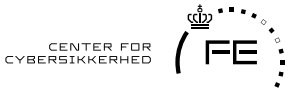
2016年度
データ漏洩/侵害
調査報告書

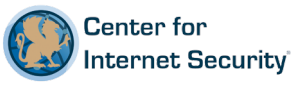
データ漏洩の89%が
金銭またはスパイ目的です

verizon

2016年度データ漏洩/侵害調査報告書（DBIR）にご協力いただいた企業および組織

（詳細なリストについては、付録Bを参照）






JPCERT CC®


swisscom


tenable
network security


FORTINET


splunk>


INTERSET
THE SCIENCE OF THREAT DETECTION


computer emergency response team
CERT-EU
for the EU institutions, bodies and agencies


CROWDSTRIKE


ASTECH
consulting


CyberSecurity
MALAYSIA
An agency under MOSTI


Homeland
Security


ICSA labs
An Independent Division of Verizon


S21sec
Committed to security


NetDiligence®


NIDDEL™


SANS
SECURING THE HUMAN


WINSTON
&STRAWN
LLP


US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM


JUNIPER
NETWORKS


GRA QUANTUM


LAW & FORENSICS


Recorded Future


tripwire


EUROPEAN CYBERCRIME CENTRE
EC3
EUROPOL


MWR
InfoSecurity


BeyondTrust™
VISIBILITY. KNOWLEDGE. ACTION.


CYLANCE


EMC²


CHUBB


.VESTIGE
DIGITAL INVESTIGATIONS

目次

2016年度DBIR―はじめに

「まるでデジャブの繰り返しだ」
―ヨギ・ベラ

今年の報告書をお届けする時期となりました。皆様とともに、昨年世界を悩ませたデータ漏洩と情報セキュリティインシデントの数々を振り返ってまいります。本報告書の発行もおかげさまで9回目を迎えました[1]。グラフだらけだった初版以来お付き合い頂いている方から今回が初めての方まで、貴重なお時間を割いて本書をご覧くださっているすべての皆様に心より御礼を申し上げます。

本題に入る前に、本書のためにデータとお時間を提供してくださった企業・組織の皆様に感謝の意を表したいと思います。簡単な言葉で恐縮ですが、ご協力いただき誠にありがとうございました。ご協力いただいた企業・組織の一覧は付録Bに掲載しております。

本書の中心となるのは、数々のインシデントデータです。「データ漏洩の動向」セクションと「インシデント分類パターン」セクションの説明も、インシデントデータを中心に展開されます。同時に、独自研究や攻撃パターンの全体像を描き出すために、インシデント以外のセキュリティデータも用いられています。幅広い企業・組織から提供された個々のデータを特定の研究テーマにまとめる試みがなされました。全体を1つのまとまりとしてとらえる、まさにゲシュタルト法則の実践です。

2014年度のDBIRでご紹介した9つのインシデント分類パターンは今年も健在です。特別に大きな動きはなかったものの、個々のパターンの内容には多少の興味深い変化が見られました。

今回は、実際にデータ漏洩が確認された3,141件を含む10万件以上のインシデントが調査対象となりました。本書の分析やグラフではその中から6万4,199件のインシデントと2,260件のデータ漏洩を厳選して使用しています。データを間引いた理由は、「被害にあった企業・組織の業界別および規模別の分析」セクションで簡単に、さらに「データ漏洩の動向」セクションの「二次的動機」コラムで詳細にご説明しています。もちろん、2015年に発生したセキュリティイベントが1つ残らず調査対象になっているわけではありません。サンプルには偏りがあることをご了承ください。本書の分析手法とデータリソースへのリンクを付録Eに記載しております。皆様の企業・組織内でインシデントを収集および分析する際にお役立てください。

2014年度のDBIRでご紹介した9つのインシデント分類パターンは今年も健在です。

1　9回も？はい、9回です。

本書で分析対象に含まれていないデータについてもお伝えしておきます。「今年はついにモバイル攻撃が我々を屈服させ、モノのインターネット（IoT）が我々を滅ぼそうと動き始めた」という宣言を期待していた方々は、がっかりするかもしれません。これらのテクノロジーについては、企業・組織への攻撃経路として分析するのに十分な実データがまだ集まっていません[2]。「自分はこれだけひどい目に遭ったのにそんなはずはない」と思われる方は、どうか心を落ち着けて、お持ちのデータをご提供ください。私たちは常に、暗い領域を照らし出す灯火を探し求めているのです。もちろん、これらのテクノロジーに関する情報がないからといって、リスク管理を考えるうえでこれらを無視してよいわけではありません。

本書は、プログレッシブロックのコンセプトアルバムのように、始めから終わりまで全体を通してお読み頂いても結構ですし、いくつかのセクションを読み飛ばしていただく事も可能なように作られています。「データ漏洩の動向」セクションに満載されている色とりどりのグラフをご参照いただくのも良いですし、「注目点」セクションで、複数のパターンに共通するいくつかのコンセプトについてご理解いただくのもよろしいかもしれません。また、興味深い情報をさらにご覧になりたい方のために、付録として「ベージュブック風」セクションをご用意しております。

2 もちろん、我々もxCodeハックのことは把握しています。しかし、データの損失が確認された企業・組織がない限り、本書の対象にはならないのです。

被害にあった企業・組織の業界別および規模別の分析

情報セキュリティの専門家を忙殺し、本書に材料を提供し続けるインシデントとデータ漏洩の陰に誰が潜んでいるのかは気になるところですが、敵の正体を暴く前に、攻撃を受ける側である被害者の概要を見ていきましょう。
2016年度のDBIRでは、82カ国にわたる幅広い業界の企業・組織が調査対象になっています。

データ漏洩/侵害の標的には、国も業界も組織も関係ありません。

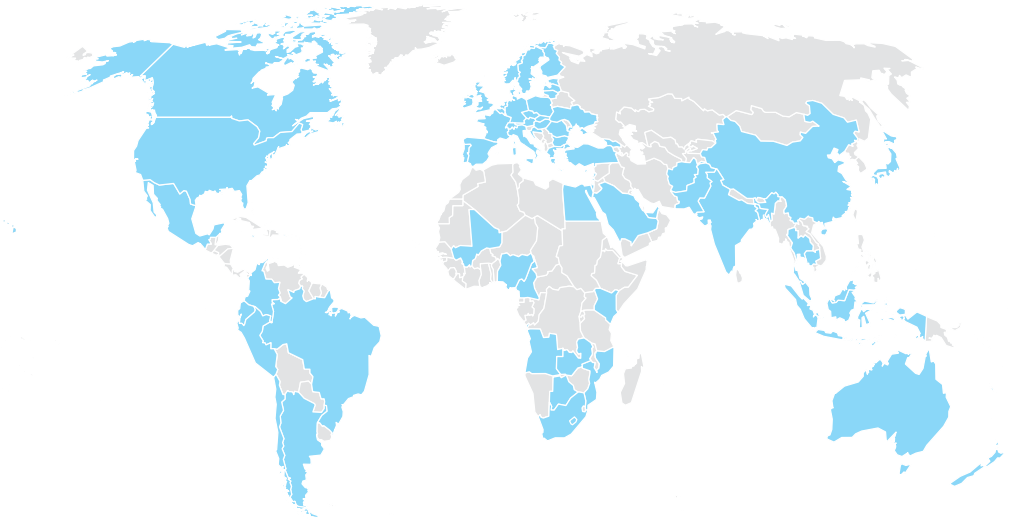


図1.
調査対象国

データ漏洩/侵害の標的には、国も業界も組織も関係ありません。いくつかの目立った偏りを鵜呑みにしないでください。たとえば公的機関が他の業界よりも危険なわけではありません。米国の政府機関には軽微なインシデントでも報告義務があり、これまでと同様、そのことが公的機関のインシデント件数を大きく押し上げているのです。表1と表2は、業界および規模別のインシデント件数とデータ漏洩件数を示します。表1と表2における合計件数が、先ほど調査対象と申し上げたインシデント数10万件とデータ漏洩件数3,141件よりも少ないことにお気づきかもしれません。これは計算ミスではなく、当初の調査対象にいくつかのフィルタをかけて対象を絞り込んでいるためです。攻撃を受けたデバイスが別の攻撃の踏み台として悪用されるインシデントは除外されています（「データ漏洩の動向」セクションの「二次的動機」コラムを参照）。また、詳細情報が不足しているため除外されたインシデントも数多くありました[3]。

3　完全性と複雑性の評価については、付録E「分析手法とVERISリソース」を参照してください。

データ漏洩を伴ったインシデントだけに注目すれば、桁外れに大きな数字はありませんが、ホテル業や小売業などの場合、インシデント件数に占めるデータ漏洩の割合は高くなっています。金銭目的の犯罪者にとってこれらの業界が取り扱う情報は非常に価値が高いことを考えれば、驚くことではありません。

業界	合計	中小規模の企業・組織	大規模の企業・組織	不明
ホテル業（72）	362	140	79	143
管理サービス業（56）	44	6	3	35
農業（11）	4	1	0	3
建設業（23）	9	0	4	5
教育サービス業（61）	254	16	29	209
芸術/娯楽業（71）	2,707	18	1	2,688
金融業（52）	1,368	29	131	1,208
医療業（62）	166	21	25	120
情報産業（51）	1,028	18	38	972
マネジメントサービス（55）	1	0	1	0
製造業（31–33）	171	7	61	103
鉱業（21）	11	1	7	3
その他のサービス業（81）	17	5	3	9
専門サービス業（54）	916	24	9	883
公的機関（92）	47,237	6	46,973	258
不動産業（53）	11	3	4	4
小売業（44–45）	159	102	20	37
貿易/通商業（42）	15	3	7	5
運輸業（48–49）	31	1	6	24
公益事業（22）	24	0	3	21
不明	9,453	113	1	9,339
合計	64,199	521	47,408	16,270

表1.

被害にあった企業・組織の業界別および規模別のセキュリティインシデント件数

業界	合計	中小規模の企業・組織	大規模の企業・組織	不明
ホテル業（72）	282	136	10	136
管理サービス業（56）	18	6	2	10
農業（11）	1	0	0	1
建設業（23）	4	0	1	3
教育サービス業（61）	29	3	8	18
芸術/娯楽業（71）	38	18	1	19
金融業（52）	795	14	94	687
医療業（62）	115	18	20	77
情報産業（51）	194	12	12	170
マネジメントサービス（55）	0	0	0	0
製造業（31–33）	37	5	11	21
鉱業（21）	7	0	6	1
その他のサービス業（81）	11	5	2	4
専門サービス業（54）	53	10	4	39
公的機関（92）	193	4	122	67
不動産業（53）	5	3	0	2
小売業（44–45）	137	96	12	29
貿易/通商業（42）	4	2	2	0
運輸業（48–49）	15	1	3	11
公益事業（22）	7	0	0	7
不明	270	109	0	161
合計	2,260	447	312	1501

表2.

被害にあった企業・組織の業界別および規模別の確認済みデータ漏洩/侵害件数

中小規模 = 従業員数1,000人未満の企業・組織、大規模 = 従業員数1,001人以上の企業・組織

インシデントとデータ漏洩の違い
この報告書では、次の定義を使用しています。

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：結果的に関係者外へのデータの暴露（単なる流出可能性ではなく）が確認されたインシデント

データ漏洩の動向

準備を怠らないように。「転ばぬ先の杖」は大切です。

情報セキュリティで防御側に立つことは、不運な兵士の運命に少し似ています。その兵士はある丘を死守するように命じられます。しかし、敵が誰でどのような姿をしているかも、いつどこからどのように攻めてくるのかも教えられていません。さらに不利なことに、渡された武器は古いライフル銃1丁と数発の銃弾だけです。これではあまりにも不公平です。アメリカ独立戦争ではポール・リビアが伝令として活躍してくれましたが、そのようなこともないのです。

皆様がこのセクションをお読みになることで、十分な防御態勢を整える助けとなり、不運な兵士の運命を避けられることを願っています。「転ばぬ先の杖」は大切です。

VERIS入門

本書の多くのセクションでは、VERIS（Vocabulary for Event Recording and Incident Sharing）の情報を参照しています。VERISは、セキュリティイベント、インシデント、データ漏洩を再現可能な形で記録および共有するためのフレームワークです。協力者には、どのような攻撃者（Actor）が、どのような手口（Action）で、どの資産（Asset）を標的に、どのような属性（Attribute）を侵害したかという質問に回答していただきます。これらの情報はまとめて「4A」と呼ばれます。4Aに加えて、タイムライン、被害者統計、発見方法、被害データなども尋ねます。

VERISに対応したツールは数多くあります。データの作成、読み込み、分析方法はすべて無料で公開されています。詳しくは、付録E「分析手法とVERISリソース」を参照してください。

過去にDBIRをお読みになったことがある方は、図2の結果に驚くことはないでしょう。これまでと同様、データ漏洩の犯人は部外者が大多数を占めています。データ暴露と聞くと、一般には内部者の犯行というイメージが強いかもしれませんが、実際は違います。どんなに大きな家でも、中にいる人間よりも外にいる人間の方がずっと多いのです。

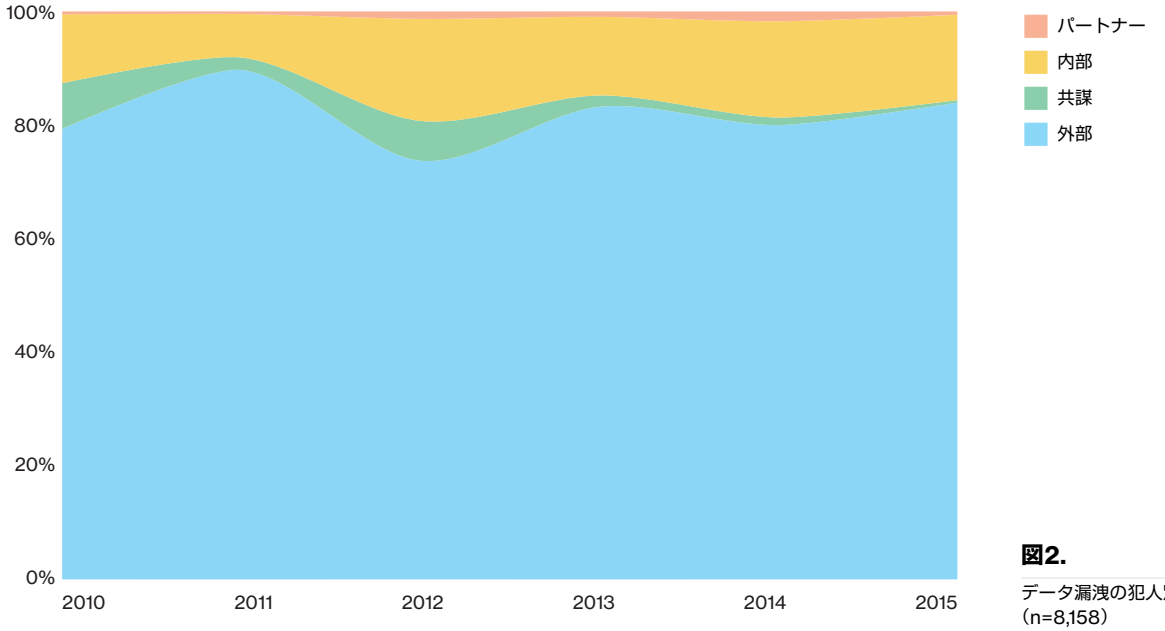


図2.
データ漏洩の犯人別割合とその推移
(n=8,158)

攻撃してくる理由は？
敵の目的は？金銭、盗んだ金、現金、悪銭、拝金…もうおわかりでしょうか。直接的ではなくとも最終的には「金」に行き着くのです（「二次的動機」コラムを参照）。2013年度のDBIRでは、「金銭目的」の王座が「スパイ目的」に奪われることが予測されました。それは実現したのでしょうか。いいえ、現実とはならなかったのです。スパイ目的の件数が最大となった時でもその差はあまりに大きく、金銭目的の独占的地位は揺るぎませんでした。図3に示すとおり、金銭目的はスパイ目的や愉快犯など他の動機をはるかにしのいでいます。

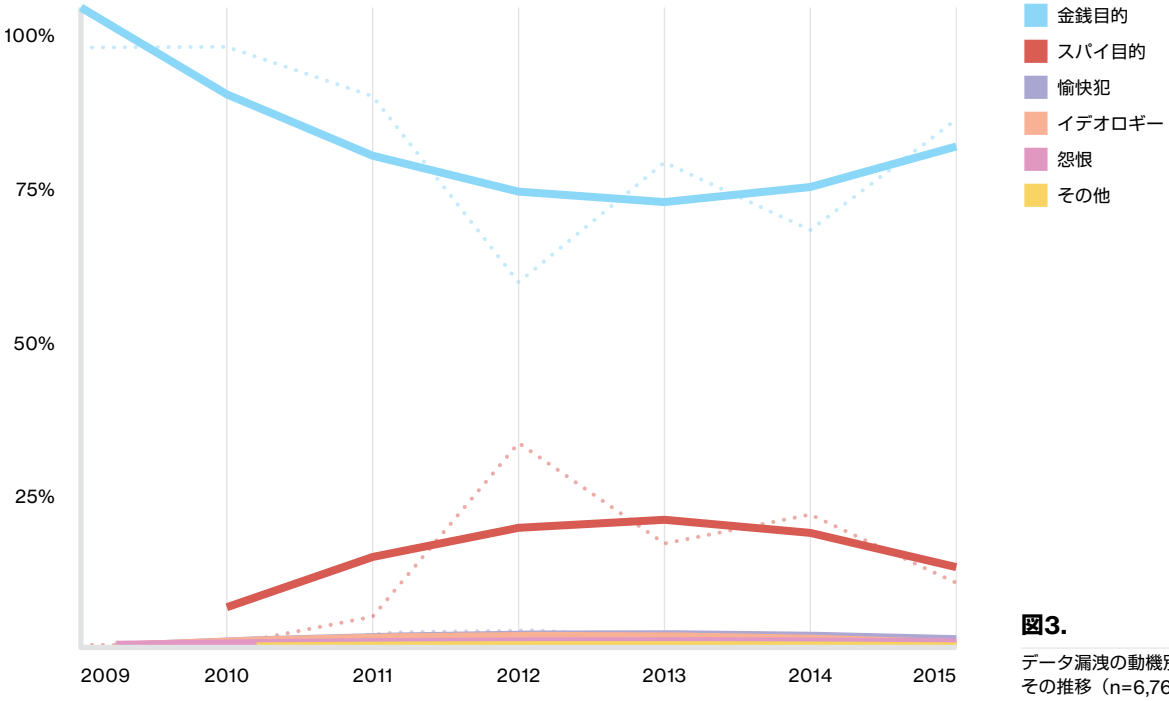


図3.
データ漏洩の動機別割合と
その推移（n=6,762）

二次的動機
本書で取り上げている攻撃の多くには「二次的動機」が含まれます。これは、別の攻撃の手助けを目的とするものを指します。二次的動機によるインシデントを含めてしまうと、他のインシデントが埋もれてしまうおそれがあるため、本書では除外しています。たとえば、攻撃者が本来の目的に利用する（悪質なファイルをホストする、スパムのばらまきやDoS攻撃に使用するなど）ためにWebサーバーを攻撃する場合が該当します。犯罪者にもインフラは必要です。それならば、自分で料金を支払ってインフラを用意するよりも、他人が管理するインフラを無料で拝借するほうがはるかに良いに決まっています。設定が脆弱なWebサーバー、NTPサーバー、DNSサーバーなどが反射型DoS攻撃に悪用されているインシデントは数多く確認されています。

ピストルでくるか、ナイフでくるか
私たちを狙っている敵の姿が少しだけ見えてきたところで、次の疑問に移りましょう。彼らはどのような武器を利用するのでしょうか。図4と5が示すとおり、多くはフィッシングです。フィッシングは、さらに深刻な影響を及ぼすさまざまな攻撃への足掛かりなのです。POS攻撃の影も見て取れます。その他の少数派については、ここでは省略して後ほどご説明します。

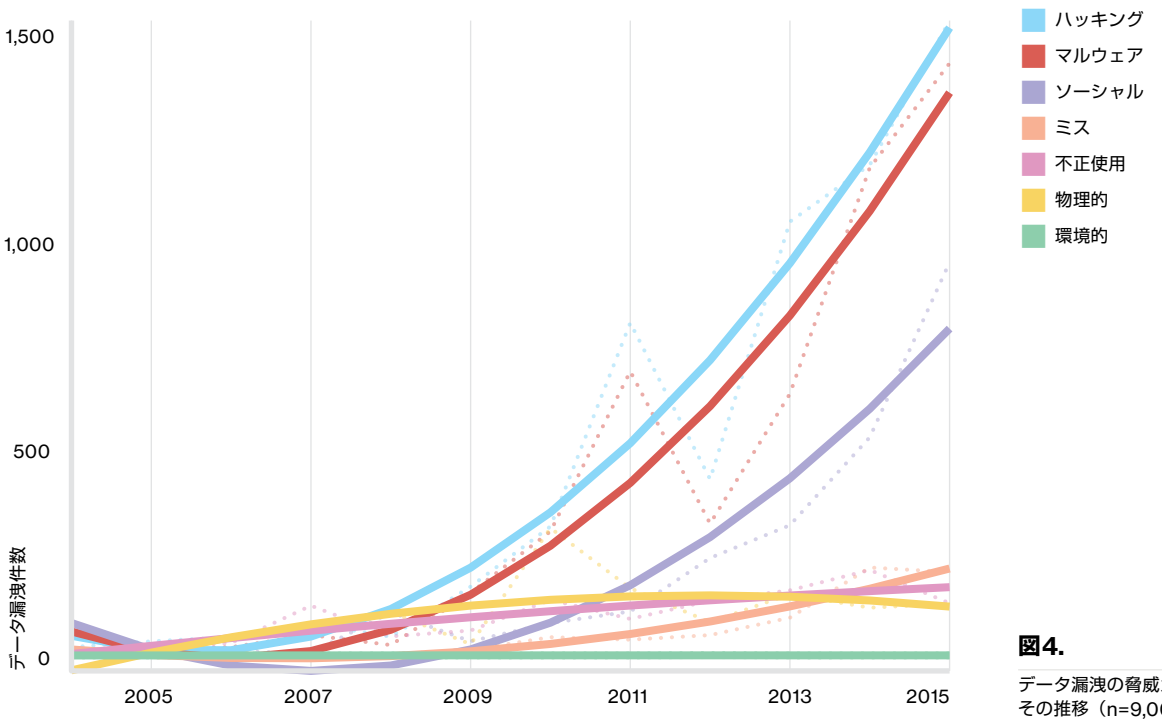


図4.
データ漏洩の脅威カテゴリ別件数とその推移（n=9,009）

他の活動も積極的に行われているのですが、今年のフィッシング（および「ソーシャル」カテゴリの上位レベルの活動）は、「Dridex」キャンペーンの影響からその件数が多めになっています。いくつかの協力企業・組織から提供された情報をまとめると、このキャンペーンは悪質なうえに、統計にある程度の影響を与えるほど勢力を拡大していることがわかりました

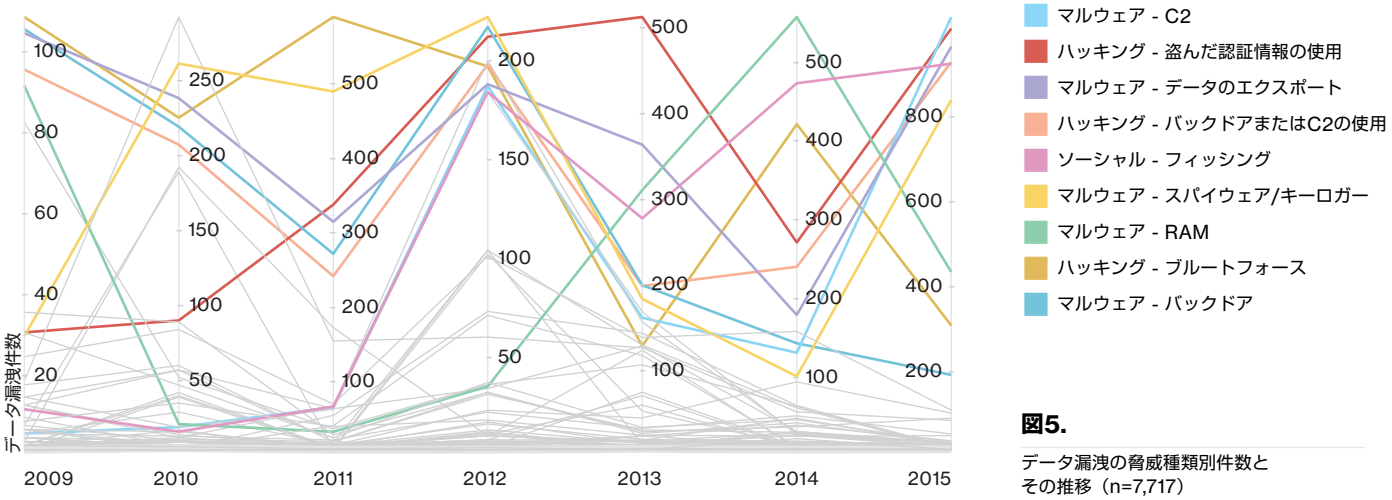


図5.

データ漏洩の脅威種類別件数と
その推移（n=7,717）

いずれにしても、現時点ではフィッシングとPOS攻撃が「脅威界の大物」と言っても過言ではないでしょう。大物のステータスに敬意を表して、POS攻撃については後ほど「インシデント分類パターン」セクションと付録「盗まれたデータの運命」で掘り下げます。フィッシングについては、「フィッシング」セクションと「インシデント分類パターン」セクションの「サイバースパイ活動」の項で詳しくご説明します。今年は認証情報についても単独のセクションを設けています。認証情報はこれまでDBIRに数え切れないほど登場してはいましたが、いつも端役で終わっていました。今年はついに、セリフのある役がもらえたというわけです。

侵入口はどこだ？

図6をご覧ください。フィッシングとPOSデバイスが攻撃の中心になっていることは、侵入口となった資産の割合にも反映されています。「人」は昨今人気が高いようで、フィッシングの被害者が増えて右肩上がりです[4]。「ユーザーデバイス」も、デスクトップPCやPOS端末のマルウェア感染が増えたことで上昇しています。

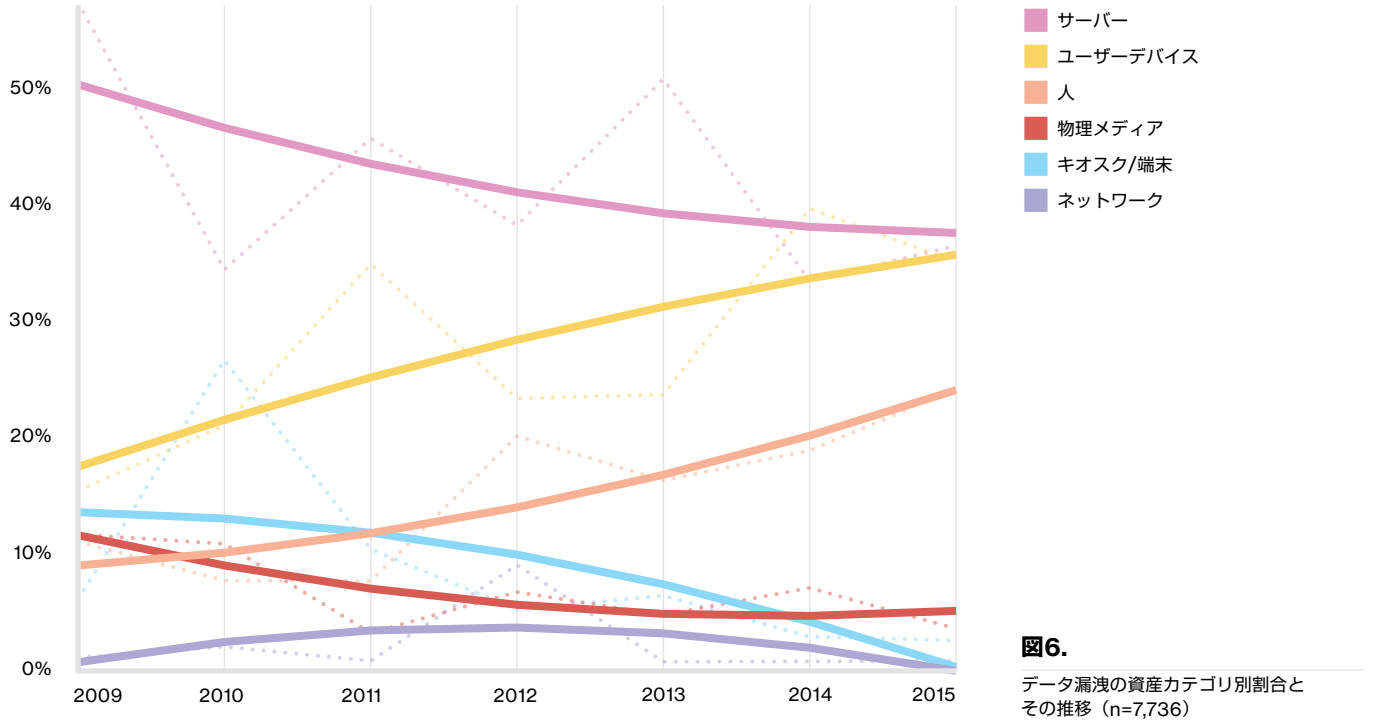


図6.

データ漏洩の資産カテゴリ別割合と
その推移（n=7,736）

4　VERISでは攻撃のこの段階を、人間の行動に影響を及ぼす点から「完全性の喪失」としてモデル化しています。

時間は私たちの味方ではない（ミック・ジャガーが「タイム・イズ・オン・マイ・サイド」と歌ったのは間違い）

ローマは一日にして成らずと言いますが、データ漏洩は一日あれば十分です。図7は、攻撃者がネットワークに侵入するのに要した時間とデータを盗み出すのに要した時間を示しています。グラフの一部が突出しているのは、限られた少数の脅威によるものです。数分でネットワークに侵入できるというのは気の重くなる話ですが、これも今年猛威を振るった「Dridex」が大きく影響しています。多くの攻撃と同様に、この脅威もフィッシングから始まります。まず、ユーザーの認証情報を盗むためのマルウェアが仕組まれた添付ファイルが送りつけられます。正規の認証情報を持っていれば、ドアを開けて入り込み、冷蔵庫を物色するのにたいして時間はかかりません。一方、データを盗み出すのに数日かかるインシデント数が多いのは、POSデバイスに対する攻撃の多さを反映しています。この場合、マルウェアは侵入後、データを収集してパッケージ化を行い、決められた日時にパッケージをエクスポートします。

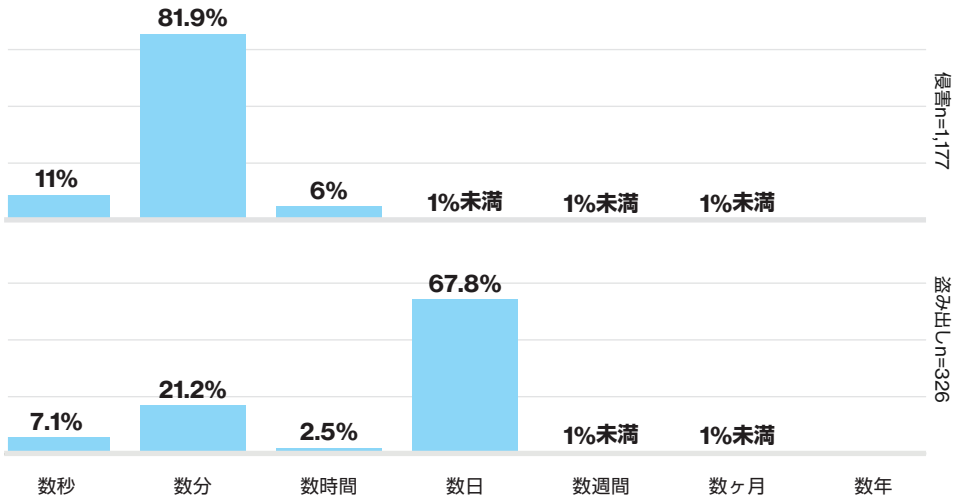


図7.

侵害に要した時間とデータを盗み出すのに要した時間

悪い知らせはすぐに広がるといっても、例外はある

図8は素晴らしいグラフです。一方の直線が勢いよく上昇し、もう一方の直線がなだらかに上昇しています。この傾斜が逆だったらもっと良かったのですが。実はこの2つのグラフは、攻撃から発見までの時間差が広がっていることを示しています。

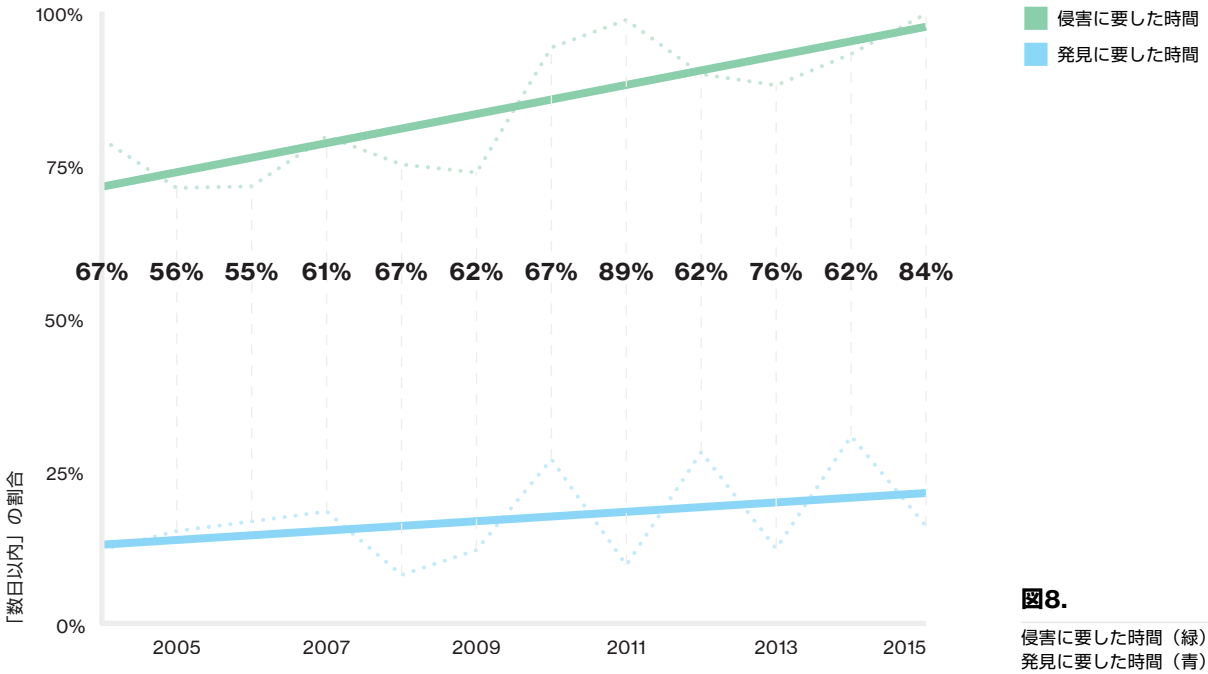


図8.

侵害に要した時間（緑）/
発見に要した時間（青）が数日以内の割合

2015年度のDBIRで「数日以内」の発見が増加するという明るい兆しが見られることをご報告しましたが、それは長くは続きませんでした。その兆しを確かな傾向として立証するには1年以上待つ必要があると申し上げましたが、残念ながら立証されなかったのです。さらに、記憶力の良い方であれば、2014年度の「発見までの時間」が昨年度のDBIRでご報告したよりも拡大していることにお気づきでしょう。年次グラフの元データはインシデントやデータ漏洩が発生した年によって分類されており、DBIR発行後もインシデントやデータ漏洩が前年分として追加されたり、年末に発生したデータ漏洩が翌年に発見されたりするため、前年度との差が生じます。

このグラフからは、侵害に要する時間がさらに短縮していることもわかります。どの脅威の発生件数が多かったかを考えれば、これは当然の結果と言えるでしょう。フィッシングは、悪質な添付ファイルをクリックさせてマルウェアを送り込むだけなので、数秒もあれば事足ります。ATMやガソリン給油機への物理的な侵入も、数秒もあれば十分です。データ漏洩を伴ったインシデントの大半では、スパイ目的であっても金銭目的であっても、攻撃者はまずマルウェアを仕掛けて制御権限を取得します。成功時には電光石火の速さです。このグラフは確認済みのデータ漏洩のみを対象にしているので、侵害に要した時間はほとんど数日以内、そうでなければ数分以内であるのも不思議ではないのです。もし、良い知らせがあるとするならば、それは数カ月間にわたってデータが漏洩し続ける件数がわずかですが減少の傾向にあることです。

侵害に要した時間はほとんど数日以内、そうでなければ数分以内です。

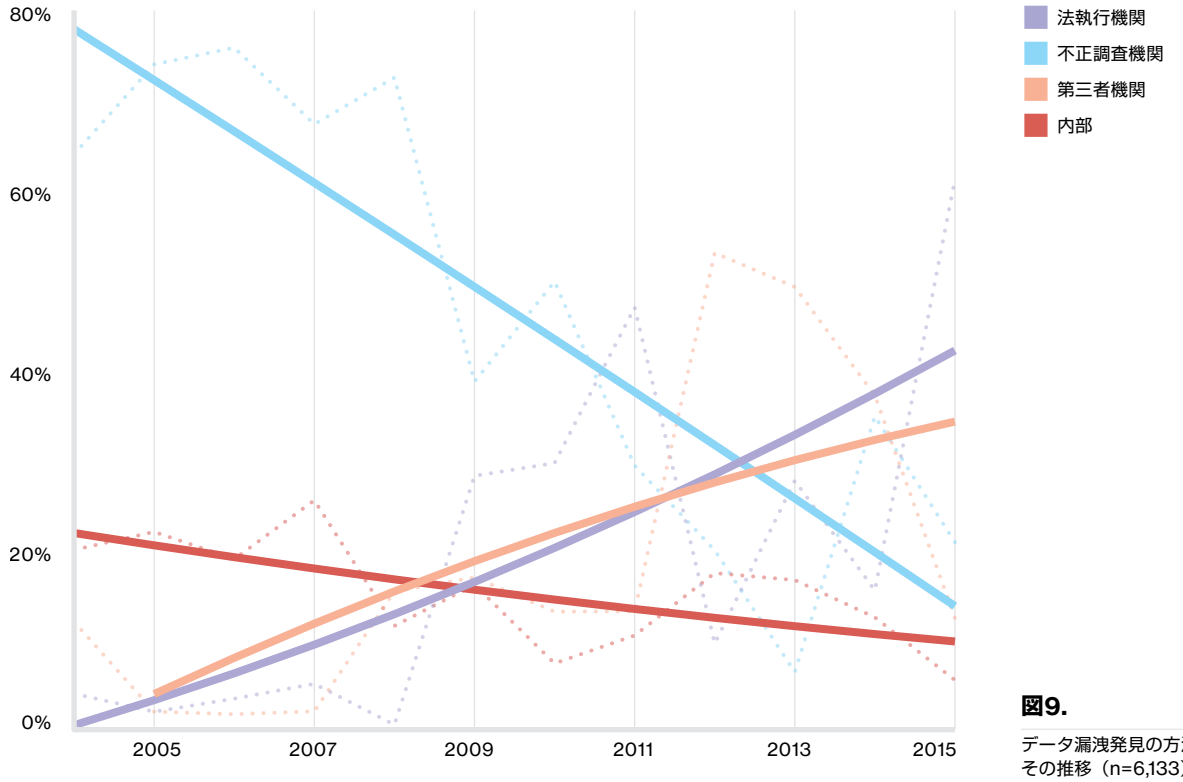


図9.

データ漏洩発見の方法別割合とその推移（n=6,133）

外部によるデータ漏洩の発見[5]については、不正調査機関と法執行当局が、80年代のバスケットボールにおけるセルティックスとレイカーズのように激戦を繰り広げています。図9に示すとおり、2015年は、ボットネットを解体してゾンビコンピュータのユーザーに通知を送り続けたことが功を奏して法執行当局が勝利しました。全体的に外部からの通報は増加しています。ただし、社内のデータを保護するうえでは、外部からの通報により初めて攻撃を知るのでは手遅れです。

5　外部からの発見とは、内部以外での発見で、パートナーが提供する監視サービスやウイルス対策サービスによる発見の事です。

注目点

インシデント分類パターンの説明に入る前にお話しすることがあります。多くのパターンに見られる3つの共通点についてです。各パターンの説明でも相応に取り上げていますが、ここに改めて抜き出して説明する必要があると判断しました。

多くのデータ漏洩でCVE（Common Vulnerabilities and Exposure：共通脆弱性識別子を示したデータベース）で特定されている脆弱性が、攻撃の足掛かりに利用されていると推測されます。ドライブバイダウンロードのことです。しかし残念なことに、これらは測定または特定が不可能だったことから、十分なCVEデータを収集できませんでした。詳細が得られないのは非常に残念です。（有能な探偵がいれば依頼したいところですが、それもできません。）幸いにも脆弱性を専門に取り扱う企業の協力により、多少は明るい見通しを得られました。

測定または特定が不可能だったために十分なCVEデータを収集できませんでした。

フィッシングは川を上る鮭のように急速な勢いで増え続け、大半の無差別な攻撃に加えて、国家機関が関わる高度な犯罪にも使われるようになっています。「フィッシング」セクションでは人的要素について掘り下げ、人間には「とりあえずクリック」してしまう傾向があることを証明するデータをご紹介します。

最後に、「認証情報」セクションでは、静的な認証について警告を出したいと思います。パスワードがだめというわけではありません。素晴らしいものですが、いわば調味料なのです。食材の味を引き立ててはくれますが、単独では食事になりません。

脆弱性

要約

説明	ソフトウェア脆弱性の動向、対策の進み具合、推奨策をご紹介します。
協力	Kenna Security（前Risk I/O）社に脆弱性および悪用データをご提供いただきました。Beyond Trust社、Qualys社、Tripwire社にご提供いただいた脆弱性スキャンデータも参照しています。
主な知見	相変わらず古い脆弱性が高い割合で標的になっています。パッチの適用は、急場しのぎで行うよりも、継続的に漏れなく対応するアプローチで行うほうが効果的です。

新しい脆弱性は日々発見されています。

分析手法
このセクションに示す悪用率に関するグラフと説明は、Kenna Security社提供の脆弱性悪用データに基づきます。セキュリティ情報/イベント管理（SIEM）ログで悪用の痕跡を突き止め、脆弱性スキャンデータと相関付け、攻撃が成功する組み合わせを特定することで、何百万件もの攻撃成功事例を反映したデータセットを導出しました。

ウサギとカメ
脆弱性管理は長年にわたり、果てしない苦行であり続けています。攻撃は何十億と発生し、エクスプロイトは自動化され、あらゆる企業・組織が手の早いハッカーの餌食になっています。さらに困ったことに、新しい脆弱性は日々発見されています。初版のDBIR以来、私たちは脆弱性管理に関してカメのアプローチを支持してきました。つまり、「ゆっくりと堅実に勝つ」ということです。

今年も脆弱性に関するデータを調査しましたが、DBIRならではの掘り下げにより、攻撃者による脆弱性悪用の傾向だけでなく、企業・組織による修復措置のタイミングと効果についても分析しました。これらの分析を継続していければ、「カメはどうすればレースに勝てるのか？」という問いについて誰もが待ち望んだ答えを見つけ出し、そこから攻撃者側と被害者側のギャップを縮める方法を学べるはずです。

「ゆっくりと堅実に」とは、どのくらいゆっくり？

今年はアプローチを変えて、脆弱性の公開から悪用までの期間を分析してみました。図10は、脆弱性が公開されてから、それを悪用した攻撃がベンダーによって初めて確認されるまでの期間を示しています[6]。この図から、公開後から悪用され始めるまでの期間について、Adobe社の脆弱性では非常に短く、Mozilla社の脆弱性ではかなり長いことがわかります。全体の半数が10日から100日の範囲内で、中央値は約30日です。この結果は、適用するパッチの優先順位とパッチの適用期限を考えるうえで参考になるでしょう。

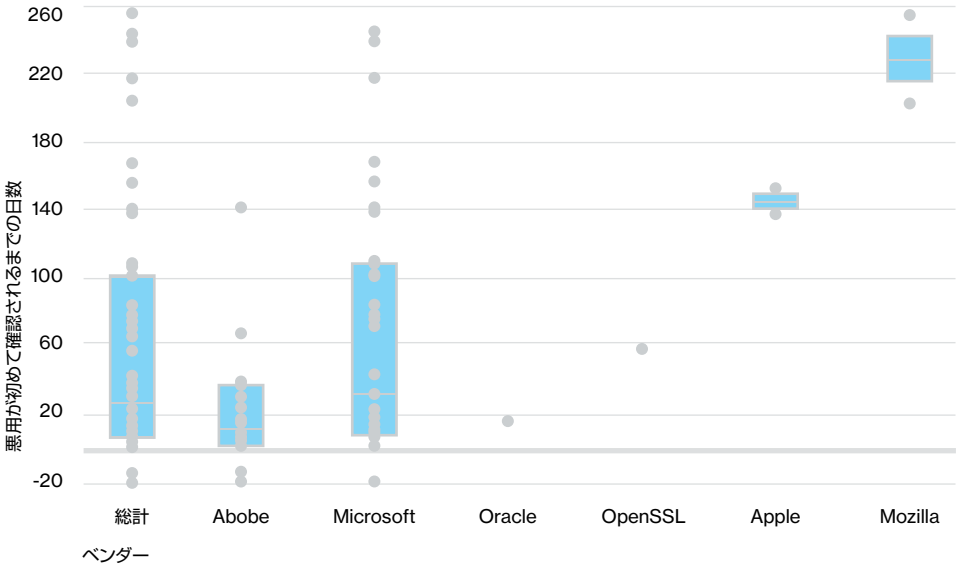


図10.

脆弱性カテゴリ別の悪用が初めて確認されるまでの期間

足踏み状態

図11は、2015年の各週について、未修正の脆弱性の数から修正済みの脆弱性の数を引いた値を、データセットに含まれる資産数で標準化したグラフです。正の値は、脆弱性の未修正数が修正数よりも多いことを示します。たとえば、新しい脆弱性が公開された、コンピュータ数が増えた、新しいソフトウェアがインストールされたなどです。負の値は、修復による脆弱性の減少数が新しい脆弱性の増加数を上回ったことを示します。

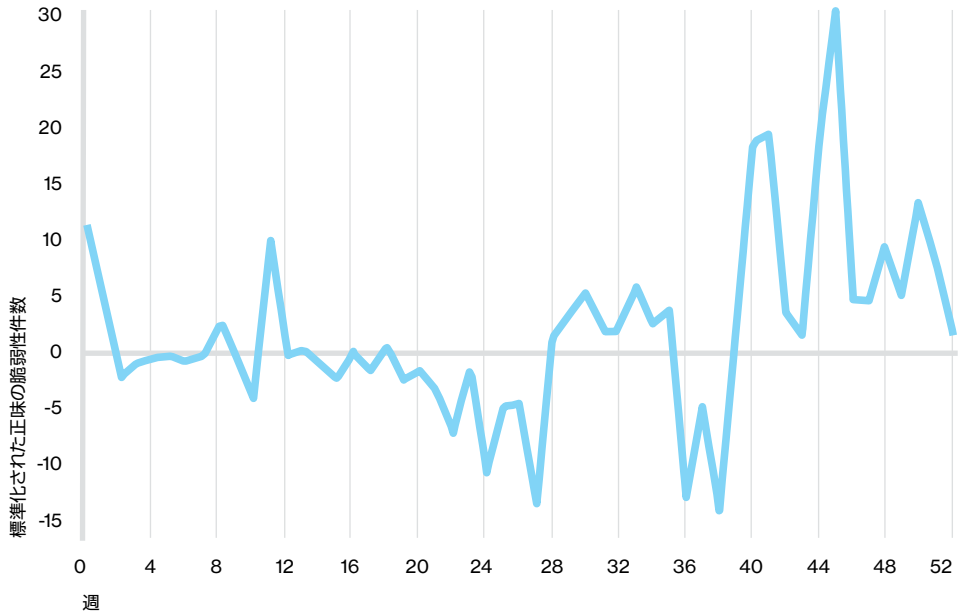


図11.

各週における、発見された脆弱性と修正された脆弱性の差分

6 図10の青いボックスは各カテゴリの値の50%を表し、ボックス内の灰色の線は中央値を表します。灰色の点は個々の値を表します。

全体的に見れば、足踏み状態と言えます。つまり、脆弱性の増加に大きな後れは取っていないものの、早急な修復と脆弱性ゼロというゴールが近いわけでもないということです。ただし、パッチを適用すべき場所に適用しなければ、修復の努力も無駄になってしまいます。足踏みするにしても、賢く行いましょう。

パッチを適用すべき場所に適用しなければ無意味です

どこを踏み固めるべきかを、攻撃者の視点から考える

どこにパッチを適用すればよいのでしょうか。2015年度のDBIRではそのヒントが示されましたが、状況はあまり変わっていないようです。

昨年の傾向を振り返ってみると、脆弱性に関する2つの黄金律は今でも有効なようです。

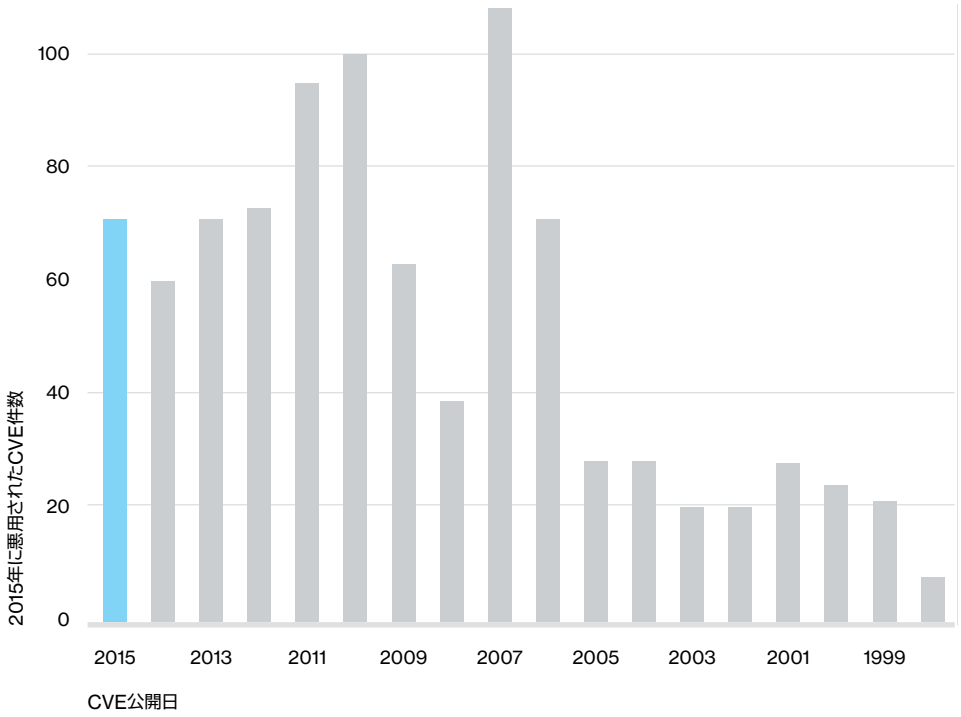


図12.
CVE公開日別の2015年に悪用されたCVEの件数

1つ目の黄金律を見てみましょう。図12は、悪用されたCVEを公開年に応じて並べたもので、年別のCVE数を示しています。2015年はCVEの悪用件数が飛び抜けて多かったわけではありません。しかし、古いCVEが依然として悪用されていることは、古い脆弱性が今なお有効であることを示しています。攻撃者は成功率の高い脆弱性を好み、成功率の高い脆弱性の内容はほとんど変わっていないということです[7]。続いて2つ目の黄金律を見てみましょう。攻撃者は脆弱性悪用を自動化してインターネットで無差別な攻撃を行い、時には大きな成功を収めています。グラフの分布は昨年とよく似ています。成功した攻撃の85%をトップ10の脆弱性が占めています[8]。もちろん、これらの「メガ脆弱性」を確認して修正することが対策の第一歩です。しかし、残り15%を構成する900以上のCVEも頻繁に悪用されていることを忘れないでください。

7 DBIRをよくご存じの皆様はお気づきのように、このグラフにはもう1つ注目点があります。昨年は、公開年に悪用されたCVEが全体的に少ないことです。ただし、より正確なデータが今年追加されて結果が変わる可能性があります。以下の新たに悪用されたCVEは（いつものことですが）多くが公開から1年以上経っています。

8 CVE-2001-0876、CVE-2001-0877、CVE-2002-0953、CVE-2001-0680、CVE-2002-1054、CVE-2015-0204、CVE-2015-1637、CVE-2003-0818、CVE-2002-0126、CVE-1999-1058

すべてを解決することはできない

図13を見ると、2015年には、2015年と2014年に公開された脆弱性のパッチ適用が進んでいることがわかります。しかしそれ以前になると件数は減り始め、やがて常に一定数を保つようになります。このデータが示しているのは、脆弱性管理の制約という、見過ごされがちな問題です。現実には、ビジネスプロセスに合わない、パッチが公開されていない、互換性が失われるなどの理由で脆弱性を修正できないことがあるのです。理由は何にしても、その場合は未修正の脆弱性を抱えたまま何とか危険を回避するしかありません。緩和策は往々にして解決策と同じくらい効果的であることを改めて認識しましょう。緩和策が唯一の選択肢という場合もあるのです。

緩和策は往々にして解決策と同じくらい効果的です。緩和策が唯一の選択肢という場合もあるのです。

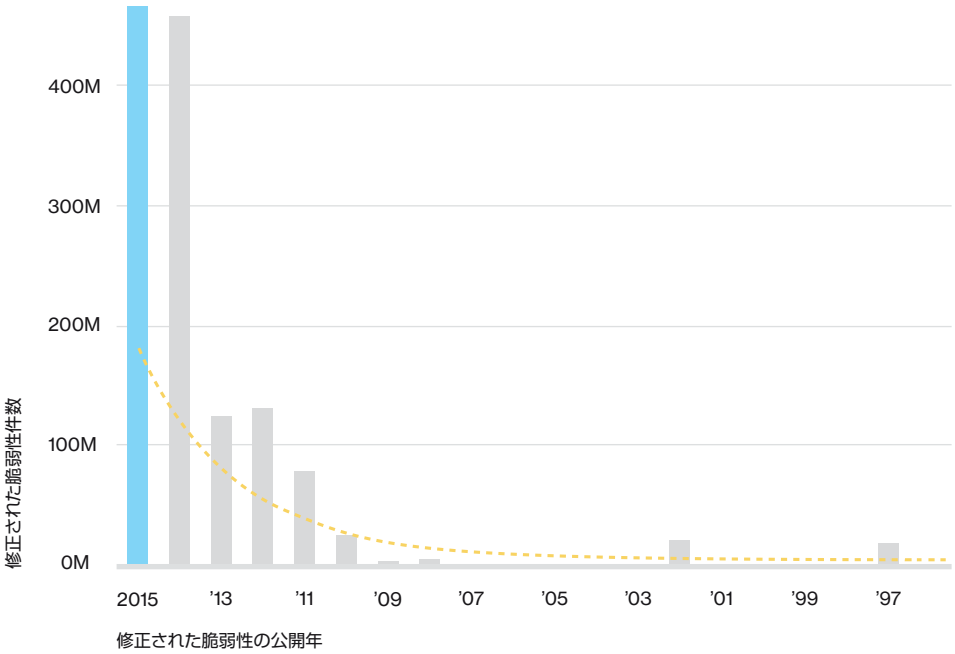


図13.
CVE公開日別のCVE修正数

推奨される対策

優先順位を考える

まずは攻撃者に悪用されやすい脆弱性、次にエクスプロイトや概念実証コードがすでに出回っている脆弱性の修正プロセスを確立しましょう。

次善策を用意する

パッチを適用できないシステムの有無や、最新のソフトウェア更新プログラムを受信できないシステムの有無を確認しましょう。そのようなシステムがある場合は、設定変更や切り離しなどのリスク緩和策を実施します。業務に深刻な影響を与えることなくデバイスを交換する方法も検討しておいてください。

社内環境を把握する

新しく追加されたデバイスやサービスを識別するには、脆弱性スキャンが役立ちます。前回のスキャン結果と比較することで、把握していないデバイスの有無や、標準設定に対する変更の有無を確認できます。

フィッシング

要約

説明	ソーシャルエンジニアリングの一種で、悪質な添付ファイルまたはリンクを含めたメッセージ（通常は電子メール）を送り、受信者をだましてファイルまたはリンクをクリックさせます。
協力	Anti-Phishing Working Group、Lares Consulting社、SANS Securing the Human、Wombat Security社にこの章で利用しているインシデントと定義されないデータをご提供いただきました。
主な関連パターン	その他すべて、WEBアプリケーション攻撃、サイバースパイ活動
頻度	インシデント：9,576件、データ漏洩を伴ったインシデント：916件
主な知見	フィッシングテストでは、メール受信者の13%が添付ファイルをクリックしました。メールを受信してからクリックするまでの時間の中央値もかなり短時間でした。

フィッシングの大半が、高度な攻撃の足場となるマルウェアをインストールするために使われていました。

「すべての人を常にだませるわけではない」というのは本当か？
ソーシャルエンジニアリングは、相手をうまくだまして、普段はしないことをさせるのが基本です。一部のオンラインデートとよく似ています。プリテキスティング[9]、誘導質問（会話をしながら巧みに情報を引き出す）、ベイティング（感染した物理メディアを標的の人物の行動範囲に放置する）など、卑劣で巧妙な手口が無数に存在します。なかでも成功率が突出して高いのはフィッシングです。名前が示しているとおり、悪質な添付ファイルやメールリンクを餌として、巧みな言葉で受信者を釣る手口です。フィッシングメールとプリテキスティングメール（偽のシナリオでメールをやり取りして目的を達成する）は、似てはいても別物であることに注意する必要があります。プリテキスティングメールでは、身分を偽ることが重要なポイントです。通常は標的組織内の人物のふりをします。たとえば、CFOのふりをして不正送金の承認を指示するといった具合です。

9　たとえば、「フリーダの上司だが、君に聞きたいことがある」

残念なことに…
添付ファイルをクリックして制御を奪われた時点で、被害が発生します。フィッシング攻撃の基本構造は従来のとおりです。ユーザーがクリックすると、マルウェアが発動して足場が築かれます。フィッシングメールから偽サイトに誘導してユーザーの入力を盗み取るケースも未だに存在します。しかし、調査対象データを見たところでは、フィッシングの大半では持続的な攻撃の足場となるマルウェアがインストールされていました。
受信者がメールを開くと、「本日のマルウェア」を含むファイルが添付されています。「これは問題なさそうだ」と思ってクリックしてしまうと、悲劇が始まります。次に何が起こるかは、攻撃者の目的次第です。

「意思の疎通が欠けていたようだ」（映画『暴力脱獄』より）
攻撃者と被害者の間のやり取りは明らかに、セキュリティ担当者と従業員の間の意思疎通よりもはるかに効率的です。私たちは2015年に、従業員のセキュリティ意識向上に関心を持つ複数のベンダーの協力を得てフィッシングテストを行い、800万を超える結果を得ました。集計した数字は図14に示しています。今年のデータセットでは、全フィッシングメールのうち30%が開封されました[10]。さらに困る結果が続きます。約12%で悪質な添付ファイルまたはリンクがクリックされ、フィッシングが成功しました。昨年度のDBIRと比較すると、フィッシングメールの開封率は23%から大幅に増加し、添付ファイルのクリック率は11%から微増しています。フィッシングの標的になったユーザーが悪質なメールを開封するまでの時間の中央値は1分40秒でした。また、添付ファイルをクリックするまでの時間の中央値は3分45秒でした。多くの人が仕事に熱心でメールのチェックが早いということでしょう。

フィッシングを仕掛けるのは主に、プロの犯罪組織や国家関連の人物です。

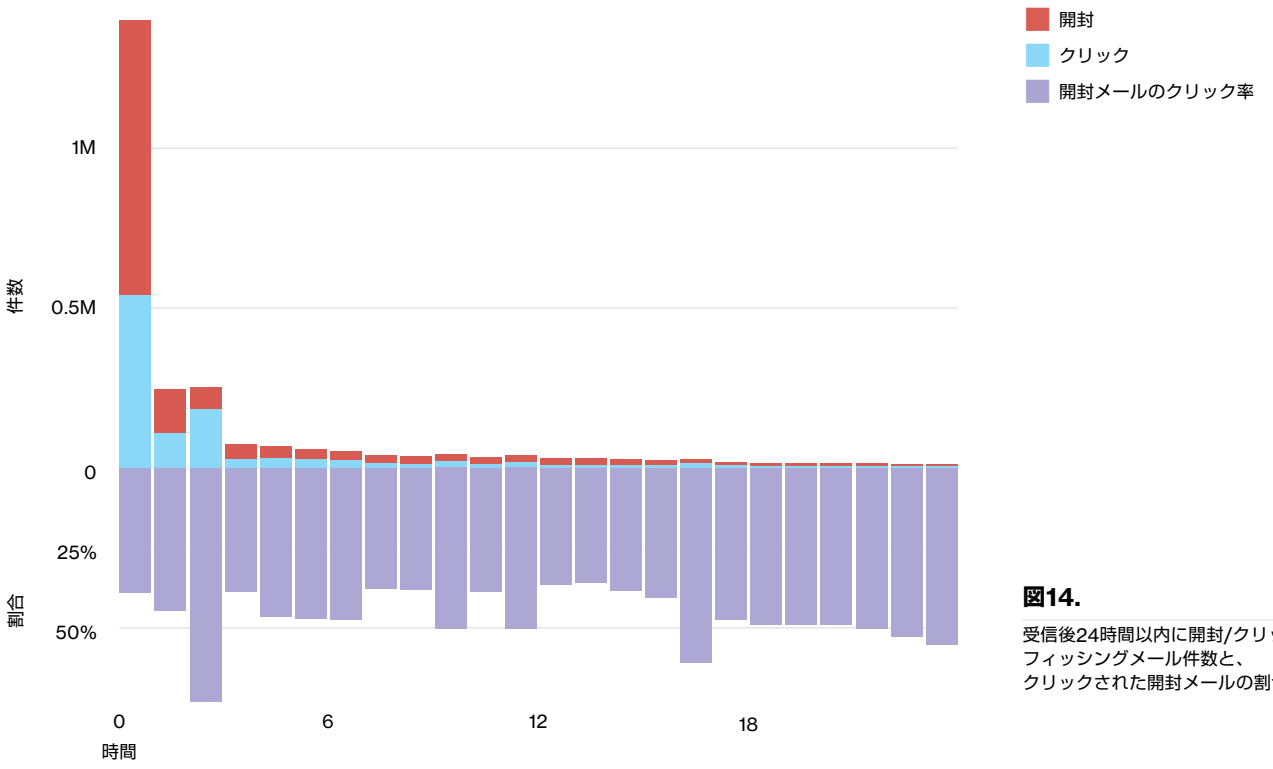


図14.
受信後24時間以内に開封/クリックされたフィッシングメール件数と、クリックされた開封メールの割合

フィッシングの被害者を引っ張り出して石を投げつける前に、彼らには同情の余地があることを理解してください。フィッシングを仕掛けるのは主に、悪知恵にたけたプロの犯罪組織（89%）や国家関連の人物（9%）なのです。テストでは約63万6,000件のフィッシングメールについて報告の有無を調べることができました。フィッシングメールの可能性があることを上司に報告した人はわずか3%でした。彼らがどのような手段で報告したのか、また、十分に注意深いために罠にかからなかったのか、それとも過去に被害に逢ったことがあるために気が付いたのかという詳細まではわかりません。

10 開封率は、メールのプレビューパネルを常に表示しているかや、メール内の画像を読み込まない設定にしているかなどの影響を受けます。

なお、今年のデータセットでは国家関連の人物が関わった割合が低くなっていますが、これは、犯罪組織にデータを流す「Dridex」キャンペーンを発見した協力者の多大なる貢献によって相対的に下がったためです。東アジアの特定のグループが良心に目覚めて悪事を改めたと考えるのは早急でしょう。

図15.

フィッシング攻撃によって漏洩したデータの種類トップ5（n=905）

結局、攻撃者は何を盗んでいるのでしょうか。まずは、膨大な量の認証情報です。多くは銀行を標的としたトロイの木馬を使った無差別な攻撃によるものです。歴史にならえば、ギリシャ人が大きなプレゼントを持ってきたらご用心ということです。そのほか、機密情報も盗みの対象となっています。

推奨される対策

フィルタの徹底活用
予防の重要性を表した「1オンスの予防は1ポンドの治療に値する」というベンジャミン・フランクリンの名言は、ここでも有効です。ありがたいことに、メールを媒介とする脅威を防ぐ最初の機会は、メールが人目に触れる前にあります。メールフィルタリングは心強い味方です。フィルタの設定を十分に理解し、実地テストで確認しましょう。

ネットワークを分離して強力な認証を設定すれば、感染の拡散を抑えることができます。

従業員教育を徹底する（しつこいようですが）
セキュリティ意識を向上させるためのトレーニングや情報提供を行って、従業員が「怪しい」と気づけるようにします。不審なメールを報告する手段も用意しておきましょう。タスクバーに報告用ボタンを追加するのがお勧めですが、効果のある方法であれば何でも結構です。

クリック後の感染拡大を防ぐ
悪質なメールがフィルタをすり抜け、受信者が不注意でクリックしてしまったとしても、被害を抑える機会はまだ十分にあります。最初に感染して足場とされるデバイスには機密情報は保管されていないことを前提としたうえで、感染したユーザーデバイスから、組織内の他の資産へのアクセスが簡単に実行できないようにしておきましょう。ネットワークを分離して、ユーザーネットワークと重要なネットワークとの間に強力な認証を設定しておけば、感染の拡散を抑えることができます。静的なパスワードは手軽で便利ですが、巧妙な攻撃の場合は防げないだけでなく、パスワードを悪用されてより深く攻撃される恐れがあります。

トラフィックの行先を監視する
アウトバウンドトラフィックを監視して、不審な接続やリモートホストへのデータ不正送信の形跡がないか確認しましょう。フィッシングの被害にいち早く気づくことができます。

認証情報

要約

説明	盗んだ認証情報の悪用と、従来のユーザー名とパスワードによる認証方法を標的にしたその他のハッキングやマルウェア攻撃は、さまざまなパターンに使用されています。
主な関連パターン	WEBアプリケーション攻撃、POSへの侵入
頻度	データ漏洩を伴ったインシデント：1,429件
主な知見	静的な認証情報は相変わらず、一般的なハッキング活動やマルウェア攻撃の標的になっています。

データ漏洩を伴ったインシデントの63%で、平易なパスワード、デフォルトのパスワード、盗まれたパスワードが悪用されていました。

怒りというよりは失望

盗まれた認証情報、平易な認証情報、デフォルトの認証情報の悪用は、最先端でもなく華やかでもありませんが、とにかく確実なのです。静的な認証方法は、ずっと昔から攻撃者に狙われてきました。情報セキュリティの世界では、パスワード推測は少なくともMorrisワームと同じくらい昔から存在し、今や感染デバイスでキー入力を記録するなどの悪事を働くDyreやZeusのような有名なマルウェアファミリーへと進化を遂げています。このマルウェア機能が広く普及したことにより、パスワードに記号、大文字、小文字、数字を必須として最低文字数も指定するなどの対抗手段はもはや通用しなくなっています。

認証情報の記録や悪用は、多くのインシデント分類パターンで使われています。標的型攻撃でも無差別なマルウェア攻撃でも使われます。犯罪組織や国家関連の攻撃者が使う標準的なツールキットもこの機能を備えています。さらに、盗まれたペイメントカードデータの不正使用でも、磁気ストライプの部分に印字されている静的なセキュリティコード（CVV）情報が使われます[11]。

11 詳しくは、付録「盗まれたデータの運命」を参照してください。

そうはいっても現実には、多要素認証の導入は簡単にできることではありません。ユーザー名とパスワードの組み合わせだけでも、自作のファンタジーフットボールリーグを守るには十分でしょう。強力な認証方法を導入しても、攻撃のハードルを上げるだけで、鉄壁を築けるわけではありません。それでも、確認済みのデータ漏洩の63%[12]で平易なパスワード、デフォルトのパスワード、盗まれたパスワードが悪用されていた事実を考えれば、ハードルを上げる価値はあると言えます。図16は、正規の認証情報が悪用された脅威活動で件数が多かったものを示しています。そのままとも言える「盗まれた認証情報の使用」が1位ですが、C2マルウェア、データエクスポート、フィッシング、キーロガーといった一般的な活動でも認証情報が使われていました。

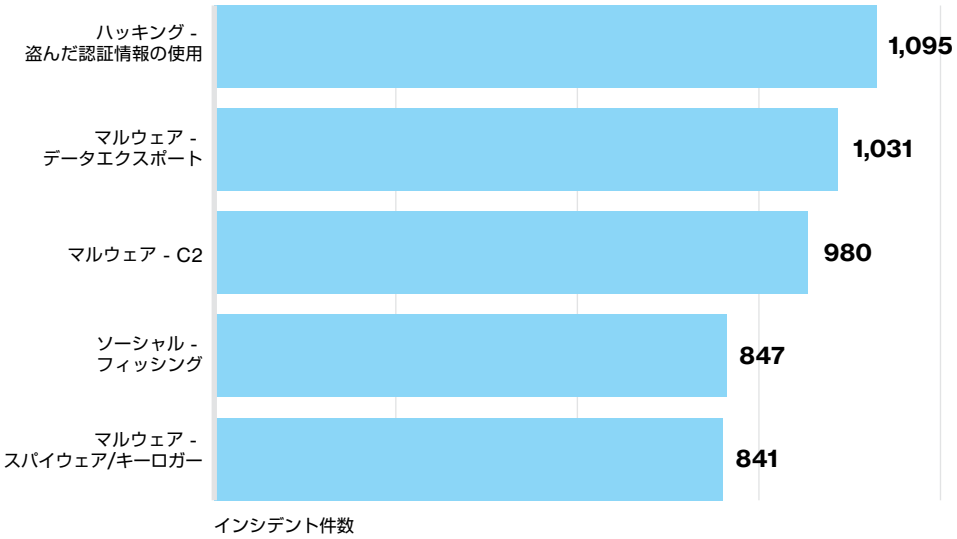


図16.

認証情報が関わるインシデントで
よく使われた脅威活動（n=1,462）

12 盗まれた認証情報の悪用、ブルートフォース、パスワードダンパー、または認証情報とみなせる各種データのうちいずれかと、データ漏洩とのすべての組み合わせを含めました。

インシデント分類パターン

数年前まではデータの変換作業中に「またこのパターンか」とぼやいていた事柄が、今や主要な分析と結果を表現方法を変更するまでに発展しました。9つのインシデント分類パターンは、インシデントに関するさまざまな特性の中で、誰が（攻撃者）、何を（資産）、どうやって（手口）、なぜ（動機）について繰り返し出現する組み合わせから生まれたのです。

2014年度版のDBIRでは、データ漏洩の90%以上が9つのパターンのいずれかに該当しました。今年もその状況は続いています。今年と過去のセキュリティインシデントデータを9つのパターンに基づいて比較することで、膨大なデータから最大限の知見を引き出せるのです。2,260種類にも及ぶデータ漏洩シナリオすべてについて対策が必要となれば、『スタートレック』のコバヤシマルのような危機的状況に絶望を感じることでしょう。そうではなく、9パターンの一部（業界によって異なる）だけでよいとなれば、セキュリティ担当者の苦労はずいぶん軽減されるはずです。

年ごとの変化と個々のパターンは後ほど詳しく見ていきますので、少々お待ちください。2015年のインシデントとデータ漏洩のパターン内訳を図17と図18に示したので、確認しておきましょう。

9つのインシデント分類パターンは、攻撃者、資産、手口、動機について繰り返し出現する組み合わせから生まれました。

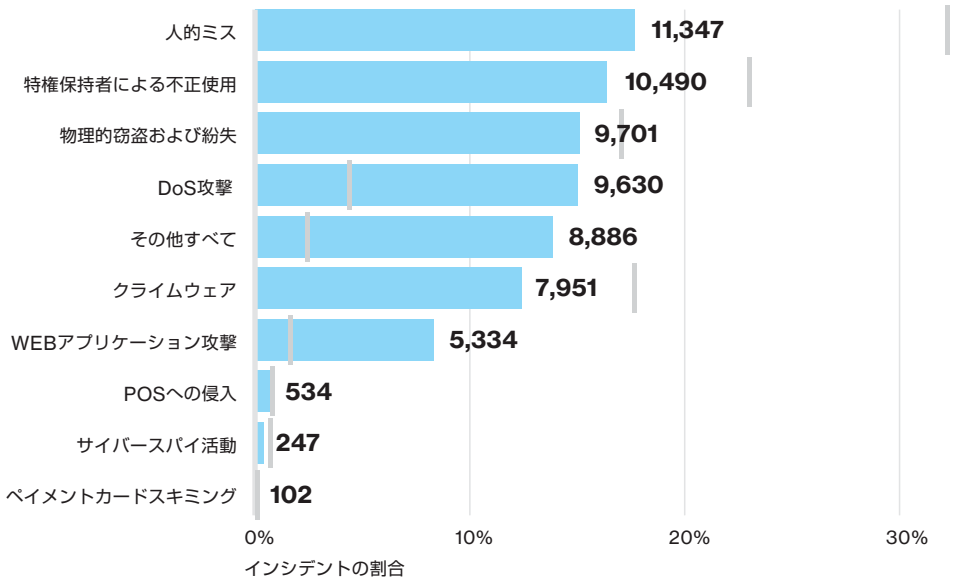


図17.

インシデントパターン別の割合（グラフ）と件数。灰色の線は2015年度版のDBIRでの割合（n=64,199）

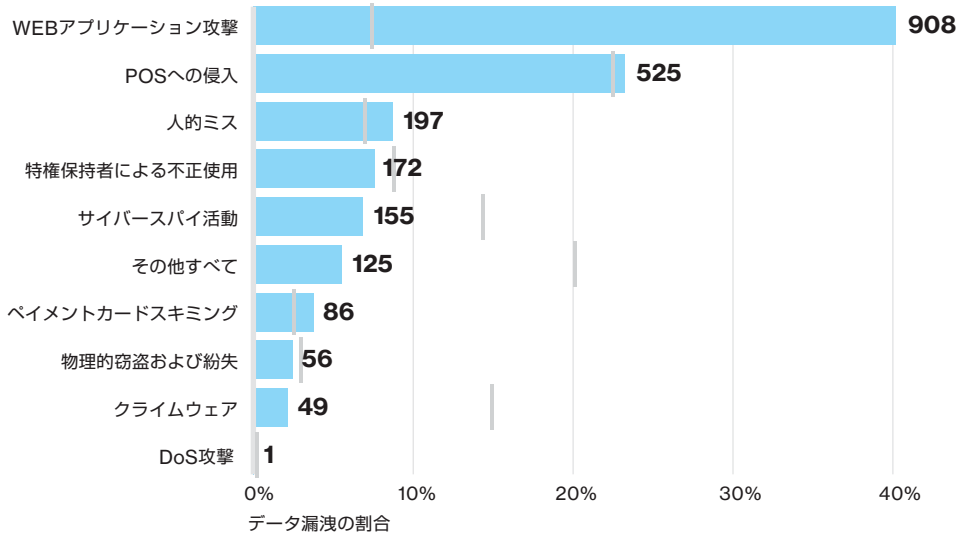


図18.

データ漏洩パターン別の割合（グラフ）と件数。灰色の線は2015年度版のDBIRでの割合（n=2,260）

「シェイキン（揺れ動く）」と歌ったジェリー・リー・ルイスには気の毒ですが、今年の順位は昨年と比べてそれほど「シェイキン」していません。ただし、1つだけ大きく順位が変わっています。クライムウェアは昨年3位でしたが、今年は6位に後退しています。この変動は、「データ漏洩の動向」セクションで説明した二次的動機を分析対象から取り除いたことによるものです。デバイスがDoS攻撃のみに悪用されたと確認できた数千のインシデントについては、/dev/null送りにして捨てたわけではありませんが、ここには含めませんでした[13]。

調査対象のデータセットは、協力企業・組織が新しく参加したり（感謝します）その年に参加できなかったりするので、毎年変化しています。協力企業・組織の多くには得意分野や専門分野があるので、収集されるデータの属性も、特定の業界、攻撃者のタイプ、国などに関連したものとなります。そのため、パターンの順位が毎年動くのは、脅威の全般的状況の変化よりも、収集したデータセットの変化によるところが大きいと言えます。脅威の状況は、後ほどご説明する、各パターンにおける脅威活動の変化から読み取ることができます。それを踏まえたうえで、図19と図20をご覧ください。恒例の「動向」グラフです。

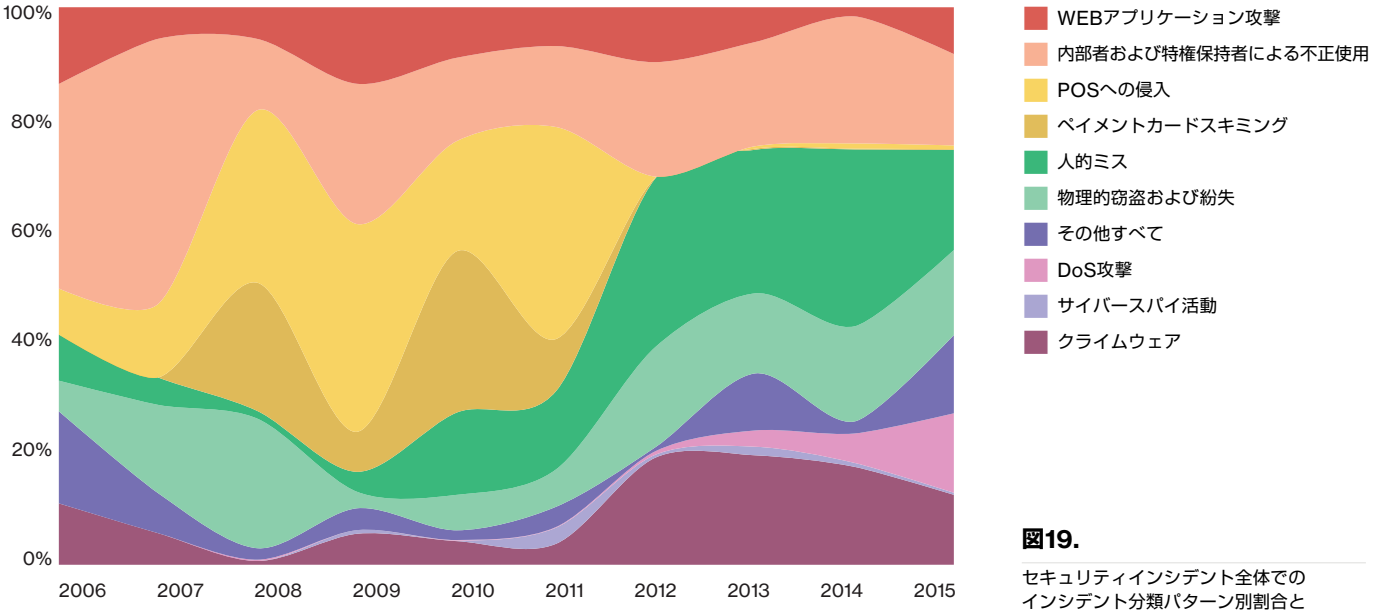


図19.

セキュリティインシデント全体でのインシデント分類パターン別割合とその推移

13 数千のWebサーバーについては、侵害されてフィッシングサイトとして悪用されたことは確認できたものの、それ以上の詳細は不明でした。
サーバーがどのように侵害されたかも、企業・組織が所有および管理しているサーバーなのかどうかも確認できなかったのです。

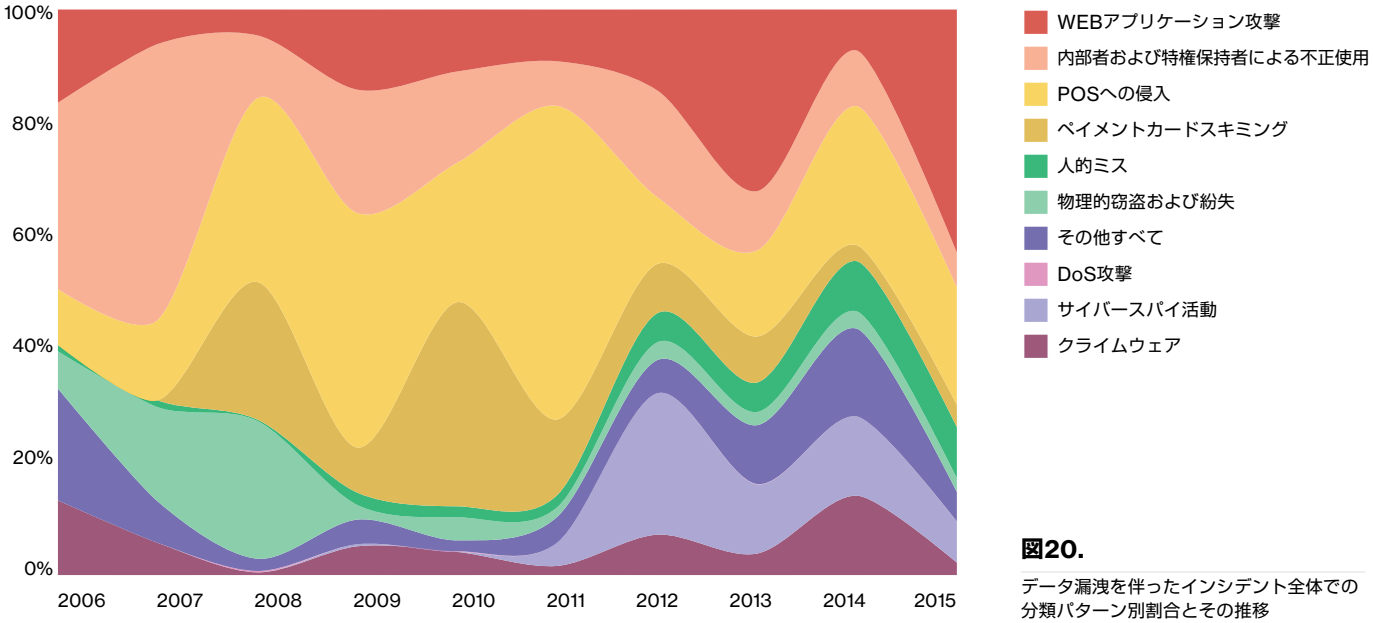


図20.

データ漏洩を伴ったインシデント全体での分類パターン別割合とその推移

順位の変化は置いておいて、パターンを有効活用する方法をご説明します。まずは、自社に関連するのはどのパターンかを知ることが重要です。下の2つの表は、各パターンの発生率を業界別に示しています。自社の業界で発生したすべてのインシデント（図21）とデータ漏洩（図22）について、どのパターンが多くてどのパターンが少ないかを確認できます。インシデントとデータ漏洩それぞれの合計数も業界ごとに示されています。一部のパターンで割合が小さくても、件数は多いことがわかるはずです。業界の分類については、NAICS（北米産業分類システム）を適用しています。自社の業界を確認するには、NAICSのWebサイトをご覧ください[14]。もちろん、ロボコップの開発で有名なオムニ社のような巨大複合企業でしたら、事業部門によって業界が異なるはずでしょう。インシデントに関してはDoS攻撃が突出しており、派手なスーツでお葬式に出席したかのごとく目立っています。DoS攻撃は常にどこかで行われています。DoSボットネットに関しては、すべてを分析対象とし

図21.

インシデント（25件以上）に関する業界別のパターン発生率

クライムウェア	サイバースパイ活動	DoS攻撃	その他すべて	物理的窃盗および紛失	人的ミス	ペイメントカードスキミング	POSへの侵入	内部者による不正使用	WEBアプリケーション攻撃	
1%未満	1%未満	20%	1%	1%	1%	1%未満	74%	2%	1%	ホテル業（72）、n=362
		56%	4%		2%		4%	22%	11%	管理サービス業（56）、n=44
2%	2%	81%	2%	3%	4%			1%	5%	教育サービス業（61）、n=254
		99%		1%未満			1%		1%	芸術/娯楽業（71）、n=2,707
2%	1%未満	34%	5%	1%未満	1%	6%	1%未満	3%	48%	金融業（52）、n=1,368
4%	2%		11%	32%	18%		5%	23%	4%	医療業（62）、n=166
4%	3%	46%	21%	1%未満	11%		1%未満	2%	12%	情報産業（51）、n=1,028
5%	16%	33%	33%		1%		1%	6%	6%	製造業（31-33）、n=171
1%	2%	90%	2%	1%	1%			2%	1%	専門サービス業（54）、n=916
16%	1%未満	1%	17%	20%	24%		1%未満	22%	1%未満	公的機関（92）、n=47,237
1%	1%未満	45%	2%		1%	3%	32%	1%	13%	小売業（44-45）、n=370
10%	16%	26%			6%			6%	35%	運輸業（48-49）、n=31

14 Census.gov/cgi-bin/sssd/naics/naicsrch?chart=2012

ていないことを覚えておいてください。もう1つ興味深い点としては、一般的に確認済みのデータ漏洩ではなくインシデントとして分類されるその他のパターン、つまりクライムウェア、内部者および特権保持者による不正使用、物理的窃盗および紛失に関することです。これらは、公的機関と医療業に集中しているのです。これらはインシデント全体のパターン別割合ではトップ3なので、他の業界においても件数ではこれらのパターンがDoSのシェアをある程度奪っていると断言してよいでしょう。

図22.

データ漏洩を伴ったインシデント（25件以上）に関する業界別のパターン発生率

クライムウェア	サイバースパイ活動	DoS攻撃	その他すべて	物理的窃盗および紛失	人的ミス	ペイメントカードスキミング	POSへの侵入	内部者による不正使用	WEBアプリケーション攻撃
			1%	1%未満	1%	1%未満	95%	1%	1%
	7%		17%	17%	27%			3%	30%
				3%			47%		50%
1%	1%未満	1%未満	2%	1%未満	2%	9%		4%	82%
3%	3%		11%	19%	22%		7%	32%	3%
1%	3%		4%		25%		1%	11%	57%
3%	47%		3%				3%	24%	21%
4%	19%		25%	4%	15%			21%	13%
12%	16%		4%	9%	37%			13%	9%
1%	1%		4%		1%	3%	64%	2%	26%

ホテル業（72）、n=282

教育サービス業（61）、n=29

芸術/娯楽業（71）、n=38

金融業（52）、n=795

医療業（62）、n=115

情報産業（51）、n=194

製造業（31-33）、n=37

専門サービス業（54）、n=53

公的機関（92）、n=193

小売業（44-45）、n=182

データ漏洩について最も興味深い点は、WEBアプリケーション攻撃が全体的に増加している中で、特に金融業で大幅に増加していることです（2015年度版DBIRでは31%）。次に注目したいことは、金融業におけるクライムウェアの減少です（昨年は36%）。この2つに相関関係はあるのでしょうか。答えは「イエス」です。今年はDridex騒動に伴い、盗まれた認証情報の悪用に分類されるデータが増えました。これがWEBアプリケーション攻撃パターンの急増を引き起こしたのです。これらのデータ漏洩を差し引けば、件数は2014年とほぼ変わりません。別のパターンに目を向けると、2014年には、クライムウェアに分類されるデータ漏洩を引き起こしたマルウェア感染が多く報告されました。2015年には、クライムウェアがデータ漏洩に大きな役割を果たさなかったということでしょうか。実は、情報提供元の協力企業・組織の観点もパターン分類に大きく影響しているのです。銀行を標的としたトロイの木馬を例にとって考えましょう。

イベント1：企業Aがドライブバイダウンロードで Zeus亜種に感染

イベント2：マルウェアがキーロギング機能を使って銀行の認証情報を記録

イベント3：マルウェアが記録済み認証情報をコマンドアンドコントロール（C2）サーバーに送信

（幕間のBGM）

イベント4：盗まれた認証情報で銀行BのWebサーバーにログイン

イベント5：不正取引を実行

銀行Bは「当行はマルウェアに感染していない」と判断するでしょう。この場合にイベント4～5だけが報告されれば、その事例はWEBアプリケーション攻撃に分類されます。一方、企業Aからイベント1～3だけが報告されると、それは別件としてクライムウェアによるデータ漏洩に分類されます。

インシデントパターンの間には、時として表面には出てこない相関関係が潜んでいることにご注意ください。ある企業・組織に侵入したクライムウェアが、別の企業・組織へのDoS攻撃や、別の企業・組織での不正取引を引き起こすことがあるのです。私たちはみなセキュリティのエコシステムに組み込まれています。背中から倒れても相手が受け止めてくれると信じたいのですが、どうでしょうか。

WEBアプリケーション攻撃

要約

説明	WEBアプリケーションが攻撃経路となるすべてのインシデントがこのパターンに分類されます。アプリケーションが持つコードレベルの脆弱性の悪用、認証メカニズムの無効化などの手口があります。
標的になりやすい業界	金融業、情報産業、小売業
頻度	インシデント：5,334件（二次的動機で追加19,389件）、データ漏洩を伴ったインシデント：908件
主な知見	このパターンのデータ漏洩には、Dridexボットネット解体に関わった協力企業・組織が収集した情報が大きく影響しています。利用者にソーシャル攻撃を仕掛け、Dridexマルウェアを送り込み、キーロガーで認証情報を盗み出して悪用するという手口が多く見られます。Webサイトの改ざんも後を絶ちません。また、CMSプラグインの脆弱性も標的となります。

インフラの複雑化により、Webアプリケーションサーバーは攻撃者にとって魅力的な標的になりました。

イルカのカイル君が活躍していた時代

Webサイトは今やすっかり変わりました。一昔前のWebサイトを思い出してください。雲模様の背景で、中央上部に企業名がComic Sans書体で誇らしげに掲げられ、左右両側をアニメーションGIFが彩り、大文字や<blink>タグが多用され、もちろん下部にはサイトカウンターが軽いドロップシャドウ付きで設けられる、といった具合でした。1997年を思い返すと、ものごとはシンプルでした。今や、企業・組織のWebサイトの多くでは、見た目は洗練され、製品/サービス紹介や電子商取引、バックエンドデータベースへの接続など、ビジネスを前面に押し出しています。ユーザーは、ホームページを見て何回かクリックして営業時間などの基本情報をチェックするだけでなく、インタラクティブな操作とさまざまな入力方法でWebインフラとやり取りできるようになりました。それを実現するためのWebアプリケーションのコードやその根底にあるビジネスロジックなどの複雑な機構は、ストレージまたはプロセス内の機密データへのアクセス経路にもなります。そのため、[15]Webアプリケーションサーバーは攻撃者にとって魅力的な標的になりました。

15 Webアプリケーションは、インターネットからアクセス可能な組織内サービスとして、おそらく唯一のものです。また、そうであって欲しいものです。

Webサイトが侵害されても、攻撃者の目的は侵害そのものではない場合があることに注意してください。侵害されたWebサイトがマルウェアのホスト、DDoS攻撃、フィッシングサイトなどに悪用されたインシデントが約2万件あります。侵害の手口も被害者情報も確認できなかったため、こうした二次的動機は以下にご紹介するデータからは除外されています。残るインシデントのうち約半分はWebサイトの改ざんでした。これらについては、動機がイデオロギーなのか私恨なのか単なる愉快犯なのかを判別する十分な情報がなかったため、図23では1つにまとめられています。多くの場合、侵害を起こしたハッキングの手口もわかっていません。ただ、改ざんに対して、以前には困ることもあったがもはや過去のものとなったblinkタグのようなものだと思っているのなら、考えを改めたほうがよいでしょう[16]。

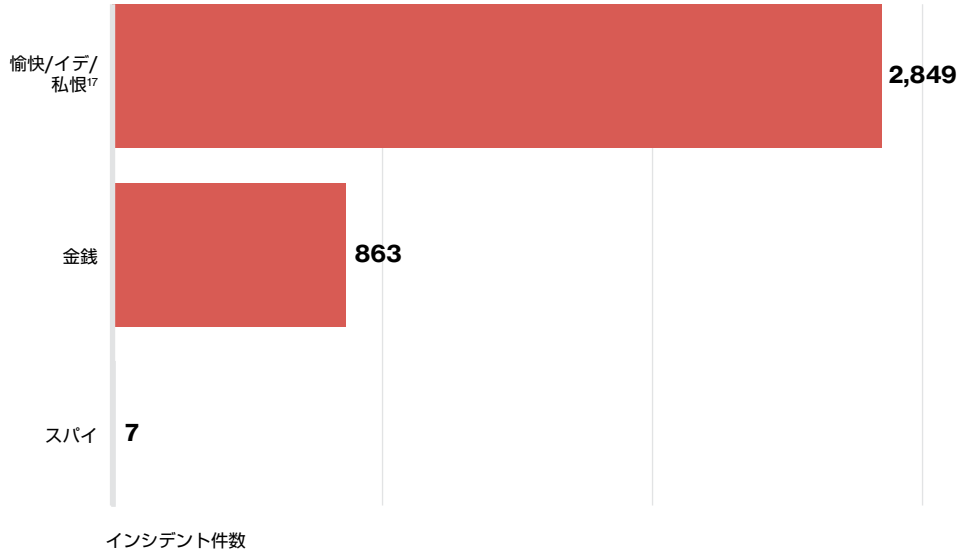


図23.
WEBアプリケーション攻撃によるインシデントでの外部実行者の動機（n=3,720）

データ漏洩を伴ったインシデントに限ると金銭目的が優勢で、95%が最終的に金銭に結びつきます。

Webアプリケーション攻撃によるデータ漏洩の95%は金銭目的でした。

エコなハッキングは、パスワードを再利用してリサイクルする
図24に示す脅威活動の分布を見ると、圧倒されてしまいます。トップ6の活動は、Dridexキャンペーンの存在を雄弁に物語っています。その説得力は、有名な学者デイビッド・アッテンボローの見識を名優モーガン・フリーマンの語り口で伝えるぐらい強力なものです。これらのデータ漏洩は、複数のC2サーバーに対するフォレンジック分析から判明しました。フィッシング→C2との通信→キーロガー発動→取得データの送信→盗まれた認証情報の悪用、という流れを見事に表しています[18]。特定の脅威がやりたい放題で数字を押し上げているにしても、トップ6の順序はともかく顔ぶれは昨年とほぼ同じです。違いは、フィッシングが上位に入ったくらいです。

実は、Dridexボットネットの影に別の物語が隠れています。私たちは、この大規模攻撃の影響を差し引いて、盗まれた認証情報の悪用に関連付けられるその他のデータポイントを探りました。このパターンにフィッシングが関連することは既知の事実ですが、今回、実はメールサーバーも関連することがわかりました。ボットネットから得られたWebアプリケーション攻撃だと認識されたデータを、玉ねぎの皮のように取り除いていったところ、Webメールの認証情報を盗み出すためのソーシャルエンジニアリングが現れたのです。これらは、「君のメールは読ませてもらった」と書かれたTシャツで自慢するような単純な脅威ではありません。

16 blinkタグをご存じでなかったら、Googleで「blink tag」を検索してみてください。予めお詫び申し上げます。
17 F/I/Gは愉快犯（Fun）、イデオロギー（Ideology）、私恨（Grudge）を表します。
18 VERISの分類に「型破り」という項目があったら、この攻撃チェーンからきたものでしょう。

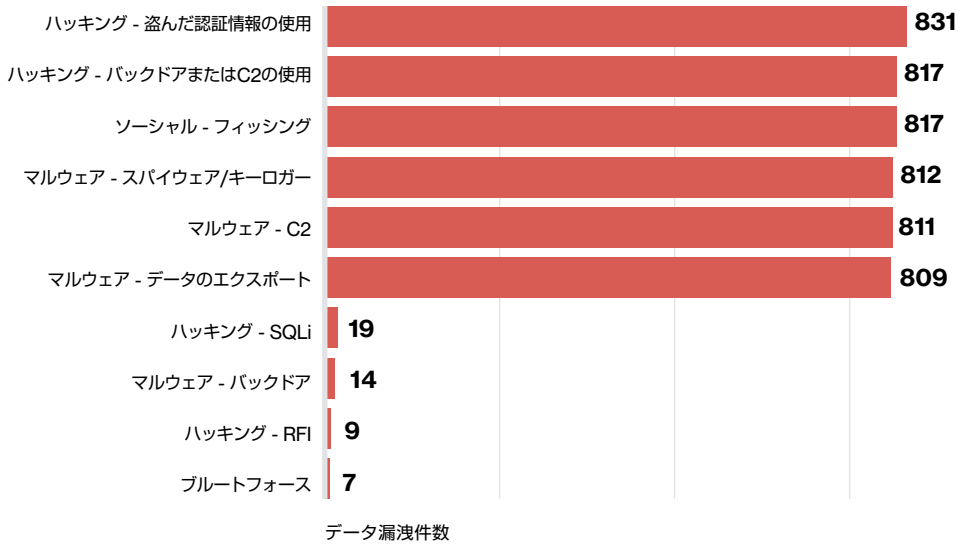


図24.
WEBアプリケーション攻撃による
データ漏洩で使われた脅威活動トップ10
（n=879）

WebアプリケーションへのWebシェルの注入

Webシェルはコンテンツ管理システム（CMS）を経由してインストールされることが確認されています。[19]Webシェルは私たちのフレームワークではバックドアにも分類されます。リモートファイルインクルージョン（RFI）の脆弱性またはセキュリティ保護されていないアップロード機能を悪用することで、Webシェルが注入されて別の攻撃への入り口として使用されます。金銭目的で電子商取引サーバーを標的とする攻撃では、Webシェルはまず支払アプリケーションコードにアクセスするために使われます。その後、機能を変えてユーザー入力を記録し、ペイメントカード番号やセキュリティコードなど必要な情報を盗み出します。数年前からこの手口は他の調査でも裏付けられています[20]。さらにDBIRとしては、Webアプリケーションハッキングの古株であるSQLインジェクション（SQLi）を取り上げないわけにはいきません。Webアプリケーションに関連する他の脆弱性にも当てはまることですが、SQLiの脆弱性も、入力されるデータが適切に検証されていないことが原因です。これにより、攻撃者がWebアプリケーションからデータベースにSQLコマンドを送り込むことが可能となります。最後に、Webアプリケーションセキュリティに関するスキャンデータと、『スタートレック』に登場するテレパシー能力であるマインドメルドを提供してくださったAsTech Consulting社、Imperva社、WhiteHat Security社にお礼を申し上げます。

電子商取引サーバーに対する攻撃では、Webシェルは支払アプリケーションコードにアクセスしてから、ユーザー入力を記録します。

19 US-Cert.gov/ncas/alerts/TA15-314A
20 Imperva社の2015年版WAARでは、RFIとコンテンツ管理システムの間に強い相関関係が示されています。

推奨される対策

とにかく多要素認証
頭にこびりついて離れない音楽のようにしつこく聞こえるかもしれませんが、ここでもう一度警告を発します。重要なデータに対しては、パスワード頼みの一要素認証は無力です。Webアプリケーションを保護するべく認証の完全性を確保しようとするなら、利用者がキーロギングマルウェアに感染しないという前提は捨ててください。キーロギングマルウェアへの感染は現実に発生するのです。

ユーザーの入力は尊重するが、検証もする
とにかく入力を検証することです。画像をアップロードするときには、Webシェルではなく本当に画像であることを確認してください。ユーザー名フィールドからデータベースへのコマンドが入力できないことも確認してください[21]。

プラグインも忘れずに管理
OSや基幹アプリケーションのセキュリティだけでも手一杯になりますが、サードパーティ製プラグインも危険をはらんでいます。CMSプラットフォームとサードパーティ製プラグインの両方について、パッチ適用プロセスを確立しましょう。

21 お勧めサイト：XKCD.com/327/

POSへの侵入

要約

説明	カードを提示する対面取引を標的としたリモート攻撃がこのパターンに分類されます。POS端末やPOSコントローラが攻撃対象になります。PED[22]パッドの物理的タンパリングやデバイスのすり替えは、ペイメントカードスキミングのパターンに分類されます。
標的になりやすい業界	ホテル/飲食業、小売業
頻度	インシデント：534件、 データ漏洩を伴ったインシデント：525件
主な知見	リモート攻撃によるペイメントカードデータの大量漏洩は、2014年は大規模小売企業で多く発生しましたが、2015年はホテルチェーンで目立ちました。手口の多くは、盗んだ認証情報を悪用してPOS環境にアクセスするというものです。今年のデータではコマンドアンドコントロール（C2）機能の使用が急増しています。これがすべて2015年の傾向というよりは、過去のデータでC2機能が少なく見積もられていた点も影響していると考えられます。 2015年もRAMスクレーピングが多く見られました。一方、多くのPOS攻撃で有効な認証情報を取得する手段として、キーロギングマルウェアも重要な役割を果たしていました。ここ数年に引き続き、今年も単独の攻撃者によって多数の被害者が出る傾向にあります。これは、不適切な構成でインターネット接続されているPOS装置を標的とする自動化された攻撃ではなく、POSベンダーに対する攻撃の二次被害が原因と考えられます。

攻撃者にとって POS装置は、 ペイメントカードデータを 手に入れるための 「信頼できるソース」です。

未だに健在

2015年もこのパターンが健在だからといって、驚くことはありません。今でも、金銭目的でペイメントカードデータを盗む人たちと、そのデータを買う人たちは活動を続けているのです。攻撃者から見ると、POS装置は、ペイメントカードデータを盗み出すための信頼できるソースです。特に、利用者の磁気ストライプ情報を直接読み取るPOS端末と、端末から送信された取引データが集積されるサーバーとなるPOSコントローラは魅力的です。

22「PIN Entry Device」（個人識別番号（PIN）入力デバイス）の略

小規模組織のPOS環境では多くの場合、1台のコンピュータで支払を処理し、支払処理サーバーと通信しています。しかも、このコンピュータをインターネットに接続して個人メールやSNSのチェックなどをしている場合もあるので、危険は高まります。これでは、ウイルス対策ソフトウェアもホストベースのファイアウォールも守ってくれない単独のPOSアプリケーションを危険にさらすことになります。

4 ～ 5年前のDBIRは、POSのデータ漏洩に関する知見で埋め尽くされました。POS攻撃の手口は単純で自動化が可能であり、ベンダーによるデフォルト認証情報も知れ渡っていました。私たちは親しみを込めてPOS攻撃を「ショーウィンドウ破り」と呼びました。この手口が何度も見つかったことが、インシデント分類パターンの作成につながりました。DBIRを初めてご覧になる方のために、POS攻撃の手口を簡単にご説明しましょう。1）POSサーバーがインターネットに接続されて丸見えで、2）POSのログインがデフォルトのままである状況で、3）犯罪者が1と2を悪用してマルウェアを送り込み、4）ペイメントカードの処理時にマルウェアがデータを盗み取る、という具合です。このシナリオは小規模組織が直面する問題です。しかし、より規模の大きい組織でも学ぶべき点があります。

2015年度版のDBIRでは、POSのデータ漏洩被害に遭う大規模組織が増えていることを指摘し、このパターンに占める割合を示しました。大規模組織の場合には1と2が該当しない点でややハードルが高くなるものの、明らかに類似する点も見られます。大規模組織でのデータ漏洩でも、「ショーウィンドウ破り」でも、静的な一要素認証の弱点が突かれます。攻撃者は、侵入するために、デフォルト設定のままではないはずの有効な認証情報を盗み出します。さらに、盗んだ認証情報をインターネットから直接入力するのではなく、POSネットワーク内に足場を作ってそこから入力します。

攻撃者は、ネットワークに侵入するために有効な認証情報を盗み出す必要があります。

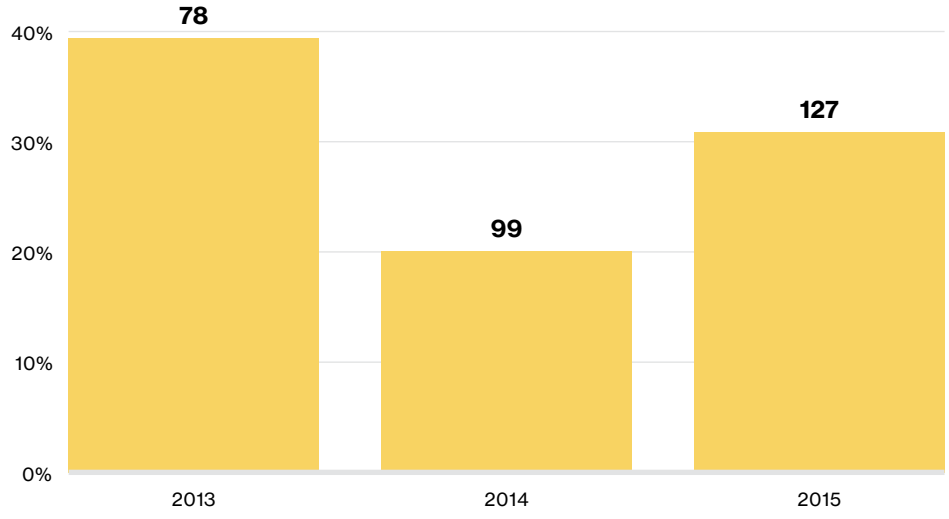


図25.

過去3年間のPOS侵入で、盗んだパスワードが悪用されたデータ漏洩の割合と件数（n=1,103）

図25は、POSへの侵入パターンで、盗まれたパスワードが悪用されたデータ漏洩の割合と件数を示しています。侵入手口としてはブルートフォースもまだ使われていますが、並の知能を持つサルでも推測できるようなパスワードの使用禁止が中小規模の組織でさらに進めば、今後はますます減っていくでしょう。

ベンダーが侵入経路に

ハッキングに使われる経路からも興味深い事実が読み取れます。盗まれた認証情報を悪用したデータ漏洩の97%では、パートナーも経路として使われていました。つまり、ハッキングに正規のパートナーアクセスが利用されているということです。今年のデータセットでも、POSベンダーに攻撃を仕掛けたうえで、顧客への不正アクセスを狙う手口が数多く見られました[23]。ビル・ゲイツはかつて「最も不満を持っている顧客からこそ最も多くのことを学べる」と述べました。POSベンダーへの攻撃によりすべての顧客に被害が及んだとすれば、そこから学べる教えの量は、映画『マトリックス』でネオが受ける格闘技の教えに匹敵するでしょう[24]。

盗んだ認証情報を悪用したデータ漏洩の97%で、正規のパートナーアクセスが使われていました。

大規模組織と小規模組織でのPOSデータ漏洩では、マルウェアが主力であることも類似点として挙げられます。図26は、よく使われるマルウェア機能を示しています。かつては汎用的なキーロガーだったのが、今や、メモリから情報をかき集めるRAMスクレーパー、そしてBlackPOSやPoSeidonなど名前が示すとおりのPOS固有のRAMスクレーパーへと進化を遂げています。データを運び出す手口も、マルウェア内に静的なコードを仕込む方法から、FTPで特定のサーバーに送信する方法、そしてC2インフラを活用して記録データを送り出す方法へと進化しています。

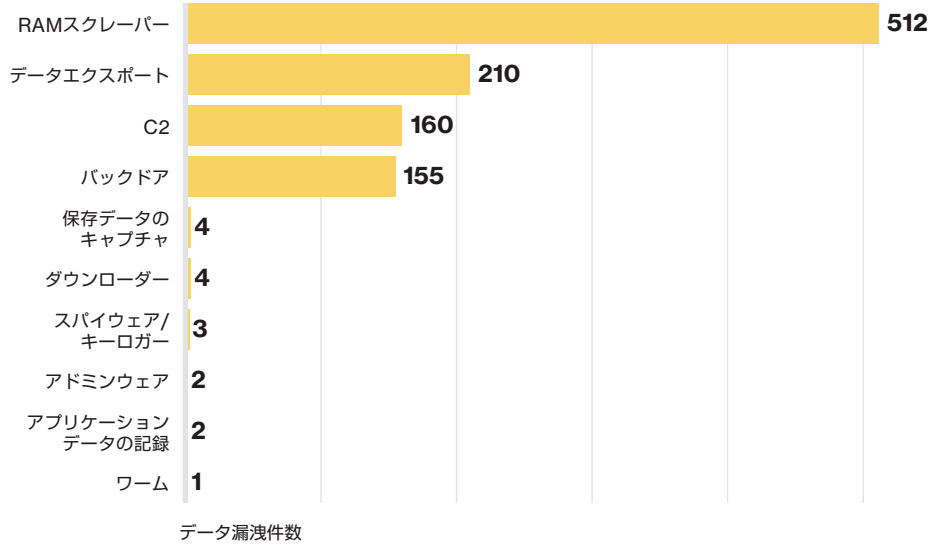


図26.

POS侵入によるデータ漏洩で使われたマルウェア機能（n=521）

C2とバックドアの件数はどちらも過去最高を記録しています。多くのPOSマルウェアファミリーは多機能で、一部の悪名高いマルウェア（Dexter、vSkimmer、Alina、Backoff、JackPOSなど）はC2とバックドアの両方を備えています。ほとんどの場合、データを盗み出すなどの一部の機能については使われたことを簡単に証明できますが、C2ビーコン送信など他の機能では証明が難しくなります。実際に、POSへの侵入インシデントの多くでは、外部への通信が行われたことを証明するログはありませんでした。つまり、C2とバックドアの件数が急増したのは、マルウェアの動作全体を把握する精度が向上したためと考えてよいでしょう。

23 このシナリオは、他のパターンでもよく使われるさまざまな活動を組み合わせているため、「まとめ」セクションでさらに詳しく説明しています。
24「カンフーを使えるぞ」（映画でのネオのセリフ）

推奨される対策

しつこいようだが静的認証は強化が必要
静的な一要素認証は攻撃者が必ず狙う弱点です。可能であれば、ハードウェアトークンやモバイルアプリケーションなどの二次的要素で認証情報を強化し、ログイン活動の異常なパターンを監視してください。ベンダーに問い合わせて、POSへのアクセスに強固な認証が使用されているかどうかを確認しましょう。

入り口は常に監視
現在のPOS環境で利用可能な監視オプションを確認して実装します。リモートログインを監視して、基準に違反するログインは必ず確認しましょう。

ネットワークの分離
POS環境を社内LANから切り離して、インターネットから見えないようにします。

内部者および特権保持者による不正使用

要約

説明	許可されていないリソースの使用や悪質な目的での社内リソースの使用など、不正使用と判断されるすべてのインシデントがこのパターンに分類されます。このパターンは、組織内部者による不正使用が主ですが、内部者と共謀する部外者や特権を付与されたパートナーが関与することもあります。
標的になりやすい業界	公的機関、医療業、金融業
頻度	インシデント：10,489件、 データ漏洩を伴ったインシデント：172件
主な知見	このパターンの犯人はファイアウォールの内側にいて、社内データにアクセスできます。エンドユーザーの場合が多く、比較的簡単に社内LANから外部にデータを不正送信できます。内部者による犯行は発見が難しく、発見までに数カ月または数年かかるケースがほとんどです。

内部者および特権保持者による不正使用のパターンは、内部者と部外者が共謀して犯罪を行う数少ないパターンの1つです。

「不満を持つ内部者」と聞いて、どのような人物が思い浮かぶでしょうか。上司に不満を持つソフトウェア開発者。組織犯罪の誘いに乗った医療従事者。お気に入りの文房具を取り上げられたことを恨む男。いずれにしても彼らは、入念に構築された防御システムの内側から攻撃を仕掛けて、社内データに大損害を与えようとしているのです。

内部者および特権保持者による不正使用のパターンは、内部者と部外者（パートナーを含む）が共謀して犯罪を行う、数少ないパターンの1つです。図27は、データ漏洩の実行者別割合を示します。

最も多いのは内部者と部外者の組み合わせですが、パートナーが共謀者となる可能性も無視できません。目立った変化としては、外部実行者のみが関係する不正使用が増加したことです。従来はほぼ「TGYFBFTDHRA」[25]による犯行でした。今年は、犯罪組織が内部者をそそのかして銀行情報を聞き出すのではなく、利用者をそそのかすケースが見られました。これは部外者同士が共謀した詐欺ということになります。

25 解雇したがリモートアクセスが有効のまま残っている者（That Guy You Fired But Forgot To Disable His Remote Access）

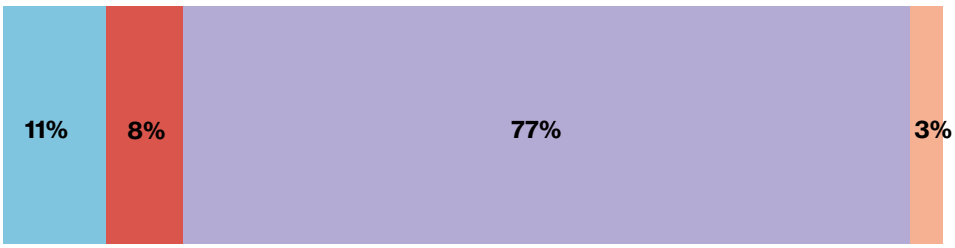


図27.

内部者および特権保持者による
不正使用でのデータ漏洩の実行者別割合
（n=172）

犯人は執事

内部者の話に戻りましょう。どのような人たちなのでしょうか。職務別に見ると、業務の必要上機密データにアクセスできるエンドユーザーが約3分の1を占めました。リーダーの役割（経営陣やその他の管理層）および高いアクセス権限を持つ役割（システム管理者や開発者など）は、ともにわずか14%です。ここでの教訓は、内部者については役職よりもアクセスレベル、そしてセキュリティ担当者の監視能力に注目すべきということです。毎日、全従業員に対して適度な疑惑の目を向ける必要があるということです。彼らが情報を持ち出したり、期待を裏切ったり、言い逃れをしたり、逃走したりすることは決してないと断言したいところですが、それはできません。ここで嘘をつくと、皆様が被害を受けることになるからです。

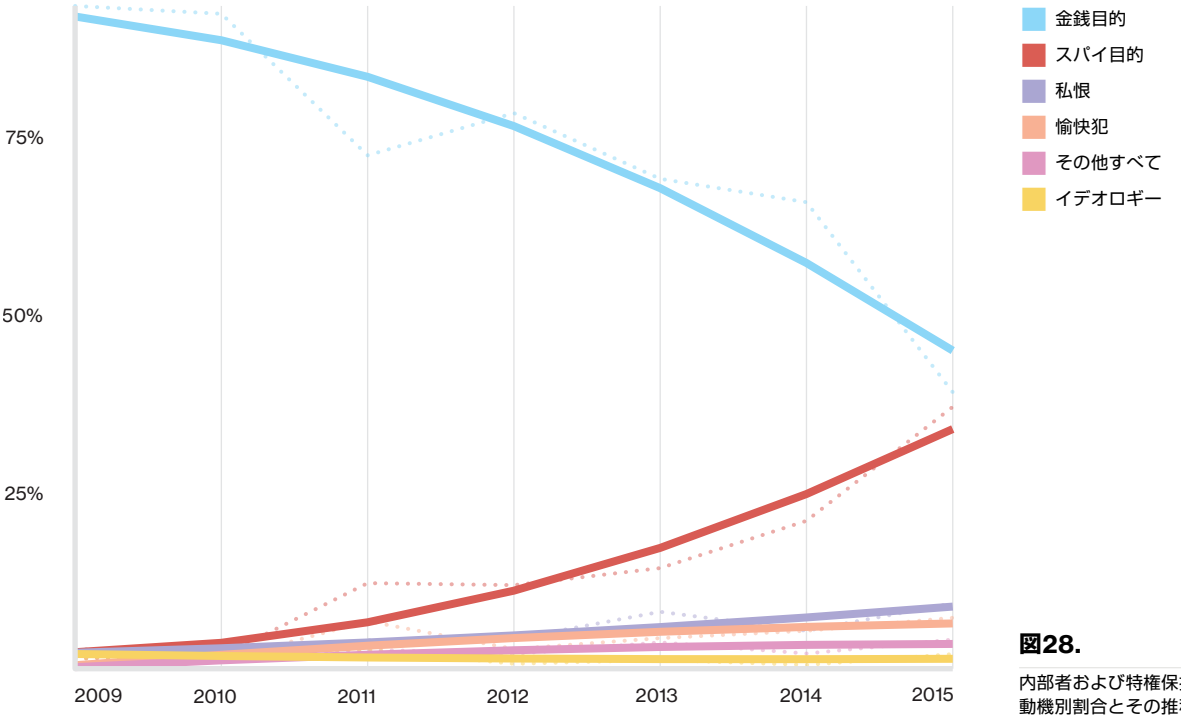


図28.

内部者および特権保持者による不正使用の
動機別割合とその推移（n=715）

動機と手口

犯人の動機は何でしょうか。一番はやはり金銭目的ですが（34%）、スパイ目的のデータ漏洩も増加しています（25%）。図28は、2009年以降の動機の推移を示します。金銭目的とスパイ目的が逆転しつつあるように見えるのは興味深いことです。このグラフにはデータセットの分析方法の進化も反映されていますが、内部者によるスパイ行為が増えているのは事実です。従業員による重要データの持ち出しを検知するプロセスの導入を検討しましょう。

図29は、内部者および特権保持者による不正使用の手口を示しています。手口の性質が判明している中では、一般的な特権の不正使用がトップを維持しています。これは、正当なアクセス権を本来の目的とは異なる形で悪用し、情報を入手する手口です。次に多いのがデータの不正処理です。たとえば、機密情報のメール送信や共有サービスへのアップロードなどです。ほとんどの場合は悪意からではなく、便利だからという理由で行われます。許可されていないハードウェアの使用とソフトウェアの使用が、3位と4位に入っています。許可されていないハードウェアはほとんどが、USBドライブ（保管した情報を後日に転職先に持参するなど）、またはハンドヘルド式のスキマー（飲食店の店員が客のペイメントカードデータを記録するときに使う装置）です。

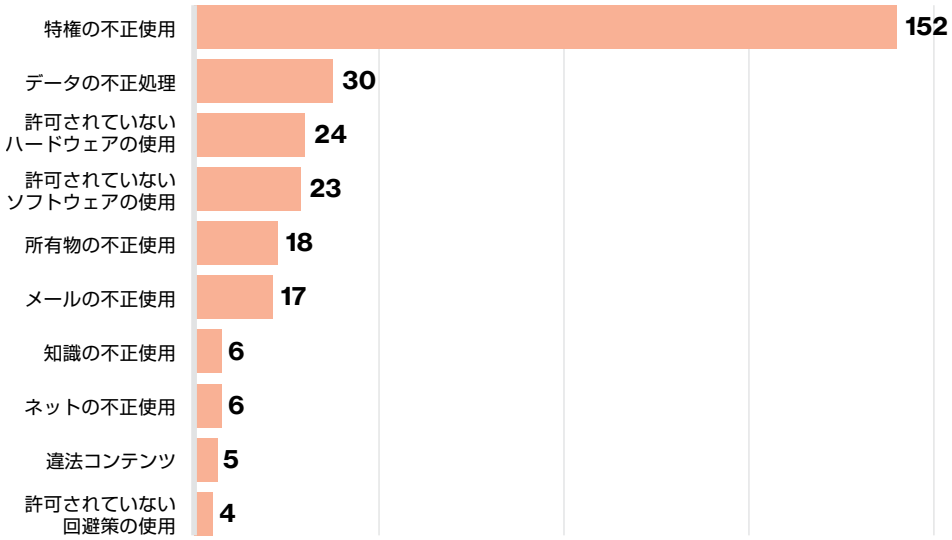


図29.

内部者および特権保持者による不正使用で多く使われた手口（n=230）

内部者の犯行は検出が最も難しいインシデントです。図30に示す、発見までの時間がそれを証明しています。ほとんどのインシデントでは発見までに数カ月以上かかっています。DBIR調査対象のデータセット全体でも、発見までの時間が最も長いのが内部者による犯行です。過去の推移を見ると、数日以内が減って数カ月以内が増えていることがわかります。以前は、銀行の従業員が詐欺者に情報を提供するケースが多く、これらのケースは発見されるのが早かったのです。この変化は「不正検出プロセスを定めないとこうなるぞ」という警告と言えるでしょう。

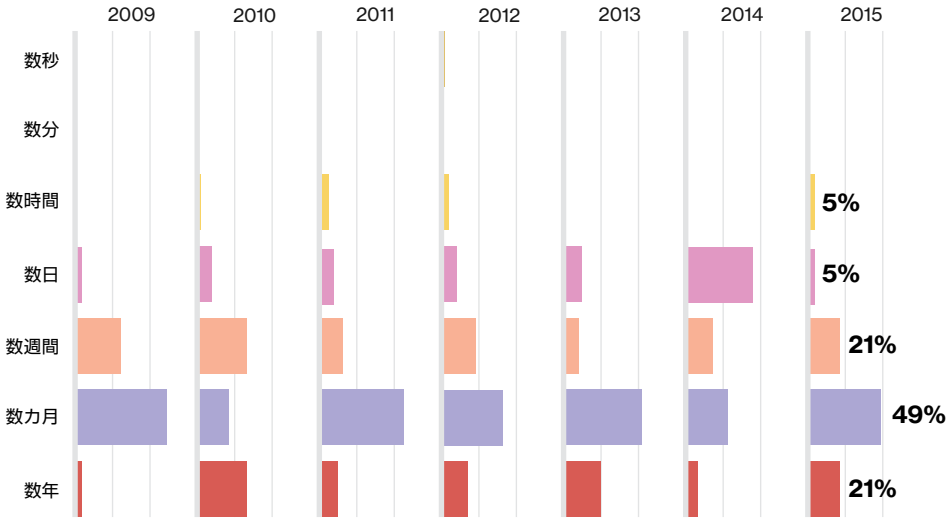


図30.
内部者および特権保持者による不正使用の発見に要する時間とその推移（n=358）

推奨される対策

従業員の行動に注意する

従業員を大切にして、社員旅行で交流を深め、金曜日にはベーグルを差し入れしましょう。ただし、日常業務で特権を持っている従業員、特に金銭価値の高いデータ（金融口座情報、個人情報（PII）、ペイメントカード情報、医療記録など）にアクセスできる従業員の監視は怠らないことです。

USBを警戒する

データセットでは、従業員が退社後に監査を実施したところUSBドライブによるデータの持ち出しが発覚したケースが数多く見られました。これらのポータブルデバイスの使用は、事後ではなくて事前に検知できるようにしましょう。

データとアクセス権の両方に注意を払う

データの保存場所を把握していなければ、データを適切に守ることはできません。さらに、場所を把握していても、そのデータに誰がアクセスできるかを把握していなければ、ほとんど意味はありません。データの保存場所をしっかりと把握すると同時に、アクセス権を誰にどの程度与えるかを慎重に検討しましょう。駐車係に車のキーは預けても、クレジットカードを預けたりはしないはずです。

データの保存場所を把握していなければ、データを適切に守ることはできません。

データ漏洩に対する厳罰化の現状

Mishcon de Reya法律事務所が過去12カ月間に取り扱った国際的詐欺や企業犯罪のほぼすべてに、コンピュータ機器と電子データの不正使用が関わっていました。サイバー犯罪の被害に遭ったある企業では、システムの停止、盗まれた重要データの不正使用、補償を求める関係者からの訴訟への準備によって収益が悪化し、短期間のうちに財務危機に陥りました。さらに今後、顧客からの信用低下が大きな影響を及ぼし、企業イメージの悪化が予想のつかないダメージをもたらすでしょう。

これだけのインパクトがあるにもかかわらず、この問題に対する各国政府の対応は大きく後れを取っています。多くの人が現在の法律は技術の進歩に追いついておらず、十分な制裁措置が定められていないと考えています。また、国境を超えてデータをやり取りする企業にとっては、国による法律の違いが混乱をもたらし、法令違反のリスクを高めています。

米国には個人情報とデータに関する保護法が多数存在しますが、包括的かつ具体的な連邦法はなく、関連法の施行についてもどの省庁に責任があるのか不明確な状態です。英国はEUメンバーとして、1998年データ保護法に1995年EUデータ保護指令（95/46/EC）を組み込んでいます。その施行と情報権利保護の責任は情報コミッショナー事務局（ICO）が持ち、ICOは個人情報の窃取と売買を抑止するために罰金ではなく実刑判決を課すなどの制裁強化を主張しています。しかし現時点では、データ保護法における英国での報告義務は任意であり、深刻なデータ漏洩に対してICOが課すことのできる最も厳しい処分は50万ポンド（約70万ドル）の罰金にとどまっています。しかも、個人情報の不正使用を抑止するために十分な強制力はありません。

法執行機関がサイバー犯罪に対して幅広く適用できる犯罪関連法は他にもあります。しかし、国境を越えた犯罪の場合は各国の当局が協力して犯行を調査し、犯人の引き渡しと起訴を行う必要があるため、管轄権とコストの問題が適切な制裁の実行を阻んでいます。さらに、犯罪者は大量データの暗号化、プロキシサーバーによるIPアドレスの隠蔽、セキュリティ保護されたVPN、匿名での通貨交換などの証拠隠滅手段を駆使しています。そのため、起訴に必要な証拠を集めようとしても、たいていは最初のハードルでつまずいてしまいます。残念ながら、サイバー犯罪の規模や発生率を抑えるために有効な法律が十分に整備されるまでにはまだまだ時間がかかりそうです。

Hugo Plowman氏、Rob Wynn Jones氏
（Mishcon de Reya法律事務所パートナー）

人的ミス

要約

説明	意図的でない行為によって、情報資産のセキュリティデータが直接的に侵害されるインシデントがこのパターンに分類されます。機器の紛失はこのパターンではなく、物理的窃盗および紛失のパターンに含まれます。
標的になりやすい業界	公的機関、情報産業、医療業
頻度	インシデント：11,347件、 データ漏洩を伴ったインシデント：197件
主な知見	最も多いのは、紙とデジタル形式の両方を含む情報の送信ミスです。

データの損失をもたらすミスには共通点が多いため、独自のパターンとして取り上げる価値があると判断しました。

人はミスを犯すもの
思い上がりや虚勢がはびこる情報セキュリティの世界にあっても決して聞くことのない言葉は「うちの従業員は絶対にミスはしません」です。なぜなら、誰でもミスをするからです。このセクションでは「しまった、間違えた」で起こるデータ漏洩について考察します。VERISに親しんでいる方ならばご存じかもしれませんが、「人的ミス」に分類される行為はかなり限定されることに注意してください。パッチ適用プロセスや検証を怠ってハッキングされた場合は、ミスには分類されません。その行為または行為を怠ったことは、データ漏洩の直接的な原因ではないからです。（つまり、攻撃者はハッキングに続いて別の攻撃を実行する必要があります。）報告されるインシデントを一律に「セキュリティ実践上の不注意が原因のミス」と分類したくはありません。そこで、ある行為がデータ損失の直接的な原因となったケースのみをこのパターンに分類しています。また、データの損失をもたらすミスには共通点が多いため、物理的窃盗および紛失（43ページ）と区別して独自のパターンとして取り上げる意義があると判断しました。この分類方法に従うと、公的機関による何千何万もの送信ミスが話題を独占してしまうため[26]、今回は興味深い事実が隠されていないかを探るために、これらを取り除きました。

データの取り扱いミスが生産性を低下させる（略してDERP（Data Errors Reduce Productivity））
このパターンは長年、送信ミス、公開ミス、廃棄ミスというトリオの独壇場でした。図31に示すとおり、今年もこの3つが上位に入っています。昨年、私たちは調査範囲を広げて、攻撃とは無関係な突発的なトラフィック急増による可用性低下を示すデータを対象に加え

26 公的機関の送信ミスのインシデントはn=10,094でした。

ました。すると今年は、そういった帯域圧迫ミスがトップとなり、その後にメールや文書の誤送信が続く結果となりました。送信ミスに分類されるケースでは、多くの人がOutlookの「宛先」フィールドが備えるオートコンプリート機能を責めたいことでしょう。

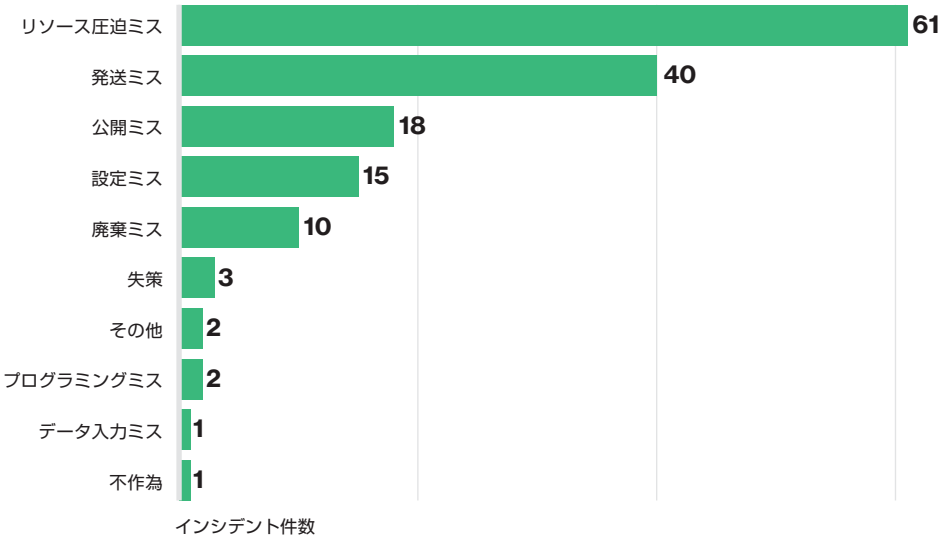


図31.

人的ミス（公的機関を除く）の内容トップ10（n=153）

公開ミスは、意図していない人（すべてのインターネットユーザーなど）が情報を見られる状態にしてしまうミスで、今年もトップ5に入っています。設定ミスも同じくトップ5に残っています。わかりやすい例を挙げれば、ファイアウォールのルールを誤入力したことにより、機密ファイルが保存されているサーバーに本来は一部のホストだけがアクセス可能にするところを、社内ネットワーク全体からアクセス可能にしてしまうといったミスです。

トップ5を締めくくるのは廃棄ミスです。大半は印刷書類の廃棄ミスです。誰でも簡単に読むことができ追跡も難しいため、このインシデントは重大です。今年のデータセットでは多くはありませんでしたが、デバイスを廃棄する際にハードドライブのデータを適切に消去しないというミスもあります。これについては標準作業手順を定めて対処する必要があります。

データ漏洩のガイドライン：VERISで「data_disclosure」（データ漏洩）フィールドが「Yes」（あり）の場合、意図しない人にデータが実際に見られたかアクセスされたことを示す事実があるということです。この変数がどのように設定されるかを以下の例に示します。

- 暗号化されていないデバイスの窃盗または紛失：Potentially（可能性あり）
- 暗号化されたデバイスの窃盗または紛失：No（なし）
- 書類またはデバイスの不適切な廃棄：Potentially（可能性あり）
- 公開Webサイトへの秘密データの不用意な公開（表示された形跡なし）：Potentially（可能性あり）
- 封書の宛先ミスで送り先不明、未回収：Potentially（可能性あり）
- 封書の宛先ミスで誤った受取人が開封：Yes（あり）
- 「No」（なし）または「Potentially」（可能性あり）のシナリオでも、部外者がそのミスを発見した場合、「Yes」（あり）に変更されます。たとえば、部外者が公開ミスを指摘した場合、この定義ではデータは漏洩したとみなされます。

人的ミスによるデータ流出を発見するのは、多くの場合、ミスの影響を受けた利用者です。他人の個人情報や医療情報を受け取った利用者が送信元の企業・組織に連絡することでミスが発覚するケースがほとんどです。図32は、人的ミスによるデータ漏洩の主な発見方法を示しています。

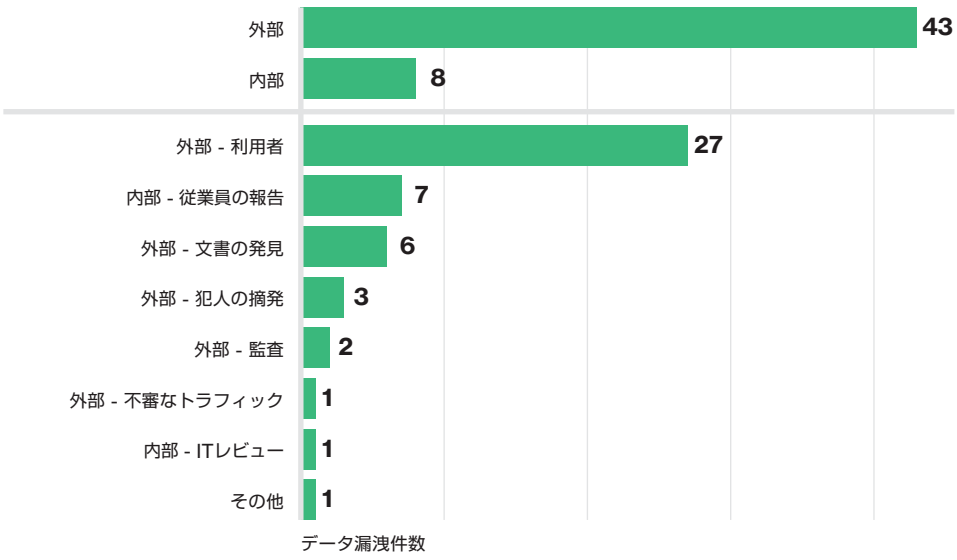


図32.
人的ミス（公的機関を除く）による
データ漏洩の発見方法（n=52）

推奨される対策

人的ミスについて推奨される対策は、ばかばかしく思えるかもしれません。「2度としないでください」とか「もっと注意してください」などと言って効果があるとは、誰も思わないでしょう。それでも、ミスを最小限に抑えるために役立つ常識的なアプローチがいくつかあります。ミスに付け込もうとする者へのせめてもの対抗手段は、付け込むすきを与えないことです。

ミスから学ぶ

起こりがちでやっかいなミスを記録しておき、社内クリスマスパーティーで同僚をからかう題材にするのではなく、もっと有意義なことに使いましょう。たとえば、セキュリティ意識向上プログラムの教材作りに役立てましょう。「ジムはまた全員にcc:でメールを送信して叱られたって？」そんなときこそチャンスです。もちろんジムの名前は伏せておきましょう。よくある「しまった」という状況を、セキュリティトレーニングに活かしてください。

資産を廃棄するときには必ず、IT部門が厳格な手順でチェックしてください。

対策を練る

過ちを記録しておく習慣は、人生ではともかく、有能なIT部門には必要です。これを身に付けたら、件数の多いミスの発生頻度と被害を最小限に抑える効果的な方法を考えましょう。

廃棄時に注意

資産の処分時にすべての保存データを消去する手順を定めた作業書を作成し、廃棄や売却前には必ず確認しましょう。すべての資産について、IT部門が厳格な手順で何重にもチェックするようにしてください。今年のデータセットでも、個人情報やその他の機密データが満載されたままの資産が他者に売却されるケースが数多く見受けられました。

物理的窃盗および紛失

要約

説明	読んで字のごとく、情報資産が行方不明になったすべてのインシデントがこのパターンに分類されます。置き忘れと窃盗の両方を含みます。
標的になりやすい業界	公的機関、医療業
頻度	インシデント：9,701件、 データ漏洩を伴ったインシデント：56件
主な知見	インシデントでは被害件数が最も多いのはノートPCです。一方、データ漏洩を伴ったインシデントでは、追跡が難しく簡単に内容を読める文書が最多です。紛失は窃盗よりも100倍以上多い結果になりました。

暗号化されていないデバイスを紛失して戻ってこなかった場合、データが漏洩しているかどうかを判断するのは困難です。

人間の悲しい性質

小さいお子様がいらっしゃるのなら、学校に用事があるときに、「忘れ物預かり所」に立ち寄ってみてください。恐ろしい光景を目にするでしょう。大量の服（生徒1人あたり2～3点）らしきものが大きい箱に詰め込まれ、持ち主に忘れ去られた古いコート、帽子、手袋など正体不明の布切れがさまよい続けているかもしれません。人はいつでも、ものを紛失しているものです。昔から周知のとおりですし、取り立てて言うほどのことでもありません。しかし、企業・組織にとっては実に深刻な悩みの種です。少なくとも新しいノートPCを支給する必要に迫られます。不運な場合には、紛失したデバイスに個人情報がなかったか、保存データが暗号化されていたかを調べ回るはめになります。たとえ従業員がそれなりに注意していたとしても、世の中には代金を支払わずに欲しい物を狙う人がいるのです。このパターンを川柳にしてみましょう。

人よりも
信頼すべきは
暗号化

何が危険なのか？
データ漏洩の詳しいガイドラインについては、「人的ミス」セクション内のコラムをご覧ください。暗号化されていないデバイスを紛失した場合、データ漏洩があったかを判断するのは困難です。危険な状態にあるかといえば、もちろんそうです。何しろデータを守るのは頼りない門番、つまりパスワードだけなのです。それでも私たちの定義では、デバイス紛失を「データ漏洩」に分類することはできません。このパターンにおけるデータ漏洩件数とインシデント件数の差が大きいということは、実際のデータ漏洩件数よりもずっと多くのデータが危険な状態にあることを示しています。

このパターンのインシデントで最も被害件数が多いのはノートPCです。ただし、データ漏洩を伴ったインシデントに限定すると、印刷書類がトップになります。発見者または窃盗犯が確実に内容を読めるからです。

物理的窃盗および紛失は古くからの問題で、多くは被害者の職場（39%）または私用車（33.9%）で起きています。つまり、狙って盗まれるよりも、目を離した隙に紛失するケースがずっと多いということです。今年のデータでも、紛失は窃盗よりも100倍以上多い結果になりました。いずれにしても行き着く先は同じです。ノートPCが戻ってくることはなく、忘れ物預かり所にも届いていないでしょう。

今年のデータでも、紛失は窃盗よりも100倍以上多い結果になりました。

推奨される対策

とにかく暗号化
モバイルデバイスやリムーバブルメディアはディスク全体を暗号化しましょう。設定時の標準手順に含めるのがお勧めです。

トレーニングで意識向上
ユーザーのセキュリティ意識や状況認識力は向上することができると信じてください。オリエンテーションや定期的なトレーニングで、資産の物理的なセキュリティ対策について教育しましょう。車にノートPCを放置しないことも徹底します。泥棒にとって車のウィンドウとは、車内をのぞき見る場所であり、欲しい物があったら壊して取り出せる場所なのです。

紙の時代は終わり
仕事で使う印刷書類は厳格に管理しましょう。データの分類ルールを定めるとともに、機密データの印刷と転送を罰則のあるポリシー違反とします。機密データが含まれた文書を印刷するときは、トークン化によって機密データを一意の識別子に置き換えることを検討してください。

クライムウェア

要約

説明	他の具体的なパターンに当てはまらないマルウェア関連インシデントがこのパターンに分類されます。インシデントの大半は金銭目的の無差別攻撃です。利用者に影響を及ぼすことが多いのも特徴です。「典型的」なマルウェア感染はこのパターンに該当します。
標的になりやすい業界	公的機関、情報産業、金融業
頻度	インシデント：7,951件（二次的動機で追加6,858件）、データ漏洩を伴ったインシデント：49件
主な知見	クライムウェアのパターンでは、外部の犯罪組織による金銭目的のインシデントが今年も多く見られます。主な攻撃には、C2マルウェアによるデバイスの乗っ取り、ランサムウェアのインストール、認証情報の盗み出し、ボットネットへの登録などがあります。

ほとんどは、詳細なフォレンジック調査の対象にならない、頻度は高いが影響は小さい迷惑なだけのインシデントです。

協力企業・組織の拡大とパターンの定義以来ずっと、クライムウェアについては、件数は豊富なものの詳細は乏しいままでした。クライムウェアに関連するインシデント情報の大半は、さまざまな企業・組織からCERT/CSIRT組織を経由して入ってきます。そのほとんどは、詳細なフォレンジック調査や文書化および分類の対象にならない、頻度は高いけれども影響は小さいインシデントです。私たちは、情報の多い少数のインシデントを重点的に分析して、それに基づいて残りのインシデントの性質を推測しています。今年はセキュリティベンダー各社の協力を得てマルウェアデータを提供していただきました。Cylance社、Fortinet社、ICSAラボ、Palo Alto Networks社、Tenable社の皆様、まことにありがとうございます。そのデータを徹底調査して、いくつかの領域について詳細を明らかにしたいと思います。

図33に示すとおり、判明している範囲で件数の多いマルウェア機能トップ5は、C2、ランサムウェア、スパイウェア/キーロガー、バックドア、データエクスポートでした。他の標的に対してDoS攻撃を実行するマルウェアは、二次的動機を持つものとして除外されています（8ページを参照）。もし除外しなかったら、デバイスが未知の標的にトラフィックを送り込んでいると確認された6,800件のケースが他を圧倒していたでしょう。

2位のランサムウェアは今年最も順位を上げており、引き続き動向を注視する必要があります。念のためにご説明すると、ランサムウェアは、感染したデバイス上のファイルを暗号化します。特に悪質なものになると、デバイスが接続するファイル共有サービスに保存されているファイルも暗号化します。その後、攻撃者がデータのロック解除と引き換えに金銭を要求してきます。ランサムウェアはDoS攻撃を使った恐喝とよく似ています。ただしその多くは無差別で、企業・組織も一般ユーザーも標的になる点が異なります。

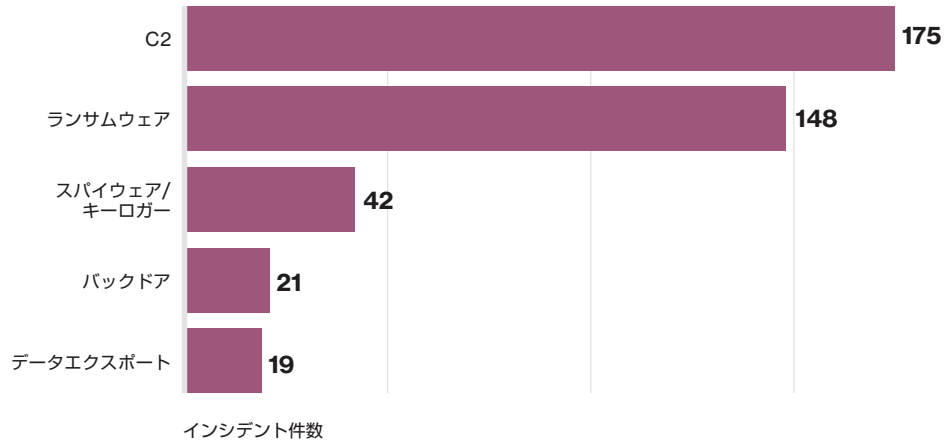


図33.

クライムウェアでよく使われるマルウェア機能トップ5（n=382）

トップ5の残り4つは通常、銀行を標的とするトロイの木馬とともに一体となって攻撃を行います。このマルウェアー味を操る犯罪組織は一連の攻撃を用意しています。感染デバイスを操作し（C2/バックドア）、銀行の認証情報を入力して（キーロガー）、送信する（データエクスポート）という手口を利用するのです。今年はこれら5つの機能が上位を独占していますが、特に新しい傾向や増加の兆しは見られません。

クライムウェアの主な侵入経路は3つあります。悪質なファイルが添付されたメール、ドライブバイダウンロードが仕掛けられたWebサイト、ドライブバイコードが仕込まれたWebページとそのページへのリンクが埋め込まれたメールを組み合わせたもの、の3つです。

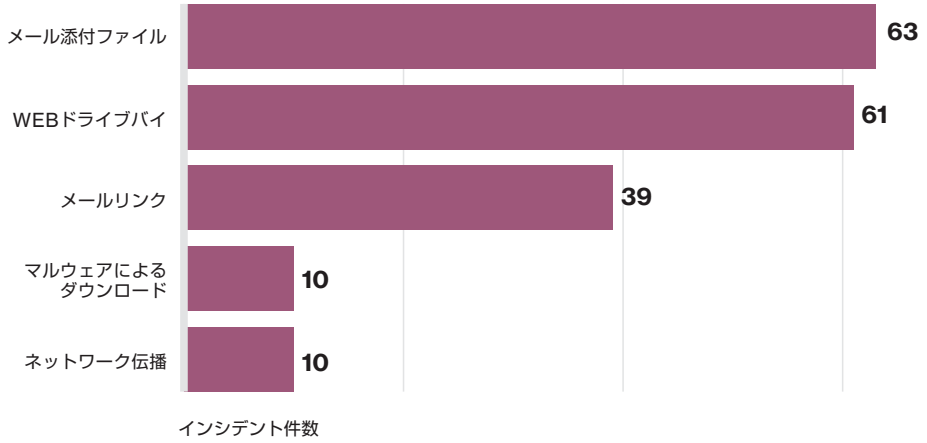


図34.

クライムウェアでのマルウェア侵入経路トップ5（n=135）

ランサムウェアを簡単に手に入れる方法
平凡なマルウェアについては、インシデント対応としてドライブを複製するなど手間暇かけて詳細を調査するメリットがほとんどないため、詳細が乏しいことはすでにご説明しました。しかし、一部のランサムウェア事例から経路が判明し（お見事！）、具体的にはFlashが悪用されたこともわかりました。運の良いことに、私たちの手元には悪用されたバージョンのFlashと最新バージョンのFlashがありました。そこで「世間の人々はFlashの更新がどのくらい苦手なのか調べてみよう」と考えました。実際、非常に苦手なことがわかりました。サンプルサイズは小さくても、この結果はかなりのインパクトがあります。多くの人を非難するつもりはありませんが、図35にグラフを示します。調査対象になったブラウザの半数以上で、最新バージョンよりも1年以上古いバージョンのFlashが使われています。つまり、ドライブバイダウンロードを仕掛けるには、F1チャンピオンであるルイス・ハミルトン並みのスピードは必要なく、荷馬車並みのスピードで十分だということです。ただし、定期的に更新を行っていても油断は大敵です。最新バージョンで被害に遭った事例や、更新が2週間遅れただけで被害に遭った事例もありました。

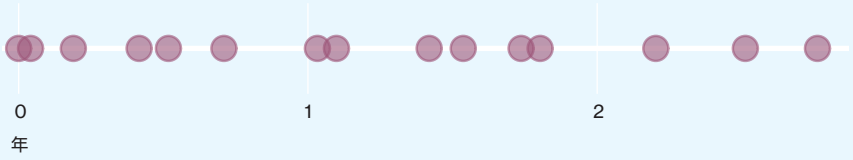


図35.
悪用されたFlashバージョンのリリース日から悪用時点における最新バージョンのリリース日までの期間（n=15）

このセクションの残りの部分では、インシデント以外のセキュリティデータを分析してマルウェアをさらに詳しく調べていきます。まずは、ハッシュの一意性について、私たちが昨年発見した事実を再確認したいと思います。

ハッシュの解釈
私たちは昨年、ハッシュが一意だからといって、国家を後ろ盾とする超精鋭のマルウェア特殊部隊があなたを狙っているわけではないと宣言しました。多くの方の想像を壊してしまったことでしょう。

今年も、多数の協力企業・組織から提供されたマルウェアレコード4,000万件のハッシュを比較した結果、企業・組織間で一致するものはほとんどないと判明しました。共通点を調べたところ、約380万種類の一意のハッシュから、複数の企業・組織にわたる約2万種類のMD5ハッシュを発見しました。

次に、ハッシュの使用期間を調べてみたところ、やはり短いことが判明しました。

「そして突然、フッと悪魔は消えてしまった」（映画『ユージュアル・サスペクツ』より）
次に、ハッシュの使用期間を調べてみたところ、やはり短いことが判明しました。1つのハッシュが初めて検出されてから最後に検出されるまでの時間を調べ、時間別のハッシュ数をグラフにしたところ、図36のとおりロングテールの形を示しています。つまり、大部分は非常に短時間のうちに使用され、その後すぐにネットワークから消えてしまうのです。

大きいデータセットの1つを分析した結果、99%のマルウェアハッシュはわずか58秒以内の間しか検出されませんでした。実際、ほとんどのマルウェアは1回しか検出されていません。これは、攻撃者が検出をすり抜けるためにどれだけ頻繁にマルウェアコードを変更しているかを示しています。

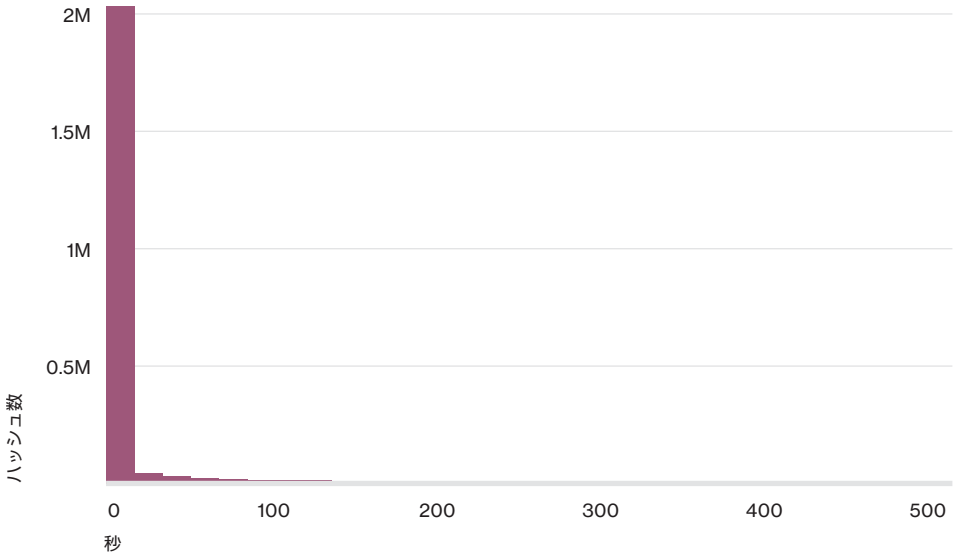


図36.
生存期間（秒）別のハッシュ数（n=230万）

推奨される対策

ここでもパッチ
多くの場合、攻撃者はマルウェアを送り込んだ後で既知の脆弱性を悪用します。大きな被害を防ぐには、OS、アプリケーション（特にブラウザ）、セキュリティツールの最新パッチを適用するように心掛けましょう。

マルウェアハッシュの生存期間は短いため、対応は困難です。

実行させない
悪質な実行ファイルから身を守るには、スクリプトやマクロを実行しないようにプログラム（文書編集アプリケーションなど）を設定する方法から、メールに添付された実行可能ファイルやその他の危険な拡張子を持つファイルをメールサーバーで分離/削除する方法まで、さまざまな選択肢があります。とにかく、そのようなファイルを実行させないようにして、攻撃の経路を減らすことです。

正面から取り組む
「見ざる、聞かざる、言わざる」は、有効な振る舞いとは言えません。きちんと見て、聞いて、話し合いましょう。昨年のDBIRでも申し上げましたが、社内でマルウェアデータを記録して分析し、どのような種類のマルウェアが侵入しているか、そして可能であればその侵入経路を調べることをお勧めします。

ペイメントカードスキミング

要約

説明	ペイメントカードの磁気ストライプを読み取る装置（ATM、ガソリン給油機、POS端末など）にスキミング機器を物理的に取り付けた（タンパリング）すべてのインシデントがこのパターンに分類されます。
標的になりやすい業界	金融業、小売業
頻度	インシデント：102件、 データ漏洩を伴ったインシデント：86件
主な知見	今年もこのパターンに大きな変化はありません。実行者は東ヨーロッパ関係者が多く、最も標的になりやすいのはATMで、発見は外部からがほとんどです。

データセットで見つかったペイメントカードスキミングの70%は犯罪組織による犯行と考えられます。

同じ事の繰り返し
変化と混乱が渦巻く世界で、常に変わらない物事があるということは、一種の安心感を与えてくれます。トーストを落とせばバターを塗った面が床につき、急ぐときほどトイレは遠いように、スキミングの手口もまた昔からほとんど変化していないのです。攻撃者はおそらく、「壊れていないものを直すな」の教えを実践しているのでしょう。ペイメントカードスキミングは依然として、犯罪組織にとっても、ときどき単独で盗みを働く者にとっても（不遇で気の毒な子なのでしょう）、成功しやすく実入りの良い攻撃となっています。

調査対象のデータでは、インシデントの多くが米国の法執行当局から報告されているため、被害は米国に集中しています。ただし、大部分（約70%）は犯罪組織による犯行であり、その一部では犯罪組織と結びついている国を特定できます。図37に示すとおり、犯罪組織の関与が確認できた過去数年間の攻撃では、関連国として東ヨーロッパ（ルーマニアとブルガリア）が多数を占めています。

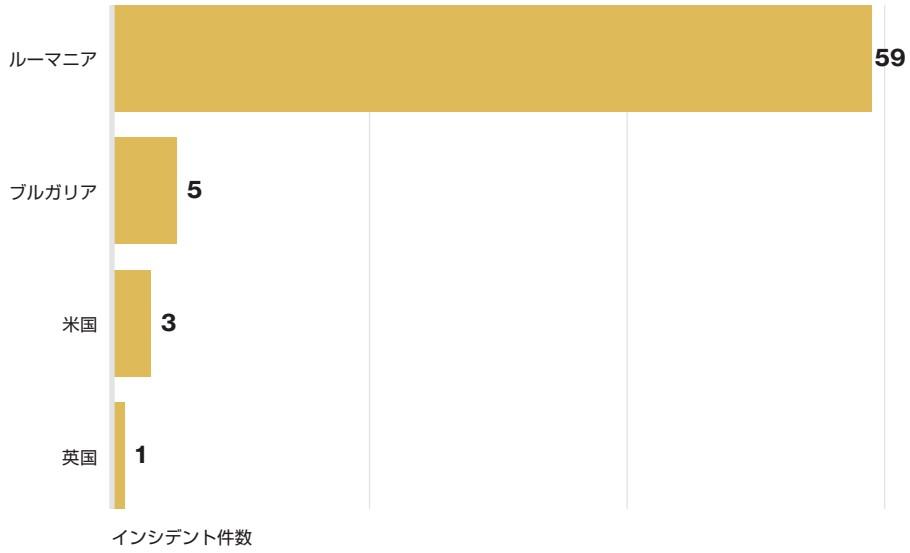


図37.

カードスキミングの実行者が関連する国（n=68）

このパターンでは標的の傾向も過去と変わりません。ATMが最多（94%）、続いてガソリン給油機（5%）、そしてPIN入力デバイス（PED）がごくわずか（1%）の順になっています。また、90%以上のケースで物理的な「監視」の手口が使われていました。これは、ピンホールカメラを標的デバイスに取り付けてPINコードを読み取る手口が多いためです。これまでと同様に、スキミング機器のほとんどは非常に精密かつ巧妙に仕掛けられているため、裸眼では（コンタクトや眼鏡をつけていても）検出が極めて困難か、ほとんど不可能です。図38に示すように、発見がほぼ外部からで、その中でもさまざまなアルゴリズムとCPP（Common Point of Purchase）手法を活用した不正検出が多い理由は、このあたりにあるのかもしれません。

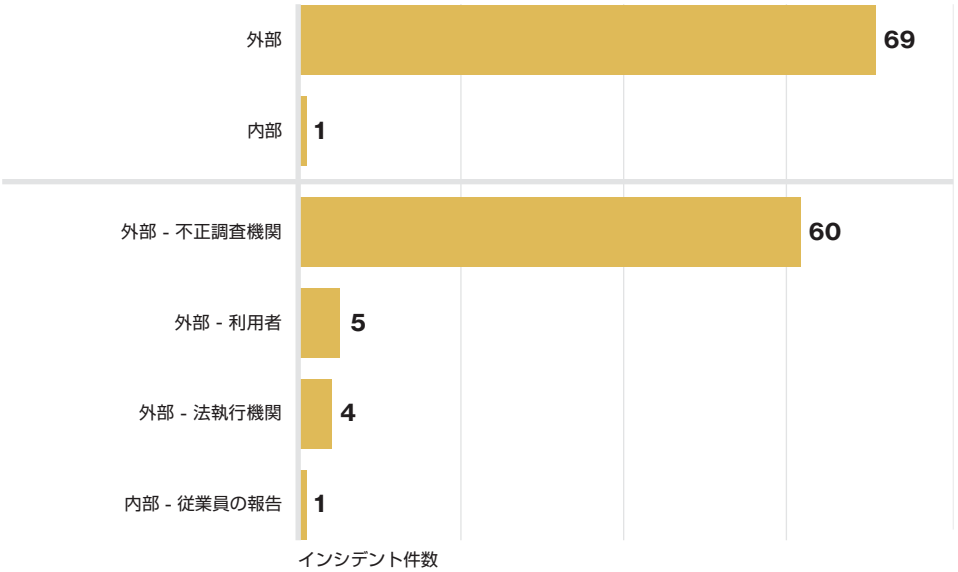


図38.

カードスキミングの発見方法（n=70）

ついに…悪報です

昨年、発見までの時間は数週間や数カ月から数日へと確実に短縮されているとご説明しました。しかし、その傾向は続きませんでした。今年は「数週間」がすっかり定着しています。今年のデータセットでは内部からの発見件数が大幅に減り、その分、不正調査機関による発見件数が増えています。その理由が、被害に遭った企業・組織の従業員の視力が原因なのか、または不正を発見した従業員がスキミング機器はすぐに取り外しても警察（またはこの調査の協力企業・組織）には通報しなかっただけなのか、どちらなのかは不明です。内部者がスキミングを直接発見すれば話は早いのですが、CPPによってスキミングの兆候をつかむには時間がかかります。そのため、発見までの時間の長期化と外部からの発見の増加には相関関係があると考えてよいでしょう。

内部からの発見件数が大幅に減り、その分、不正調査機関による発見件数が増えています。

推奨される対策

サービス提供側の対策

- 改変されにくい端末を購入する：端末の中には改変が容易なものもあります。ATMの一部のモデルは改変を防止する設計になっています。端末を新しく購入するときは、この点をチェックしましょう。
- 不正を発見しやすい管理方法を採用する：できるだけ、不正が検出しやすくなる手段を講じましょう。たとえば、端末の扉の開閉部分にシールを貼る、ATMやガソリン給油機付近にビデオカメラを設置して不審人物を監視するなどの手段があります。
- 定期点検を実施する：ATMへの改変などを物理的に点検するプロセスを定めましょう。従業員に不正の痕跡を発見する方法を教育し、業務スケジュールに点検を組み込みます。

消費者側の対策

- PINを盗撮から守る：PINを入力するときは、ピンホールカメラで指の動きを盗撮されるのを防ぐため、手で隠して入力しましょう。
- 直感を信じる：装置に違和感を覚えたら、利用を中止しましょう。不正の痕跡を見つけるのは難しくなってはいますが、方法はあります。怪しいと思ったらサービス提供者に連絡して、別のサービススポットに移動することをお勧めします。

サイバースパイ活動

要約

説明	ネットワークやシステムへの不正アクセスのうち、国家機関に関わる攻撃者と結びつくインシデント、またはスパイ活動の目的が明らかであるインシデント、あるいはその両方の要素を合わせ持つインシデントがこのパターンに分類されます。
標的になりやすい業界	公的機関、情報産業、製造業
頻度	インシデント：247件、 データ漏洩を伴ったインシデント：155件
主な知見	スパイ活動の初期段階では、他の多くのパターンと同じ手口で攻撃経路が確保されます。その後の攻撃は、攻撃者の最終目的によって異なります。

実行者の多くは国家機関に関わるグループですが、競合他社や国家も登場しています。

サイバースパイの特徴
ジェームズ・ボンドとサイバースパイとはずいぶん違います。マシンガンになる傘は持っていないし、切れ味のよい帽子をかぶる部下を引き連れてもいないし、催涙ガスを仕込んだスーツケースも持ち歩いていません。

それでもサイバースパイは、世界各地で多数の被害者を出しています。盗んだデータを火山に見せかけた地下の秘密基地に送ることはないとしても、スクリプトキディのような稚拙な初心者よりはるかに狡猾で執拗であることは確かです。サイバースパイの人物像を詳しく知りたい方は、「サイバースパイ調査書」コラムでご紹介している、一部のDBIR協力企業・組織とその他機関による調査研究書をご覧ください。

まずは、サイバースパイ活動の定義についてご説明します。サイバースパイ活動とは、外部の実行者が標的企業・組織のネットワークに侵入して、機密情報や企業秘密を探し回る行為を指します。一方、従業員がデータベースから顧客情報を盗み出して自営のレモネード屋台を開くといった場合は、内部者および特権保持者による不正使用のパターンに該当します。実行者の多くは国家機関に関わるグループですが、犯罪組織、競合他社、国家も登場しています。図39は、標的になることの多い業界を示します。上位は昨年と同じ顔ぶれで、今年は1位が公的機関で、後には製造業、専門サービス業、情報産業と続きます。5位以下には、件数は少ないものの各業界が並んでいます。つまり、他人の利益になるものを持っていればサイバースパイの標的になりうる、ということです。

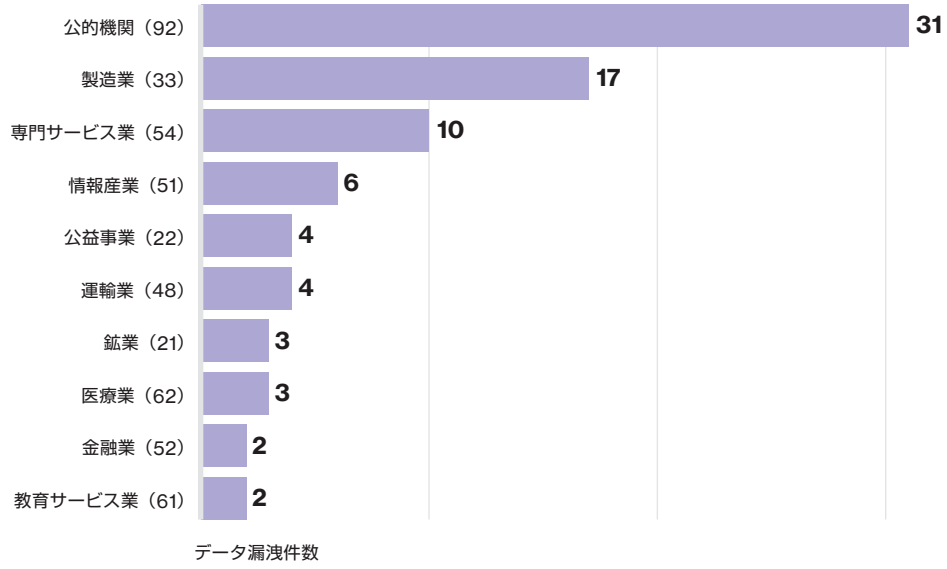


図39.

サイバースパイ活動による
データ漏洩の業界別件数。かっこ内の
数字はNAICS業界コード（n=86）

高度な攻撃のための入念な準備

最初に、これからご紹介する具体的な手口の説明は、初期段階の足場確保の活動に重点が置かれていることをお断りしておきます。サイバースパイ活動によるデータ漏洩では、通常、攻撃者はまず信頼のフィッシングによってバックドアマルウェアやC2マルウェアを送り込み、攻撃経路を確保します。フィッシングを他の多くの手口と比べると、先行活動として多くの利点が見られます。何よりも、短い時間で標的ネットワークに侵入できます。また、企業・組織内の特定の標的に攻撃を仕掛けることもできます。さらに、業務のためにインターネットに接続する必要のあるサービスを利用することで、多くの防御をすり抜け、企業・組織内のエンドポイントにリモート攻撃の拠点を確立できます。

フィッシングには、サイバースパイの先行活動として多くの利点があります。わずかな時間で標的ネットワークに侵入できるほか、特定の標的に攻撃を仕掛けることもできます。

マルウェアを送り込む手段としては、フィッシングの他にブラウザも使用されます。ブラウザまたは一般的なプラグインの脆弱性を突いたドライブバイダウンロードによって、社内LANに接続されたデスクトップPCにマルウェアを送り込み、そこから攻撃を仕掛けます。特定の個人を標的にするのは難しいにしても、特定の部署の従業員がよくアクセスしそうなサイトを利用するなら成功率は上がります。また、Webサイトの侵害に無差別なクライムウェア攻撃を利用できるのも、ドライブバイダウンロードの利点です。

足場を確保した後で攻撃者がとる行動は、目的のデータの保存場所と、目的達成のために乗り越えるべき障害次第です。もちろん社内には、運動会でよくある平凡な障害物競走ではなく、世界最高峰の障害物レース「ウォリアーダッシュ」並みに多種多様な障害を設けることが重要です。この防御のための障害については後ほど詳しくご説明します。図40から、足場の確保後に行われる、ネットワークのフットプリンティングと盗んだ認証情報の悪用による攻撃の手口を多少読み取ることができます。認証情報を盗む手口について詳細は不明ですが、未特定のマルウェアが関わるデータ漏洩が多数あることから、キーロガーとパスワードダンパーが使われていると推測されます。

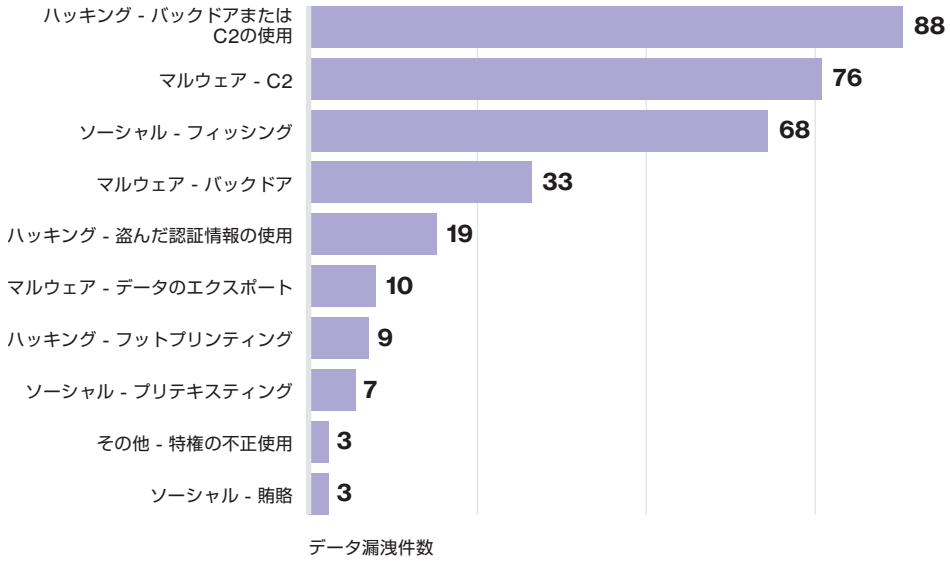


図40.
サイバースパイ活動で多く使われた脅威活動（n=154）

狙われるデータ

サイバースパイ活動によるデータ漏洩の対象で最も多いのは企業秘密（別名、専有情報）で、90%以上を占めます。他には、攻撃経路を決めるために役立つ情報（環境のフットプリンティングとフィンガープリンティングによって収集された構成情報）や、ネットワーク内を動き回るために役立つ情報（認証方法）などがあります。

サイバースパイ活動で漏洩したデータの90%が企業秘密（専有情報）です。

推奨される対策

サイバースパイ活動の実行者は、一見したところでは私たちとさほど変わりません。しかし、ひとたび仕事に入ると、不屈の精神で根気強く時間をかけてテラバイト単位のデータを盗み出します。DBIRでこれまでにご説明したとおり、前段階の攻撃ではツールも技法もシンプルですが、その後の攻撃は巧妙なものとなります。そのため、サイバースパイ活動を防ぐには、特別なセキュリティ対策に加えて、基本的なセキュリティ対策が重要になるのです。

エンドポイントの保護

今年は、サイバースパイ活動によるインシデントの90%に悪質なソフトウェアが関係していました。侵入経路がメール、ドライブバイダウンロード、直接インストール、リモートインストールのいずれであっても、エンドポイントを保護することが重要です。エンドポイントを保護するには、以下の対策が効果的です。

- ブラウザとプラグインを定期的に更新する
- ウイルス対策（AV）ソフトを使用し、定期的に更新する
- データ実行防止（DEP）ソリューションを使用する
- エンドポイント脅威検出/対応（ETDR）ソリューションを使用する

メールの保護
サイバースパイ活動で攻撃経路を確保するために最もよく使われるのがフィッシングです。そのため、フィッシングを防ぐ対策が重要です。メール経由の攻撃を防ぐには、以下の機能を備えたソリューションをお勧めします。

- スパム対策
- ブロックリスト
- ヘッダー解析
- 静的/動的なメール添付ファイルおよびURL解析
- フィッシングが疑われる活動の報告

ネットワークの保護
万一足場が築かれても社内システムに危害が及ぶのを防ぐには、ネットワークを保護することが重要です。ネットワークを保護するには、以下の対策が効果的です。

- 二要素認証を使用する
- ネットワークを分離する
- C2通信をブロックし、侵害を修復する

監視/ログ記録
ハッキングの記録を後の対策に役立てるには、ネットワーク、デバイス、アプリケーションを監視することが重要です。少なくとも以下が必要です。

- アカウントの監視
- 監査ログの監視
- ネットワーク/IDSの監視

2015年から2016年第1四半期にかけて発行されたサイバースパイ調査書
DBIRでは、サイバースパイ活動によるインシデントとデータ漏洩について全体的な傾向と統計に重点を置いています。DBIRに長年ご協力いただいているいくつかの企業・組織では、知的財産を狙う攻撃者に関する詳細な調査研究書を独自に発行しています。

- APT28（FireEye社）
- APT30（FireEye社）
- Duqu Threat Actor（Kaspersky社）
- Morpho Group（McAfee社）
- さまざまな攻撃者/攻撃活動（Kaspersky社）
- Project CameraShy（ThreatConnect社）
- さまざまな攻撃者/攻撃活動（CrowdStrike社）

DoS攻撃

要約

説明	ネットワークやシステムの可用性低下を狙った攻撃がこのパターンに分類されます。パフォーマンスの低下またはサービスの中断を目的としてシステムリソースを浪費させ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。
標的になりやすい業界	ゲーム業界、情報産業およびITサービス業、金融業
頻度	インシデント：9,630件、 データ漏洩を伴ったインシデント：1件
主な知見	攻撃は規模が大きいか期間が長いかのどちらかで、両方ということはまずありません。規模が小さく期間が短いものも多数あります。

データの正確さを維持するため、データを共有している協力企業・組織が使用する命名規則とNAICSのカテゴリを併用しています。

NAICSカテゴリについて
このセクションでは、データを共有している協力企業・組織が使用する命名規則とNAICSのハイレベルカテゴリを併用しています。（将来、変更される可能性はあります。）これは、私たちが怠慢という事ではなく、協力企業・組織の命名規則をNAICSカテゴリに対応付ける際にデータの正確さが失われてしまう懸念があるためです。たとえば、被害に遭った企業の多くがギャンブルサイトだったとしましょう。これらをインターネット娯楽/ゲームサイトやカジノに分類してしまうと、業界別の統計として大切な情報が見えなくなってしまいます。完璧なフレームワークというものはありえないので[27]、このセクションでは2つの分類を併用するのが最善だと考えました。

遠い昔、はるか彼方の銀河系で…（映画『スターウォーズ』より）
このセクションは2014年度版のDBIRで初めて登場しました。そのとき私たちは、このパターンは2012年以前から進化を重ねていることと、DoS攻撃の新しい波が登場しつつあることを指摘しました。

その昔、DDoSボットを拡大させる手段は、両親が使っている15年前のデスクトップPCに限られていました。『マクベス』に登場するバンクォーの亡霊のように家族の訪問の度に現れ、勇敢にもパッチを適用しようとする者に感染の息を吹きかけるごとくです。その後、ボットネットがステロイドを常用して攻撃力を増強するようになると、攻撃者は自分たちの創

27 VERISでさえも、完璧ではないのです。

造力が相当なものであり、対象をさらに拡大できることに気付き始めたのです。こうして生まれたのが、ブラウザセッションへのスクリプト挿入攻撃や分散反射型DoS（DRDoS）攻撃でした。さらに、時間差集中攻撃も新しく登場しています。[28]これは、異なるパスから時間差をつけてパケットを送信することで、標的システムにパケットが同時に到着して過負荷をかける攻撃です。これらの攻撃は規模だけでなく件数も拡大しています。私たちは、Akamai Networks社、Arbor Networks社、ベライゾンDoS防御から、DDoS攻撃に関する生々しい詳細（バイト/秒、パケット/秒、期間など）を入手しました。規模と期間の話に入る前に、密度について簡単に確認しておきましょう。

過去2回のDBIRでもご紹介しましたが、図41の2つのグラフはそれぞれ、DoS攻撃の帯域幅とパケットの密度を表します。今年のデータセットでは、1秒あたりのバイト数とパケット数の平均はそれぞれ5.51Gbpsと1.89Mppsでした。

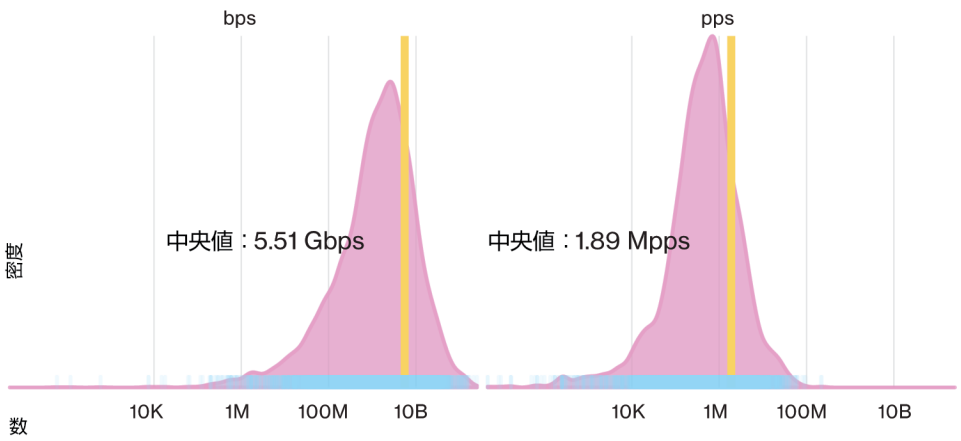


図41.
DoS攻撃の帯域幅とパケット数のレベル（n=10,808）

このサイズを試してみて
図42に示すとおり、私たちの分析では攻撃は規模（パケット/秒）が大きいか期間が長いかのどちらかであり、両方ということはまずなく、多くの場合は小規模で短期間でした。規模の大きい攻撃は、原点からY軸に沿って上に伸びています。つまり、攻撃は鋭いイナズマ型か永遠に続きそうな会話型のいずれかであり、攻撃の初期段階を見ただけでどちらになるか予想できるということです。

DoS攻撃は規模が大きいか期間が長いかのどちらかで、両方ということはまずありません。

28 EECS.Berkeley.edu/Pubs/TechRpts/2014/EECS-2014-129.pdf

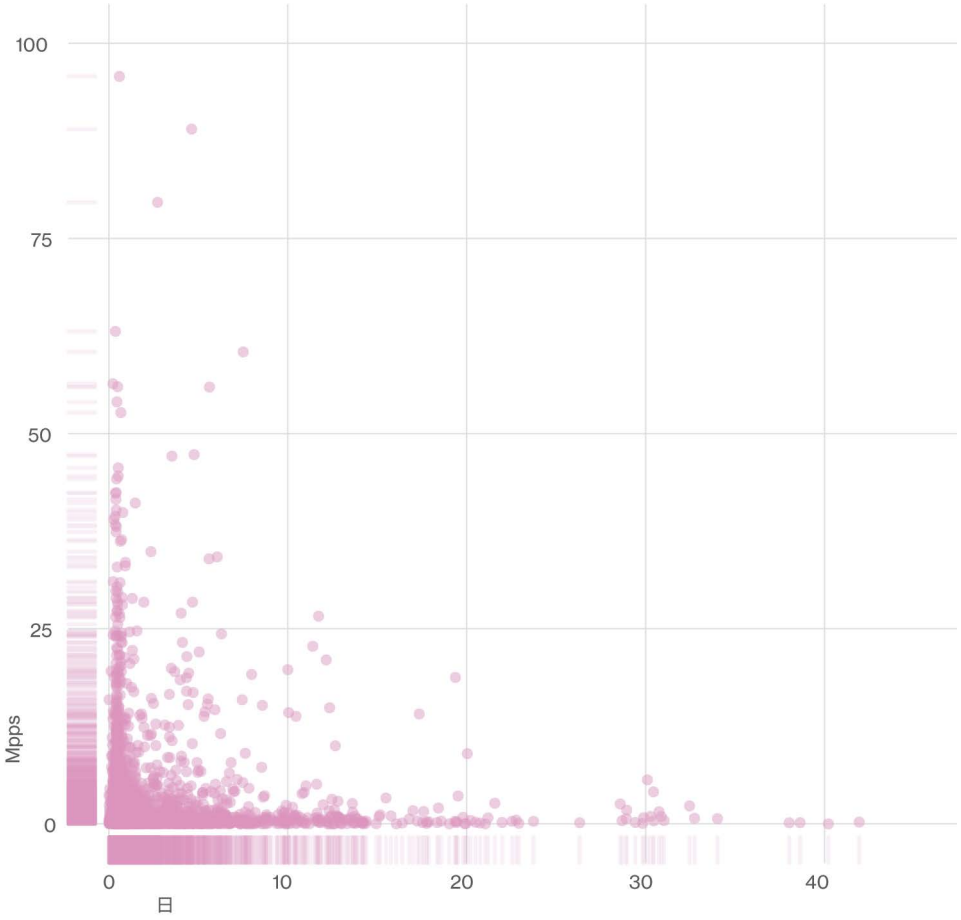


図42.

DDoS攻撃の規模（パケット/秒）と期間（n=5,800）

密度、規模、期間を確認したところで、いよいよ業界別の1秒あたりのパケット数（pps）とその見方についてご説明します。各業界についてppsの最大値と中央値を比較すると、予想どおり大きな差がありました。たとえば、調査対象のデータセットで今年最も大きい最大値を記録したのはメディア業界（2億2,200万pps）でした。だからといって、メディア業界の人たちが常に攻撃を受けて慌てふためいているわけではありません。図43を見れば、メディア業界の中央値は約60万ppsにすぎないことがわかります。同様の現象はハイテクコンサルティング業にも見られ、最大値は2億1,400万ppsでも中央値は約54万ppsです。一般的には、最大値は継続した攻撃ではなく1回きりの攻撃による可能性があるため、中央値が重要です。

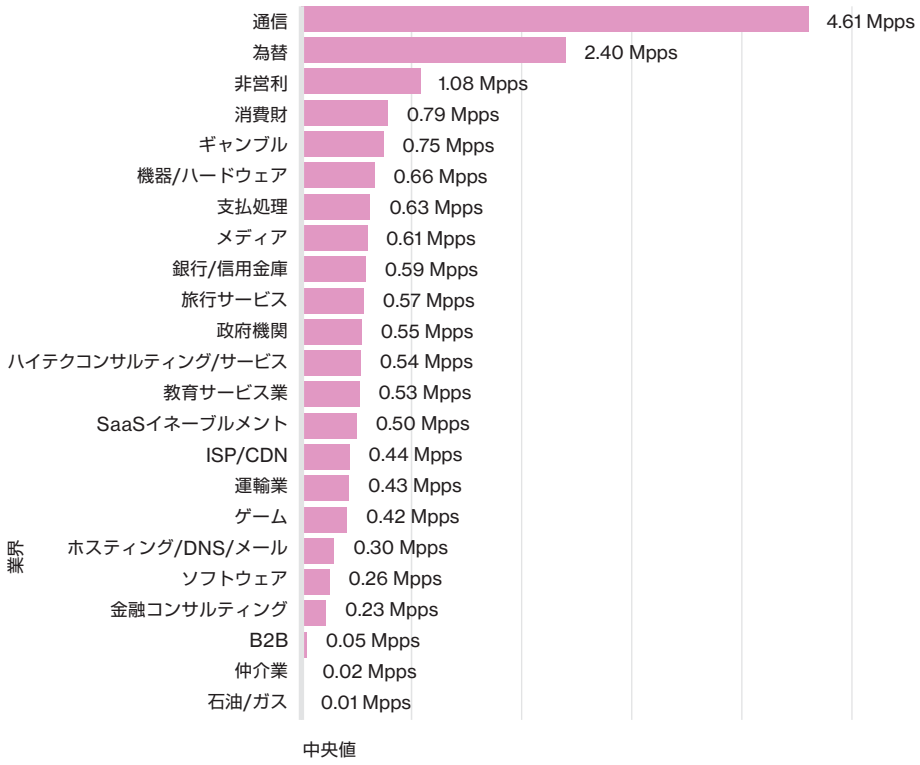


図43.

DDoSパケット数（Mpps）の業界別中央値（n=5,800）

それではまとめてみましょう。「連中はすぐに俺にかまってほしがるけれど、それはごめんだね」という態度では、「スターウォーズ」のハン・ソロの場合は乗り切れたかもしれませんが、現在のDoS攻撃には太刀打ちできないということです。DoSはもともと攻撃に多用されているうえ利用がさらに増加しているため、多くの攻撃者がダークサイドに集まっています。ハン・ソロも私たちも、今こそパラダイムシフトを図るべきかもしれません。

推奨される対策

備えあれば憂いなし
重要な資産を隔離して、デバイスが攻撃拠点として悪用されないようにしましょう。たとえば、与える権限を最小限に抑える、不要なポートは閉じるなどです。つまり、不要なものは使わないようにすることです。また、攻撃への備えも重要です。サーバーやサービスにパッチを適用する、IDS/IPSを導入して不審なトラフィックを検出および阻止する、ファイアウォールを使ってトラフィックをフィルタリングする、対応計画を作成するなどの対策をとりましょう。

クラウドサービスの対策をチェックする
DoS攻撃の規模、複雑さ、頻度の高まりを受けて、クラウドサービスプロバイダはサービスとインフラの可用性を維持するためのソリューションを提供しているはずです。

DoS攻撃の進化を受けて、クラウドサービスプロバイダはインフラの可用性を維持するためのソリューションを提供する必要があります。

自社の防御策を確認する
DDoS攻撃を緩和するためのサービスレベル契約について、十分に理解しておきましょう。また、一般に知られているDoS対策が自社のDoS対応手順に反映されていることを確認するとともに、異常事態の発生時にその手順を活かして最善の対応ができるように運用チームを訓練することも重要です。

その他すべて

要約

説明	9つのパターンのいずれにも該当しなかったすべてのインシデントがこのパターンに分類されます。
標的になりやすい業界	公的機関、金融業、専門サービス業、医療業
頻度	インシデント：8,886件、 データ漏洩を伴ったインシデント：125件
主な知見	ソーシャルエンジニアリングが非常に多く、そのほとんどは、9つのパターンに分類するために十分な詳細のないフィッシングでした。また、金銭目的のプリテキスティングが昨年から増加傾向にあります。

このパターンに入るインシデントで最も多いのは、フィッシング攻撃であること以外はほとんど何もわかっていないフィッシング攻撃です。

これまでに見てきたパターンが中心街にある流行のバーだとしたら、「その他すべて」のパターンは街外れのたまり場といったところでしょうか。2014年度版と同様に、このパターンに含まれるのは、目新しくユニークなインシデントではなく、メインストリートから外れた場所でたむろしているようなインシデントです。

すみませんが会員制です

あるインシデントが9つのクラブのメンバーに入れてもらえず、クラスタ分析という名の用心棒によってベルベットロープの外側に追いやられる理由は2つあります。1つ目の理由は単に、9つのパターンのいずれかに関連付けるうえで十分な情報がないためです。「その他すべて」パターンに入るインシデントで最も多いのは、フィッシング攻撃であること以外はほとんど何もわかっていない攻撃です。その大部分は2つの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）から報告されたものです。他にも、10社の協力企業・組織からこのパターンに該当するフィッシング攻撃が報告されています。フィッシングについては独自のセクションでご説明したので、ここで深掘りはしません。興味深いのは、これらのインシデントがなぜ複雑なフィルタ（付録E「分析手法とVERISリソース」を参照）で除外されずにここまでたどり着いたかです。単にフィッシングと判断するのにも、ある程度の情報が必要です。それは、標的が人間であり、特定の脅威活動が使われ、侵入経路がメールで、人間の行動に影響を及ぼす「完全性の喪失」を確認または推測できるといったものです。このような情報は入手できても、それ以外の情報がわからなかったために、このパターンに行き着いたのです。

これらのインシデントがこのパターンに分類される2つ目の理由は、他の標準的なパターンとは明らかに異なるためです。増加しているシナリオの1つは金銭目的のプリテキスティングで、「CEO詐欺」とも呼ばれるものです。経理担当の従業員を標的にした、昔からあるソーシャルエンジニアリングです。CEOまたはその他の重役からのメールを装い、もっともそうな理由を付けて外部への送金を指示するというものです。他の連絡手段を併用することもありますが、要点は同じです。もちろん、差出人は本物のCEOではありません。本物の指示に従ったと思い込んでいた受信者には、面倒な結果が待っていたのです。今後の調査によってこのタイプのサイバー犯罪の詳細が明らかになれば、これらのインシデントが映画で言えば独立系からメジャー系に躍り出ることになるかもしれません。

「その他すべて」の興味深さがわかったところで、「その他すべて」におけるその他すべてについて見てみましょう。

ソーシャルエンジニアリング以外のデータ漏洩に注目すると、具体的な手口が不明なハッキングが目立ちます。図44を見ると、データ漏洩の実に半数以上を占めています。

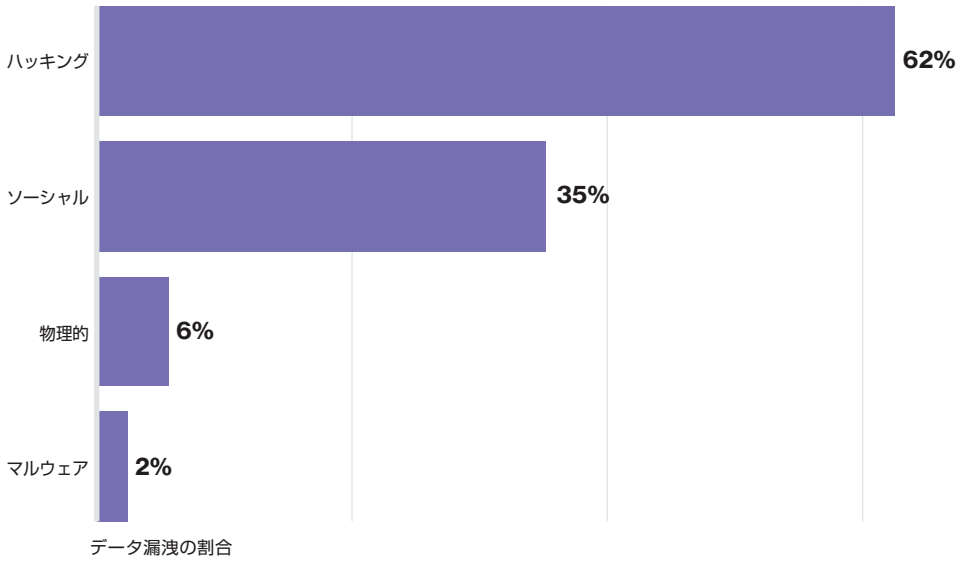


図44.
「その他すべて」のデータ漏洩で使われた脅威活動（n=125）

先ほどご説明したとおり、これらのハッキングがパターンセクションの末尾に追いやられたのも、未知の部分が多いためです。ここで改めまして、企業・組織の皆様にはデータ漏洩に関してできるだけ多くの詳細を集めていただくようお願い申し上げます。それにより、本報告書の内容がいっそう充実するとともに、「その他すべて」のデータ漏洩が表舞台に立てる日が来るかもしれません。

企業・組織の皆様にはデータ漏洩に関してできるだけ多くの詳細を集めていただくようお願い申し上げます。それにより、「その他すべて」のデータ漏洩が表舞台に立てる日が来るかもしれません。

まとめ

まずは、ここまでお読みいただいたことに感謝いたします。皆様にとって今年も、セキュリティデータをめぐる長くて奇妙な旅が有意義だったことを願っています。また、この旅を通じて、外部の攻撃者との戦いや内部の反対意見の説得に役立つ洞察や数値情報を獲得されましたら幸いです。復習しますと、本報告書では、まず複数のインシデント分類パターンに共通する注目点をご紹介した後、各パターンについてご説明しました。

特に認証情報とフィッシングに関しては、攻撃者の活動が単一のパターンに限定されない点が重要です。

攻撃者の活動は、単一のパターンに限定されません。

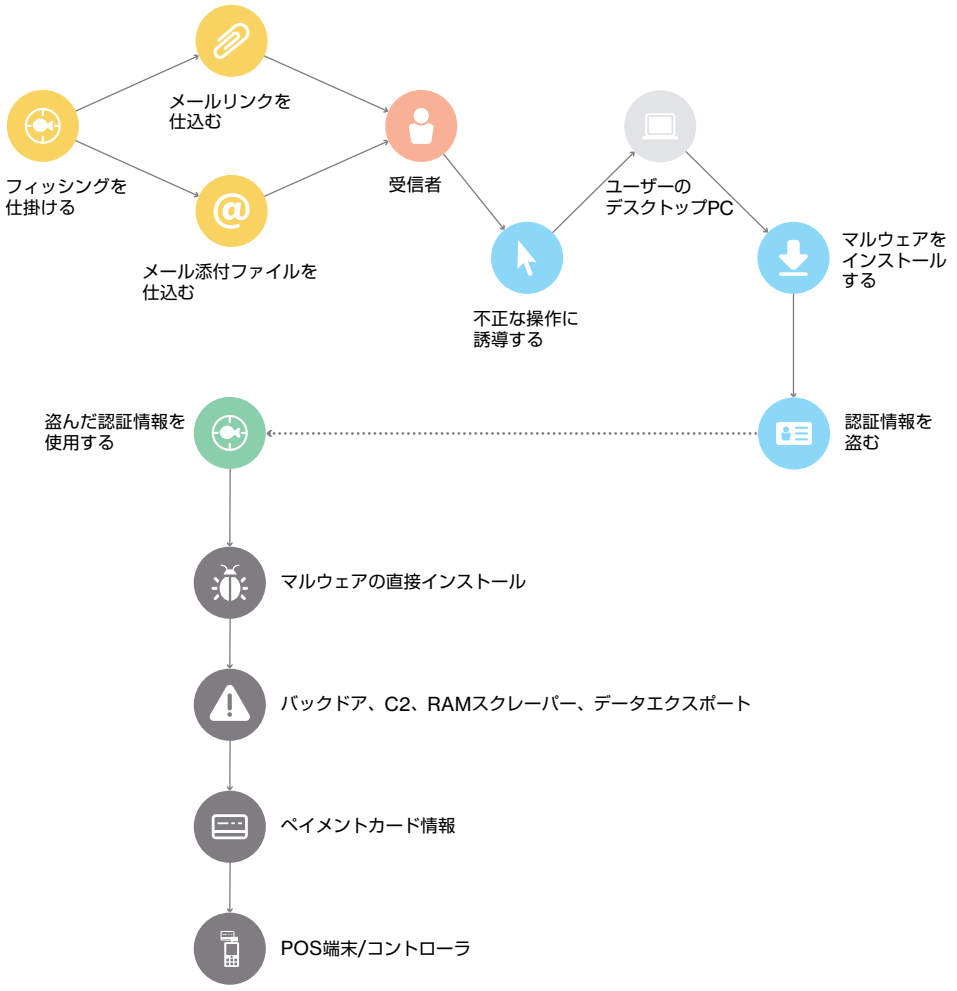


図45.

データ漏洩の一般的な流れ

個々の手口からデータ漏洩全般の状況に目を移してみると、図45に示すシナリオは、多くのデータ漏洩で使われる脅威活動、経路、資産のほとんどが登場しており、興味深いものです。この図は、攻撃者がPOSベンダーを標的として機密データを盗み出し、それを利用して次の被害者グループを攻撃するまでの流れを示しています。これが、データ漏洩に関する一連の流れの全体像です。

攻撃者はまず、ベンダーに対して標的型のフィッシングキャンペーンを仕掛けます。メールの受信者がリンクまたは添付ファイルをクリックすると、使用しているデバイスにマルウェアがインストールされます。このシナリオの最終目的はペイメントカードデータを盗み出すことです。ただし、このような初期段階の流れは、PCIセキュリティ基準への対応に忙殺されていない方々にとっても他人事ではありません。同じ手口が、国家機関が関わるサイバースパイ活動や完全に無差別のクライムウェア攻撃でも使われるからです。足場を確保した後にどのような攻撃をするかは、攻撃者の最終目的によってさまざまです。

このシナリオでは、感染デバイスから、このベンダーが顧客との取引に使っている認証情報を盗み出しています。この段階で使われるマルウェアについてはある程度の予想が付きます。おそらく、外部からの制御とアクセスを可能にするバックドアまたはC2と、最初のデータ（認証情報）漏洩をもたらすキーロガーでしょう。

インシデントパターンがどのように補完しあっているのかを理解すれば、限られたリソースで何を優先すべきかの判断に役立ちます。

ここまでくれば攻撃者にとって大成功です。ユーザーをだまし、デバイスを侵害して、データを盗み出しました。これで終わりなのでしょうか。『原始家族フリントストーン』のフレッドだったら、「ヤバダバドゥ～！」と叫びながらペットの恐竜ディノのしっぽを滑り降り、仕事の成果に満足して帰宅するのでしょうか。いいえ、ここからが本番なのです。

攻撃は新たな局面に移ります。盗んだ認証情報を使って静的な認証を突破し、顧客のネットワークに侵入します。ネットワークからシステムに侵入したら、マルウェアを直接インストールします。ここでは、RAMスクレーピングやデータエクスポート機能、外部からの制御を可能にして常駐する機能を持つマルウェアが使われます。これらのマルウェアが連携してペイメントカードデータを記録し、パッケージ化して運び出すことで、データ漏洩が完了します。

インシデントパターンがどのように補完しあって、イベントチェーンのどこを担当しているのかを理解しておきましょう。限られたリソースで対応を行うにあたり、何を優先すべきかの判断に役立ちます。攻撃の流れ、攻撃を成功させるために使われるツール（手口）、多くのパターンに共通する同一または類似の手口をしっかりと把握しておきましょう。

コストの考察

コスト再考
私たちは昨年、サイバー保険の支払請求があった漏洩の被害データを分析して、2つの結論を導き出しました。1つ目は、レコードの損失コストは件数に単純比例するわけではないことです。レコード単位で考えると、最初の数レコードの漏洩コストは10万件目のレコードよりもずっと高くなります。2つ目は、漏洩コストについてはまだ不明な点が多いということです。実際に、レコード漏洩とそのコストの因果関係は半分程度しかわかっていません。（わかっている半分というのは、漏洩したレコード件数が影響するということだけです。）私たちは1年を経た今でも、人生の意味、そしてインシデントのコストをより正確に予測する方法について、探究を続けています。

今年は、新しいアプローチを試みました。データ漏洩コストについて入手できる具体的なデータは限られており、昨年の方法では敵を倒せそうにないからです。私たちは、NetDiligence社からご提供いただいた実際のサイバー保険金支払データを再び細かく分析し、興味深くて役に立つ別の特性がないかを探りました。データの種類に注目したところ、ペイメントカード情報（PCI）の漏洩で報告されたレコード損失の中央値が、保護医療情報（PHI）や個人識別情報（PII）よりもずっと高いことがわかりました。

PCIの漏洩で報告されたレコード損失の中央値は、PHIやPIIよりもずっと高いことがわかりました。

データの種類	インシデントの割合	中央値
PCI	27%	53,100
PHI	11%	1,000
PII	48%	761
カード以外の金融情報	5%	55

表3.
レコード漏洩コストのデータ種別中央値

保険契約者の詳細像が不明なため、各種データの度数については結論を出さないことにしました。一方で、私たちが「データ損失の種類」と呼ぶ軸でデータを分析すると、いくつかの興味深い発見がありました。それを以下にご紹介します。

フォレンジック調査には、自由でいるのと同様にコストがかかる

箱ひげ図はご存知でしょうか。[29]図46のグラフに戸惑う必要はありません。簡単に言えば、保険金の支払い対象の大半は、データ漏洩の回復段階における現状把握と危機管理のコストで占められることを示しています。最もコストが高いのは、危機管理段階の法律相談と、フォレンジック調査です。その後に、データ漏洩の通知とクレジットモニタリングが続きます。被害者にお見舞いの花を贈れば済むわけではないので、これは当然です。

最もコストが高いのは、危機管理段階の法律相談と、フォレンジック調査です。

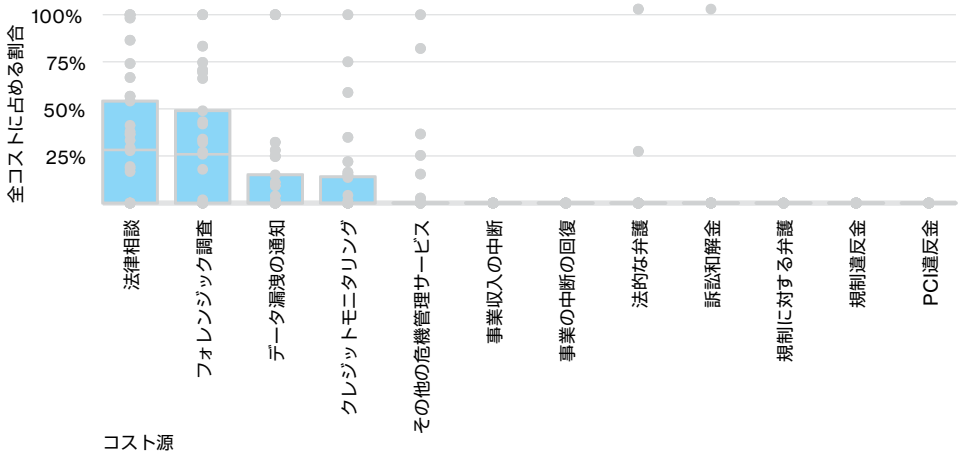


図46.

保険金支払のコストタイプ別内訳（n=41）

コストのタイプをよく見ると、対応策を進める順序で並んでいることがわかります。まずは、漏洩被害に遭ったと考えられるときに第三者の指導や専門会社の調査を受けて現状を把握するための初期コストがかかります。その後、不本意ながら漏洩を認め、利用者に対してできるだけ顔が立つようにするためのコストが必要になります。最後に、法定代理人、和解金、罰金などが長期的なコストとして、データ漏洩ストーリーの終章を飾ることになります。サイバー保険に関する調査からはこのように有用な情報が得られますが、他にも考慮すべきことがあります。保険が適用されない項目もあるのです。多くのサイバー保険契約では、高額になりやすい問題改善コストや懲罰的損害賠償金は補償されません。特に懲罰的損害賠償金は、多くの地域ではそもそも法律的に保険の適用外とされています。さらに、これらのコストは初期コストに比べて見落とされがちです。

法定代理人や調査員への報酬は、漏洩したレコード件数単位ではなく、通常は事前に定めた固定料金または個別相談での時給で支払われます。こうしたサービスが必要になった場合に備えて、あらかじめ適切な関係を築き、準備を整えておきましょう。そうすれば、万一の事態が発生しても手続きをスムーズに進め、調査に必要なレベルのアクセス権限と情報をすばやく提供できます。ネットワーク図やSLAの確認に何時間もかけている間、手持ち無沙汰の代理人や調査員が会議室でスマートフォンを眺めている状態は避けたいでしょう。

本書に関するご意見、ご感想、ご質問

をお待ちしております。メール（dbir@verizon.com）、LinkedIn、Twitter（@VZdbir、ハッシュタグ#dbir）をご利用いただけます。（英語にて受付）

29 グレイの線は中央値を表します。この線でデータが上下半分に分けられます。箱の中において、この線の上に全データの4分の1に相当するデータが、線の下に別の4分の1のデータが含まれます。残りのデータは箱の外側にあります。箱ひげ図はデータが集中している範囲を知るために便利です。

付録A：盗まれたデータの運命

闇市場には、果てしない数のソースから果てしない種類の漏洩データが流れ込んできます。

あなたの知らない世界
サイバー犯罪者が釣りをしたら、キャッチアンドリリースはしないでしょう。釣られた魚はクーラーボックスに直行です。
このセクションでは、盗んだデータを攻撃者がどう扱うのかについて次の2つのトピックを中心に見ていきます。なお、このセクションのデータはIntel Security社にご提供いただきました。

- 盗まれたデータのマネタイズ（換金）の分析
- 漏洩レコードの闇市場の調査

マネタイズ方法
闇市場には、果てしない数のソースから果てしない種類の漏洩データが流れ込んできます。しかし、この報告書は『戦争と平和』級の大作ではないので、データの種類を限定して範囲を絞り、できるだけ簡潔に分析することにしました。対象データの選定では、理解しやすいこと、大量のデータが盗まれていること、ある程度解明された市場で売買されていることを基準にしました。その結果、次の3種類のデータが選ばれました。もちろん、これらは市場で流通するデータのほんの一部に過ぎません。

- ペイメントカード情報
- 金融口座情報
- 個人識別情報（PII）

知的財産や企業システムへのアクセス権などその他のデータも、頻繁に盗み出されてマネタイズされています。オープンな市場では、多様なデータの窃取に関連するサービスはよく見かけますが、取引の詳細はまず見ることができません。そのため、データの市場価値を評価することは困難です。データによっては、手元に置いて利用するほうが市場で転売するよりも価値が高い場合もあります。たとえば、盗んだ知的財産を使って、研究開発に必要な労力やコストをかけずに優れたウィジェットを開発するなどです。そのためこのセクションでは、現時点で十分な情報が入手できた、上記のカテゴリを中心にご説明します。

ペイメントカードのマネタイズ
盗まれたペイメントカードデータの入手方法や換金方法はさまざまです。さらに、換金方法の選択を左右する要因がいくつかあります。たとえば以下の点です。

- データを盗んだ手口とデータの出所となった資産の種類。データを盗んだ手口によって、ペイメントカード番号（PAN: Primary Account Number）以外に含まれる情報が異なります。ここからは、できるだけインシデント分類パターンに沿って手口をご説明します。
- 1回または一連のデータ漏洩で盗み出されたペイメントレコード件数。
- データ漏洩の実行者（単独犯か組織犯罪か）。

まず、データ漏洩の実行者は、盗み出したデータを転売するか自分で悪用するかを選択します。レコード件数が数百万に及ぶ大規模なデータ漏洩では、卸売業者のように仲介者にデータをまとめて売りさばき、その後の不正使用をまかせる方法が好まれます。盗まれたデータが扱われる闇市場については、後述の「子ぶたちゃん市場へいった」セクションを参照してください。

盗まれたペイメントカードデータをマネタイズするには多種多様な方法があります。ここでは最も一般的でわかりやすい分類として、カードを提示しない非対面取引とカードを提示する対面取引の2種類に分けてご説明します。

非対面取引の場合

まずは、カードを提示しない非対面（CNP: Card Not-Present）取引でのペイメントカードデータの不正利用についてご説明します。通常は、オンラインショッピングやテレフォンショッピングで使われます。この方法は理想的に思えるかもしれません。店舗に出向く必要もなければ、顔を見られる心配もないからです。しかし、難点もあります。それは、セキュリティコードまたはCVV2（Card Verification Value）と呼ばれる、実際のカードに印字された3桁または4桁の番号が必要なことです。セキュリティコードは、ほとんどの商取引サイトで入力が必須です。カード発行会社は非常に頑固で、セキュリティコードを決してカードの磁気ストライプに記録しようとはしません。そのため、不正利用者が現金を手にするには、実際に「働く」必要があるのです。不正なCNP取引を成功させるうえで不可欠の情報を手に入れるには、通常、正規のCNP取引情報を盗み出します。よく使われる手口は2つあります。

盗んだ非対面（CNP）取引情報を利益化する方法は、昔ながらの盗品売買に似ています。

1つ目はクライムウェアです。利用者のデバイスにスパイウェアやフォーム入力を盗むマルウェアをインストールします。請求情報とあわせてカード所有者であることを証明するために必要となる、PAN、有効期限、セキュリティコードの組み合わせを盗み出します。

2つ目はWEBアプリケーション攻撃です。ペイメントアプリケーションに侵入してコードを改変し、PAN、有効期限、セキュリティコードを収集して外部に送信します。

盗んだCNP取引情報を利益化する方法は、昔ながらの盗品売買に似ています。トラックの荷台からたばこのカートンを取り出して「割引」価格で売るようなやり方です。商品やサービスをオンラインのCNP取引で注文し、複数の仲介業者を介することで、真の受取人をわかりにくくします。最終的に商品は倉庫に収められ、その後現地のWebサイトで販売されます。

対面取引の場合

POSへの侵入とペイメントカードスキミングは、ペイメントカードデータ漏洩の91%を占める2大パターンです。この2つには共通点があります。ペイメントカード情報の処理に使われる特定の資産を標的にする点と、カードを提示する対面取引のデータを盗み出す点です。対面取引で盗み出されたデータは、ほとんどの場合、対面取引で不正利用されます。「対面取引ではチップと暗証番号（PIN）も必要なはず」と思われた方には、後ほどご説明いたします。

これらの攻撃パターンが成功すれば、磁気ストライプ情報を盗み出すことができます。そして、現実に成功率は高いのです。詳しい手口については各セクションをご参照いただくとして、ここでは磁気ストライプに注目しましょう。カードの裏面にある太くて黒い線には、カードが本物であることを証明するためのPAN、有効期限、その他の重要情報（特にCVV）が記録されています。

CVVはペイメントカードの偽造防止を目的としたコードです。デビットカードの写真をTwitterに投稿してしまう人を守るうえでは、役立っているようです[30]。しかし、多くの攻撃では静的な磁気ストライプデータがまるごと盗まれるため、CVVの存在意義は薄れています。なお、CNP取引で使われるCVV2はCVVとは異なることに注意してください。代わりに登場したのが、Europay、MasterCard、Visaが共同開発したEMV規格です。この認証方式ではチップとPINを組み合わせています。静的なCVVではなくワンタイムセキュリティコードによって、カードが本物であることを証明する仕組みです。

ATMスキミングでは、磁気ストライプ情報とともに利用者のPINが狙われます。これらの情報を組み合わせれば、チップとPINによる認証方法が十分に普及していない国や地域である米国、南米、アジアで簡単に不正利用ができます。

以上をまとめてみます。CNP取引での不正は、通常、正規のCNP取引情報を盗むことで成立します。対面取引での不正は、対面取引情報を盗むことで成立します。CVVとCVV2は2つの不正手段が結びつくのを防止するうえで役立ってはいるものの、いずれもペイメントカード情報の窃取とマネタイズを防ぐには十分ではない状況です。

銀行データのマネタイズ

オンラインバンキングが普及すると、サイバー犯罪者は目ざとくそのログイン認証情報を狙うようになりました。金融口座のログイン認証情報を入手すれば、オンラインバンキングアプリケーションを使って口座から不正送金できます。フィッシングとマルウェアを組み合わせて銀行コードと口座番号を盗み出し、ACHなどの決済システムを使って不正送金するケースもあります。クライムウェアのパターンも多用されており、静的で不正利用が可能な銀行情報を効率的に盗み出せるように工夫されたトロイの木馬（Zeus、Dyre、Dridexなど）が出回っています。さらに、内部者および特権保持者による不正使用のパターンも見られます。簡単に言えば、銀行の従業員が認証情報に不正アクセスして、単独でまたは外部の犯罪グループと共謀して悪用するという手口です。

内部者および特権保持者による不正使用のパターンでは、銀行の従業員がデータに不正アクセスして、単独でまたは外部の犯罪グループと共謀して悪用する手口が使われます。

個人識別情報のマネタイズ

個人識別情報（PII）もまた、金銭目的での不正利用が多いデータです。個人識別情報の盗難や窃取のニュースはもはや珍しくはありません。個人識別情報をマネタイズする方法は多種多様です。米国では、なりすましによって新しいクレジットラインを無断で開設される、偽の確定申告で還付金をかすめ取られるなどの不正が相次いでいます。また、ソーシャルエンジニアリング攻撃でプリテキスティングメールをより本物らしく見せるためにも個人識別情報が利用されます。個人識別情報漏洩の多くは、人的ミス、内部者および特権保持者による不正使用、物理的窃盗および紛失のパターンで起こります。

子ぶたちゃん市場へいった

盗まれたデータの中で最も大量に売買されるのがペイメントカードデータです。McAfeeラボが2015年秋に公開した『The Hidden Data Economy』[31]によると、盗まれたデータの平均売価は以下のようになっています。

セキュリティコード付きペイメントカード番号	米国	英国	カナダ	オーストラリア	EU
PCI	$5 ～ $8	$20 ～ $25	$20 ～ $25	$21 ～ $25	$25 ～ $30
PHI	$15	$25	$25	$25	$30
PII	$15	$30	$30	$30	$35
カード以外の金融情報	$30	$35	$40	$40	$45

表4.

盗まれたカードデータ
（Visa、MasterCard、Amex、Discover）
1件あたりの予想価格（米ドル）
出典：McAfeeラボ

30 @NeedADebitCard
31 McAfee.com/us/resources/reports/rp-hidden-data-economy.pdf

価格を考察するうえで難しいのは、表で示している他にも多数の変動要因があることです。変動要因には、国や地域、PINの有無、利用可能残高、有効率、追加データ、そしてもちろん売り手の評判などがあります。

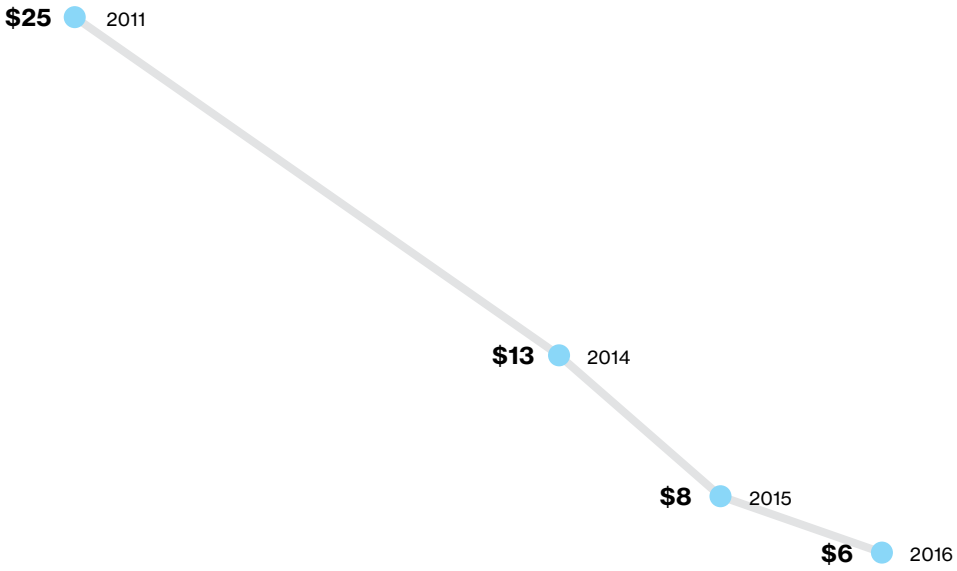


図47.
ペイメントカードレコード1件あたりの価格（米ドル）とその推移
出典：Intel Security

購入オプションが多すぎるため、市場の傾向を判断するのは困難です。図47は、米国で盗まれたペイメントカードの単体モデルの価格変動を、最大限の努力を払って示したグラフです。

一般的な市場と同じように、盗まれたペイメントカードの市場も需要と供給で成り立っています。2011年度版のDBIRでは大規模なペイメントカードデータ漏洩は報告されませんでした。前年の1億4,400万件に対して約400万件ということで、レコード件数があまりに少ないことが懸念されていました。しかし、その年には現実に大規模データ漏洩がなかったことが確認されました。それを証明するかのように、上のグラフでも2011年は供給が減り、市場価格が上昇しています。2014年には小売業を標的にした大規模データ漏洩が相次いだため、ペイメントカードデータが過剰になり、価格が3年前と比べて50%も下落しました。その後2016年に入っても価格は下がり続けています。供給過多によって低下した価格を下支えるために、盗まれたカードデータの売り手は他の面で差別化を図り始めています。たとえば、大規模データ漏洩の直後に、データが地域別（市など）および有効率別に販売されているのが確認されました。買い手にとっては、カードデータを疑われずに使用できる地域とカードが有効である確率がわかることには、大きな価値があります。最近では、買い手が追加料金（確認したケースでは8ドル）を支払えば国やカードの種類を指定できる場合もあります。また、請求先住所や社会保障番号などカード所有者の個人識別情報が含まれるデータは、非常に高い価格で売られています。しかし全体としては、過去4年間を通じて価格は下落傾向にあります。

盗まれたカードデータの売り手は、地域やカードの有効率によって価格を変えるなどの差別化を図り始めています。

金融口座の認証情報については、価格の傾向を判断するうえで十分なデータが得られませんでした。それでも、最新の価格情報を多少入手できました。

250ドル出せば、主要銀行の残高5,000ドルの口座にアクセスする認証情報を1件購入できます。数量割引の仕組みもあり、400ドル出せば残高10,000ドルの口座認証情報を1件購入できます。つまり、購入価格の20倍～25倍の口座残高が割り当てられる仕組みです。

金融口座の認証情報を求める犯罪者には、PayPalアカウントも人気があります。ある市場ではさらに「お得」な数量割引が適用され、60ドルで4,000ドル相当（購入価格の約67倍）のPayPalアカウント情報が手に入ります。

価値のあるものに人は喜んで代金を支払います。そして、何かに対して需要があれば、それを供給して利益を得ようとする人が必ず現れます。市場におけるこのような一般法則は、サイバー犯罪市場にもぴったりと当てはまります。私たちはユーロポールの協力を得て、闇市場サイトであらゆる違法商品が取引されている様子を目撃しました。闇市場サイトは、高度な技術に基づく匿名性を利用するダークネットに設置されたものもありますが、多くはオープンネットで運営されています。盗難データは需要が高いため、供給する犯罪者はいくらでも登場します。データを簡単に盗み出せて、支払ったリスクとコストを上回る利益が得られるとなれば、供給者は後を絶ちません。

保護されているデータを求めてサイバー犯罪者が狙う標的は、一般市民から企業や政府にいたるまで、インターネットコミュニティ全体です。個人ユーザーは、オンラインバンキングの認証情報や機密文書を狙うフィッシングやスパムキャンペーンの標的になります。顧客情報、市場戦略、業界情報などのデータを重要資産として持つ企業は、規模にかかわらず、技術的に高度な攻撃や初歩的なソーシャルエンジニアリング攻撃に常時さらされます。ユーロポールのiOCTA（Internet Organised Crime Threat Assessment：インターネット組織犯罪脅威評価）レポート2015年版によると、多くのメディアが2014年を「データ漏洩の年」と呼んでいます。しかし、ネットワーク攻撃件数は最高記録を更新し続けており、大規模データ漏洩の発生する傾向は定着しつつあると言えます。将来改善される兆しは見えません。

警察当局は犯罪市場とその管理者を休みなく捜査し、盗難データの不正取引を取り締まっています。しかし、この脅威に的確に対抗するためには、警察、民間企業、金融機関、インターネットセキュリティ業界を含むあらゆる関係者が連携して統合的な取り組みを進める必要があります。

Fernando Ruiz（ユーロポール、欧州サイバー犯罪センター（EC3）最高責任者）

付録B：ご協力いただいた企業・組織

Akamai Technologies
Anti-Phishing Working Group（APWG）
Arbor Networks
AsTech Consulting
オーストラリア連邦警察（AFP）
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
ポーランドCERT/NASK
CERT-EU
チャン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
Checkpoint
Chubb[32]
Cisco Security Services
ルクセンブルクコンピューターインシデント対策センター（CIRCL）
サイバーセキュリティ評議会
CrowdStrike
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
Daylight Security Group
Deloitte and Touche LLP
DFDR Forensics
EMC
欧州サイバー犯罪センター（EC3）
Fortinet
G-C Partners, LLC
GRA Quantum
Guidance Software
産業制御システム・サイバー緊急事態対応チーム（ICS-CERT）
Imperva
Intel Security
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
JPCERT/CC[33]
Juniper Networks
Kaspersky Lab
Kenna
LARES
Law and Forensics
Mishcon de Reya
MWR InfoSecurity
米国サイバーセキュリティ・通信統合センター（NCCIC）
NetDiligence
Niddel
Palo Alto Networks
ブエノスアイレス市警察（アルゼンチン）
Qualys
Recorded Future
Risk Analytics
S21sec
SANS Securing the Human
Splunk
SwissCom
Tenable
TRESsPASS Project
Tripwire
英国コンピューター緊急事態対策チーム（CERT-UK）
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）
ベライゾンサイバーインテリジェンスセンター
ベライゾンDoS防御
ベライゾンRISKチーム
Vestige, Ltd
WhiteHat Security
Winston & Strawn LLP
Wombat Security Technologies

32 ご提供いただいた情報はACE Ltd.に帰属します。ACE Ltd.のThe Chubb Corporation買収前のポリシーと権利が適用されています。
33 2016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。

付録C：ベージュブック風

米国12地区の連邦準備銀行が地域の経済状況をまとめ、連邦準備制度理事会（FRB）が公表している経済報告書、いわゆる「ベージュブック」[34]に敬意を表して、このたび協力企業・組織の皆様からご提供いただいたセキュリティインシデントデータをベージュブック風にまとめてみました。なお、取り上げる内容は確認済みのデータ漏洩の一部に限定されていることをご了承ください。物理的窃盗および紛失と人的ミスのパターンは含まれておりません。参照データはDBIR公開の年ではなく2015年時点のインシデントですが、大きな影響はないものと考えております。

犯罪組織の活動は全体的に増加傾向にあり、活発化しているボットネット活動および安定した水準を保つPOSへの侵入がそれを牽引しています。

脅威実行者の活動
データ漏洩における外部実行者の割合は昨年から微増しているものの、過去の記録から見れば正常範囲を外れるものではありません。内部実行者は割合および件数において逆に同程度の減少が見られます。内部実行者と外部実行者の共謀は、2012年に平均値を上回って以来停滞が続いています。データの多様化並びに銀行職員を抱きこんだデータ漏洩の減少がその要因と考えられます。パートナーの実行者は横ばいでした。

犯罪組織の活動は全体的に増加傾向にあります。2015年に入って活発化しているボットネット活動および安定した水準を保つPOSへの侵入がそれを牽引しています。昨年は国家関連の実行者の増加にやや陰りが見え、これは提供データの変化が要因とみられます。

活動家グループの活動に関しては、データ漏洩の水準は下がり気味で、中心がSQLiからDoSキャンペーンにゆるやかに移行している点が注目されます。

脅威活動の傾向
ハッキングおよびマルウェア活動は急増していると断定でき、件数では2011年の水準に達しています。これは、ボットネット解体の影響に加えて、ソーシャルエンジニアリングに分類される脅威活動が増加傾向にあることが要因として考えられます。2015年のフィッシングは、既知のクライムウェアによるデータ漏洩との強い関連性を示しています。

物理的な活動は2013年の水準から減少していますが、法執行当局以外のデータ提供者が著しく増加していることが大きく影響しているとみられます。スキミング活動は2014年と比較して、横ばいかやや減少の動きを示しています。

盗んだ認証情報の悪用およびバックドアまたはC2の使用は、2015年も引き続き増加傾向にあります。銀行を標的としたトロイの木馬においてこの2種類の脅威が併用されることが活動増加の一因と考えられます。POSへの侵入市場においては、盗んだ認証情報の増加によってブルートフォース活動が抑制される傾向が続いています。

34 FederalReserve.gov/monetarypolicy/beigebook

WEBアプリケーション攻撃の定着化により、SQLiおよびRFIの活動は2015年も一定の水準を保っています。識者によれば、クライムウェアによるデータ漏洩の急増がC2およびキーロギングマルウェア機能の顕著な増加をもたらしていると考えられます。マルウェアによるデータエクスポートもまた増加の見通しを示しています。

RAMスクレーパーも全体としては大きな割合を占めますが、活動低下の兆しが見られます。それと関連してか、推測可能なPOS認証情報に対する大規模リモート攻撃では、被害者数が全体的に落ち込みを示しています。

2015年のデータ漏洩に関するデータセットでは、複数のインシデント分類パターンでフィッシングの浸透が進んでいることが明らかになりました。ソーシャルエンジニアリングの脅威活動は変わらず成長を示しています。プリテキスティング活動は増加し、誘惑/賄賂よりも高い割合を占めています。これは2014年からの大きな変化であり、2011年にも同様の変化が見られました。金銭目的のデータ漏洩におけるプリテキスティング使用は2015年には増加しており、活動全体の増加にもつながっています。一方でこの増加は、許可されていないハードウェアの不正使用の伸び悩みによって相殺されます。報告書によると、ハードウェアの不正使用によるデータ漏洩の大多数は、USBドライブを使用したデータ窃取で、スパイ目的の動機が関連しているとみられます。金銭目的の犯行におけるハンドヘルド式のスキマーの使用は2014年から減速気味で、2013年と同程度の水準となっています。

ハードウェアの不正使用によるデータ漏洩の大多数は、USBドライブを使用したデータ窃取で、スパイ目的の動機が関連していると考えられます。

報告書においては、金融業、情報産業、オンライン小売業で活動が増加しています。ホテル業は2014年と比較してやや目立った活動が見られます。逆に、公的機関、小売業（オンラインを除く）、医療業、専門サービス業では活動が減っています。その要因は、協力企業・組織の構成の変化に加えて、多くの4A局面に影響を与えた2015年の複数の大規模データ漏洩によるものと考えられます（4Aについては「データ漏洩の動向」セクションを参照）。

いずれのデータ漏洩にも、外的な環境要因の影響は見られません。

付録D：攻撃図

攻撃図の作り方
この攻撃図はどのように作られたのでしょうか。実は、VERISを利用して作られています。

VERISの分類では、活動から属性を導き出すことができます。逆に、属性から活動を導き出すこともできます。これらのつながりを1つ1つ積み上げていくことで、攻撃の要素間をつなぐ経路が形作られています。

図に反映されているのは、実際に起きた攻撃ではなく、起きる可能性のある攻撃です。この情報こそ、攻撃を評価するうえで必要なものです。

地図で道を探す
「データ漏洩の動向」セクションでは、情報セキュリティにおける防御を丘の死守に例えました。ここまでお読みになった方は、敵の攻撃がどのようなものか理解されたことでしょう。ここでもし、土地全体を見渡せる地図があったらどうでしょうか。大小の道や交差点が描かれた地図です。大きな助けになることでしょう。この地図を使って、主要経路に加えて代替経路についても防御策を立てることができます。そうすれば、敵の攻撃を全面的に阻止できるでしょう。

それこそが、ここでご紹介する攻撃図です。このロードマップがあれば、敵の攻撃を線ではなく面で防御できます。右に示す攻撃図[35]は、2016年度版DBIRのデータセットで確認された攻撃の流れを1つの図にまとめたものです[36]。開始から終了までのすべての経路をたどる事ができますでしょうか[37]。これでも、かなり簡略化した図なのですが、もっと詳細の図ですべての経路をたどる事を想像してみてください。活動や属性はそれぞれ、VERISで取り上げられている個々の種類や経路に細分化されることになります。

特定の攻撃について注意が必要になった場合、その攻撃のパスは開始から終了まで1つです。多くの場合は、そのような特定のパス1つについて有効な緩和策を考えます。1つ1つのパスではなく、一度に複数のパスにまとめて緩和策を実施できたら素晴らしいのではないでしょうか。確かにそうです。

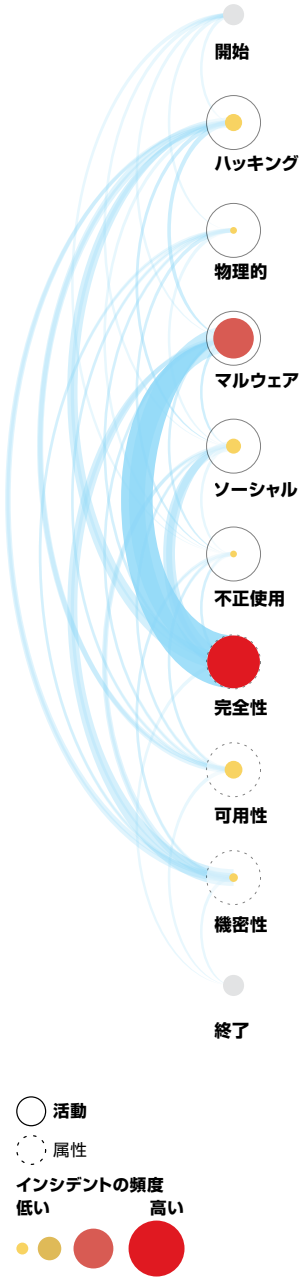


図48.
2016年度版DBIR攻撃図

35 紙上で見ても興味深いものですが、この図のインタラクティブバージョンもご用意しております。
http://vz-risk.github.io/dbir/2016/52をご参照ください。
36 この図を作るまでにどのくらい時間がかかったと思われるでしょうか。思い出したくもありませんが、
さまざまな図を何千何万と考えました。
37 弁護士たちは、すべてのパスを追跡する方向で助言しない方がよいと思っていたようです。皆様の検討事項があまりに多すぎて永遠に終わらず、その間に会社から解雇され、配偶者に逃げられ、労働組合から追い出されかねないからです。

攻撃図を使って攻撃全体を分析すれば、それが可能になるのです。演算方法は割愛しますが[38]、攻撃図を使えば、受ける可能性が最も高い攻撃のパスに加えて、複数のパスの対策を割り出すことができます。

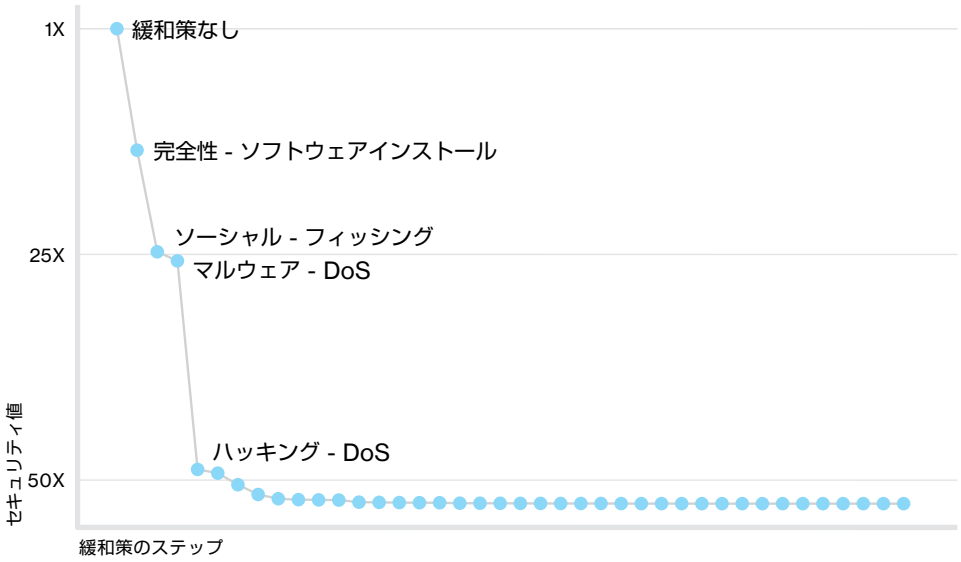


図49.
発生確率の高いパスに対する緩和策1件あたりの有効性

2016年度版のDBIR用に、発生確率の高いパスに対処するため優先すべき領域を図49に示します。概略図からおわかりのように、最初にとるべき最善策は、無許可のソフトウェアインストールを防止することです。マルウェアのインストールは完全性の喪失をもたらします。今年のインシデントデータセットでも無許可のソフトウェアインストールが広く行われていました（すでにご存知のとおりです）。また、フィッシングについては、皆様が魚菜食主義者の気分になるほど、これまでしつこいくらい注意を喚起してきました。フィッシングはDoS攻撃とともに、インシデントデータセットに幅広く見られます。

守るべき道を選ぶ
最優先の緩和策をいくつか実施すれば、敵の攻撃力はかなり弱まります。実のところ、攻撃者が好んで使う「高速道路」は数本しかありません。これらの道の防御対策は必須です。そうすると攻撃者は脇道を使うでしょうが、すべての脇道をブロックするのは賢い選択ではありません。

攻撃者が好んで使う「高速道路」は数本しかありません。これらの道の防御対策は必須です。すべての道を防ごうとするのは、賢い選択ではありません。

どれが高速道路でどれが脇道かは、業界によって異なります。たとえば今回の調査によると、人的ミスは医療業では高速道路ですが小売業では脇道になります。敵が最もよく通る道と[39]、攻撃による被害が最大となる道を見つけることが重要です。あらゆる人のあらゆる情報セキュリティの問題を解決することは不可能です。

最終的には、対処すべき道は数学的に見つけることができます。数学が苦手な方は、私たちの手軽で使いやすいWebアプリケーションをお試しください[40]。脅威（業界またはパターン）を選択し、守りたいもの（機密データ、完全性、可用性、すべてなど）を選択して、分析タイプ（可能性のあるすべての攻撃者、可能性の高い攻撃者のみなど）を選択するだけで答えが見つかります。

攻撃が考えられる範囲全体に適切なレベルの対策を施す必要があります。さもないと、ドアに鍵を掛けても窓は全開という状況になりかねません。

38 SecurityBlog.VerizonEnterprise.com/?p=6949
39 本書の「インシデント分類パターン」セクションの業界別データがお役に立ちます。
40 DBIR-Attack-Graph.Infos.ec/

付録E：分析手法とVERISリソース

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、提示における高度な厳格さと誠実さがあります。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を読んでくださっていることを知ることは、ベライゾンが誠実さを維持する上で大きな力となります。分析手法について詳細に説明することも、その誠実さの重要な一部です。

本報告書の分析手法は、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。本報告書で使用されたすべてのインシデントは精査され、（必要に応じて）VERISフレームワークに変換されて、単一の匿名化された総合データセットが作成されました。しかし、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。

全般的に、主に次の3種類の方法が使用されました（詳細については後述します）。

1. ベライゾンがVERISを使用して実施した外部フォレンジック調査サービス（有料）とそれに関連する情報収集活動で直接記録
2. 協力企業・組織がVERISを使用して直接記録
3. 協力企業・組織の既存の記録システムからVERISに変換

再現可能な調査手法を用いて分析が行われ、複数のチーム構成員がすべての結果を検証しました。

協力企業・組織にはいずれも、事案データの中に関係する企業・組織または個人を特定できる情報があれば、すべて削除するように依頼しました。そのような詳細は、DBIRの作成に不要だからです。

インシデントではないデータ

2016年度データ漏洩/侵害調査報告書（DBIR）には、弊社の「インシデント」と「データ漏洩」のいずれの通常カテゴリにも該当しないデータの分析を必要とした章があります。それぞれについて、データ要素をVERISフレームワークに対応させ（適切な場合）、分析プロセスの一部始終を通じて各協力企業・組織とともに弊社の仮定とアプローチを検証しました。再現可能な調査手法を用いて分析が行われ、複数のチーム構成員がすべての結果を検証しました。

完全性と複雑性

インシデントまたは漏洩データを記録する目的は協力企業・組織によって異なるため、VERIS分類が示されていないレコードもあります。分類が少ないほど、分析時にレコードを意味のある方法で使用することが困難になります。ベライゾンでは、多くの情報を取り込んだ分析に役立つインシデントから、ほぼ何の計数も測定されていない低品質のインシデントを分離する自動選択アルゴリズムを採用しました。ここで使用したアルゴリズムでは、

各レコードにスコアが割り当てられます。スコアは「完全性」と「複雑性」という2つの主要な基準に基づきます。「完全性」は「実行者、アクション、資産、属性、被害者、タイムライン、発見方法、標的」などの主要記入項目の内容、「複雑性」は「各項目がどの程度詳しく記入されているか」ということです。結果として、より意味があり、かつ記述的であり、実用的な知見が得られます。この戦略に当てはまらないものは、該当する箇所で説明しています。

もう1つ重要な点は、知見に関して「未確認」は「未測定」と同等であることです。つまり、あるレコード（またはレコードグループ）に「未確認」とマークされた要素が含まれる場合、そのレコードに関してはその特定の要素について意見を述べられないことを意味します。それがインシデントで影響を受けたレコード件数といった基本的なものでも、マルウェアの機能といった複雑なものでも同じです。たとえば、実行者の動機が「未確認」のケースが10,000件、「金銭目的」が500件、「愉快犯」が100件あったとします。最初の10,000件は、測定可能な値のある他のケースについて何も示してはいません。このことを理解しておくことが重要です。

知見に関して「未確認」は「未測定」と同等で、情報がほとんどないことを示します。

漏洩データサンプルの偏りについて
この報告書の知見の多くは、統計学上の「一般化」の点で適切だと考えていますが、偏りや分析手法上の欠点は間違いなく存在します。弊社の全協力企業・組織からのレコードを組み合わせることで単独のレコードよりも正確に現実が反映されているとはいえ、所詮サンプルはサンプルに過ぎません。この報告書の知見の多くは、統計学上の「一般化」の点で適切だと考えていますが（これについての自信は増しています。より多くのデータを収集し他社のデータと比較しているからです）、偏りは間違いなく存在します。あいにく、偏りがどの程度存在するかについては正確に測定することができません（誤り分に相当する余地を正確に設定することはできません）。すべてのデータ漏洩の何割がこの報告書に現れているかを知る手立てはありません。世のすべての組織において2015年に発生したデータ漏洩の総数を知る手立てがないからです。多くのデータ漏洩は報告されずじまいです（ただし、この報告書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、被害者に認識されていません（そのため弊社でも認識できていません）。

VERISリソース
VERISは無料でご利用いただけます。ぜひ既存のインシデント対応報告システムに統合していただくか、少なくとも一度お試しください。

VerisCommunity.net：フレームワークの概要、使用例、分類の一覧をご確認いただけます。

GitHub.com/vz-risk/veris：すべてのデータ形式の詳細をご確認いただけるほか、公表済みのデータ漏洩を集めたデータベース、VERISコミュニティデータベース（VCDB）にアクセスいただけます。

Splunkbase.Splunk.com/app/2708/：インシデント分類パターンに対応付けられたSplunk用のコミュニティベースのアプリケーションです。

付録F：2015年の総括

ベライゾンサイバーインテリジェンスセンター（VCIC）の2015年の年明けは、1年のリスクの動向を予感させるインシデントの追跡で始まりました。私たちは、2014年11月にSony Pictures Entertainment（SPE）社で発生した巨大規模のデータ漏洩から実用的な知見を得ようと努めていました。この年最初のビジネスメール詐欺（BEC: Business Email Compromise）被害者とみられるのは、オンライン送金サービスを手がけるXoom社で、被害額は3,100万ドルに上りました。Palo Alto Networks社は、銀行を標的にしたトロイの木馬Dridexが「2015年初めの衝撃」と報告しました。レストランチェーンのChick-fil-A社と駐車サービスを手がけるOneStopParking社でペイメントカードデータの漏洩が発覚し、ニュースの見出しを飾りました。AOLやハフィントン・ポストなどの大手サイトに大規模な不正広告キャンペーンが仕掛けられたのもこの月です。不正広告からエクスプロイトキットを介して、Adobe Flash Playerのパッチ未適用のブラウザが攻撃されます。**1月**後半に、3つの広告ネットワークを標的にしたゼロデイ攻撃を緩和するFlash Playerの新バージョンがAdobe社から公開されました。

2月4日に、健康保険会社Blue Cross社の会員会社であるAnthem社が約8,000万名分の個人情報漏洩を発表しました。この事件については、2月27日にThreatConnect社が中国の攻撃グループ「Deep Panda」の関与の可能性を指摘しています。Invincea社とiSIGHT Partners社がそれぞれ、2014年11月に発生した中国のサイバースパイ活動キャンペーンに関する見解を公表しました。銀行を標的としたトロイの木馬Dyre、Vawtrak、Carbanakの活動が活発化し、注意リストに追加されました。Symantec社とMicrosoft社は、Ramnitボットネットを解体したことを発表しました。これは2015年初めての大規模ボットネット解体となりました。しかし犯人は特定されませんでした。多くの人が予想したとおり、約1カ月後にDr. Web社がRamnit復活の兆しを報告しています。

3月に入ると、やはりBlue Cross社の会員会社であるPremera社が約1,100万名分の個人情報漏洩を発表しました。ThreatConnect社の調査によると、この事件もDeep Pandaが関与しているとみられます。マンダリン・オリエンタルホテルグループは、ペイメントカードデータの漏洩を報告しました。POSベンダーであるNEXTEP社も、データの漏洩を報告しています。闇市場Webサイト「Evolution」が閉鎖され、関係者が逮捕されました。この市場は現在も閉鎖されたままです。カナダセキュリティインテリジェンスサービス（CSIS）は、Vawtrakがカナダの銀行を標的にしていることを報告し、AVG社は、Vawtrakキャンペーンが銀行の認証情報を世界中で収集していることを報告しました。

4月上旬に、中国が自国のサイバー攻撃システム「Great Cannon」を使用してGitHubにDDoS攻撃を仕掛けたという報告がもたらされました。これは、中国の検閲システムの回避を目的としたGitHubプロジェクトを標的にしたと考えられます。反検閲組織GreatFireもGreat Cannonの攻撃を受けています。ニュースアグリゲーターサイトのドラッジ・レポートは、エクスプロイトキットを介してクリック詐欺のトロイの木馬Bedepを送り込む不正広告を仕掛けられました。インターポール、Microsoft社、数社のセキュリティ会社が協力して、SimdaボットネットとBeeboneボットネットのインフラに打撃を与え、閉鎖に追い込みました。4月に私たちが入手した複数のインテリジェンスレポートでは、ロシアの国家機密機関との関与が疑われるサイバースパイ活動、Pawn StormとCozyDukeが注目を浴びていました。

1月
Xoom
ビジネスメール詐欺で
3,100万ドルの被害

2月
Deep Panda
8,000万件分の
データ漏洩に関与か

3月
Premera
1,100万名分のデータ漏洩

4月
Great Cannon
GitHubとGreatFireに
DDoS攻撃

5月には、インターコンチネンタルホテルズグループ、Sally Beauty Supply、FireKeeperホテル/カジノがペイメントカードデータの漏洩を発表しました。医療業界でも、Partners HealthCare、CareFirst Blue Cross & Blue Shield、MetroHealth、Bellvue Hospitalなど、データ漏洩が相次ぎ報告されました。ドイツ連邦議会とペンシルベニア州立大学に対するサイバースパイ攻撃が報告されましたが、詳細が乏しく実用的な知見は得られませんでした。5月は、銀行を標的としたトロイの木馬の中でも特にVawtrak、Dyre、Tinbaの報告が目立ちました。

6月に入り、健康保険情報の大規模漏洩を押しのけてニュースの見出しを新しく飾ったのは、米連邦政府の人事管理局（OPM）が発表したデータ漏洩でした。ニューヨークタイムズ紙は、OPMが攻撃を受けた時期は2014年3月であったと報じています。当初は400万件の漏洩と発表されましたが、最終的には2,100万件が漏洩していたことが判明しました。ThreatConnect社は、OPMのデータ漏洩がAnthemの事件と関連していることを突き止めました。『Fortune』誌は、SPE社のデータ漏洩に関する4部構成の調査レポートを掲載しました。また、『Wired』と『Der Spiegel』は、5月に初めて報告されたドイツ連邦議会に対するサイバースパイ攻撃に関するレポートを掲載しました。Cisco社は、3種類のセキュリティ製品でリモートアクセス用のSSH（Secure Socket Shell）キーに同じデフォルト値が使われていたことを報告しました。

7月にはデータ漏洩の報告が相次ぎました。まずはハーバード大学、2度目となるペンシルベニア州立大学、トランプホテルコレクション、カリフォルニア大学ロサンゼルス校（UCLA）です。それから数週間のうちに、さらに2件のデータ漏洩が報告されました。ソーシャルネットワーク/オンラインデートサイトのアシュレイ・マディソンでは、100GBにも及ぶデータが流出してインターネットに暴露されました。イタリアのセキュリティ/監視会社であるHacking Team社でも400GBのデータが漏洩しました。Hacking Team社で盗まれたデータからは未知の脆弱性情報が数件発見されています。

8月に入ってもデータ漏洩の嵐はやまず、American Airlines社、米国国防総省、米国保健社会福祉省、米国国税庁で漏洩が発覚しました。モバイルフォン小売業者のCarphone Warehouseは、VCICが知る限り、DDoS攻撃で標的の注意をそらしてその隙にデータを盗み出す複合型攻撃の被害者第1号となりました。無線ネットワーク会社のUbiquity社は、ビジネスメール詐欺によって4,700万ドルを失いました。AOLとハフィントン・ポストに不正広告が再び掲載され、MSN、Telstra社サイト、デートサイトのPlentyofFish.comにも不正広告が仕掛けられました。

中国のサイバースパイグループBlue Termiteが日本企業を標的とした複数の攻撃に関して、新しい知見が**9月**に公表されました。Proofpoint社は、ロシア軍とロシアの通信会社を標的にした、中国の別のサイバースパイ活動に関する報告を発表しました。Blue Cross & Blue Shield社の会員会社でのデータ漏洩が再度発覚し、Excellus社が2013年12月からあわせて1,000万件の個人識別情報（PII）と個人金融資産情報（PFI）が漏洩していたことを発表しました。

10月に入ってもデータ漏洩は続きます。信用調査会社のExperion社が攻撃を受け、同社のシステムに保存されていたT-Mobileユーザーの個人情報1,500万件が漏洩したことを発表しました。英国の無線プロバイダTalkTalk社でも契約者400万名分のデータが漏洩しました。デイリー・メールのサイトに不正広告が仕掛けられ、その間1,500万人の訪問者が影響を受けました。Trend Micro社は、Hacking Team社のデータキャッシュから初めて発見されたAdobe FlashとJavaの脆弱性を突く複数の攻撃にPawn Stormが関与していることを突き止めました。銀行を標的としたトロイの木馬Dridexの大規模ボットネットが解体され、Dridexの作者であるAndrey Ghinkulが逮捕されました。

11月の初旬に、Dridexが復活して活動を再開したという情報がVCICに届き始めました。DDoS恐喝実行グループの「The Armada」が登場し、複数の電子メールサービスプロバイダを攻撃しました。2014年に起きたJPモルガン・チェースのデータ漏洩事件の犯人が起訴され、攻撃は株価操作の一環として行われたことが明らかになりました。オーストラリアの小売業者であるFarmer's Direct社は、5,000人以上の顧客のアカウント登録情報が漏洩したものの、その中にペイメント情報は含まれていなかったことを発表しました。

5月
医療業
保険会社のデータ漏洩が相次ぐ

6月
米国人事管理局
2,100万名分のデータ漏洩

7月
アシュレイ・マディソン
100GB分のデータ盗難に世界が注目

8月
Ubiquity
ビジネスメール詐欺で4,700万ドルの被害

9月
Blue Termite
中国のサイバースパイグループが日本の企業を攻撃

10月
Experion
1,500万名分のデータ漏洩

11月
Dridex
銀行を標的としたマルウェアが復活

情報セキュリティの世界では、最新の大規模データ漏洩で1年を締めくくるのが恒例のようです。**12月**に、オーストラリア気象局（BOM）でデータ漏洩が発生した模様です。調査機関からの情報によると、中国の犯罪グループが関与しているとみられます。しかし、BOMのデータ漏洩について詳細情報が含まれた報告書や情報はありません。このほか、インディペンデント、ガーディアン、デイリーモーションに不正広告が掲載されました。Juniper社は、ScreenOSにバックドアの脆弱性を発見したことを報告しました。2015年の幕が閉じようとしている12月23日、ウクライナで大規模停電が発生しました。ウクライナの電力会社からBlackEnergyマルウェアが発見されています。このため、VCICと多くのセキュリティ会社は多忙な年末を過ごすことになったのです。

12月

BlackEnergy

ウクライナでマルウェアによる停電が発生

verizonenterprise.com/jp/

表紙について
表紙は3種類の図で構成されており、2016年度のDBIRで使用されている
インシデントデータを象徴しています。今年は最終的に6万4,199件の
インシデントと2,260件のデータ漏洩が調査対象になりました。

まず、背景の白線で8つに分割された図は、ツリーマップを示しています。
各ボックスは、属性または活動の分類を表します。上部の3つのボックスは、
左から時計回りに、機密性の喪失、完全性の喪失、可用性の喪失を伴う
インシデントを表します。下部の5つのボックスは、左から時計回りに、ミス、
ハッキング、ソーシャル、マルウェア、不正使用の脅威活動を伴うインシデントを
表します。各ボックスの大きさは、全インシデント件数に対する各分類の
比率を表します。

2つ目に、円に囲まれたピラミッドの図は、米国の1ドル紙幣の裏面に
描かれている絵柄です。今年は金銭目的のデータ漏洩が多かったことを
象徴すると同時に、企業や個人がサイバー犯罪から自身を守るには
高いコストがかかることを暗示しています。全能の目は意図的に
やや下を向かせていますが、これには2つの意味があります。
サイバーセキュリティ防御者にとって見えざる攻撃者はあらゆる場所に
存在するように思われることと、そして、ピラミッドの石（3つ目の図）が
象徴するデータを監視する必要があることを表しています。

3つ目の図のピラミッドを構成する石はワッフルチャートになっており、
漏洩データについて種類別の件数を表しています。このワッフルチャートには、
可用性の喪失をもたらしたデータ漏洩を表す石も含まれています。
それぞれの石（両端にある台形の石を含む）は、石の数に対応する78件の
インシデントを表します。下から上に、属性が認証情報（赤紫）、ペイメント
カードデータ（紫）、個人情報（ピンク）、企業秘密（青）、可用性の喪失（緑）、
医療データ（濃い黄）、銀行データ（明るい黄）、組織内部情報（濃い紫）、
そして右上のオレンジ色の石が「その他すべて」を表します。