のインターネットの弊害で、感染してシステムを暗号化したのち、人や組織から何百万ドルも巻き上げます。2014年度のDBIRでは、22番目に一般的なマルウェアの種類でしたが、今年のデータでは第5位に浮上しています。我々はこのセクションを、ランサムウェアの脅威の本質とそれを阻止するセキュリティ業界の手段を一変し得るランサムウェアの技術向上を解明するため、脅威インテリジェンスを活用しているMcAfeeに譲りたいと思います。

ランサムウェアの増加

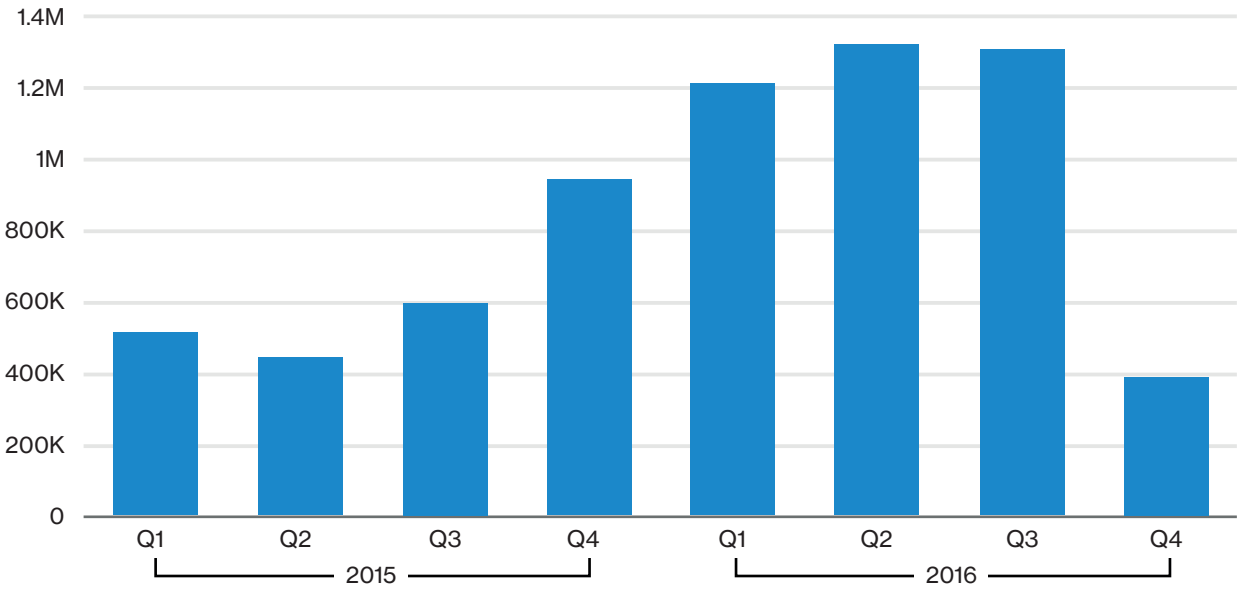


図32：四半期ごとの新しいランサムウェアのサンプル―提供元：McAfee Labs

ランサムウェアの登場は1989年まで遡りますが[19]、昨年はビットコインによる匿名での支払い方法が考案されたため、かつてないほどの技術とプロセスの刷新がありました。初期攻撃の成功に後押しされ、ランサムウェアインシデントの件数は2016年度DBIRの159件から、今年は228件に増加しています。上の図32は、DBIRの調査結果を裏付けています。

実行者がコードを修正し、新しい攻撃形式、暗号化方式、脆弱性攻撃ツール、回避技法を実装したことで、2015年から2016年のほとんどの期間、McAfee Labsのテレメトリーで新しいランサムウェアサンプルの着実な増加が見られました。しかし、2016年第3四半期になると、新しいサンプルはわずかに減少し、第4四半期には70%と大きく落ち込みました。この大きな低下の最大の原因は、一般的ランサムウェアの発見件数が減少したことと、LockyおよびCryptoWallの亜種・変種が減少したことです。

[19] https://www.theatlantic.com/technology/archive/2016/05/the-computer-virus-that-haunted-early-aids-researchers/481965/

技術とプロセスのイノベーション

昨年はランサムウェアの技術と恐喝の手口に、目覚ましい刷新が見られました。ランサムウェア作成者が標準的に行うファイル暗号化から、マスターブートレコードのロックと部分的または全体的なディスク暗号化に移行し、身代金を支払わずにシステムを復旧させることをさらに困難にしました。また、セキュリティサンドボックスによる発見を回避する、さまざまな手法も試しました。これには実マシンと仮想マシン間の実行時間の相違、予期しないコマンドライン引数、Microsoft Officeの異常に短い「最近使用したファイル」リストが含まれていました。昨年半ば、ランサムウェアに使用する脆弱性攻撃ツールがアングラーからニュートリノに突然移行し、さらに9月にはニュートリノからRIGに変わりました。これらのツールを監視することは、どの脆弱性が狙われたか、どのパッチを優先すべきか、どのように防御を強化すればよいかを突き止める上で有効です。

ランサムウェアの高い利益性は、犯罪者によるサービスとしてのランサムウェア（Ransomware-as-a-service）の提供を促し、分け前を支払うことで誰でも狙ったターゲットを恐喝できるようになりました。このアプローチのあとに、身代金要求のさまざまな試みが続きました。犯罪者は時間制限を取り入れ、その時間が過ぎるとファイルが削除されるようにしました。また、時間とともに増額される身代金、ファイル名から推定した機密度に基づいて算出される身代金、さらには、被害者が自ら攻撃者に転じ、2人以上に感染させたら、無料でファイルを復号化するオプションまで取り入れられました。まさに、最強のマルチ商法です。

標的設定および攻撃経路の変化

2016年で最も重大なランサムウェアの変化は、個々の消費者向けシステムを感染させることから、脆弱な組織を標的にするようになったことでしょう。全体としてのランサムウェアは、いまだにきわめて日和見的で、大部分の攻撃は、感染したWebサイトや従来のマルウェア配信に頼っています。もう一度、DBIRのデータというレンズを通して見てみると、2016年度の報告書では、ドライブバイダウンロードがトップのマルウェア経路でしたが、今年は電子メールが取って代わっています。ソーシャルエンジニアリング行為、特にフィッシングは、インシデントにおいて昨年はわずか8%暴露でしたが今年は21%まで上昇しました。このような電子メールは、人事部や経理部の担当者など、添付ファイルを開いたり、リンクをクリックしたりする可能性の高い、特定の職務または特定個人を標的にすることがよくあります。

医療業のランサムウェアキャンペーンは、医療データが閲覧できなくなることによる患者治療に与えかねない潜在的インパクトもあり、2016年に広く認知されました。DBIRのデータから、標的となる業界第1位は公的機関、第2位は医療業界、第3位は金融業だったことがわかります。組織を狙ったランサムウェアキャンペーンは、認証情報を窃取して組織全体に攻撃を拡散させる、暗号化を遅らせて発見までに可能なかぎり多くのマシンを感染させる、会社のサーバーやユーザーシステムを標的にするコードなど、付加的な特徴が見られることもよくあります。

ランサムウェアの減少 – セキュリティ業界の対抗策

セキュリティ業界はランサムウェアの増加を容認しません。セキュリティベンダーはさまざまな分野に取り組んでおり、感染が深刻にならないうちにランサムウェアを発見し、一連の犯罪行為から個人と組織を守り、攻撃側に利することなく、身代金対象になったシステムを救出することに貢献しています。

セキュリティソフトウェア

大部分の脅威に対して、セキュリティ業界に期待される対応は、早期発見ができるようにツールを強化することです。ランサムウェアとの闘いも、例外ではありません。エンドポイント保護システムでは現在、何百万というランサムウェアサンプルを検知することができ、発見されるたびに、追加されています。すべての攻撃を阻止するには、このプロセスでは不十分なのは明らかですが、セキュリティ業界はユーザーの環境をまねて難読化されたランサムウェアを捉えるサンドボックス、ランサムウェアの実行の完了を阻止する行動解析、ランサムウェアがファイルを暗号化できないようにする、ファイル作成阻止などの検知技術も追加しています。このようなアクションは検知率と阻止率を高めましたが、ランサムウェアに大量の亜種・変種があり、また、犯罪者が素早く順応するため、これらの技術が100%有効であるとは考えられません。したがって、さらなるアクションが必要です。

脅威インテリジェンスの共有

法令で犯罪者を捕まえることに加えて、ランサムウェア（およびその他の不正な活動）がシステムに到達する前に検知できるように、セキュリティベンダー、法執行機関、あらゆる規模の企業・組織で脅威インテリジェンス情報がますます共有されるようになりました。脅威情報の迅速な共有は、ワクチンのように作用し、システムと企業・組織に免疫を与えるので、既知で疑わしいランサムウェア攻撃が持続的な損害を引き起こさないように予防できます。

法執行機関との協力

セキュリティ業界は、悪意のあるコンテンツ、Webページ、掲示板などを封鎖、削除し可能なかぎり関係者を特定して逮捕できるように、法執行機関とも協力体制にあります。2016年にこのような取り組みが行われ、現在も進行中です。

nomoreransom.org

昨年のランサムウェアに対抗する最も重要なアクションは、No More Ransom! というプロジェクトの創設と継続的な発展でしょう。2016年7月、4つの企業・組織を創設メンバーとして始まったこのグループは、現在、セキュリティベンダー、コンサルタント、法執行機関、インシデントレスポンスグループ、保険会社、情報共有センター、必要なWebサービスを提供するホスティング企業を含め、57の会員を擁しています。このグループの目的は、情報の共有、ユーザの教育、そして攻撃者に身代金を支払うことなく、被害者が暗号化されたデータを取り戻せるように支援することです[20]。

そのために、nomoreransom.orgは現在、27種類の復号ツールを提供しています。復号ツールを利用すると、広範囲に及ぶランサムウェアファミリーからファイルを取り返すことができます。No More Ransom! の計算によると、世界全域の大勢の被害者に、無料で復号ツールを提供することによって、犯罪者の手に渡ることを阻止できた金額は、300万ドル以上になります。

[20] ベライゾンは現在、No More Ransom! プロジェクトに参加しています。

インシデント分類パターンの概要

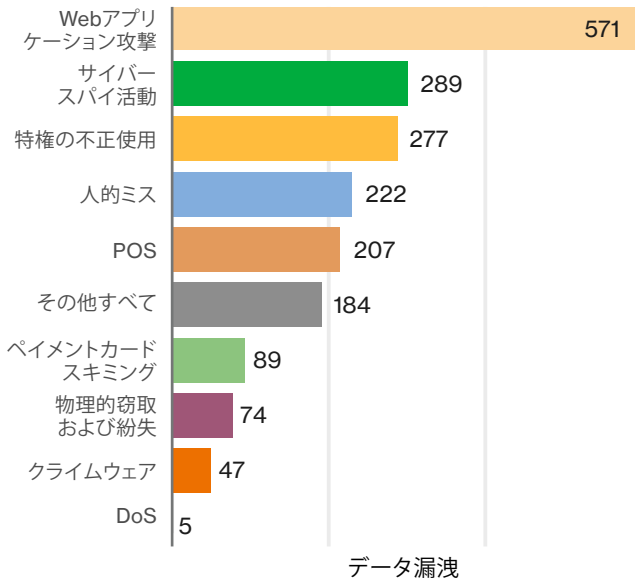


図33：パターン別データ漏洩の割合と件数（N=1,935）

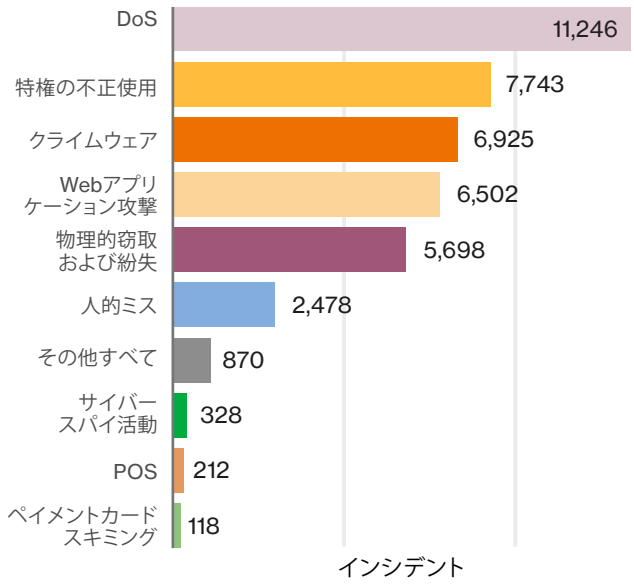


図34：パターン別インシデントの割合と件数（N=42,068）

ニュートンは頭の上にリンゴが落ちてきたときに、重力を発見したという言い伝えがあります。同様に、アインシュタインは夢の中で相対性理論を思いついたと伝えられています。インスピレーションはどこで閃くかわかりません。数年前、我々、DBIRチームは何気ない会話の中で、大部分のデータ漏洩はいくつかの大まかなカテゴリーまたはパターンに分けられ、同じことが繰り返されるようだということに気づきました。こうして9つのパターンが生まれ、その後の報告書で紹介することになりました。もちろん、この観察とアインシュタインやニュートンの才能を引き比べるつもりはありません。我々の閃きの方がはるかに重要であることははっきりしているからです[21]。

インシデントパターンが初めて組み込まれた2014年度の報告書では、確認されたデータ漏洩の90%がいずれかのパターンに当てはまりました。今年はデータ漏洩の88%が同じ基本パターンに当てはまります。Webアプリケーション攻撃が相変わらず最も優勢ですが、これもやはり、大量のボットネットがデータをそのパターンに引き寄せたからです（図33を参照）。ボットネットを除外して、今年のデータ漏洩のランキングをやり直すと、サイバースパイ活動がトップになり、Webアプリケーション攻撃は第6位に下がります。

データ漏洩のみではなく、すべてのインシデントを検証すると（図34）、2016年はDoS攻撃が大差で人的ミス（昨年の第1位）を押しのけ、トップに君臨しています。

毎年繰り返し申し上げていることですが、インシデントパターンの本当の価値は、相互に比較することにあるのではなく、企業・組織に最も悪影響を与えそうなものを知る、ガイダンスとして利用することにあります。たとえば、ホテル業の場合、注意すべき主な領域はPOSへの侵入です。一方、小売業者であれば、製造業ほどスパイ活動を心配する必要はありません。では、このような組織別の状況のいずれかに当てはまる場合、その領域だけを守ればよいのでしょうか。もちろん、そんなことはありません。しかし、このような懸念領域を理解することによって、常に対応を迫られているセキュリティの専門家は、どこに、どのように、限られたリソースを投入すればよいかについて、知見を得ることができます。インシデントパターンは、どこで最も危険が発生しそうかというベースラインを迅速かつ容易に評価することを可能にします。例えば、あなたが蛇に噛まれるとすれば、それは南極ではなくアリゾナである可能性が高い、といったように。

パターンはセキュリティの星占いを見るようなものだと考えてください（天体運動ではなく、データのみに基づく）。この報告書はもちろん、我々が観察した傾向を読者に伝えるだけであり、お客様の未来すべてを実際に予言することはありません。それでも、我々のデータは、お客様のラッキーナンバーは7、29、60、であり、フラッグデーの恋愛運と金運が良好であると示すでしょう。

[21] 何ですって!?

クライムウェア

特定のパターンに当てはまらないマルウェアが関連するあらゆるインスタンス。このパターンを構成するインシデントの大部分は、本質的に日和見的であり、金銭目的です。このパターンは顧客に影響を与えることがよくあり、「典型的」なマルウェア感染が発生するところです。

概要

被害が多かった業界
公的機関および製造業
頻度
合計6,925件のインシデント、47件でデータの漏洩を確認
主な調査結果
ランサムウェアは、ここ数年増え続けており、現在はこのパターンにおけるマルウェア第1位の種類です。インシデント以外のデータを検証すると、マルウェアの99%が電子メールまたはWebサーバーを介して送付されています。

「金持ちのおじさんが誕生日に自分の財産を分けてやると、言い続けていますが、それはいつも次の誕生日のこと。」クライムウェアのパターンは、常にある意味こんな感じだとお考えください。言い換えるとすれば、お金はありそうですし、本当にあげたいとも思っているようですが、実際には決してもらえません。毎年、このパターンは何千というインシデントで構成されますが、実際に使える情報、または分析に大いに役立つような情報が得られるデータ漏洩またはインシデントはほんの一握りです。

一般に、情報はコンピューター緊急事態対策チーム（CERT）またはコンピューターセキュリティインシデント対策チーム（CSIRT）から届きます。これらの組織は、多種多様な協力企業・組織からデータを取得し、全体を非常に大まかなカテゴリーに分類しています。詳細が不明であるにもかかわらず、我々が辛抱強く続けていると、時には有用なデータポイントが垣間見えてくることもあります。

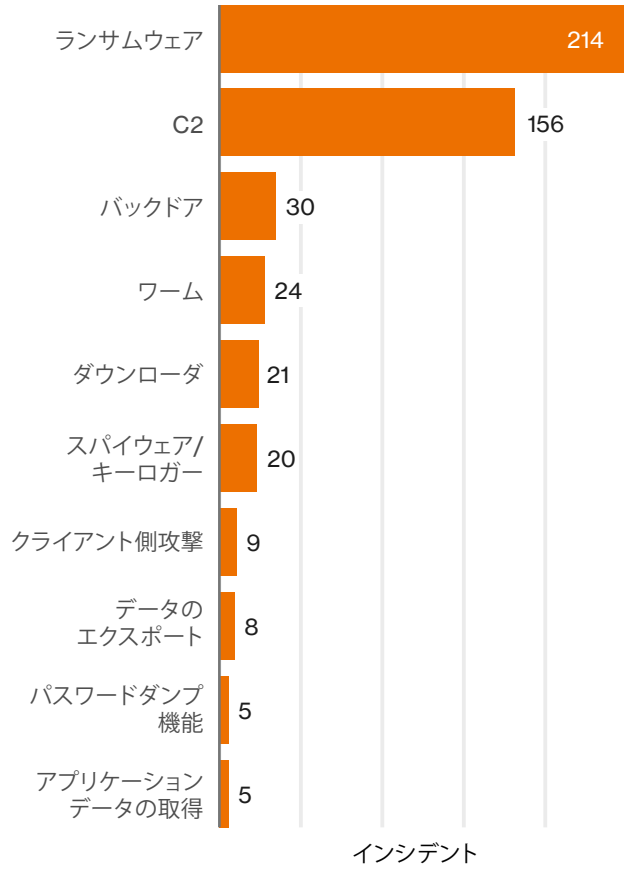


図35：クライムウェアインシデントにおける上位のマルウェア（N=430）

ランサムウェア! どうして、そのことを考えなかったのだろう

ご存知のように、ランサムウェアはマルウェアの1種で、システムに感染すると、犯罪者が要求した身代金を支払うまで、データを暗号化してしまいます。たちの悪い悪党にとって、生計を立てる絶好の手段です。データセット全体で実際に多いのは、ランサムウェアではなく、ボットネットのマルウェアインシデントです。しかし、ボットネットは決まって金銭絡みのWebサイトで使用するための認証情報を盗むため、Webアプリケーション攻撃のパターンに分類されます。その結果、図35のクライムウェアパターンでは、ランサムウェアが現在トップです。これは将棋界の新星のように、突然現れたわけではありません。ランサムウェアは毎年増加してきました。犯罪者にさまざまなメリットをもたらすため、この傾向はまだまだ続く見込みです。ランサムウェアは通常の攻撃経路を迂回するため、攻撃者は継続的に攻撃を続ける必要がありません。容易に換金でき、かつ非常に高速で、攻撃側にとって低リスクでもあります。

物事がうまくいくと

しかし、朗報もいくつかあります。インシデント以外のデータ（マルウェアを除去—5千万のオンザワイヤ—検知サンプル）を見ると、マルウェアの99%以上が電子メールまたはWebサーバーを介して送付されています。つまり、メールサーバーまたはWebプロキシーを経由しているので、そこでマルウェア駆除対策を講じることができます。この正常に駆除されたマルウェアのデータセットは、我々のインシデント調査から取り出したデータを裏付けています。この調査でも、ほぼ80%のクライムウェアが電子メールを使用しており、自動ダウンロードによるチェックインが8%です。

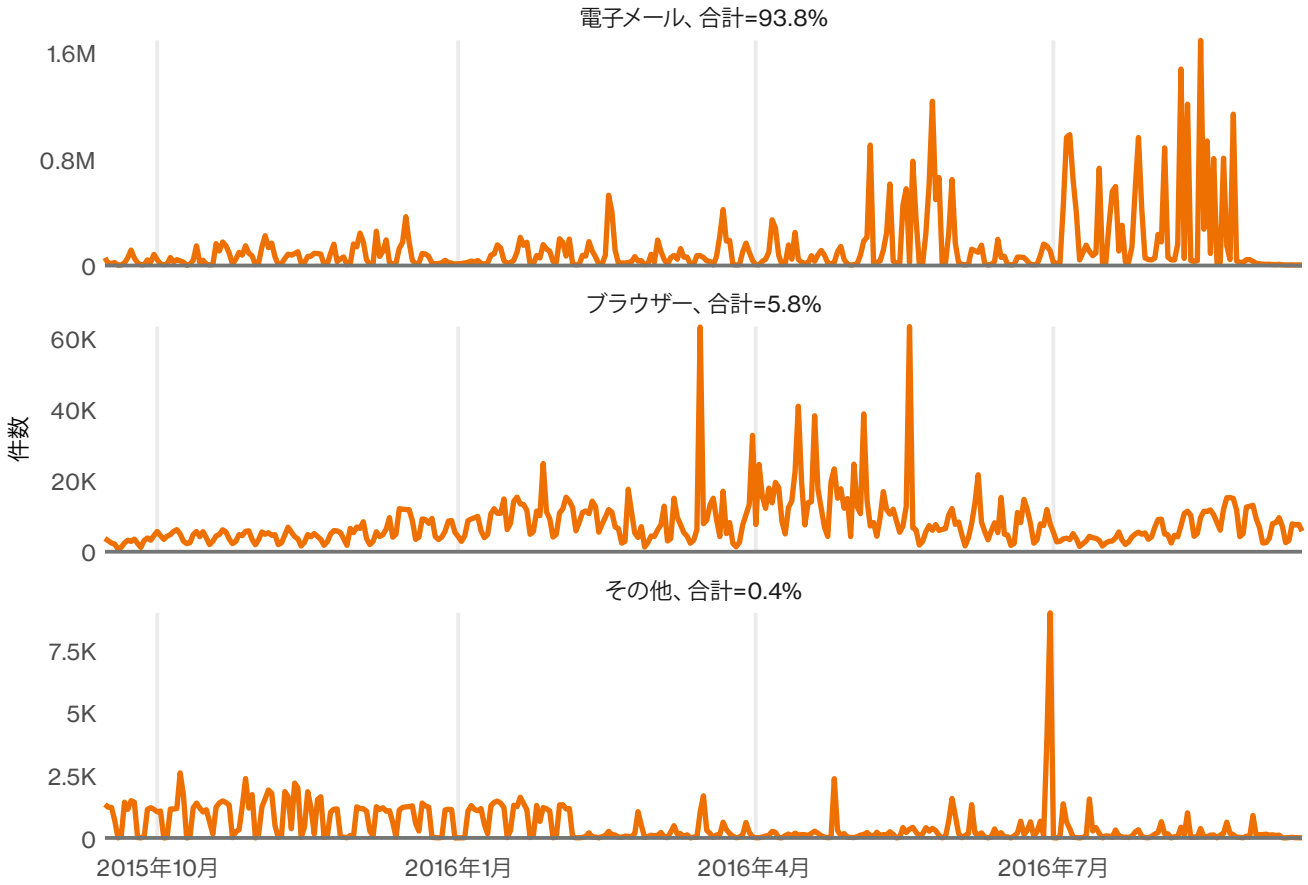


図36：経路別に示した1日のマルウェア数（N=50,366,956）

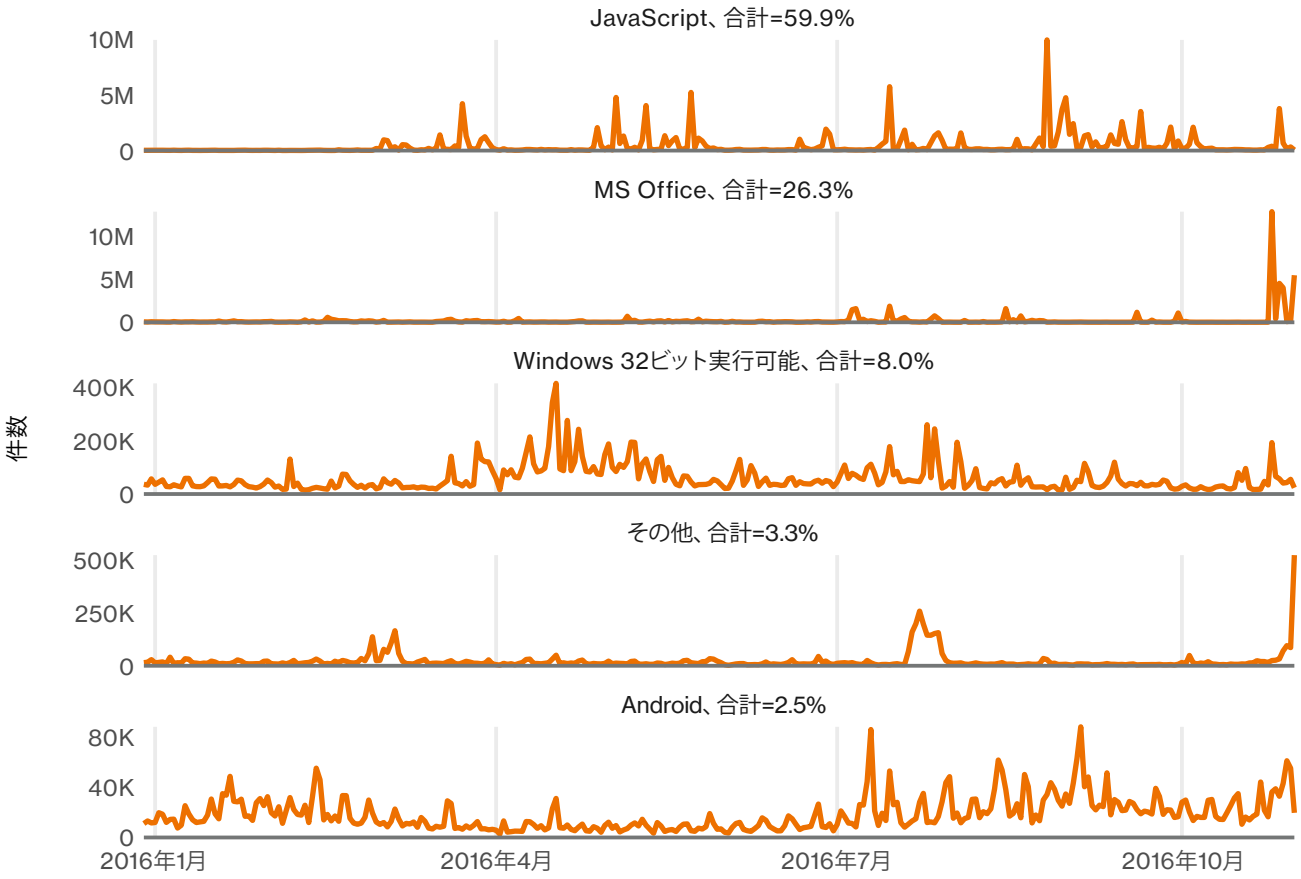


図37：ファイルタイプ別に示した1日のマルウェア数（N=227,109,781）

図36からわかるように、ムラもあります。きわめて周期性があり、週間労働時間によって決まるようです。3月から8月にかけて、急増している週があり、配信方式によってピークが異なります。

少し見方を変え、別のインシデント以外のデータを掘り下げてみましょう。図37では、マルウェアのパッケージ方法が見えてきます。特に注目すべきなのは、JavaScriptの優位性であり、不正なOffice文書と32ビット版Windowsの実行可能プログラムがそのあとに続く点です。

VERIS（Vocabulary for Event Recording and Incident Sharing）のフレームワークには、マルウェアの種類と経路の両方について一覧表があり、潜入する際にどのようなファイルタイプが最もよく使用されているかが分かります。

注目すべき領域

お客様の企業・組織でソフトウェア更新を電子メールで通知している場合を除き、マクロに対応するOffice文書を無効にして電子メールの出入り口で実行可能プログラムを阻止する必要があります。具体的には、明らかに必要とする人を除き、MS WordとExcelを無効にします[22]。また電子メール経由の.jsをブロックし、不正なJavaScriptが起動しないようにします。そして、ブラウザーのソフトウェアを最新の状態で維持します。

さらにはクライアントベースのマルウェア検知、アプリケーションのホワイトリスティング、サンドボックス、感染ホストからの通信を検知するネットワーク防御策を組み込み、堅実なマルウェア防御戦略を導入します。

ブラウザーの不正使用に関連する脆弱性に、最優先でパッチを適用します。これにはブラウザーのソフトウェアはもとより、プラグインも含まれます。

[22] https://decentsecurity.com/block-office-macros/

サイバースパイ活動

このパターンのインシデントには、国家の支援を受けた実行者やスパイ活動の動機の顕示に結びつく不正なネットワーク/システムアクセスが含まれます。

概要

被害が多かった業界
公的機関、製造業、専門サービス業、教育サービス業
頻度
328件のインシデント、289件でデータの漏洩を確認
主な調査結果
スパイ活動関連のデータ漏洩では、今後も標的型フィッシングキャンペーンが先陣であり続けるようです。今年は教育機関が被害者層の中で顕著になってきました。

暗闇の中での戦略的画策

情報を取得して戦略的メリットを確保することは、孫子の時代からの伝統です。孫子は5種類のスパイ、郷間、内間、反間、死間、生間について書いています。不正なPDFをこしらえる輩がどの分類になるのか、よくわからないので、6番目の種類、お気楽スパイを作ることにします。

直接、換金可能なデータを奪おうとする組織犯罪グループと異なり、国家の支援を受けた実行者は、辛抱強く、また、標的の選り好みが強くなります。図38は、不幸にも選ばれてしまった業界の一覧です。

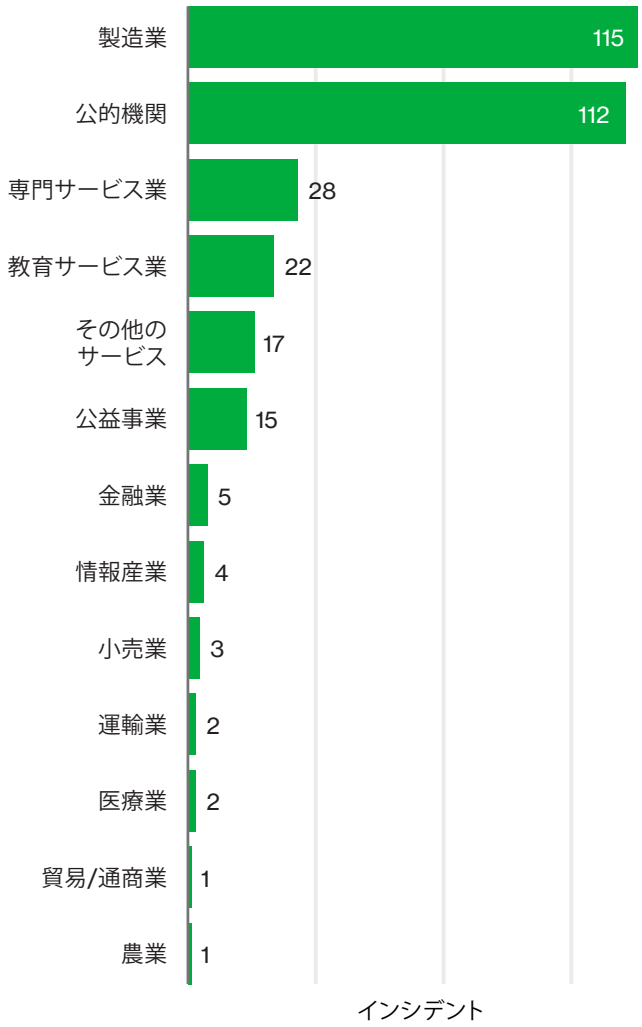


図38：サイバースパイ活動におけるデータ漏洩の件数および割合（N=271）

製造業と公的機関はまたもや、標的になった業界のトップであり、専門サービスが2年連続で第3位です。興味深い変化は、このような攻撃の標的として、学界が浮上したことです。大学はイノベーションの中心であり、国家の支援を受けたグループによって狙われるような新たなテクノロジーを生み出しています。1985年のCrossbowプロジェクトを支持する、Pacific Technical Universityの学生たちによって設計された化学レーザーのプロトタイプは、全くの架空ではありますが、素晴らしい例です。高度な事前調査を重ね、巧妙さと忍耐をもって標的を絞り込んだこれらの攻撃は、日和見的な攻撃ほどには記録されないと理解しておくことが重要です。図38の統計にお客様の業界が含まれていなかったとしても、攻撃者にとって有用な情報を持っている、もしくは持っているとみなされれば、潜在的に標的となってしまうのです。

私を釣り上げたスパイ

データ漏洩の90%以上は、国家の支援を受けたグループに起因し、国家、ライバル企業・組織、および退職した従業員が存在しますが、そこまで一般的ではありません。用いられる戦術は一貫性が保たれており、いまだにフィッシングが攻撃者に最も好まれています[23]。通常、攻撃者は、狙った被害者にファイルを添付した不正な電子メールを送付します。添付ファイルを開くと、コマンドを実行してマルウェアをコントロールし、デバイスの支配が確立、維持されます。そこから先、実行者が用いる手口は、群衆に紛れることです。任務の第一段階を果たした実行者は通常、不正利用の集中砲火を浴びせて、特権を拡大するような、検知されやすいアプローチを避けます。ネットフリックスで見るような、ミレニアム世代が大騒ぎするショーとは異なり、すぐに得られる喜びは、データ漏洩後のアクションに影響しません。

図39は、漏えいポイントの確保後に発生する各種の活動を示しています。他のマルウェアのダウンロード、内部ネットワークのマッピング、キーロガーとパスワードダンプのマルウェアの使用などによって、データを持ち出すという目的に向かって邁進します。上位15の攻撃行為のうち、7種類はマルウェアの機能であり、データから不正なペイロードが通常、電子メール（73%）と自動ダウンロード（13%）によって配信されていることがわかります。

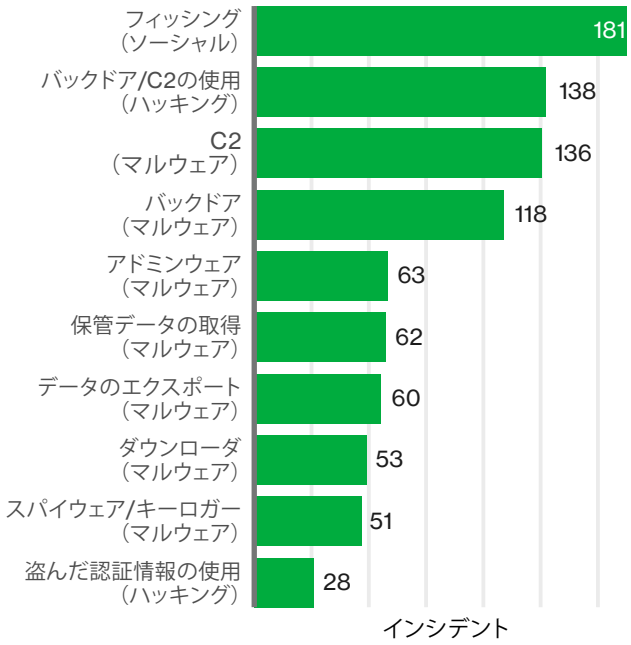


図39：サイバースパイ活動における上位の攻撃行為（N=271）

注目すべき領域

内部ネットワークへの足がかり確保を困難にします。コントロールするには、電子メールの出入り口でのマルウェア対応策、セキュリティ意識向上トレーニング、Webブラウザー（およびプラグイン）を最新の状態で維持することが不可欠です。データ実行防止（DEP）およびエンドポイント脅威検知/対策（ETDR）テクノロジーをテストし、導入します。

フィッシングの可能性が確認された場合は、ユーザーがセキュリティチームに報告し、組織がデバイスの動作に関して必要な情報を収集するプロセスを正式に策定します。内部と外部の両方について、やりとりをしていた相手を特定します。アカウントとデバイスの活動をレビューできるように、監視とロギングが有効になっていることを確認します。

侵害されたユーザーデバイスの影響を軽減します。特権を拡大する、または次のデバイスを侵害することを妨げるものがユーザー名とパスワードだけの場合、実行者を阻止する手立てが十分ではありません。ネットワークを分割すると、よりきめ細かいセキュリティゾーンが確立され、多要素認証を要求することによって、攻撃者に戦術の変更を迫り、群衆の中からあぶり出すことができます。

[23]「対人攻撃」より先にこのセクションをお読みになった場合は、次にそのページをお読みください。

DoS攻撃

ネットワークやシステムの可用性を損なうことが目的のあらゆる攻撃です。システムの性能低下やサービス停止を引き起こすことを目的とする、ネットワーク攻撃とアプリケーション攻撃の両方が含まれます。

概要

被害が多かった業界
芸術/娯楽業、専門サービス業、公的機関、情報産業、金融業
頻度
11,246件のインシデント、5件でデータの漏洩を確認
主な調査結果
組織の規模を調べたところ、DDoS攻撃のターゲットは大規模な組織に偏っていました（98%）。大部分の攻撃は、数日以内に終結しています。

HTTP 503エラー：サービス利用不可

Webプレゼンスのフル稼働の維持を担当している人々にとって、DDoS攻撃（またはそれによる脅威）は、苛立たしく厄介なものです。インターネットの記事を読んで頭痛の根本原因を自己診断するのと同様[24]、ニュースで最新最大の攻撃を調べた挙句、本当の心配性になってしまいます。

この攻撃に対応する究極の対応策はありません。企みを防ぐことはできませんし、企みが試された場合は、ISPなど上位の協力者に支援を頼んで防御する必要があります。誰かがボットネットを差し向けた場合、ISPやDoS緩和サービスと契約して、最小限の停止またはサービス低下で攻撃を阻止するアクションプランが用意されているといいのですが。いずれにしても、遡上するサケの末路を見るようなものです。確かに、たくさんのサケがいますが、どこから来て、どの程度がクマのエサになるかなど、誰も考えません。

サケすなわちパケットのたとえ話は、DDoSプロセスのごく初期段階まで遡ります。この場合、侵害され、ボットネットの働き蜂として、換金に駆り出されているデバイスに満ちているのがインターネットという海です。デフォルトのTelnet認証情報[25]によってハッキングされたデバイスを使用して作成されるMiraiボットネットは、タイムリーな例です。

[24] きっと腫瘍ではありませんよ!

[25] モノのインターネット（IoT）に焦点があたっています。可用性に対する攻撃を仕掛けている側の場合、ボットネットがカメラであろうと、デスクトップであろうと、関係ありません。また、インターネットに対してリモートアクセスポートが空いていて、デフォルトの認証情報を使用しているデバイスは、90年代初期の安全ではないサーバーと似ています。もっと小さいプラスチックの箱に入っているというだけです。IoTというキャッチーな言葉にばかり注目するのではなく、データ漏洩がこれほど容易になるのかというような脆弱性に注目してください。

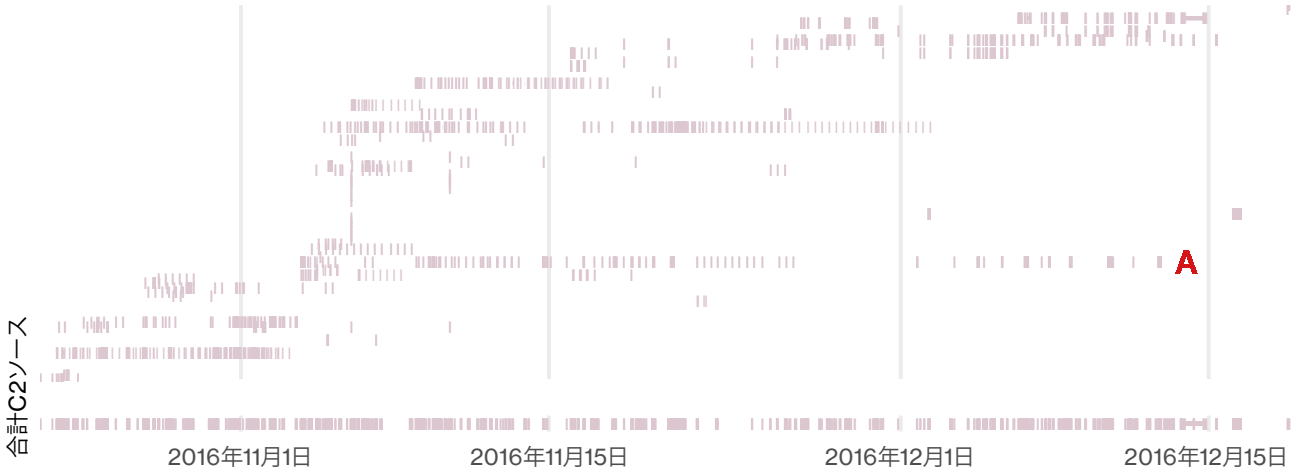


図40：C2ソースに見るMiraiボットネットが課すタスクの経時変化

試算

ボットネットの作成後、デバイスにはインターネットの多方面からターゲットに向かって上流へ、パケットを送信するタスクが与えられます。図40は、2016年10月22日から2016年12月18日にかけて、約50のC2ソースに基づき、各種Miraiボットネットのタスクを示しています。いささかランダムサンプリングのようですが、あることを示しています。Miraiについてはよく聞きますが、たえず世界を攻撃しているのは、このジャガノートではありません。多くのC2ソースがタスクを課すのは一定期間であり、繰り返すことは決してありません。11月初めから12月半ばまで、継続的に活発だったソースは、**A**だけのようです。総計のみがボットネットの常時使用に近づき始めます。

ネットは広大で無限

パケットはそこから、インターネットという海原を越えなければなりません。途中で一部は、特定のプロトコルで転送速度制限を超えたパケットをブロックする、ネットワークインフラストラクチャによって「喰われて」しまったり、トラフィックを最小限に抑えるためのDDoS緩和ツールに飲み込まれてしまうものもあります。それでも、多くは上流に向かい、目的のターゲットにたどり着きます。

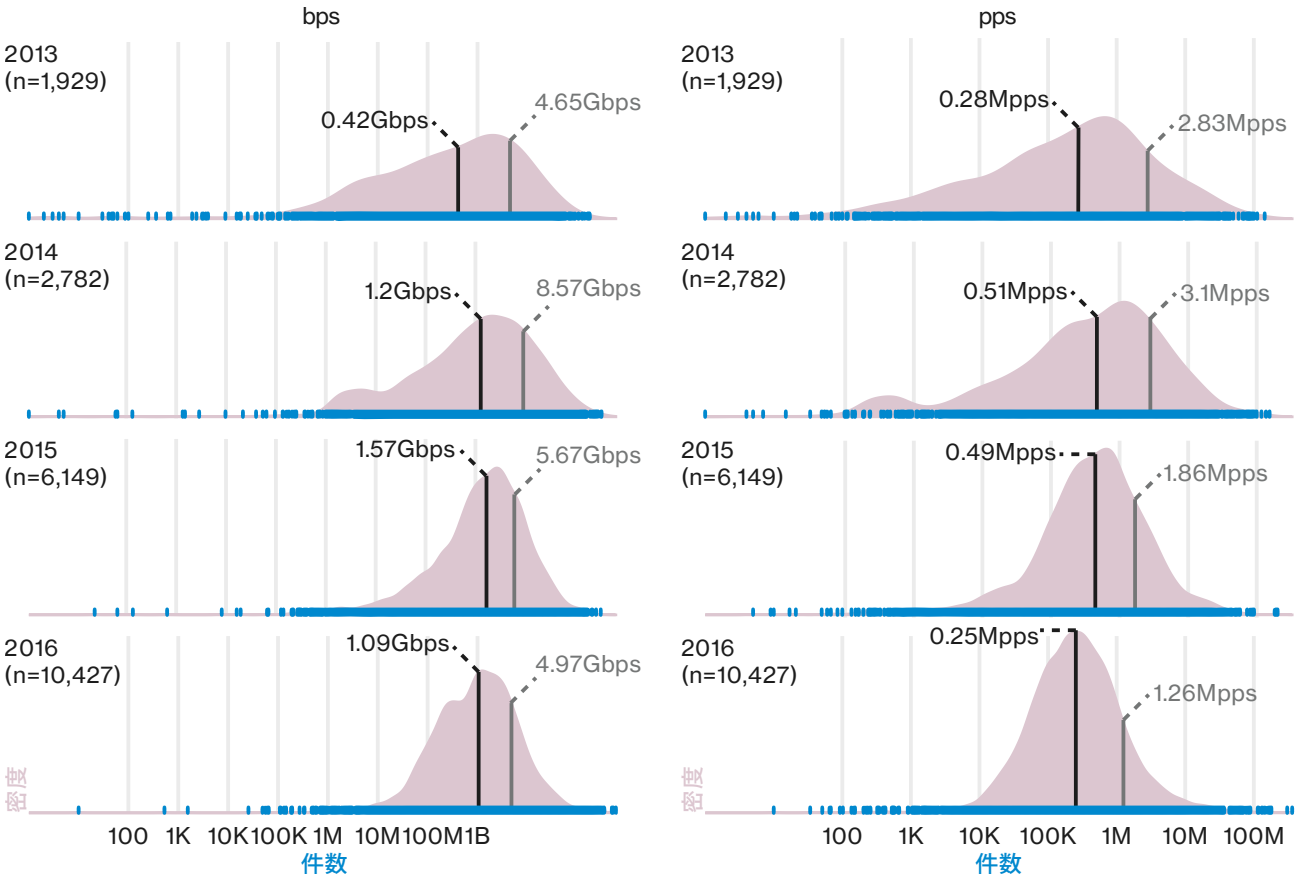


図41：DoS攻撃の帯域幅およびパケット数の水準

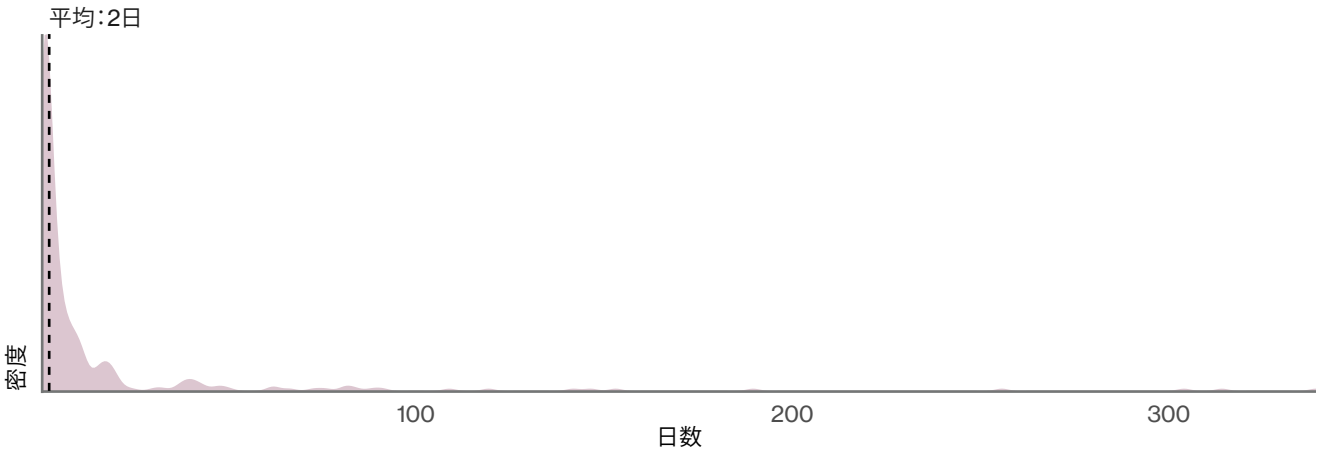


図42：組織別に見た攻撃されている年間日数の密度

図41は、緩和サービスによって測定されたDDoSインシデントの平均的な攻撃規模が、実際に縮小したことを示しています。組織が攻撃を受けていた期間についても幅があります。

図42から、年間を通じてたえず攻撃されている企業は、ごくわずかで、大部分は数日間の集中砲火に対処するだけだと分かります。

注目すべき領域

必要な緩和のタイプとレベルを理解することが重要です。DDoSにさらされた可能性があるのは、どのような資産ですか？ それらの資産がなかった場合、どのような影響がありますか？ 業務は普段どおりできていますか？ それともこの世の終わりですか？ DDoSサービスはそれぞれ、キャパシティ、検知方法、サービスのタイプが異なります。（規模、期間共に）平均的な攻撃に対抗する必要がありますか、または大規模で長期的な攻撃から身を守りたいとお思いでしょうか？

TDoS（Telephone Denial of Service）— Because you didn't have enough problems already

DoSのタイプは、パケットベースのDDoSだけではありません。TDoS（Telephone Denial of Service）も、VoIPという通話システムの台頭によって可能になった攻撃タイプの1つです。

TDoSは従来のDDoSと同様、組織にとって本物の脅威になり得ます。リスク軽減を支援するサービスがあり、データサイエンスとマシンラーニングの進歩によって、日々向上しています。したがって、DDoSの場合とまったく同様、防御策を講じなかった場合にビジネスが受ける影響と防御策を導入するコストを比較して、よく考えることが重要です。必要である場合は、攻撃が始まる前に導入方法について知っておいたほうがいいでしょう。

図43に、単発のTDoS攻撃の事例を示しており、TDoSの平均的な特徴や傾向などを示唆するものでは決してありません。（私見では）興味深いものであり、この攻撃はどのようなものかを知る上で参考になるはずです。

- **A**は、平常の日を表しています。
- **B**で、TDoSが始まります。
- しばらくは上昇を続けているように見えます。
- しかし、**C**で、既存ソースからの通話量が上昇します。
- **D**で、攻撃に第2のソースが加わります。
- 1日ほど攻撃が止まりますが、**E**で再開し、範囲を狭めながら、**F**（**D**からのソースはなしで）に進みます。

図43：TDoS攻撃中の通話量

内部者による特権の不正利用

承認を得ずに企業・組織リソースを使用、悪用するなど、不正利用というアクションカテゴリーのインシデントはすべて、このパターンに分類されます。これは主に、内部者のみによる不正利用ですが、外部者（共謀による）およびパートナー（特権が与えられているため）も登場します。

概要

被害が多かった業界
公的機関、医療業、金融業
頻度
合計7,743件のインシデント、277件でデータの漏洩を確認
主な調査結果
攻撃実行者がセキュリティーの内部にすでにいる場合、発見はかなり難しく、大部分のインシデントは、発見に数か月、数年を要します。こうした加害者の大半は、金銭目的ですが、競争上の優位性を確保するために、データを使いたがる人々もいるので、排除してはなりません。

そのような従業員の場合、誰が敵を必要とするでしょうか？

悪意のある内部者は必ずしも、膨大なデータをつかみ取り、リボンをつけて梱包し、WikiLeaksに渡す人というわけではありません。この種のデータ漏洩は、大きく報道され、称賛されるか、あるいは実行者が捕まって投獄される可能性があります。それよりもっと一般的な話として、データを持ち逃げする平均的なエンドユーザーは、どこかでそのデータを換金したいと考えています（60%）。従業員が好奇心に負け、認められない詮索に手を染めることも時としてあります（17%）。このような不正利用のシナリオは、各種のデータ漏洩が反映されています。個人情報と医療記録（71%）は、アイデンティティ窃取や納税の不正申告など、金銭目的の攻撃のターゲットですが、ゴシップ的な価値のみで狙われることもまれにあります。

このパターンには、ライバル会社の立ち上げまたは転職のためにデータを盗むなどのスパイ行為（15%）も含まれます。これらのケースでは、極秘内部データ、企業機密、またはその両方が盗まれました（24%）。販売予測、マーケティングプラン、見込み顧客リスト、またはその他の知的財産が含まれている可能性があります。

このパターンの攻撃実行者は、境界の内側で攻撃し、データベースを不当に占拠し（57%）、印刷物の文書をくまなく探り（16%）、他の従業員の電子メールにアクセスします（9%）。

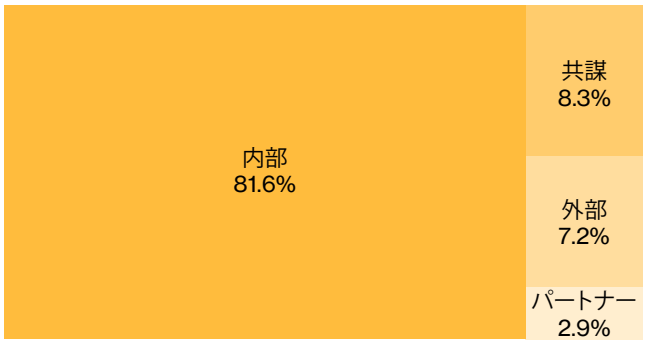


図44：内部者による特権の不正利用における攻撃実行者のカテゴリー別データ漏洩の割合（N=277）

このパターンでは、内部実行者が突出していることが予測され、実際そうなっています。しかし、内部実行者がインシデントの89%を占める一方、図44には外部およびパートナーの実行者も含まれています。これは、複数の実行者が共謀している可能性のある（8%）、最も一般的なパターンです。

内部者による脅威は、データ漏洩では外部の実行者ほど一般的ではありませんが、非常に重要で、データ漏洩の15%を占めています。(ミスを含まないすべてのパターン) 内部アカウントの使用を制限、記録し、監視するという防御策は、不誠実な従業員のためだけではありません。外部の敵にとって、主要な目的の1つは、攻撃を進めるために内部の正当な認証情報にアクセスすることです。

お客様の企業の全従業員が、強欲さや不誠実、悪意と無縁の模範的な従業員だとしても、内部者の不正利用を突き止めるために設計されたセキュリティコントロールにより、特権ユーザーになりすましている外部の攻撃者も発見できます。

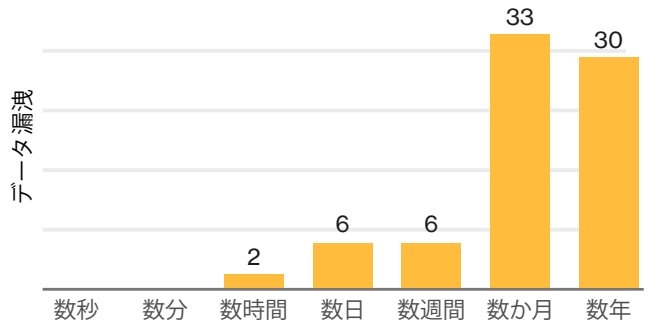


図45:内部者による特権の不正利用におけるデータ漏洩発見のタイムライン (N=77)

図45に示したこのパターンの発見のタイムラインから、データ漏洩の検知に週単位以下ではなく、数か月または数年かかる可能性が高いことがわかります。自身の組織が、機密情報のコントロールを失ったことを発見するまでに数年かかるというのは、新たに発見された星を眺めているようなもので、最初の事象が発生したのは、はるか昔なのに、今になって詳細を学んでいるというわけです。

注目すべき領域

ここでは、公的機関と医療業界、不適切なデータベースアクセス、金銭的な動機、さらに好奇心について取り上げます。これらのデータから3つの共通点があります。

- 医療業の従業員は、アイデンティティ窃取を目的にPIIを盗むか、または患者の医療履歴を詮索するために、医療データベースにアクセスしています。
- 公的機関のデータ漏洩には、法執行機関に雇われ、犯罪データベースにアクセスして、誰かのスキャンダルを手に入れようとする従業員が関与することがよくあります。
- 許容範囲内の使用に関するトレーニングや、正当な必要性なしに個人情報にアクセスした場合は、警告を受け、処分されることを明確に伝えるバナーによって、スヌーピングを阻止することができます。

退社後の従業員のデバイスに対するフォレンジック調査が発端となって、データ漏洩が発見されることもあります。さらに、企業・組織はリアルタイムに近い状態で、データ転送またはUSBの使用を捉える (および阻止する) ためのモニタリングに注力し、潜在的な影響を軽減することも重要です。

人的ミス

意図したものではない行為によって、セキュリティ資産の属性が侵害されるインシデント。
デバイスの紛失は、窃取で分類されるため含まれません。

概要

被害が多かった業界

医療業、公的機関、教育サービス業、専門サービス業（データ漏洩のみ）

頻度

2,478件のインシデント、222件でデータの漏洩を確認

主な調査結果

電子媒体であるか紙の書類であるかに関係なく、情報の誤配が相変わらず人的ミスの大きな部分を占めています。公開ミスや廃棄ミスも、それなりの割合を占めています。

起きてしまったミス

アレキサンダー・ポープは、「失敗するは人間なり、それを寛容するのは神なり」と書きましたが、それはデータ漏洩通知法ができるずっと前のことです。我々はこれからも人間であり続けることは間違いないですが、今や、我々の愚行を披露する舞台ははるかに大きくなっています。

人的ミスに関しては、2つのポイントを押さえておくことが重要です。まず、VERIS（Vocabulary for Event Recording and Incident Sharing）によると、人的ミスが選択されるのは、そのミスそのものがデータ漏洩の主因の場合に限られます。すべてのデータ漏洩は、一連の出来事のどこかにミスがあるという説が熱く論じられていますが、データ漏洩に直接つながらなかった場合は、その他のパターンに分類されます。次に、この報告書の調査結果は、主に協力企業・組織からいただいたデータに基づいています。この企業・組織は、毎年同じではありません。新しく参加する企業・組織もあれば、脱退または一時的に参加を取りやめる企業・組織もあります。

この報告書では、人的ミスの大部分は、報告書に協力していただいた政府機関で発生しています。ただしこれは、政府機関がそれ以外の組織に比べてミスを犯しやすいということではありません。むしろ、他の業界より厳格な報告要件が適用されているからです。今年は昨年に比べ、これらの組織からのデータが大幅に少なくなりました。さまざまな原因がありますが、ほとんどの場合、人間の行動が大きく変化したからではなく、提供されたサンプルに関係があります。

何が起きたかというと...

図46では、今年のエラーの種類がほとんど、いつもと同じ領域に分かれていることが確認できます。誤配、公開ミス、廃棄ミス、および設定ミスです。誤配の最も一般的な形は圧倒的に、紙の書類を誤った相手に送ってしまうことです（残念ながら、粘土板やパピルスの巻物が行方不明になったという事例は1つもありませんでした）。

公開ミスが発生するのは、想定外の対象者に情報が利用可能になる、または電子的に表示可能になったときです。たとえば、イントラネットを想定していた文書が、インターネット全体に公開されてしまったような場合です。図46では、廃棄ミスが第3位です。しかし、顎が外れるほどびっくりする露骨なコメディとくれば、それは必ずブルーリボン受賞者でしょう。

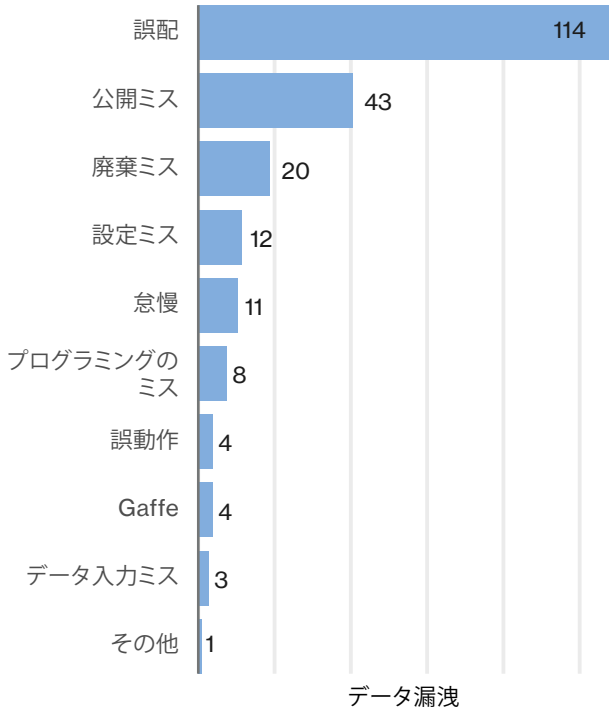


図46：人的ミスによるデータ漏洩の脅威となるアクショントップ10（N=212）

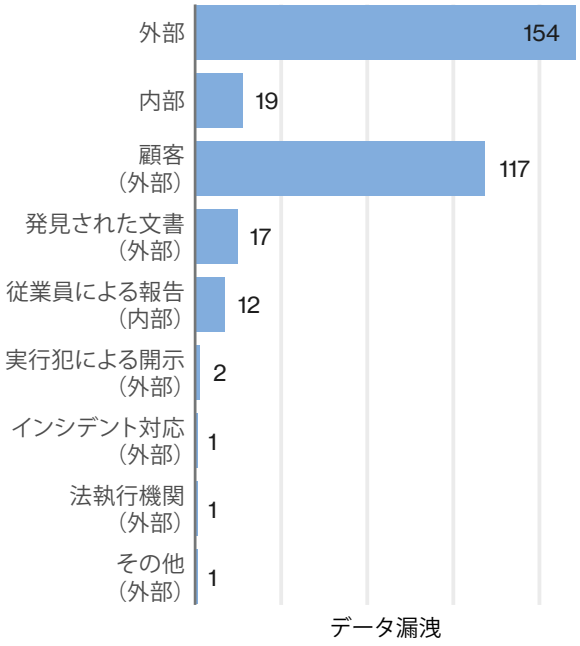


図47：人的ミスにおけるデータ漏洩の発見方法（N=174）

この報告書には、首をかしげるようなことが溢れています。例えば、オークションサイトで医療記録の詰まったファイルキャビネットを売ったり、大手新聞社から記者が気付かれないように視察に来ていた際、ある企業・組織が市のごみ処理場でPIIをこっそり破棄していました。我々は、データ廃棄の大失敗を対象に、ダーウィン賞を創設すべきでしょうか？

最後は設定ミスです。公開ミスと似ているようで違います。管理者がファイアウォールのルールを入力する際に間違ったため、想定されていた特定の対象者ではなく、ある個人情報が誰でも閲覧できるようになった例があります。または、管理者がデバッグログをオンにしたため、クリアテキストファイルに機密情報がダンプされた例もあります。

図47から、失敗を指摘するのは通常、顧客であることがわかります（76%）。Webサイトに自分の情報が表示されているのを見つけたり、誰かほかの人の医療記録が自宅に配達されたりすれば、知らせてくるのが普通です。

第2位の11%は外部関係者が見つけた文書で、1位とは大差があります。これらは、部外者（例えば、上記のオークションサイトからファイルキャビネットを受け取った人物）からの通知です。外部関係者が機密文書を発見したその他さまざまな方法をすべて開示してしまうと、読者のみなさんが人間に対する信用を失うので、これについては秘密にしたまま、先に進みます。

ポジティブな事実で締めくくると、約8%のケースでは、良心的で思いやりのある従業員が、何か変だと気付いて報告することによって、ミスが発見されました。

注目すべき領域

人間の不注意に対応するファイアウォールルールはありません。不注意のアラートシステムもありません。しかし、人的ミスを最小限に抑える、基本的なポリシーと手順関連のステップはいくつかあります。

破棄しようとしているものが少しでも機密情報が含まれている可能性のある、「すべての物」に対して、正式な処分の手順を策定します。これにはデスクトップからくずかごまで、あらゆるものが含まれます。さらに、ポリシーが適用され、適用されたことを証明する記録が保管されていることを確認します。

過去の過ちについて、記録を保管し、セキュリティトレーニングで使用します。公園のベンチにPIIを置き忘れると、スピアフィッシングのターゲットになり、企業・組織に被害・損害を与えたりします。問題になる可能性があるか、過去に問題になったものの取り扱い、保管、配信、破棄の場合の基本事項を忘れずに守ってください。

何かを公開したり、企業サーバーやWebページに送信する場合は、必ず複数人でチェックします。Webページを監視し、外部の関係者より先に、公開ミスを発見してください。

ペイメントカードスキミング

スキミング装置がカード情報を読み取る機器（ATM、ガソリン給油機、POS端末など）に物理的に埋め込まれたすべてのインシデント。

概要

被害が多かった業界
小売業、金融業
頻度
合計118件のインシデント、89件でデータの漏洩を確認
主な調査結果
相変わらずATMがインシデントの大半を占めていますが、ATM攻撃の件数は25%下がりました。一方、ガソリン給油機関連の攻撃は3倍以上になっています。攻撃者は東欧とキューバからが大部分です。

パターンは変わっていません... ほとんどは

犯罪者にとって、ペイメントカードスキミングは今なお、金になる有利な手口であり、以前にも指摘したとおり、こうした犯罪者が手口を変えることで、波風を立てたくないと考えているのは明らかです。皆様もYouTubeでSupermanが電話ボックスで着替えるより素早く、ATMにスキミング装置が取り付けられる動画を見たことがあるはずです。迅速かつ容易に攻撃を遂行できる、比較的割の良い成果が得られる可能性が高い、捕まる可能性が比較的低いといった事柄を全部ひっくるめて、スキミングは我々のデータセットにおいて、非常に人気の高い攻撃行為になっています。

一般に、この分野の調査結果は、毎年それほど変わりません。しかし、今年はこれまでと比べて、注目すべき変化が1つありました。ガソリン給油機の端末が関係するインシデントの件数は、昨年から3倍以上増加しましたが、ATMが影響を受けたインシデントの件数は、約25%減少しました。これは単に、今年、ご協力いただいている企業・組織から提供された事例の数とタイプが原因、またはそういう傾向になりつつあることが考えられますが、いずれにしても、これが続くかどうか、注視し続けましょう。

誰のせいでもなく、自分のせい

人間の基本的なニーズの1つは、誰か責める相手が必要だということです。そこで、次の問いにつながります。この犯罪は、誰の責任なのか。過去にも述べましたが、このセクションのデータに関して、ご協力いただいている企業・組織の性質上、被害者は、ほぼ米国に集中しています。しかし、加害者の観点から見ると、堂々と、組織犯罪の責任にすることができます。以前の報告書と同様、ペイメントカードスキミングに関しては、引き続き東欧が大多数を占めており、犯罪者の出身を明確に特定できた場合は、攻撃の60%がルーマニアの実行者に起因していました。キューバは今年から登場し、スキミングの約16%を占めています。当然、こうした犯罪グループのリーダーは、カヌーでやってきて自分で装置を取り付けるわけではありません。現地の協力者が物理的な作業を行います。

チップ＆ピン方式―リビング越しに聞こえる銃声

遡ること2015年、我々はその年の10月までに米国で義務付けられた、EMV（チップ＆ピン）方式の採用予測に関する短いセクションを組み込みました。それから2年経っているので、スキミングに関して、このテクノロジーがどこまで状況を変えたか、振り返っておくのが妥当でしょう。当時、生じている主な変化が（とにかく最初は）単に法的責任の変更であったため、「そこまで大騒ぎする必要はありません」と読者に指摘しました。つまり、データ漏洩の発生時に劣ったテクノロジーを導入していたのが誰であろうと、端末をまだアップグレードしていなかった会社、または光り輝く新しいEMVカードを発行できなかった銀行が責めを負うことになります。とはいえ、結論はまだ出ていません。EMV対応のATMを見かけることはあまり（いえ、ほとんど）ありませんが、チップリーダーを装備したガソリン給油機の数より、ビッグフットの目撃報告の方がはるかに多いでしょう[26]。したがって、比較的導入件数が少ないことを考えると、チップ＆ピン方式のテクノロジーがこのパターンにおいて、我々の調査結果を大きく変化させたとは考えられません。しかし、チップリーダーは「ゆっくり」普及してきているので、今後、犯罪者の用いる戦術がどのように変化するのか、興味深いところです。creditcards.com[27] によると、2016年後半の時点で、米国のATMの25%がチップ対応です。しかし、こうしたATMは基本的に大量のトラフィックを扱う、大手銀行が所有していると覚えておくことが重要です。一方では、設置費用が比較的高いこと、もう一方では、遵守していない場合は金銭的責任が発生するため、それらが相まって、トラフィックの少ないコンビニエンスストアのATMが消滅するかもしれません。

お客様の時代が来ます

相変わらず、外部関係者がほぼすべてのデータ漏洩を発見しています。注目すべきは、昨年に比べて、法執行機関による発見が増え、CPP（Common Point of Purchase）アルゴリズムによる不正検知にほぼ追いついていることです。図48から、内部者による発見が遅れを取っていることがわかります。内部で発見された場合は、我々の報告書にサンプルとしてあがってこないような形で処理されているのではないかと楽観的かつ期待を込めて推測します。しかし、小規模なガソリンスタンドであろうと、我々は現実的にならなければなりません。係員はロトやツリー型のエアフレッシュナーを売る方に熱心ですし、同時にすべての売り場で目を光らせているというようなことは期待できません。

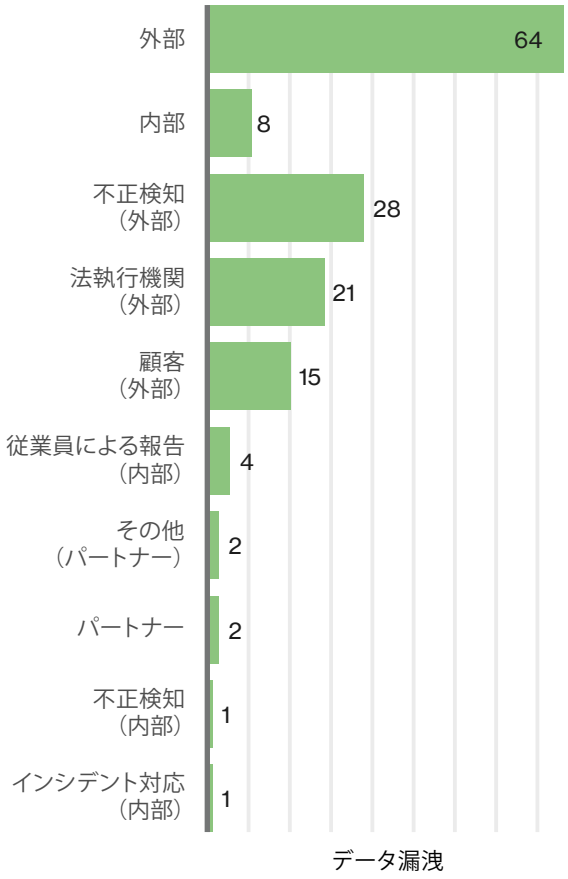


図48：ペイメントカードスキミングによるデータ漏洩の発見方法（N=74）

注目すべき領域

屋外の端末をビデオカメラで監視し、定期的にテープを見直してください。これにより、より早く取り付けられた不審な装置の存在を知ることができるので、それだけ影響を少なくできます。日常の閉店または開店手順の一部として端末をチェックしてください。全端末の目視点検をスケジュールし、従業員が何を探すべきか分かるようにトレーニングしてください。

可能であれば、不正改ざん防止策を行ってください。例えば、ガソリン給油機の扉の上から不正改ざん防止テープを張り、毎日、そのテープが破られていないか確認します。さらに、異物の痕跡がないか、端末の内部も確認します。

[26] 公平な立場で言うと、ATMおよびガソリン給油機は、まだ法的責任変更の期日に至っていません。
https://usa.visa.com/visa-everywhere/security/emv-at-the-pump.html

[27] www.creditcards.com/credit-card-news/atm-change-accept-emv-chip-1273.php

POSへの侵入

カードを使用する小売業務環境に対するリモート攻撃。POS端末とPOSコントローラーが標的となる資産です。PIN入力デバイス（PED）パッドの物理的改変またはデバイスの交換については、ペイメントカードスキミングのセクションで扱っています。

概要

被害が多かった業界

ホテル業および外食産業、小売業

頻度

合計212件のインシデント、207件でデータの漏洩を確認

主な調査結果

ホテル業、特にレストランがPOSへの侵入の被害を最も受けています。盗んだ認証情報を使用して、POS環境にアクセスする行為は増え続けており、ハッキング行為としては、ブルートフォースのほぼ2倍です。

相変わらず、RAMスクレーピングが蔓延していますが、POSシステムを狙う多機能マルウェアの一種として、キーロガー/スパイウェアのマルウェアが大幅に増加しています。過去数年間と同様の傾向が続いており、このデータが示している猛攻撃（1人の攻撃者、多数の被害者）は、POSベンダーに対して成功した攻撃の副産物であり、設定が不十分かつインターネットに接続されたPOSデバイスを狙った自動攻撃が原因ではありません。

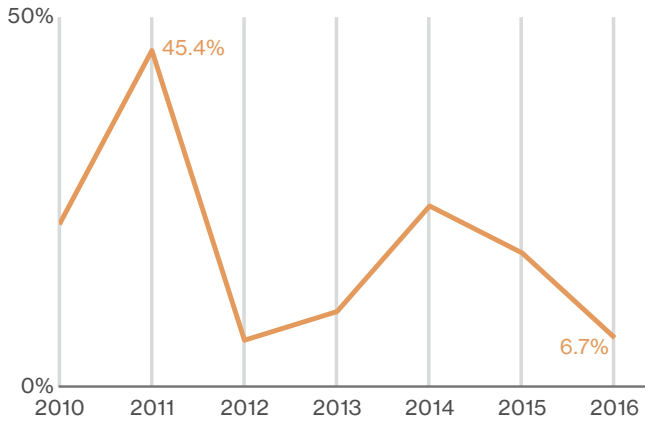
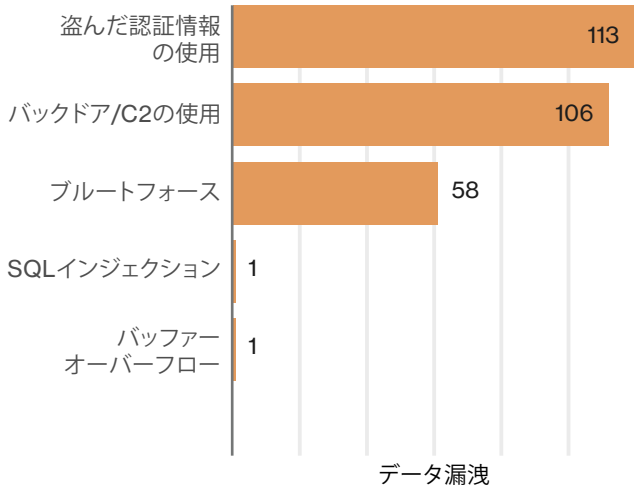


図49：すべてのデータ漏洩におけるPOSへの侵入パターンの割合（経時変化）

お伝えしたい要点

POSのデータ漏洩―基本的に日和見的であり、外部実行者により主導されます。今年のデータ漏洩全体のうち10%強です。図49からお分かりいただけるとおり、POSのデータ漏洩は年々減少しています。

2011年度の報告書に遡ると、我々の調査結果では、インターネットに接続され、デフォルトの認証情報を使用しているPOSサーバーを狙った、拡張性のある自動攻撃が圧倒的多数を占めていました。このデータ漏洩の手口は、主に小規模な企業・組織で繰り返し見られました。2014年度の報告書になると、2013年を「小売業界のデータ漏洩の年」と呼んでいます。これは、被害を被った企業・組織の数ではなく、POSへの侵入が大手小売業者に重大な影響を及ぼしたことによるものです。良かったのは、このパターンが（少なくとも今年は）企業・組織にとって多大な影響を及ぼすビジネス上の問題ではなくなっていることです。



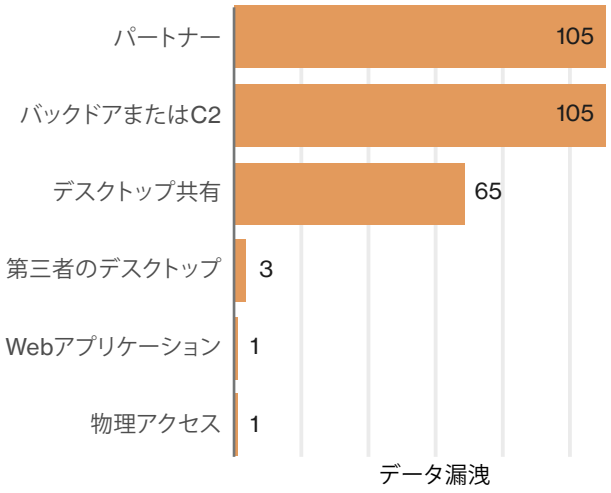


図50：POSへの侵入におけるハッキングの種類（N=175）および経路（N=176）

図50は、POSハッキングの特徴を示しています。データ漏洩のほぼ65%で、盗まれた認証情報がハッキング手段として使用されているのに対して、POSシステム侵害の3分の1強はブルートフォースによるものです。昨年と同じ傾向をたどっており、盗んだ認証情報を使用したデータ漏洩の95%で、ベンダーのリモートアクセス権を利用して、顧客のPOS環境をハッキングしています。

マルウェアは、ほとんど必ず実行メモリからデータを取得している（95%）のに対して、POSのデータ漏洩では、半数強がキーロガーを使用していました。これは昨年から大幅に増加しています。この調査結果は、RAMスクレーピングとキーロガーの両方の機能を備えたPOSマルウェアが特徴である猛攻撃がもたらしたものであることを注意事項としてお伝えします。POSマルウェアファミリーは今後も、C2インフラストラクチャとの通信、データの取得とエクスポートをはじめ、さまざまな機能を果たすことが予測されます。

最後に、調査結果に移りましょう。図51は、大部分のデータ漏洩が不正検知によって発見されていることを示しており、昨年の25%増です。年ごとに比較すると、法執行機関による発見は9分の1まで、顧客による発見は6分の1まで下がっています。どのような経緯で発見されたかに関係なく、外部関係者による発見はほぼ必ず、データ漏洩後の不正に結びついています。すなわち、法執行機関の場合、最初の被害者がCPP（Certified Protection Professional）または顧客からの通知によって確認され、その後同一の攻撃にあった犠牲者に通達されます。

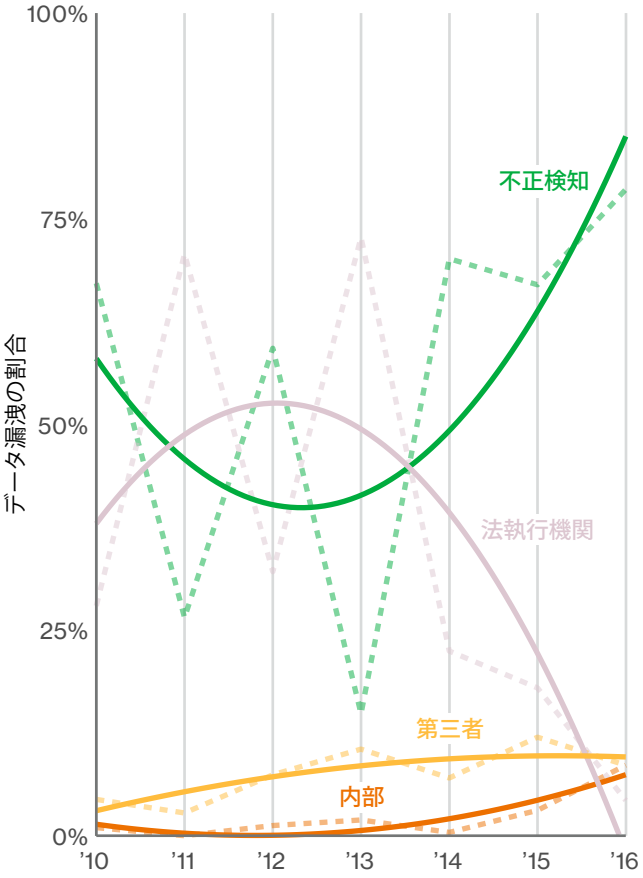


図51：POSへの侵入によるデータ漏洩の発見方法（経時変化）

注目すべき領域

POSベンダーが、顧客に対してより一層安全なリモートアクセスメカニズムを保証できるように取り組んでいくことを願ってやみません。規模の大小を問わず、すべての企業・組織は第三者のベンダーに、そのベンダーのセキュリティ対策、特に2要素認証の使用について、確認する必要があります。

認証を強化し、POS環境へのリモートアクセスを制限することが必要不可欠です。小規模な家族経営であれば、システムがインターネットにアクセスできないようにするだけでもかまいません。大規模な標的の場合は、もっと根気のいる作業になりますが、今年の我々のデータが示しているとおり、決して不可能ではありません。

物理的窃取および紛失

置き忘れまたは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。

概要

被害が多かった業界
公的機関、医療業
頻度
5,698件のインシデント、74件でデータの漏洩を確認
主な調査結果
これまでの報告書と同様、置き忘れが窃取より一般的です。被害が多かった業界は、紛失の可能性が高まったのではなく、データ提供にご協力くださった企業・組織および規制条件による影響があります。

さようなら、またね、私の資産

サイバースパイ活動が陽とすると、このパターンは陰です。インシデントの数は多いですが、話すことはあまりありません。繰り返しになりますが、セキュリティ意識向上トレーニングで、車にラップトップを放置したり、地下鉄にタブレットを置き忘れたりしないように注意喚起し、従業員を指導します。しかし、このセクションで最も理解し、覚えていただきたいのは、誰しも忘れ物をするということです。オスカー・ワイルドはかつて、このような皮肉を言いました。「片親を亡くすことは不幸とみなされるかもしれないが、両親を亡くすことは不注意としか思えない。」この名言は、遠回しながら、窃取と紛失に当てはまります。人はしばしば油断します。しかし、適切な対策を講じれば、資産の物理的損失の影響を大幅に軽減できます。

まずは、暗号化から始めましょう。Windows（BitLocker）とMac（FileVault）の両方で、ネイティブのフルディスク暗号化を利用できます。個々のデバイスごとに3ないし4ステップの簡単なプロセスで導入が可能です[28]。モバイルデバイスの世界では、このようなテクノロジーを標準仕様に組み込むことができます。また、集中管理によって導入と検証を行うことができます。

しかし、特に紙の書類など、すべての資産を暗号化できるわけではありません。確認されたデータ漏洩の大半は、文書紛失を伴っています（いくつかの事例では、記録紛失件数の合計が数千にのぼります）。すべてのデバイス紛失で機密情報が漏洩するとは思いませんが、データが文字どおり白黒で印刷されている場合は、偏見にとらわれず漏洩を推測しても良いのかもしれません。それには、業務に必要のない機密情報を印刷しないように、また、印刷しなければならない場合は、データをトークン化するように、企業文化を順応させる必要があります。これは、別のパターンで扱う廃棄ミスにも役立ちます。

ユーザーが機密情報を印刷するか、または外付けドライブにダウンロードした結果、それが紛失する、もしくは盗まれるといった、不正利用行為のパターンに関連する事例はあります。データの取り扱いに関するポリシーを徹底させ、不適切なデータ転送がないか監視します。

注目すべき領域

資産の紛失をゼロにすることはできませんが、防御可能な体制を作ることで、データ漏洩の通知を受け取るという不愉快な事態を回避できます。

[28] https://support.apple.com/en-us/HT204837

Webアプリケーション攻撃

攻撃経路としてWebアプリケーションが用いられた、あらゆるインシデント。これには、アプリケーションのコードレベルの脆弱性を利用することや認証メカニズムを妨害することが含まれます。

概要

被害が多かった業界
金融業、公的機関、情報産業
頻度
合計6,502件のインシデント（二次的な動機で3,583件追加）、571件でデータの漏洩を確認済み
主な調査結果
このパターンのデータ漏洩は、Dridexボットネットの制圧に関与した協力企業・組織が収集した情報に大きく左右されます。何百というデータ漏洩では、顧客に対するソーシャルエンジニアリングに続き、Dridexマルウェア、その後のキーロガーで不正取得された認証情報の利用が大半を占めます。

昨年と比較して、Webアプリケーションのインシデントが増えていますが、データ漏洩の件数は減少しています。具体的に言うと、このパターンでは、大部分のインシデントがWebサイトの改ざんに関係していたことが複数のCERTによって報告されていますが、データの漏洩は確認されませんでした。改ざんまたは転用以外のインシデントに焦点を合わせると（次頁「目的を果たすための手段」をご参照ください）、データは盗んだ認証情報の使用、フィッシング、C2/バックドアが再び今年の主な攻撃行為で、残りのインシデントの60%以上あったことを示しています。

ボットネットとの闘い

データ漏洩に移ると、77%がボットネット活動の標的でした。これは、このパターンで目立ち、繰り返されている傾向です（Dridex、また遭ったね）。そこで、ボットネットのサブセットがある場合とない場合を含めて、Webアプリケーションのデータ漏洩を検証し、全体像を把握して、偏りを調整することにしました。ボットネットを含めた場合、データ漏洩の93%が組織犯罪と結びついていました。昨年と同じ行動が繰り返されています。顧客への電子メールの添付ファイルを使用したソーシャルエンジニアリングを伴う何百というデータ漏洩が発生し、バンキング型トロイの木馬が続き、さらに、キーロガーまたはフォームグラバーによって盗まれた認証情報が使用されています。

ボットネットによる偏りを除外

機密情報の発見を目的としない、ボットネットの情報漏洩のデータを分析したところ、残りの131件の情報漏洩では、上の説明に比べ、多くの点で変化があったことがわかりました。トップの外部実行者は、どの組織にも所属しない攻撃者（42%）になり、その結果、組織犯罪が第2位（32%）に格下げされました。ハッキングの種類の観点から見ると、盗んだ認証情報の使用が今なお第1位ですが、図52が物語るように、昔からおなじみのSQL Injection（SQLi）も安定した地位を得ています。

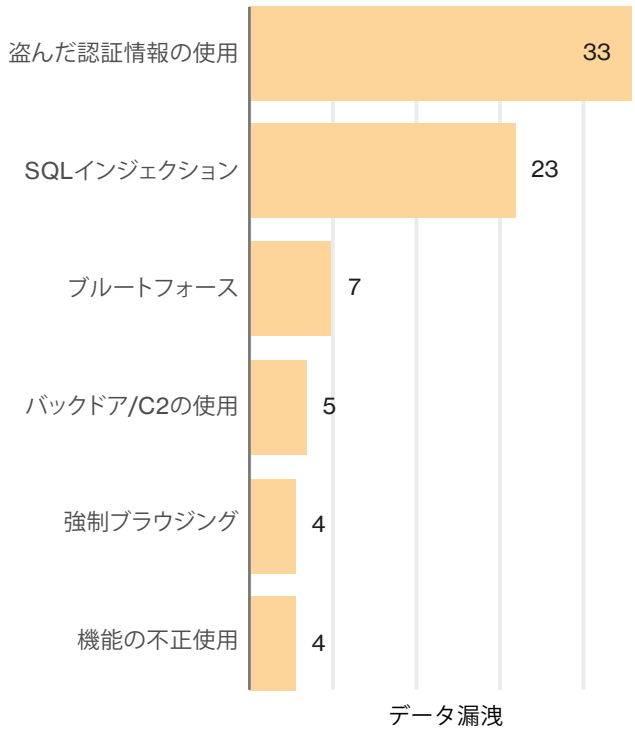


図52：Webアプリケーション攻撃によるデータ漏洩で上位のハッキング—ボットネットの活動を除く（N=72）

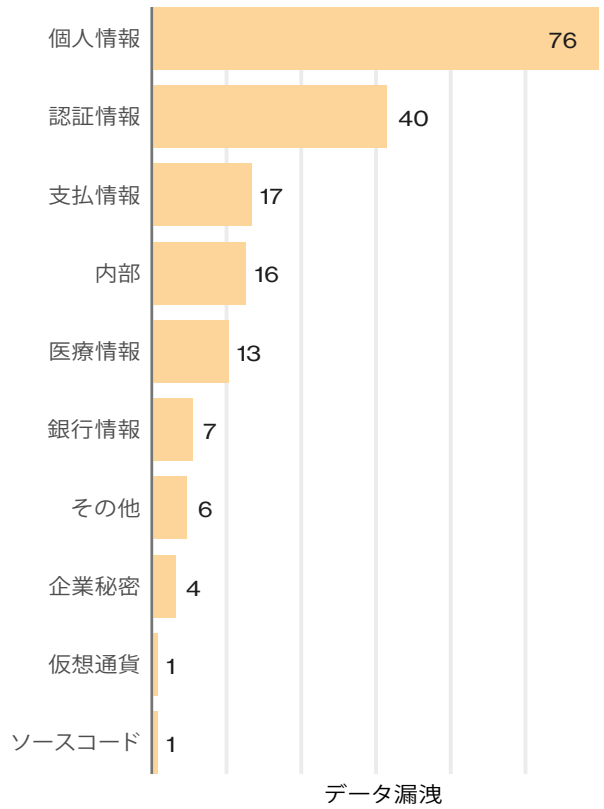


図53：Webアプリケーション攻撃で漏洩したデータの種類—ボットネットの活動を除く（N=161）

図53から、Webアプリケーションを介して標的となり、取得されるデータのタイプについて、手掛かりが得られます。最も頻繁に漏洩したデータのタイプは、個人情報が認証情報に取って代わり、データ漏洩の半分以上に見られました。

目的を果たすための手段

ここで、二次的特性を見逃さないようにしましょう。そこにも目的があります。2015年度のDBIRで指摘したとおり、功利主義の進行が顕著です。別の標的に攻撃を仕掛ける手段として、ハッカーがWebサーバーを狙う事例が目立っています。水飲み場型攻撃と呼ばれる戦術です。ウェブサイトの改ざんは主な動機ではありません。スパイ活動の主な動機は、Webサイトのビジターでした。それ以上によく発生するのは、Webサイトを日和見的に侵害し、攻撃者のインフラストラクチャ（C2サーバー、マルウェアの提供、フィッシングサイトへの転換など）を構築することです。現在、我々の報告書には、二次的な動機を持つインシデントが合計34,000以上あり、ほとんどそのすべてが組織犯罪グループと結びついています。これまでと同様、こうした攻撃の詳細な情報は限られているため、我々の分析から再び詳細情報を選択しました。攻撃者のインフラストラクチャについて、状況判断ができるようになったのは良かったですが、この調査における、これらのインシデントの有用性はそこまでです。

注目すべき領域

確かなユーザーエクスペリエンスを提供するために、Webサイトのインタラクティブな要素が強まり、より多機能化・複雑化するにつれ、基盤となるインフラストラクチャ、ロジック、およびこれらの資産の機能性と、そこに保存されているデータに、もっと焦点を当てる必要があります。

- Webアプリケーションまたはバックエンドのデータベースに保存する、個人情報やサイトの認証情報の量を、業務の実行に必要な最小限に制限し、暗号化で残りを保護します。
- Webアプリケーションに対し2要素認証を使用することにより、侵害するには、初期パスワードとは全く異なる攻撃パターンが必要になります。
- CMSとプラグインの一貫性が保てるようにパッチを適用し、不定期なパッチが利用可能になった際には通知されるようにします。
- SQLインジェクション（SQLi）はまだまだ健在です。Webアプリケーションのスキャンとテストを実行し、SQLiおよびその他の入力検証の潜在的な弱点を突き止めます。

その他すべて

9パターンのいずれにも分類できないインシデントです。

概要

被害が多かった業界
製造業、教育サービス業、公的機関（インシデント）
頻度
合計870件のインシデント、184件でデータの漏洩を確認
主な調査結果
DoSボットネット、ソーシャルエンジニアリング、およびネットワークフットプリントによる情報収集が、このパターンのインシデントの大半を構成しています。

必要な詳細はどこに...

「その他すべて」は包括的なパターンであり、特に、ある程度の情報はあるが、他の9パターンに当てはめるのに適切な情報が足りないというインシデントおよびデータ漏洩を分類するものです。詳細が全部、天から降ってくればよいのにと思いますが、とりあえずは、手元にあるものを利用するのが賢明です。そうすることで、何か役立つ情報を発見できます。図54の上から3つの棒グラフは明確に物語ってくれるタイプの攻撃です。

先頭の棒グラフは、真実味の低いフィッシングによるデータ漏洩を表しています。フィッシングが発生し、罠に引っかかりましたが、それ以外の被害はあまりありませんでした。大部分のフィッシングはマルウェアを伴うため、少なくとも、一部のフィッシングインシデントがその経路をたどったと推測できます。

2番目の棒グラフは、フットプリントのインシデントを表していますが、データはほとんどが同じ協力企業・組織から提供されたものです。ネットワークマッピングの前後に、どのような攻撃行為があったかはわかりません。知りたくてたまりませんが・・・

3番目の棒グラフは、最も興味深い、ビジネスメール詐欺（BEC）を表しています。これらのインシデントは通常、電信送金を指示する「CEO」からの電子メールによる連絡を伴います。もっともらしいシナリオを用意して、迅速な対応を求めるのです。

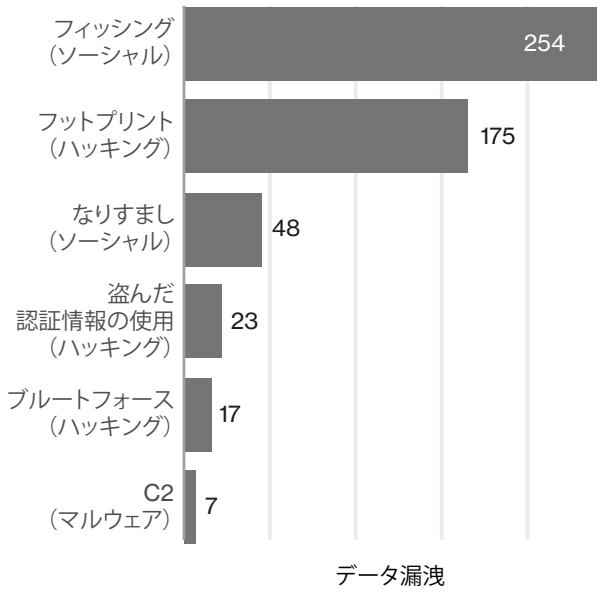


図54：「その他すべて」における上位の攻撃行為（N=529）

まとめ

では、第10回目となる今回の報告書をまとめましょう。10年は長い期間です。ブルックリン橋の建造に10年かかりました。ミケランジェロはシスティーナ礼拝堂天井画におよそ10年かけています。スタンダード版モノポリーゲームには、1ゲームを終わらせるのに平均10年が必要です。（いえ、そんなことはありませんが、そう感じることがあります）10年間には色々なことが起こり得ます。その間、1社（ベライゾン）単独で調査したデータ漏洩のみで構成され、主に金融業と小売業に的を絞った手短な報告書だったDBIRは、世界中に広がる70の企業・組織にご協力いただくまでに発展しました。この10年間に、我々の対象範囲は、世界中の企業・組織で発生している、サイバー関連のほとんどあらゆることを網羅するまでに広がりました。

この間、多くの新しい脅威が出現して進化を遂げました。可用性に対する攻撃から、発達したデータ漏洩に移行したハクティビズム、国および国の支援を受けたスパイ活動の蔓延、フィッシングの台頭と優勢性、DDoS攻撃、複雑かつ多様な形状になったマルウェアなど、リストはまだまだ続きます。

DBIRも同様に、業界や対抗しなければならない脅威とともに進化し、成熟しました。きわめて小規模で、単純な形で始まったDBIRですが、年月を重ねた結果、力強く大々的なものになりました。2010年度の報告書から、アメリカ合衆国シークレットサービスに情報提供組織として加わっていただいたことが契機となり、他の企業・組織も、それまでほとんど耳に届かなかったデータ漏洩関連の情報を抵抗なく共有してくださるようになりました。VERIS（Vocabulary for Event Recording and Incident Sharing）フレームワークの追加と改良、インシデント以外のデータを含めたことにより、データ漏洩に関する我々の見識が深まり、2014年の9パターンの発表と業界別のセクションを設けたことが相まって、各企業・組織が毎年登場する課題に対して備えることが可能になりました。

我々の目的は最初から、そして今でも、企業・組織が直面している脅威を理解し、証拠に基づいて、リスク管理の適切な判断を下せるように支援することです。改めて、読者の皆様とご協力いただいた企業・組織の皆様にお礼を申し上げます。この報告書を無事に発表できたのも、皆様のご支援があってこそです。今後も引き続き、知見と役立つ実用的な情報を提供できればと考えております。

> **私たちは「一緒の方が強い（Stronger Together）」**

最後になりましたが、我々がより強くあるためには個人が単独でいるより、協力し合うことが重要です。ですから、これからもぜひ、お客様の情報、ご意見、ご感想を共有していただきたく、お願い申し上げます。皆様のご支援のおかげで、10年間、綿密な分析を公開し、共有することができました。映画「スパイナルタップ」で偉大な賢者、ナイジェル・タフネルは「11は10より一段階でかい音だ」と雄弁に語ったように、DBIRも第11版は第10版より一段階上の報告書になればいいと思います。

付録

付録A：

進化を続ける国境を越えたサイバー犯罪の脅威に対抗するには

アメリカ合衆国シークレットサービス
副次長補
ロバート・ノービ

国境を越えたサイバー犯罪は過去20年間、着実に進化を遂げており、この脅威に戦略的に対抗するために、継続的な適応が求められています。1990年代後期から2000年代初期にかけて、この国際的サイバー犯罪活動を取りまとめるため、Boa Factory、Carder Planet、ShadowCrewなどのWebサイトが立ち上げられました。しかしこれらのWebサイトは、主に東欧に拠点をおき不法な金銭的利益を得るためサイバースペースを悪用するサイバー犯罪者たちの複雑なネットワーク網を可視化しているにすぎません。米国の金融および決済システムは、依然変わりはありませんが、この犯罪活動の多くでうってつけの標的となりました。理由は単純で、銀行強盗ウィリー・サットンが言ったと伝えられているように、「そこに金がある」からです。

> **そこに金があるからだ。**

シークレットサービスには、犯罪がつけ入らないように、金融/決済システムを守ってきた長い歴史があります。1865年、我々シークレットサービスは偽造通貨の横行という脅威に対処するために設立されました。金融決済システムが紙からプラスチック、さらに現在のデジタル情報へと進化したため、我々の調査任務も進化しました。現代の金融システムは、利便性と効率性を理由に、情報テクノロジーに大きく依存しています。それに応じて、犯罪者も手段を変え、不正やその他の非合法活動に携わることにより我が国の決済システムを悪用するため、ますますサイバースペースを利用するようになりました。

シークレットサービスのサイバー犯罪調査は、認知度が高い最大級のデータ漏洩に関与した数多くのサイバー犯罪者を逮捕し、見事に起訴にまで持ち込みました。この中には当初の国際的サイバー犯罪グループのリーダーが多数含まれています。

それにもかかわらず、初期のサイバー犯罪に加わった者の一部は複数年にわたる金融詐欺活動に従事しており、被害を受けた企業・組織とその顧客が被るコスト以外の損害は総額（何十億ではないにしても）何億にもなります。このような犯罪者たちは恐るべき犯罪事業の展開と、様々な不法サイバー活動を可能にする広範なサイバー犯罪サービスを提供する強力な地下組織の発展のため利益を再投資してきました。

しかし、最も重大なサイバー攻撃の実行者の一部は、概してこのような犯罪市場には加わりません。代わりに彼らはカルテルのような性質の組織を立ち上げ、密接な信頼関係で結ばれた集団を通じて、犯罪行為を取りまとめてきました。これらの犯罪組織は、技術的および財務的素養の両面で急成長を遂げており、ネットワークに不正にアクセスする新たな方法や、そのアクセスから利益を得る新たな方法を見出しています。

このような国際的な犯罪組織に対抗することがシークレットサービスの優先すべき重要事項になっています。米国の金融/決済システムの完全性を守ることが我々の仕事だからです。こうしたサイバー犯罪事業の知識、能力、金銭的誘因が高まったため、ネットワーク防御や従来の抑止対策が非常に不十分なものになっています。その代わり必要なのは、非合法活動に対抗し、その勢力を低下させ、封じ込める積極的な取り組みです。

このようなキャンペーンによって、こうした組織がもたらす祖国の重大なセキュリティリスクを軽減し、広範な攻撃者（国家組織から比較的知識の浅い犯罪者まで）による脅威の不正なサイバー攻撃能力を低下させる、絶好の機会が得られると確信しています。

こうした国際的なサイバー犯罪に対抗するキャンペーンには、さまざまな活動と目標が伴い、そのほとんどは、シークレットサービスが単独でなしえるものではありません。まず最初に、コンピュータネットワークへの不正アクセスや損害を防止することから、不正サイバー活動で利益を得る犯罪者の能力を最小限に抑え込むことに、現在の焦点をある程度、移行させる必要があります。シークレットサービスはこれを遂行するために、例えばLiberty ReserveとeGoldを業務停止に追い込んだケースでは、サイバー犯罪者が使うマネーロンダリングとデジタル通貨の調査から、進行中のネットワーク侵入について被害者に通知するなど、様々な手段を使用します。被害者に知らせる目的の1つは、被害者がネットワークのセキュリティを回復できるようにすることですが、それ以上に重要なのは、サイバー犯罪者がその活動から利益を得たり、被害者となった企業・組織に金銭的な損害を与えたりする可能性を最小限に抑えることです。

残念ながら、一部の企業はサイバーセキュリティインシデントの通知をすぐに受け入れることができず、自社、自社の顧客、パートナー、および他社を悪意のサイバー活動による経済的損失から守るためのアクションを開始するまでにあまりにも時間をかけすぎてしまいます。シークレットサービスでは、企業および企業のセキュリティ/法務/IT部門がサイバーセキュリティインシデントに迅速かつ責任を持って対応できるようにするため、専門弁護士、外部のサイバーインシデント対応およびフォレンジック組織、法執行機関を含めた、サイバーインシデント対応計画を作成して実施することを各企業・組織に促しています。

次に、我々は同一の利害を有する共同体として、脅威およびインシデントに関する情報共有をより有用にする必要があります。これには、侵害の指標（マルウェアハッシュ、YARAルールなど）を共有するだけではなく、法執行機関と共同で加害者を調査し、裁きを受けさせることも含まれます。さらに、特に損害の大きい脅威に対抗するために、より一般的なサイバーセキュリティインシデント情勢を共有し、サイバーセキュリティ対策の優先順位および法執行機関の取り組みを知らせることも必要です。

情報共有の目的をサイバーセキュリティに限定して考えないでください。むしろ、加害者の不正な利益と被害者の金銭的損害をどうやって最小限に抑えればよいか、広い視野で考えてください。

シークレットサービスは、我々の電子犯罪タスクフォースのネットワーク、民間企業および法執行機関との信頼できるパートナーシップを通じて、サイバー犯罪に関する重要情報を効果的に共有できるようになると同時に、個人の利益やきわめて機密性の高いおとり捜査、最も手ごわい国際サイバー犯罪組織に侵入した秘密情報提供者などの調査方法や情報源を保護できています。

シークレットサービスが「データ漏洩/侵害調査報告書」で初めてベライゾンと協力したのは、この情報共有が目的でした。この報告書のために多くの企業・組織がデータの提供してくださったことを光栄に思うとともに、さらに多くの企業・組織へも協力を呼び掛けてまいります。どのような企業・組織でも単独では、サイバーセキュリティのあらゆる脅威について、理解を深めることは不可能ですし、こうした脅威に効果的に対抗するにあたってはなおさらです。

“DBIRは重要なリソースに発展しました...”

DBIRは、サイバーセキュリティの脅威の性質を見極めるための重要なリソースへと発展し、これらの脅威に効果的に対抗する機会の特定のため我々は能力を結集するようになりました。シークレットサービスは今後も変わらず、サイバー犯罪の防止、発見、調査という目的のため、パートナーとなり得る企業・組織と協力し取り組んでいます。

付録B:

パッチプロセスの積み残し

今回のDBIRで、脆弱性の悪用が関係したデータ漏洩の割合は、わずか1桁でした。それを聞くと安心しますが、脆弱性スキャンまたは脆弱性に対応するパッチの適用の停止を容認しているということではありません。適切なパッチプロセスを適用することは、不可欠なセキュリティ対策です。しかし、何が「適切」であるか、どうやって定義すればよいのでしょう。どうすれば、どの程度適切であるか、判断できるのでしょうか。

図55は、パッチの進行状況を示しています。企業・組織の脆弱性スキャンに関する調査結果[29]が時間とともに、どの程度修正されたかを示しています。グリーンの線が標準的な組織[30]を表しているのに対して、オレンジの線は（その他、すべての条件が同じだとして）、同業の約4分の3より優れている組織を表しています。これらの例は、パッチが繰り返し適用されていることを示しています。

上の線では、発見された脆弱性に即座にパッチを適用し、1か月ごとのスキャンの前に再度適用しています。下の線では、1週間ごとおよび1か月ごとのスキャンの前にパッチを適用し、パッチが必要なあらゆるものに適用された状態です。実際には、組織ごとに大きく異なる曲線になります。即時にパッチプロセスを行う企業・組織もあれば、ゆっくり時間をかけて適用する企業・組織もあります。

各組織のパッチ適用は、2種類の数字で表すことができます。Area Under the Curve（AUC）およびCompleted On Time（COT）の割合です。AUCは、積極的にパッチを適用している場合、どの程度保護されているかを表します。発見された脆弱性の大半を迅速に処理すると、AUCが高くなります。COTは、調査完了時（図57では12週間）でパッチが適用された脆弱性の数です。昨年のDBIR[31]で示したとおり、パッチが迅速に適用されなかった脆弱性は、長期間パッチが適用されていない状態になりがちです。これを「積み残し」と言います。

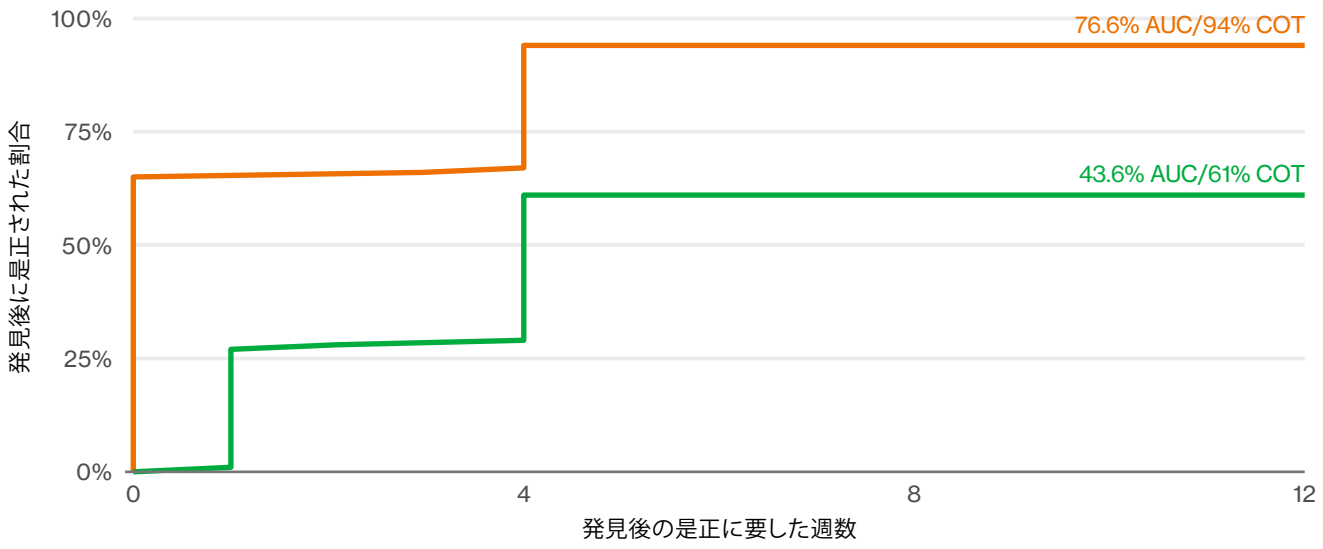


図55：組織のAUC（曲線下面積）の割合の比較

[29] このセクションの分析はすべて、情報（informational）の調査結果を取り除いてあるので、お客様の組織の状況に沿って調査結果を考える必要があります。「Telnetイネーブル」は、Web画像でデフォルトの認証情報を見つけるまでは参考情報です。

[30] 厳密には55%で、中央値のような50%ではありませんがご想像いただけるでしょう。

[31] 2016年度データ漏洩/侵害調査報告書の16ページ、最初の段落および図13

いつ完了したか

定時完了と言ったばかりですが、それは「いつ」のことでしょう。発見された脆弱性に積極的に対処する前の調査完了時に企業・組織でパッチプロセスを行う場合は、そのパッチサイクルのことです。約11万6千の脆弱性を分析した結果、これらの企業・組織のほとんどが12週間でパッチプロセスを完了していることが判明しました。これは、四半期ごとのパッチプロセスとも一致します。先に、「すべての条件が同じだとして」と言いましたが、そうではないことは承知の上です。お客様が取り組んでいるセキュリティホールとなり得る脆弱性において、プロセスを設定する必要があります。

すべての脆弱性が出回っている攻撃を受けるわけではありません。したがって、すべての脆弱性に当てはまる普遍的なパッチサイクルや「対処有効期限の指標」は実現不可能で、非効率です。最終的には、実行者が攻撃を開始する前に、脆弱性を修正すればよいわけです。実際に攻撃を受けた脆弱性には、短期間のパッチサイクルが与えられます。特定された重要資産の脆弱性も同様です。したがって、調査結果によっては、7日間が適正なパッチサイクルになることもあれば、四半期のパッチサイクルが「標準」になることもあります。言い換えると、AUCおよびCOTは、調査結果のサブセットごとに計算できます。

脆弱性がセキュリティーホールとなる可能性、ビジネスにおける資産の重要性、攻撃実行者が脆弱性を不正利用する可能性に基づいて、各サブセットに優先順位を設定できます。サンクスギビングで食べ残しがあっても良いのと同様、積み残しがあっても結構です。しかし、企業・組織にとって重要なのは、パッチが適用されていない脆弱性はどれか、リスクにどのように対応したのか、または容認が記録されているかを把握することです。このセクションの後半で、今年の脆弱性スキャンデータセット全体における積み残しの調査結果を分析します。

全体の数字に戻りましょう。出発点が必要であれば、全企業の半分は、AUCが51%を下回っており、COTは76%です。4分の1のトップ企業は、AUCが約80%、COTがほぼ100%です。図55では、上の線はAUCが76.6%で、これは12週間にわたる調査結果の約23%に対する、脆弱性の可能性を示しているだけで、このデータセットにおける誤判定については説明できません。下の線はAUCが大幅に下がり、43.6%です。これは、パッチサイクルの期間、調査結果の過半数に脆弱性があることを意味します。12週間の調査完了時点で、上の線はCOTが94%です。これは、調査結果の94%が修正済みであることを意味します。一方、下の線はCOTが61%で調査結果の約40%が積み残しです。

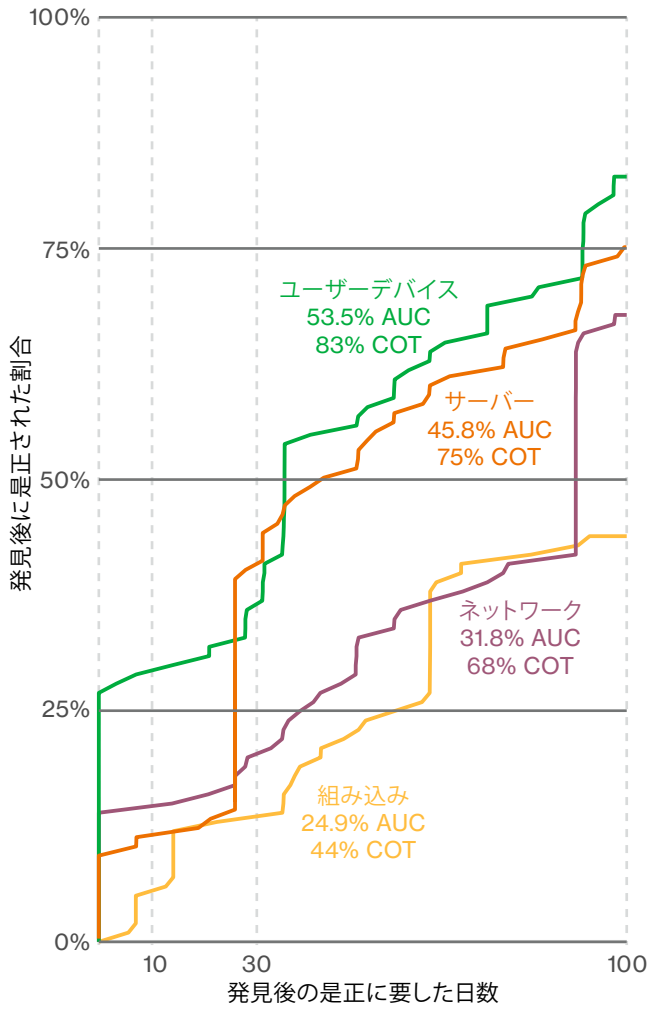


図56：資産タイプ別のパッチの比較

図56では、資産タイプに基づいて結果を分け、100日という調査完了期限を使用しています。このグラフは、サーバー（AUC46%、COT75%）、ネットワークデバイス（AUC32%、COT68%）、組み込みデバイス[32]（AUC25%、COT44%）に対して、ユーザーデバイスのAUCとCOT（それぞれ53%と83%）が高いということを示しています。ユーザーデバイスは迅速にパッチが適用され、さらに1か月後にも再び適用されていますが、サーバーへの対応は発見から約1か月後です。ネットワークデバイスにパッチが適用されたのは、四半期の終わりです。

[32] ほとんどがVOIPアダプターと環境モニターです。

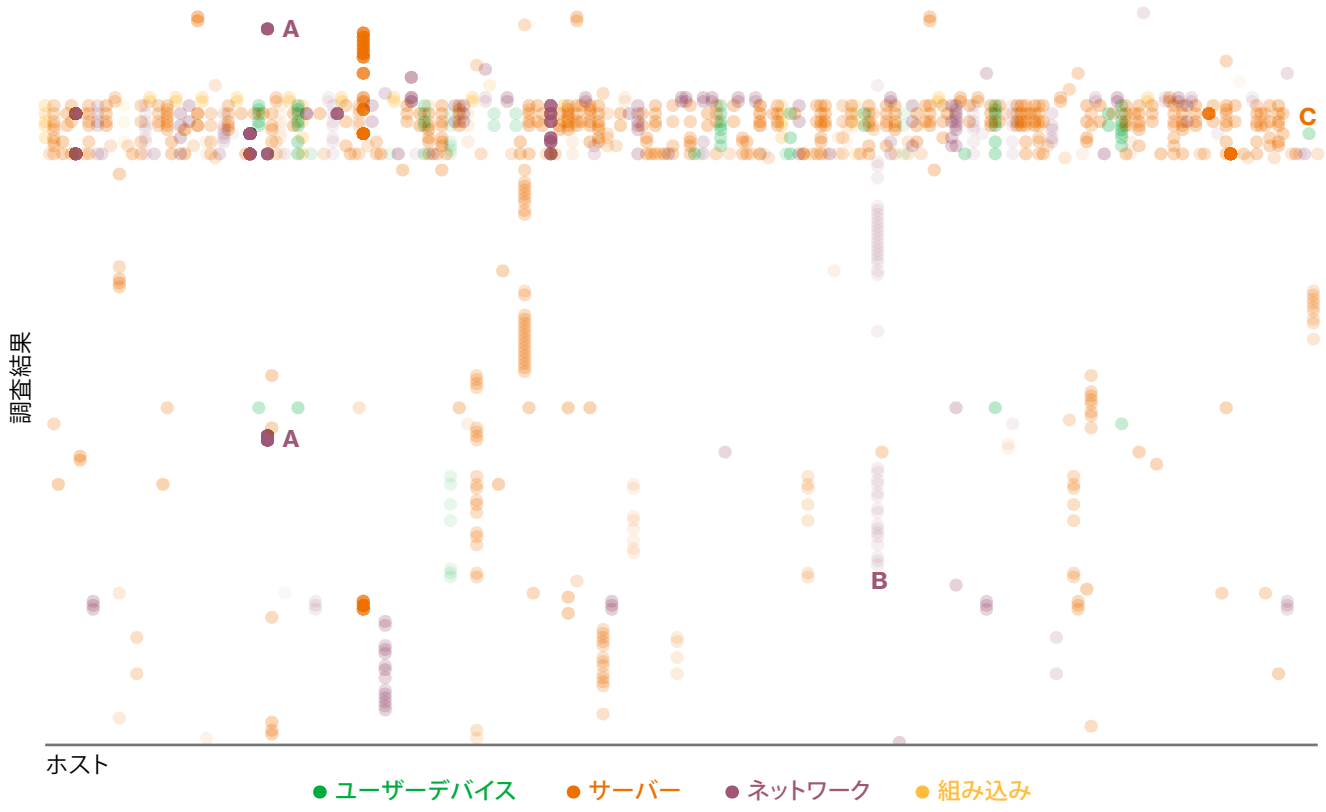


図57：積み残しの調査結果分析

積み残しの分析

では、未対応の調査結果は実際どうなっているのでしょうか。図57は、残りすなわち積み残しの調査結果のある種のパターンを示しています。各点は単一のホストにおけるそれぞれの結果です。点の色が濃いほど、その調査結果が繰り返し出現していることを示しています。

- **ベリーカラー**のドット**A**は、少数のネットワークデバイスで、単にパッチが適用されていないという調査結果が繰り返されていることを示します。

- 一方、**B**列は、単一デバイスに、1回または数回出現する脆弱性が多数あることを意味します。これは、他の資産では発見されていない脆弱性がなぜ発見されたのかを調査する、よい機会です。

- 最後に**C**は、複数のサーバーで繰り返し発見された、類似した一連の脆弱性を表します。この場合、SSLの脆弱性です。これらの調査結果は、誤判定のこともあれば、組織によって低リスクが確定している場合もあるので、連なったオレンジのドットの集合体でも問題ではない可能性があります。

重要なのは、お客様の環境でどの脆弱性が残って延々と続くかを理解し、その存在に驚かないことです。

最後に、このセクションでは、お客様が自己分析できるデータをいくつか用意していますが、それ以上に重要なのは、お客様の組織状況に沿って、AUC、COT、および積み残しの調査結果を理解することです。調査結果がリスクになり得る、組織にとっての脅威と影響を想定してください。さらに、最終的には、リスクを相互に関連付け、組織の攻撃対象領域[33]を把握してください。

[33] 攻撃対象領域の詳細については、2016年度ベライゾンデータ漏洩/侵害調査報告書の付録Dをご参照ください。

付録C：

1年を振り返って

1月

VTRAC（Verizon Threat Research Advisory Center）では、情報セキュリティリスクに影響を与える重大な出来事が満載の1年であったと、2016年を振り返っています。2016年はこの点で、DBIRが始まって以来、どの年より際立っています。2015年12月23日にウクライナを襲った停電は、同様の事件の皮切りとなり、関連インテリジェンスの展開が1月および第1四半期全体の優先課題になりました。確かに、過去の年月で経験したように、他のトレンドも進化しました。オーストリアに拠点を置く航空機メーカーのFACC AGは、ビジネスメール詐欺（BEC）攻撃を受け、5千万ユーロの被害を被りました。会社が攻撃を公表してからの数日間、時価総額にして約4,500万ユーロが失われました。ほぼ同じ頃、ベルギーの銀行、Crelanが7,800万ユーロのBEC詐欺に遭ったと公表しました。

2月

2月には次のとおり、4つの重大な出来事がありました。十数を超えるセキュリティ関連企業と対策チームの共同作業によって、2014年11月のソニー・ピクチャー・エンターテイメント（SPE）に対するサーバー攻撃の詳細を伝える報告書、Operation Blockbusterが作成されました。我々は、バングラデシュ中央銀行の8千万米ドルに及ぶ侵害について、新しい報告書の収集を開始しました。攻撃者はソーシャルエンジニアリングとマルウェアを使用して、SWIFTシステムを悪用しました。あとになって、攻撃の実行者は、SPEとバングラデシュ銀行の両方を手掛けたらしいということが分かりました。カペルスキーが中心になって、Equation Group（ほとんどのアナリストがアメリカ合衆国の国家安全保障局に関係しているのではないかと憶測する、サイバースパイ活動の攻撃実行者）に関する報告書が作成されました。医療機関に対するランサムウェア攻撃がその次の重大事件であり、トレンドでした。ランサムウェアが原因で、Hollywood Presbyterian Medical Centerは院内緊急事態を宣言しました。その後、交渉に成功し、身代金は350万ドルから1万7千ドルに引き下げられました。

3月

医療機関へのランサムウェアは、3月も続き、ワシントンDC地域のMedStarネットワークに加盟している、10の病院と250の外来センターが攻撃されました。ケンタッキー州ヘンダーソンのMethodist Hospitalは、Lockyというランサムウェアの攻撃を受けました。Samsamランサムウェアは、カリフォルニアのビクタービルにあるChino Valley Medical CenterとDesert Valley Hospitalの2施設を攻撃しました。全米展開の21st Century Oncologyは、データ漏洩が発生し、220万人分の患者記録が流出したことを報告しました。米国では確定申告の期限が近づいており、サイバー犯罪者はW-2損益計算書の書式を狙って、BECの亜種を組み込みました。Cloudmarkによると、この年、4月を含めた4か月間に68社がW-2フィッシングによるデータ漏洩を経験しました。ニューヨークタイムス、BBC、AOL、MSNを含めた一流のWebサイトで、Anglerエクスプロイトキットを使用したマルバタイジングにより、Teslacryptというランサムウェアにビジターがさらされました。

4月

法律事務所、Mossack Fonsecaから1,100万を超える文書の盗難、または漏洩を手始めに、4件の重大事件が4月を特徴付けました。エドワード・スノーデンによる漏洩よりも規模は小さいものの、「パナマ文書」は世界中の事業と国際関係に影響を与えました。次に発生した事件は、GozNymマルウェアキャンペーンによる米国とカナダの22の銀行が攻撃されたことで、被害は400万ドルに達しました。4月には、オランダの主要なすべてのWebサイトがマルバタイジング攻撃の被害を受けています。フィリピン共和国の人口の約半分は、選挙管理委員会におけるデータ漏洩の被害者です。

5月
5月の重大事件は、サイバースパイ活動の攻撃実行者による、2016年最初の大規模な活動でした。Turlaグループは2008年から活動しています。5月、スイスの防衛関連企業、RUAGを狙った、20か月にわたるTurla作戦がスイスのCERTによって報告されました。BAE Systemsはバングラデシュ銀行詐欺で使用されたマルウェアを分析し、Lazarusという攻撃実行者と結びつけました。ベトナムのTien Phong Joint Stock BankとエクアドルのBanco del Austroが2月のバングラデシュ銀行に対する攻撃とよく似た、SWIFTシステムの悪用を阻止したことが判明しました。

6月
6月に、ロシアの警察がLurkグループの55名を逮捕したことは、この年最大の偉功です。この逮捕によって、AnglerおよびNuclearエクスプロイトキットが無力化されました。ウクライナの銀行がSWIFT詐欺によって1千万ドルの損害を被りました。6月15日、CrowdStrikeが『Bears in the Midst: Intrusion into the Democratic National Committee（Bears in the Midst：民主党全国委員会に侵入）を発表しました。米国では、これより2016年の末までずっと、情報セキュリティと地政学は切り離すことができなくなりました。

7月
休暇を取るなら7月が最適だと、先にわかっていればと思いますが、後の祭りです。恒例となった、OracleとJavaScriptの重大なパッチのアップデートがセキュリティに関する最も重要な発表でした。マルウェア市場の新顔は、PetyaおよびMischaという、サービスとしてのランサムウェアの形（Ransomware-as-a-service）で始まりました。この年の始めに起きた、SWIFTネットワークを不正使用する攻撃は、サットンの法則を極限まで実証しました。7月には、そのテーマのバリエーションによって、インドのUnion Bankが米ドル当方勘定への攻撃を阻止しました。

8月
8月1日、攻撃実行者「Peace」が2億件のYahooアカウントログイン情報を「The Real Deal」というサイバー犯罪市場に持ち込みました。悪党たちは、ビットコイン取引所のBitfinexから、約12万のビットコインを盗み取りました。当時の金額で約6,500万ドル相当です。「Shadow Brokers」がNSAのEquation Groupから盗み出したか、または漏洩した250MBのファイルを売りさばくキャンペーンを開始しました。Anunakという攻撃実行者がOracle MICROS POSシステムのカスタマーサポートポータルを侵害しました。世界第4位の規模のワイヤー/電線メーカー、Leoni AGがBEC詐欺で4千万ユーロを失いました。オーストラリアのブリスベンがBEC詐欺で、45万オーストラリアドルの損害を被りました。

9月
9月、Yahooは2014年から始まった5億件のアカウントのデータ漏洩を公表しました。その3か月後、Yahooは2013年に始まった別のデータ漏洩で10億件のアカウントが侵害されていたことを発表しました。9月20日、セキュリティ専門のジャーナリスト、ブライアン・クレブスのWebサイトが600 Gbpsを超えるDDoS攻撃を受けました。その2日後には、フランスのホスティング会社、OVHが1 Tb GbpsのDDoS攻撃の標的だったことを報告しました。あとでわかったことですが、これらのDDoS攻撃はどちらも、IoTデバイスに感染させたMiraiワームを使用して遂行されました。

10月/11月
北半球では、秋の重大事件に「IoT（モノのインターネット）」に押し寄せるDDoSマルウェア攻撃がありました。中でも、影響が広範囲に及んだDoS攻撃は、10月21日のホステッドDNSプロバイダー、DYNに対するものと、11月27日のDeutsche Telekomに対するものの2件です。Palo Alto Networksが『SilverTerrier』報告書を公開し、ナイジェリアのサイバー犯罪における次なる進化と特徴づけました。Palo Altoでは、8千を超えるマルウェアサンプルを分析し、100ほどの攻撃実行者が毎月5千～8千件のBECおよび「419詐欺」の攻撃を開始するために不正使用している、500以上のドメインを特定しました。

12月
モスクワを拠点とするセキュリティ会社、Group-IBがプレスリリースを公開しました。「Cobalt」攻撃実行者が銀行にATMジャックポットマルウェアを感染させていると主張しています。しかし、Positive Technologiesによる12月の報告書が出るまで、Cobalt ATM攻撃の技術詳細は不明でした。最悪のサイバー犯罪グループの1つ、AnunakがCobaltギャングのATMジャックポット攻撃に関係しているのはほぼ確実です。TrustwaveによるとAnunakは医療機関を狙っていました。VTRAC（Verizon Threat Research Advisory Center）は今も、Anunak、Buhtrap、およびCobalt間の関係を明らかにしようと取り組んでいます。2016年最大の朗報は12月に入って届きました。5名の逮捕と39のインフラストラクチャサーバーの差し押さえにより、Avalancheサイバー犯罪行動を壊滅させたことです。

付録D：

メソドロジー

本報告書に関するご意見やご提案の中で、読者の方々に本報告書を高く評価していただいている点の1つに、データの収集、分析、提示における高い厳密さと整合性があります。読者の方々がそのような点に注意を払い、厳しい目で本報告書の情報を読んでくださっていると知ることは、ベライゾンが公正さを維持する大きな力となります。メソドロジーについて詳細に説明することも、その公正さの重要な一部です。

本報告書のメソドロジーは全体として、これまでの報告書と同じで、大きな違いはありません。本報告書に含まれているすべてのインシデントは、単一の匿名化された総合データセットを作成する為個別に確認され、（必要に応じて）VERIS（Vocabulary for Event Recording and Incident Sharing）フレームワークに変換されました。VERISフレームワークはVocabulary for Event Recording and Incident Sharingの略語であり、無料でご利用いただけます。VERISリソースのリンクは本報告書の冒頭にあります。

収集方法や変換方法は、協力企業・組織によって異なります。全般に、次の3種類の基本的な方法が使用されました（詳細については後述します）。

1. VERISを使用しベライゾンによって行われた、有料の外部フォレンジック調査および関連情報収集活動を直接記録

2. 協力企業・組織がVERISを使用して直接記録

3. 協力企業・組織の既存の方式をVERISに変換

すべての協力企業・組織に対して、関係する組織または個人を特定できるような情報があれば、すべて削除するようにお願いしました。

インシデントの適格性

インシデント/データ漏洩報告書へのエントリの適格性を確保するには、2つの要件を満たす必要があります。エントリは、機密性、完全性、または可用性の損失として定義された、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」の基本的な定義を満たす以外に、エントリの質がチェックされます。ベライゾンでは、クオリティフィルターを通過するインシデントのサブセットを作成しています（サブセットの詳細については後述します）。「質の高い」インシデントの詳細は、次のとおりです。

- インシデントは、34の分野にわたって7つ以上の分類（攻撃実行者の種類、攻撃行為のカテゴリー、完全性損失の種類など）を備えるか、またはDDoS攻撃である必要があります。確認済みのデータ漏洩は例外で、分類が7つ未満でもかまいません。

- インシデントは、既知のVERIS攻撃行為カテゴリー（ハッキング、マルウェアなど）を1つ以上備えている必要があります。

インシデントは、クオリティフィルターを通過するために必要な詳細度を備える以外に、分析の期間内に収まることが必要です。2016年に取り扱った件数は、基本的な分析が報告書のフォーカスですが、特にトレンドの数字では、データ範囲全体がくまなく参照されています。組織属性の損失に結び付けることのできない、個人に影響を与えるインシデント/データ漏洩も除外しています。たとえば、友人のノートパソコンがCryptoLockerの被害に遭っても、この報告書には含まれません。

最後に、ある事案がDBIRに含める資格があると判断するためには、我々はその事案について知る必要があります。そこで必要となるのがサンプルの偏りに対する理解です。

サンプルの偏りに関する認識

この報告書の知見にすべての組織のすべてのデータ漏洩を表していると主張するつもりは一切ないということを重ねて申し上げます。すべての協力企業・組織からのデータを組み合わせることによって、単独のデータよりも正確に現実が反映されているとはいえ、あくまでもサンプルです。また、この報告書の知見の多くは、一般化に関して適切だと考えており、収集するデータが増え、それを他社のデータと比較するにつれ、その自信はますます強くなっていますが、偏りは間違いなく存在します。残念ながら、偏りがどの程度存在するか（すなわち、明確な誤差の範囲を確保するために）を厳密に測定することはできません。2016年にすべての組織で発生したデータ漏洩の総数を知る手立てがないため、すべてのデータ漏洩の何割がこの報告書に反映されているか、知る術はありません。多くのデータ漏洩は報告されないままです（ただし、我々のサンプルには、その多くが含まれています）。さらに多くは、被害者によって確認されていません（そのため、我々も確認できていません）。

この報告書で提示された知見の多くが適切で、一般化されていると確信していますが、偏りやメソドロジー上の欠陥は間違いなく存在します。しかしながら、65の協力企業・組織を得た本年度の報告書では、協力企業・組織のさまざまなデータ収集方法、優先度、目標が集約されています。このようにデータを集約することで、個々のサンプルで不足していた部分の影響を最小化し、この調査報告書全体がより価値のあるものになることを願っています。

統計分析

我々は、DBIRで統計上の正しさを確保しようと努力を重ねています。今年のデータサンプルにおいて、信頼区間はデータ漏洩で±1.4%、インシデントで±0.4%です[34]。データのサブセット（スパイ活動パターンにおけるデータ漏洩など）は、サンプルサイズが小さいため、信頼区間はむしろ拡大されます。我々は、あらゆる考察を仮説として扱うように心がけ（データを見たあと出てきたものは、仕方ありませんが）、個々の考察が所定の信頼水準（通常は95%）において正確であるかを確認しています。

我々のデータは包括的な多項性を備えています。たとえば、「アクション」のような単一特性に複数の値（「ソーシャル」「マルウェア」「ハッキング」）を与えることができます。したがって、パーセンテージの合計は必ずしも100%になりません。たとえば、5件のボットネットによるデータ漏洩があった場合、サンプルサイズは5です。しかし、各ボットネットでフィッシングを使用し、キーロガーのインストール後、盗んだ認証情報を使用したため、5件のソーシャルアクション、5件のハッキングアクション、5件のマルウェアアクションが生じ、合計300%になります。我々の分析と行程において、これは正常かつ予期されるものであり、正しく処理されます。

もう1つ、調査結果を見るときに重要なのは、「不明」は「測定不能」と同じだということです。たとえば、データまたはデータの集合体に「不明」と指定された要素が含まれている場合、それがインシデントに関係したデータ数のように基本的なものであるか、マルウェアに含まれていた具体的な機能のように複雑なものであるかに関係なく、そのままのデータでは、その要素について考察することはできません。また、情報が少なすぎる場合は、測定できません。「測定不能」であるため、サンプルサイズではカウントされません。しかし、「その他」という分類は、値が既知だということなので、カウントされますが、VERISには含まれません。最後に「該当しない」（通常は「NA」）は、仮説によって、カウントされる場合とされない場合があります。

[34] ウィルソン法、95%の信頼水準。

データのサブセット

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すでに述べましたが、分析の一部としてデータのサブセットを定義する事例がほかにもあります。このようなサブセットは、小規模なトレンドが残っていたとしても、それを上回る正当なインシデントで構成されます。これらは取り除かれて個別に分析されます（関連するセクションの付記を参照）。今年、全体を通じて個別に分析した唯一のサブセットは、二次的ターゲット（マルウェアを拡散するためにWebサイトを占拠するなど）として確認されたWebサーバーで構成されていました。

最後に、我々は今後の分析に役立ちそうなサブセットをいくつか作成しました。今年は、データに対するボットネットの影響を分析する際に役立つボットネットのサブセットを作成しました。昨年と同様、コア分析用にこのデータのサブセットを残し、一部の図では取り除いて、他の結果が出現するようにしました。その場合は、図の見出し、注釈、またはその両方でその旨を示しています。

インシデント以外のデータ

2016年度のDBIRには、「インシデント」または「データ漏洩」という、ベライゾンの通常のカテゴリーに当てはまらないデータの分析を必要としたセクションがあります。インシデント以外のデータの例には、マルウェア、パッチ適用、フィッシング、DDoS、その他のタイプがあります。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はるかに大きくなる傾向がありますが、ソースの数は少なくなります。我々はデータの標準化に向けて、あらゆる努力をしています。たとえば、すべてのデータの平均ではなく、中央値に位置する企業・組織に関して報告することなどです。また、可能な限り、データが類似している複数の協力企業・組織を組み合わせて分析することを試みました。分析の完了後は、関係した協力企業・組織（複数可）と調査結果について話し合い、データに関するそれぞれの知識に基づいて検証しました。

付録E:

ご協力いただいた企業・組織


INTERSET
The Science of Threat Detection


wombat
security technologies


CROWDSTRIKE


MWR
INFOSECURITY


WINSTON & STRAWN


RAPID7


LIFARS
your digital world, secured


Pavan Duggal Associates
Advocates


SOCIAL ENGINEER


US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM


sparkcognition


JUNIPER
NETWORKS


DFDR
CONSULTING


GRA QUANTUM


panaseer


Skycure
Mobile Threat Defense


QUALYS


AsTech
SECURITY. GUAF


tripwire


DELL


CHUBB


GDT
GRUPO DE DELITOS TELEMÁTICOS


KRYPTOS LOGIC


CYLANCE


NetDiligence


LARES


KASPERSKY lab


JPCERT CC


BeyondTrust
VISIBILITY. KNOWLEDGE. ACTION.


VESTIGE
Digital Investigations


V
C
D
B


mnemonic
- securing your business

ご協力いただいた企業・組織

Akamai Technologies
Arbor Networks
AsTech Consulting
BeyondTrust
インターネットセキュリティセンター
CERTインサイダー脅威センター
チャプレイン大学のパトリック・リーヒ上院議員
デジタル調査センター
Check Point Software Technologies LTD
Chubb
Cisco Security Services
ルクセンブルクコンピュータインシデント対策センター（CIRCL）
CrowdStrike
グァルディアシビル内サイバー犯罪中央ユニット（スペイン）
サイバーセキュリティマレーシア、マレーシア化学・技術・
イノベーション省（MOSTI）内の部門
Cylance
Deloitte
DFDR Forensics
Digital Edge
DSS
EMC重大インシデント対策センター
Fortinet
GRA Quantum
産業制御システム・サイバー緊急事態対応チーム（ICS-CERT）
Interset
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）
ICSAラボ
一般社団法人JPCERTコーディネーションセンター（JPCERT）※
Juniper Networks
Kaspersky Lab
KnowBe4
Kryptos Logic
Lares Consulting
LIFARS
McAfee
Mishcon de Reya
mnemonic
MWR InfoSecurity
米国サイバーセキュリティ・通信統合センター（NCCIC）
NetDiligence
Palo Alto Networks
Panaseer
Pavan Duggal Associates
Pwnie Express
Qualys
Rapid7
S21sec
Skycure
Social-Engineer, Inc.
Spark Cognition
SwissCom
Tripwire
アメリカ合衆国シークレットサービス
米国コンピューター緊急事態対策チーム（US - CERT）
Veracode
VERISコミュニティデータベース
ベライゾンデジタルメディアサービス
ベライゾンDoS防御
ベライゾン不正チーム
ベライゾンネットワーク運用およびエンジニアリング
ベライゾンエンタープライズサービス
Verizon Threat Research Advisory Center（VTRAC）
Vestige Ltd
WhiteHat Security
Winston & Stawn, LLP
Wombat Security Technologies

※ 2017年度版データ漏洩/侵害調査報告書（DBIR）では、一般社団法人JPCERTコーディネーションセンター（略称：JPCERT/CC）が発行する「インシデント報告対応四半期レポート」よりデータ提供のご協力を賜りました。感謝申し上げます。

VerizonEnterprise.com