2012年度データ漏洩/侵害調査報告書

オーストラリア連邦警察、オランダハイテク犯罪ユニット、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ーサービス(IRISSCERT)、
ロンドン警視庁サイバー犯罪合同捜査本部、アメリカ合衆国シークレットサービスの各機関による協力のもと、ベライゾンRISKチームによる調査が実施されました。

verizon

2012年データ漏洩/侵害調査報告書

ベライゾンRISKチームによる調査。協力は、オーストラリア連邦警察、オランダハイテク犯罪ユニット、
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ーサービス（IRISSCERT）、
ロンドン警視庁サイバー犯罪合同捜査本部、アメリカ合衆国シークレットサービスの各機関。

2012 年度データ漏洩 / 侵害調査報告書

目次

最新情報や関連情報については、verizon.com/enterprise/securityblog をご覧ください。

エグゼクティブサマリー

2011 年は民主化の波が渦巻いた年として、間違いなく歴史に残るでしょう。各国で市民が立ち上がり起こった反乱が波及し、ドミノ倒しのように政権を打倒しました。「アラブの春」と言われるようであり、しかも激動は一時で終わることはありませんでした。また、「1%の富裕層」に不満を覚えた市民がウォール街をはじめ、世界中の都市で占拠運動を展開しました。そういった例には限りがありません。

2011 年に見られた混乱は、現実の世界だけに留まりませんでした。オンラインの世界では悪意に満ちた観念が、社会的・政治的行動主義や抗議、報復、嫌がらせの形で、その姿を現しました。この種の現象は、一般的なデータ漏洩 / 侵害（DDoS 攻撃など）の範囲を逸脱しているように見えますが、結局は企業･組織や個人の情報の窃盗が目的でした。「ハクティビズム」という名の正体の見えない脅威が力を取り戻して世界中の企業・組織の前に立ちはだかったのです。この正体の見えない脅威の出所と癖や性格といったものは隠されたままであり、だからこそ厄介であり、また想像の産物もしくは現実のものであるかを問わず、一般の脅威より恐ろしいと感じる人が多いのです。ハッカーは一般に金銭や貴重な情報を標的にしますが、このようなハクティビズム集団の標的は必ずしもそうではなく、これが企業・組織や幹部にとっては一層の頭痛の種です。その行動を予測できない敵こそ、真に恐ろしい敵と言って間違いはありません。

「ハクティビズム」という名の正体の見えない脅威が力を取り戻して世界中の企業・組織の前に立ちはだかったのです。

とはいえ、攻撃は、その全部が抗議や面白半分のいたずらだった訳ではありません。2011 年の場合、サイバー犯罪の主な手口は前年と同じく、自動化し、効率の良い最新の方法を駆使し、大量かつ低リスクとなる脆弱な標的を狙い、データを入手するというものでした。一方、発生件数ははるかに少なかったのですが、損害が大きかったと思われる攻撃、つまり企業秘密や機密情報、その他の知的財産に対する攻撃も前年に引き続き見られました。また、ハッカーやその手法、動機は多岐に渡っていましたが、主な犯罪は企業データの窃盗で、その種類や内容は様々でした。今回の 2012 年度データ漏洩 / 侵害調査報告書（DBIR）は、そのまとめです。

データ漏洩 / 侵害の件数は 855、侵害されたレコードの数は 1 億 7400 万でした。

今回、協力機関が増えたこともあり、本年の DBIR で扱ったデータ漏洩 / 侵害の件数は前年よりも増加しており、地域的範囲も広がっています。また、侵害レコード数は、前年は 400 万件と記録的に少なかったのに対して（もっともそれでも多いという人もいるでしょう）、今回は 1 億 7400 万に跳ね上がっています。実際、2011 年の 1 億 7400 万というレコード侵害数は、2004 年からの記録の中では 2 番目に多い数字です。

本年もアメリカ合衆国シークレットサービス（USSS）とオランダハイテク犯罪ユニット（NHTCU）から協力を頂戴しましたので、ここで報告します。また、オーストラリア連邦警察（AFP）、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ーサービス（IRISSCERT）、ロンドン警視庁サイバー犯罪合同捜査本部（PCeU）からも協力を賜りました。**上記の機関からいただいた資料により、今回の DBIR で扱うことができたデータ漏洩 / 侵害事例（データ漏洩 / 侵害または単に事例と呼ぶこともあります）は、これまでと比較して大幅に増加しました。各機関の協力精神に感謝申し上げるとともに、本報告書がサイバー犯罪に対する警鐘として、また犯罪防止の有効な道具として寄与することを願うものであります。**

攻撃は、その全部が抗議や面白半分のいたずらだった訳ではありません。2011 年の場合、サイバー犯罪の主な手口は前年と同じく、自動化し、効率の良い最新の方法を駆使し、大量かつ低リスクとなる脆弱な標的を狙い、データを入手するというものでした。

ベライゾンの 2011 年の事例データのほか、上記の各機関から提供された事例データを加えると、過去 8 年に渡る DBIR シリーズで扱ったデータ漏洩 / 侵害数は 2000 を優に超え、侵害レコード数は 10 億を上回ります。このシリーズは、興味深く有意な記録です。多くの読者に、感謝の意を表します。本調査の目的はこれまでと同様、読者が所属する企業や組織において事業計画やセキュリティ対策を策定する上でその一助として活用されることにあります。では以下に、報告書の要点と主な分析結果を列挙します。

データ漏洩 / 侵害の背後にいるのは誰か?

98% が外部因子によるもの（+6%）

4% が内部の従業員（内部因子）によるもの（-13%）

<1% がビジネスパートナーによるデータ漏洩 / 侵害（同）

データ窃盗の 58% が活動家グループの関与によるもの

これまでと同様、ほぼ全てのケースで外部の者（外部因子）による企業データ窃盗が起きていますが、これは特に驚くに値しません。2011 年の場合、外部因子によるデータ漏洩 / 侵害としては、組織犯罪によるものが大半を占めていました。また、2011 年は活動家グループによるデータ漏洩 / 侵害もかなりの割合を占め、この場合、一般の企業・組織より、別のグループや組織からデータを盗むというケースが多く見られました。活動家グループが舞台に登場したせいで、データ漏洩 / 侵害の動機という点で、状況にいくぶん変化が生じました。つまり、いまだに金銭がデータ漏洩 / 侵害の主たる動機ですが、一方、イデオロギーの違いや恨み、憎しみが主な動機になっている事例も増えたことです。このように外部の攻撃者が増加したことから想像できるように、部内者によるデータ漏洩 / 侵害の割合は大幅に減少し、4% まで低下しました。

データ漏洩 / 侵害はどのようにして発生するか?

昨年は、ハッキングによるインシデントとマルウェアによるインシデントがともに増加し、とくに侵害レコードのうち、ほぼ全部がハッキングによって侵害されています。この 2 種類の脅威アクションは外部因子が好んで使う手法であり、したがって外部因子によるデータ窃盗が非常に多いことと（上記）、この 2 種類の脅威アクションが増加していることは符合します。窃盗もしくは推測した認証情報を組み合わせて認証を突破または迂回し（アクセスを開始）、その後、バックドア（アクセスを保持）を介して攻撃するという方法が依然として多く発生していました。一方、ATM やガソリンスタンドの給油機でのスキミング事例は減少し、その結果、本報告書では物理攻撃によるデータ漏洩 / 侵害の割合はかなり減りました。権限の不正使用によるデータ漏洩 / 侵害は減っており、これは内部因子による侵害事例が減ったことを考えると当然です。ソーシャルエンジニアリングは若干減っていますが、それでも大量のデータ漏洩が起きたケースはソーシャルエンジニアリングによって発生しています。

81% が何らかのハッキングによるもの（+31%）

69% がマルウェアによるもの（+20%）

10% が物理的攻撃により発生（-19%）

7% がソーシャルエンジニアリング（-4%）

5% が権限の不正使用によるもの（-12%）

どのような共通点があるか?

79% がオポチュニスティック（無作為）型の攻撃（-4%）

96% の攻撃は、技術的にそれほど高度とは思われない（+4%）

全データ漏洩 / 侵害の 94% がサーバー上のデータの侵害（+18%）

データ漏洩 / 侵害の 85% が数週間以上経過した後に発見（+6%）

データ漏洩 / 侵害の 92% が第三者によって発見（+6%）

97% の侵害は、初歩または中級レベルの対策を実施していれば回避できたと考えられる（+1%）

96% の被害者はクレジットカード業界のセキュリティ基準（PCI DSS）への準拠義務があったにもかかわらず非準拠（+7%）

昨年の事例データからは、これまでと同様、標的を意識して選ぶというより無作為に攻撃するという傾向があることが分かりました。事前に攻撃の対象として選定されていたからではなく、悪用可能な脆弱性があったため（それも相当脆弱な場合が多い）、データ漏洩 / 侵害を受けたという企業・組織がほとんどでした。

攻撃が標的型か無作為かを問わず、データ漏洩 / 侵害を受けた企業・組織のうち、その大半が決して技術的に高度ではない攻撃によって侵害を受けました。防御態勢がある程度できている企業・組織の場合も通常、最初のアクセスの後、しばらく経過すると上記と同様の傾向があることが分かりました。

上記の結果を考慮すると、技術的に高度で高価な防御措置を講じなくても、ほとんどのデータ漏洩 / 侵害が回避可能であり（少なくても後から考えるとそう言えます）、これは不思議ではありません。PCI DSS に対する準拠義務がある企業のうち、完全に準拠している企業は少なく、これは準拠しなければならない項目が多すぎることが足枷となっていることを示しています。

データ漏洩 / 侵害を受けた場合、少なくとも通常は何らかの証拠が残っているのですが、その被害者自身が発見することは稀です。第三者からの情報によって発見されるのが普通で、それも数週間後もしくは数カ月が経過してから発見というケースが少なくありません。

2011 年はどこがどう「悪化」したのでしょうか。

この報告書を作成するときに思うのは、私どもにはデータの処理や分析に必要なツールが揃っているということです。ここで大事なのは、適切なツールを選ぶと同時にその切れ味を鈍らせ錆びつかせないようにすることです。これを怠った途端、ハッカーはすぐさま、そこに付け入ってくることは今までの経緯からも明らかです。

本報告書では、小中規模の企業・組織のデータ漏洩 / 侵害と大規模企業向け・組織のデータ漏洩 / 侵害を対比させる形で解説します。両者では直面している問題が大きく異なり（場合によっては非常に類似）、この対比により、両者の傾向が把握できるはずです。また、当然のことながら問題解決の方法も両者で異なり、このことも理解していただけます。本報告書の巻末には推奨事項を掲載してありますが、いずれも大規模企業向けのものです。といっても小中規模企業・組織を無視しているのではありません。記載していないのは、小中規模企業・組織にとって、サイバー犯罪は家の中で発生する疫病みたいなもので、ほとんどの場合、簡単な方法で防げるからです。

一方、大規模企業向け・組織では、問題は複雑かつ多様であり、したがって解決策も複雑かつ多様です。上記のようなケースでは、個々の対策の優先順位を設定するとともに、基本的な戦略を構築し対応しなければなりません。その場合、豊富な情報をもとに自らを省察することによって脅威を評価する必要がありますが、本報告書の分析結果がその一助となれば幸いです。

被害軽減策で重点を置くべき領域は?

小中規模の企業・組織

- ファイアウォールをインストール、またはリモートアクセスサービスに ACL（アクセス制御リスト）を設置する。
- POS システムのデフォルトの認証情報、またインターネットに繋がっている機器のデフォルトの認証情報を変更する。
- サードパーティベンダーが上記の POS システムまたはデバイスを管理・運用している場合、デフォルトの認証情報を変更するように指示し、確認する。

大規模企業向け・組織

- 不要なデータを削除し、残っているデータを監視・管理する。
- 基本的な管理事項が守られているかどうかを確認し、また定期的にチェックする。
- イベントログを監視し、内容をチェックする。
- 脅威状況を評価し、対策に優先順位を付ける。
- 本報告書の結論を参照し、一般的な脅威の徴候を見分け、必要な対策を実施する。

データ漏洩 / 侵害報告書に関するご意見、ご質問は、大いに歓迎します。
ご意見やご質問は dbir@verizon.com までお寄せください。Facebook や Twitter（hashtag #dbir）もご利用いただけます。

メソドロジー

本報告書に関する意見や提案から察すると、私どもがデータの収集や分析、提示に対してどこまで厳格かつ真摯に取り組んでいるか、それが読者の大きな関心事のひとつのようです。これは当然、私どもにとっても重要事であり、その点で読者には感謝します。しかしながら忌憚のないところを話せば、データの収集や分析を含め、本報告書の作成は公園の散歩とはまったく異なります（855 件のデータ漏洩 / 侵害の分析は、決して楽な作業ではありません）。実際、誰も分からず誰も気がつかないのであれば、手抜きをしてサッサと済ませたいところです。ただし読者には見破られると思うと、そのようなことはできません。以下は、その姿勢の結果です。

ベライゾンのデータ収集メソドロジーは、基本的には今までの方法と同じです。つまり、2004 年から 2011 年の間にベライゾンが実施したフォレンジック調査（デジタル鑑識）で得られた直接証拠を事例データとし、分析を行っています。

ベライゾンのデータ収集メソドロジー

ベライゾンのデータ収集メソドロジーは、基本的には今までの方法と同じです。つまり、2004 年から 2011 年の間にベライゾンが実施したフォレンジック調査（デジタル鑑識）で得られた直接証拠を事例データとし、分析を行っています。分析では、主に 2011 年のデータを使用しましたが、2004 年以降の累積データも必要に応じて使いました（複数年の傾向分析などに使用）。ベライゾンの RISK チームが扱った事例（2011 年は 250 件超）の中には、データ漏洩 / 侵害が確認されなかったものもあり、そのうちデータ漏洩 / 侵害が確認された事例だけを採用しました。結局、2011 年の場合、データ漏洩 / 侵害が確認され、かつこの報告書で取り扱われているのは、90 件になりました。入力の信頼性と一貫性を確保するため、ベライゾンエンタープライズリスク / インシデントシェアリング（VERIS）フレームワークを用いてこれら事例データと関連情報を記録しました（詳細は後述）。データ漏洩 / 侵害事例の調査が完了した後、そのデータをアナリストが VERIS フレームワークを使って入力しました。データの入力後、RISK チームの他のメンバーがチェックし、誤りがないかを確認しました。また、安全のため、企業や機関、個人の身元が判明する可能性のある情報をすべて、集計処理の際に事例データから削除しています。

各協力機関のデータ収集メソドロジー

各機関でのデータの記録方法は、厳密に言えば（アメリカ合衆国シークレットサービス（USSS）、オランダハイテク犯罪ユニット（NHTCU）、オーストラリア連邦警察（AFP）、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ーサービス（IRISSCERT）、ロンドン警視庁サイバー犯罪合同捜査本部（PCeU）、と各機関によって異なりますが、基本的には同じです。つまり、各機関のデータはすべて VERIS を介して入力されましたが、機関によって具体的な方法が多少異なりました。例えば、USSS の場合、USSS のスタッフが VERIS ベースのアプリケーションを使って事例のデータを入力しました。AFP の場合、責任者に連絡して各データ漏洩 / 侵害事例について尋ね、得られた情報を VERIS で入力しました。その後、必要に応じて連絡を取り、最新情報を入手し、記録しました。データの収集･記録は、その方法より、データが実際のインシデント（データ漏洩 / 侵害事例）に基づいたデータであるかどうかが大事であり、また何より肝要なのは、データがインシデントの事実を忠実に反映しているかどうかです。各機関には、調査メモのほか、データ漏洩 / 侵害を受けた企業・組織やフォレンジックス調査会社から提出された報告書、さらに現場での経験もあり、このような資料や経験も勘案してデータが入力されました。最後に、企業や機関、個人を識別できる情報がデータから削除された後、ベライゾンの RISK チームに渡され、集計と分析が行われました。

事例について言えば、2011 年に各機関が扱った事例のうち、企業・組織に関連するデータ漏洩 / 侵害事例であり、かつデータ漏洩 / 侵害が実際に確認されたものだけを抽出しました。[1] これは、DBIR の編集方針に合わせるためです。さらに、その中からベライゾンがフォレンジックス調査を行わなかった事例だけを抽出しました。[2] 結局のところ、各協力機関のデータ漏洩 / 侵害事例のうち本報告書で使用したのは、全部で 765 件でした。本報告書で扱った全事例データの中ではベライゾンの事例データは比較的少なく（90 件）、これには不安を覚える読者もおられるかもしれません。ただし、私どもとしては喜ばしい限りといったところです。情報が多ければ多いほど、目の前の問題を一層、完璧かつ正確に把握できるからです。ベライゾンの出版物なのにベライゾンのデータが脇役なのはどうか、という向きもおられるかもしれませんが、それはそれでいいでしょう。共有データに対して意見を交わすことは大歓迎です。

1　「企業・組織に関連するデータ漏洩 / 侵害」とは、企業・組織によって非公的情報が保管、処理、使用、転送されているときに、その非公的情報が侵害されること（無許可アクセス、窃盗、不正開示など）をいいます。

2　ベライゾンは、各機関が捜査を行う際、何らかの形で共同で捜査・調査に当たることがよくあります。その関係から、いずれかの機関の事例データとベライゾンの事例データが重複していることもあり、そのような場合にはベライゾンの事例データを採用しました。

貴社の組織で発生したデータ漏洩 / 侵害を内部で調査･処理し、その結果を今後の DBIR に役立てたいとお考えの方は、ベライゾンにご連絡ください。DBIR シリーズは今後も継続する予定であり、皆様のご協力は大歓迎です。

VERIS について

VERIS は、共通の言語でセキュリティインシデントに関する情報を記録できるフレームワークです。反復可能な構造化形式で情報を入力でき、「誰が、何にまたは誰かに、どの様なことをして、結果はどうなったか」という物語風に情報を入力すると一定形式のデータ（本報告書に記載されているようなデータ）に変換されます。ベライゾンでは、DBIR のデータ収集方法について質問を受けることが多く、また今以上にセキュリティインシデントに関する情報をより多くの企業・方々と共有したいと考えていることから VERIS は公開されており、誰でも無料で使用できます。VERIS の概要については弊社ウェブサイト[3] に掲載されていますが、詳しい説明は VERIS コミュニティ wiki.[4] で閲覧できます。弊社のウェブサイトと VERIS コミュニティはどちらも、本報告書の内容や用語を理解する上で有用です。

VERIS でのインシデント分類

VERIS フレームワークには、「インシデント分類」というセクションがあります。ここでは、「誰が何に（または誰に）何をして、結果はどうなったか」という物語風の形式でインシデントを記録でき、この方法は、後日にデータ分析を行う上でも有効です。具体的には、VERIS では A4 脅威モデル（A で始まる分類項目を 4 つ使用するモデル）にしたがってインシデントを記録します。このモデルは、ベライゾンの RISK チームが開発したものです。A4 脅威モデルでは、企業･組織の情報に悪影響を与える一連のイベントを 1 件のセキュリティインシデントとみなします。イベント（脅威イベントとも呼びます）はそれぞれ、次の要素（A で始まる 4 つの要素）で構成されます。

- **脅威因子（Agent）**：誰が資産を侵害したか。
- **脅威アクション（Action）**：どのような行為または方法によって資産が侵害されたか。
- **資産（Asset）**：どの資産が侵害されたか。
- **属性（Attribute）**：どの属性が影響を受けたか。

上記の 4 つの A は、あらゆるセキュリティインシデントや脅威を適切に記述する場合に必要となる最小限の情報です。また、VERIS フレームワークは、発生頻度や関連コントロール、リンク効果など、リスク管理に必要となる多数の事象を測定するのに最適のフレームワークです。

A[4] 脅威モデルでは、脅威因子が 3 種類、脅威アクションが 7 種類、資産が 5 種類、属性が 3 種類ありますので、脅威イベントは全部で 315 種類[5] 存在することになります。下記は 315 種類の脅威イベントをすべて示した表で、それぞれ脅威イベント番号で識別されます（脅威イベント番号は、先頭に TE# を付加して表します）。例えば、TE#1 は、脅威因子が外部、脅威アクションがマルウェアであり、かつサーバーの機密情報が侵害された脅威イベントを表しています。なお、315 種類の脅威イベントがすべて存在するとは限りません。例えば、少なくても私どもの知る限りにおいては、マルウェアが人間に感染することはありません（もっとも SF 小説や映画であれば、この筋立ては面白いかもしれませんが）。

上記の 4 つの A は、あらゆるセキュリティインシデントや脅威を適切に記述する場合に必要となる最小限の情報です。

インシデントを構成する脅威イベントの特定

上述のように、インシデントは、複数の脅威イベント（一連の脅威イベント）で構成されるのが普通です。したがって、どのような脅威イベントが発生したかを特定するとともに、各脅威イベントがどのような順番で発生したかを把握することがインシデントの理解に有効であり、VERIS でも、この方法を踏襲しています。以下、簡単なインシデントを例にして、この方法を説明します。例では、最初の攻撃の手口は「スピアフィッシング」、目的は、企業の機密データと知的財産（IP）の窃取と仮定しています。

後述のフローチャート図で分かるように、このインシデントは、4 つの脅威イベントと 1 つの条件イベント（菱形マーク）で構成されています。[6] 脅威イベントの下にはそれぞれ、簡単な説明を記載してあります。また、脅威イベント番号（TE#）と、そのイベント番号が示している 4 つの分類項目（脅威因子、脅威アクション、資産、属性）の内容を記載してあります。

3 http://www.verizonbusiness.com/resources/whitepapers/wp_verizon-incident-sharing-metrics-framework_ja_xg.pdf
4 https://verisframework.wiki.zoho.com/（内容英語）
5 お気づきの方もいるかもしれませんが、2011 年度データ漏洩 / 侵害調査報告書では、脅威イベントの種類は全部で 630 種類でした。この違いは、今年から属性（セキュリティ属性）の種類を減らしたことによります。具体的には、「パーカーの 6 要素」は今後も使用しますが、本年から対の形式で表記することにしました（例えば、機密性と所有を組み合わせて「機密性と所有」と表記します）。このようにすることで、機密性と所有という概念が残り、しかもデータの分析と結果の理解が容易になります（VERIS のユーザーから多くの要望があったため変更しました）。この変更については、VERIS wiki（https://verisframework.wiki.zoho.com/）の" Attributes" のセクションに詳しい説明があります。
6 条件イベントについては、詳しくは「脅威アクション」の「過失」の節を参照してください。

図 1. VERIS の 315 種類の脅威イベント（A^4 脅威モデル）

		マルウェア			ハッキング			ソーシャル			不正使用			物理的脅威			過失			環境面の脅威		
		外部	内部	パートナー	外部	内部	パートナー	外部	内部	パートナー	外部	内部	パートナー	外部	内部	パートナー	外部	内部	パートナー	外部	内部	パートナー
サーバー	機密性と所有	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
	整合性と信憑性	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42
	可用性と有用性	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
ネットワーク	機密性と所有	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84
	整合性と信憑性	85	86	87	88	89	90	91	92	93	94	95	96	97	98	99	100	101	102	103	104	105
	可用性と有用性	106	107	108	109	110	111	112	113	114	115	116	117	118	119	120	121	122	123	124	125	126
ユーザー機器	機密性と所有	127	128	129	130	131	132	133	134	135	136	137	138	139	140	141	142	143	144	145	146	147
	整合性と信憑性	148	149	150	151	152	153	154	155	156	157	158	159	160	161	162	163	164	165	166	167	168
	可用性と有用性	169	170	171	172	173	174	175	176	177	178	179	180	181	182	183	184	185	186	187	188	189
オフラインデータ	機密性と所有	190	191	192	193	194	195	196	197	198	199	200	201	202	203	204	205	206	207	208	209	210
	整合性と信憑性	211	212	213	214	215	216	217	218	219	220	221	222	223	224	225	226	227	228	229	230	231
	可用性と有用性	232	233	234	235	236	237	238	239	240	241	242	243	244	245	246	247	248	249	250	251	252
人間	機密性と所有	253	254	255	256	257	258	259	260	261	262	263	264	265	266	267	268	269	270	271	272	273
	整合性と信憑性	274	275	276	277	278	279	280	281	282	283	284	285	286	287	288	289	290	291	292	293	294
	可用性と有用性	295	296	297	298	299	300	301	302	303	304	305	306	307	308	309	310	311	312	313	314	315

インシデントを構成する脅威イベントと、その流れを特定できれば、各脅威イベントについて 4 つの分類項目の具体的内容（脅威因子が外部、脅威アクションがソーシャルなど）を決定します。この作業はインシデントの「VERIS 化」であり、VERIS でも、この方法でデータを入力します。また、入力により、各種の指標を使って分析を行えるようになります。

インシデントを構成するイベントの特定と、その流れの把握は、
インシデントを理解するだけでなく、インシデントを阻止するのに何をしたか
（または何をしなかったか）を把握する上でも有効です。
インシデントを阻止する方法は、単純にして明快です。最初のイベント、
もしくはイベントの連鎖を断ち切ればよく、これでインシデントを阻止できます。

このセクションの最後にひとつ付け加えます。上記の方法、つまりインシデントを構成するイベントの特定と、その流れの把握は、インシデントを理解するだけでなく、インシデントを阻止するのに何をしたか（または何をしなかったか）を把握する上でも有効です。インシデントを阻止する方法は、単純にして明快です。最初のイベント、もしくはイベントの連鎖を断ち切ればよく、これでインシデントを阻止できます。例えば、トレーニングによるセキュリティ意識の改善や電子メールフィルタリングの使用は、E1 の発生を抑える上で効果的です。また、ノートブックにアンチウイルスソフトウェアをインストールしたり、パスワードなどでノートブックを保護することで、E2 を阻止できる確率は高まります。E3 は、出口フィルタリングやネットフロー分析を行い、バックドア経由のアクセスを検出するという方法で防止できる可能性があります。さらに、システム管理者の設定ミス（CE1）は、トレーニングの実施と変更管理手順の厳格化を通じて回避できる可能性があり、回避できれば、E4 の知的財産の流出に至ることはありません。以上は、実施可能な対策のほんの一部ですが、このような階層化アプローチ（多重手法）は、インシデントの阻止、防止、検出に有効であることは明らかです。

図 2. VERIS 化したインシデントの例

企業の役員が、外部の脅威因子（外部因子）からフィッシング電子メールを受け取りました（ここでは、外部因子はハッカーです）。役員は、電子メールを信用し、その添付ファイルを開きました。	役員のノートブックがマルウェアに感染し、その結果、バックドアが作成されました。	外部因子（ハッカー）がバックドアを使って役員のノートブックに侵入し、電子メールや重要文書など、会社の機密データを物色。	システム管理者が新規ファイルサーバーを構築する際、アクセスコントロールを誤って設定。	ハッカーが役員のノートブックを介してファイルサーバーにアクセスし、知的財産を窃取しました。
TE#280 外部 ソーシャル 人間 整合性	TE#148 外部 マルウェア ユーザー機器 整合性	TE#130 外部 ハッキング ユーザー機器 機密性	TE# 38 内部 過失 サーバー 整合性	TE#4 外部 ハッキング サーバー 機密性

標本の偏りについて

繰り返しになるかもしれませんが、本報告書の分析結果はいずれも、今まで世界中の企業・組織で発生した全データ漏洩 / 侵害を代表するものではないことをここに明記します。本報告書ではベライゾンと各協力機関のデータを合わせて使用しているため、いずれかのデータを単独で使用したときに比べ（推定上）、より現実を反映した結果が表れているといえますが、データはあくまで「サンプル」です。本報告書の分析結果は、その多くが「標準」（したがって普遍的）であると信じていますが（事例データの量が増え、今まで以上に正確な比較が可能になるにつれてこの自信は深まっています）、それでも偏りは疑いなく存在します。残念ながら、標本（サンプル）に存在する偏りを正確に測定することは不可能です（測定できれば、許容誤差を正確に計算できます）。2011 年に世界中の全企業・組織で発生した全データ漏洩 / 侵害の総数は不明で、したがって本報告書で扱ったデータ漏洩 / 侵害が、そのうちどのくらいの割合を占めるのかも不明です。公表されていない事例も少なくありません（ただし、本報告書の事例の中には、未公表のものも多数含まれています）。また、被害者が気づいていない事例も多く存在します（この種の事例は、本報告書で扱われることはありません）。確かなのは、年を追って事例データが増えるにつれて分析や研究から得た知識も増えることであり、とくに本年の場合、事例データ（2011 年のデータ）はかつてないほど増えました。結局、私どもの仕事は分析結果を読者の皆さんに渡すことに他ならず、本報告書の評価や使用は読者に一任します。

データ漏洩 / 侵害報告書に関するご意見、ご質問は、大いに歓迎します。
ご意見やご質問は dbir@verizon.com までお寄せください。Facebook や Twitter（hashtag #dbir）もご利用いただけます。

結果と分析

2011 年の総合事例データ（ベライゾンと各協力機関の事例データを合わせたもの）によると、データ漏洩 / 侵害数が 855 件、侵害レコード数が 1 億 7400 万を超えており（2004 年からの記録の中では 2 番目）、これは 1 年間のデータ漏洩 / 侵害の規模としては過去最大でした。以下、本報告書で使用した事例データについて、いくつか留意点を説明します。

本報告書では、2004 年から 2011 年までの全事例データを使用して分析を行っている箇所がいくつかあります。この種の分析の結果を読む場合、分析の基礎となっている事例データは決して「静的」ではないことを念頭に置いておいてください。数値や傾向、事例データの入手元（捜査・調査機関や場所）は、時間とともに大きく変化するのが普通だからです。にもかかわらず、同じような傾向が何年も続いている場合もよくあります（このような傾向は、普遍性がある傾向といえます）。一方、傾向が変化した場合でも、それは外部の脅威環境における大きな変化でなく、事例データの「異常」といったほうが妥当なこともあります。本報告書では、主に 2011 年の総合事例データを使って分析を行い、ベライゾンや協力機関の事例データの間に相違点（または類似点）があれば、必要に応じて、その相違点などを本文中で説明してあります。また、分析によってはベライゾンの事例データだけを使用している場合もあり、そのようなケースでは適宜、その旨を付記してあります。

本報告書に掲載されている図は、いずれも同じ形式で作成されています。いずれの図でも、データ漏洩 / 侵害に関する数値は**濃いグレー**、レコードに関する数値は**赤**で記載されています。本報告書では、「データ漏洩 / 侵害」とは分析対象となったインシデントをいい、「レコード」とは侵害されたデータ（ファイルやカード番号など）を指します。図によっては、侵害レコード数の記載がなく、代わりに赤い「#」記号が付記されている場合があります。この「#」記号は、全侵害レコード数の中で、その侵害レコード数の割合（%）が高いことを示しています。また、侵害レコード数の割合が前年と比べて大幅に増加しているときは「+」（オレンジ色）、大幅に減少しているときは「−」（同じくオレンジ色）が付記されています。図と表の中には、記載されている%値を合計すると 100%を超えるものも少なくありませんが、これは計算間違いやタイプミスではありません。これは、項目（脅威因子など）の中には必ずしも相互排他的ではないものもあり、そのため、同一のデータ漏洩 / 侵害に複数の項目が該当する場合もあるためです。

表 1. データ漏洩 / 侵害事例の数と割合（%）の関係を示した表（2012 年 DBIR の事例データ）

漏洩件数 855 件

%	#
1%	9
5%	43
10%	86
25%	214
33%	282
50%	428

いずれの図でも、データ漏洩 / 侵害に関する数値は**濃いグレー**、レコードに関する数値は**赤**で記載してあります。本報告書では、「データ漏洩 / 侵害」とは本報告書で分析の対象となったインシデントをいい、「レコード」とは侵害されたデータ（ファイルやカード番号など）を指します。図によっては、侵害レコード数の記載がなく、代わりに赤い「#」記号が付記されている場合があります。この「#」記号は、全侵害レコード数の中で、その侵害レコード数の割合（%）が高いことを示しています。また、侵害レコード数の割合が以前と比べて大幅に増加しているときは「+」（オレンジ色）、大幅に減少しているときは「−」（同じくオレンジ色）が付記されています。

本報告書で扱っているデータ漏洩 / 侵害の数は非常に多く、パーセンテージを使うと誤解を招く恐れがあります（例えば、本報告書で 5%のデータ漏洩 / 侵害というと数は少ないように見えますが、40 件を超えるデータ漏洩 / 侵害を指します）。そのため、必要に応じてデータ漏洩 / 侵害事例の量をパーセントではなく実際の数で記載したり、もしくはパーセントと併記してあります。表 1 は、データ漏洩 / 侵害事例の数とパーセントの関係を示した表です。両者を変換したいときに便利です。また、図や表に示してある項目はいずれも、その値が 0 を超えている項目です（切り捨てたときに値が 0 を超える項目も含みます）。図や表に記載されていない項目も VERIS フレームワークにはすべて記載されていますので、そちらを参照してください。

昨年の 2011 年度データ漏洩 / 侵害調査報告書については、建設的なご意見をいくつかいただきました。その中に、以前と異なり最近の報告書は、小中規模の企業･組織がデータ漏洩 / 侵害を受けた事例の説明が多すぎて大規模の企業･組織にとってはあまり意味がない、というご批判を受けました。

このご意見に対して、ここで説明させていただきます。大量のデータを使って多種多様の企業・組織を分析する場合、問題がいくつかあります。そのひとつは、どうしても全体の平均値を算出する傾向があり、算出した平均値はあくまで平均値にすぎないということです。平均値はもちろん、すべての企業・組織を物語っていますが、反面、具体的な企業・組織の状態

データ漏洩 / 侵害事例はいくらでも細かく分類できますが、本報告書では、データ漏洩 / 侵害に関して、小規模と大規模（従業員数が 1,000 人以上）の企業・組織の間でどのような相違点（または類似点）があったかが明白になるような方法で分類しました。

を表しているわけではなく、業界や企業・組織の規模も考慮されていません。これは、方法上、避けられないことです。そこで、あらゆる種類の企業・組織、あらゆる種類のデータ漏洩 / 侵害を対象として分析を行い、その結果、データ漏洩 / 侵害を受けた企業・組織が大規模より小規模の企業・組織のほうがはるかに多かった場合でも、排除せずに丁寧に取り込むという方針で作業を行うことにしました。といっても、とくに中小の企業・組織に焦点を絞ったわけではなく、何らかの基準で企業・組織を分類し、分析を行うという方法をとりました。これで、分析結果は実用的なものになるはずです。

データ漏洩 / 侵害事例はいくらでも細かく分類できますが、本報告書では、データ漏洩 / 侵害に関して、小規模と大規模（従業員数が 1,000 人以上）の企業・組織の間でどのような相違点（または類似点）があったかが明白になるような方法で分類しました（読者からのご意見を意識しました）。この方法により、上記の懸念が払拭されるとともに、本報告書の分析結果が全体と個別の両面で有益なものになったと考えています。

業界別と企業の規模別の統計

毎年、まず業界や企業・組織の規模を基準にしてデータ漏洩 / 侵害を分析するという作業から始めていますが、理由は、この分析結果が以後の説明の基礎資料となるからです。さらに具体的に言えば、データ漏洩 / 侵害を業界（産業）、企業の規模、国や地域を基準にして分類・分析することにより、その後の分析結果の要点を解釈しやすくなるためです。

ただし本年は、分析に使用する基準を一部変更しました。つまり、業界の分類基準としては今まで私どもの独自の基準を使用していましたが、本年は代わりに北米産業分類システム（NAICS）を使うことにしました（一般的な分類でも、この基準が使用されています）。その結果、業界別の分析結果や傾向がこれまでとは異なったり、過去の分析結果との比較が難しくなったりする場合も多少はあります。しかしながら、総じて言えば一貫性は保持されており、したがって比較が無意味になるようなことはありません。

図 3 にあるように、3 位までは昨年度の報告書と同じです。被害が一番顕著だったのは本年も「ホテル・飲食業」で、内訳はレストランが多く（約 95%）、ホテルはわずかでした（約 5%）。「金融・保険業」は、2010 年は 22%でしたが昨年は約 10%に減少しました。「ホテル・飲食業」と「金融・保険業」の差は非常に大きく、その妥当な理由は（妥当ではない理由も含め）いろいろありますが、詳細は後ほど所定の節で説明することにします。昨年の報告書では、サイバー犯罪の「産業化」が進み、その影響が強く現れていると指摘しました（サイバー犯罪関連の他の報告書でも指摘されています[7]）。ここでは、この傾向が今も衰えていないことが両者の差の原因かもしれないと言うにとどめます。図 4 は侵害レコード数を業界別に示したものですが、この結果は図 3 とは大きく異なります。つまり、図 4 では「情報」と「製造業」の 2 つの業界が突出していますが、図 3 では、この 2 つの業界の割合はわずかです。また、昨年の報告書では、この 2 つの業界の侵害レコード数の割合はこれほど大きくはありませんでした（「その他」の部類でした）。この問題については後ほど詳述することにしますが、主な理由は、2011 年には大規模なデータ漏洩 / 侵害がいくつか発生したことによるものと思われます。大規模企業が標的となる場合、特定の業界というより、企業のブランドと関連機密情報が狙われるケースが多いようです。

"「北米産業分類システム（NAICS）は、米国の各連邦統計機関が企業の分類に使用している基準で、この分類に基づいて米国の企業経済に関する統計データが収集・分析され、公表されます。

NAICS は米国行政管理予算局（OMB）の支援の下で策定され、1997 年に標準産業分類（SIC）システムに代わる分類体系として採用されました。NAICS は、米国経済分類政策委員会（ECPC）、カナダ統計局、メキシコの国家地理統計院が共同で策定したもので、この基準を利用することで、北米各国の間で統一され、したがって公平な比較が可能な企業統計を作成することができます。」

出典：
http://www.census.gov/eos/www/naics/

7 例えば、Trustwave 社の「2012 年グローバルセキュリティレポート」では、フランチャイズ企業に対する攻撃が増加していると報告されています。

図 3. 業界別のデータ漏洩 / 侵害事例の割合

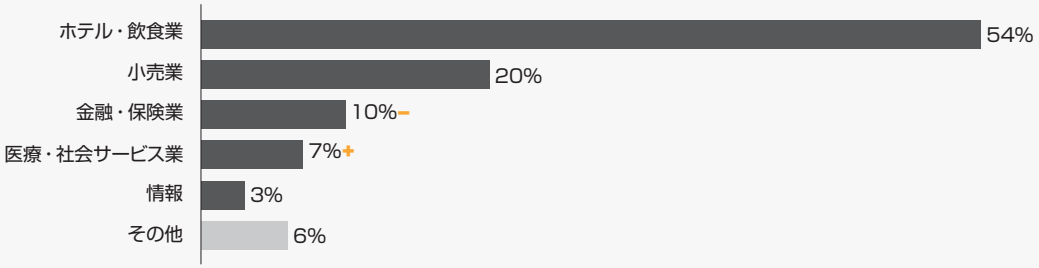


図 5 は侵害レコード数が極端に多い業界、つまり「情報」と「製造業」の事例を調整（侵害レコード数が 100 万を超える事例を除外）し、再作成したグラフです。このグラフのほうが、各業界の侵害レコード数の通常の分布、もしくは代表的な分布を示しています。一方、図 4 はどちらかというと一時的な（つまり今回だけの）データを表したグラフで、特定の業界が突出しているという点では図 3 に似ています。

図 4. 業界別の侵害レコード数の割合

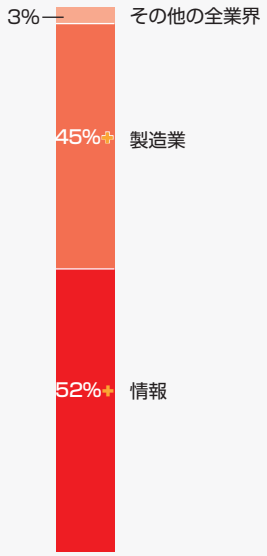
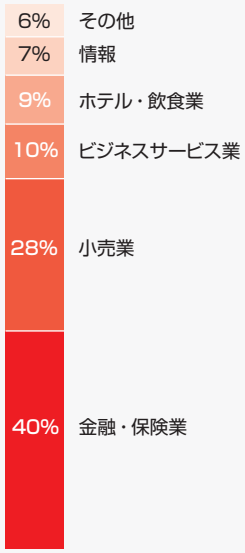


図 5：業界別の侵害レコード数の割合（侵害レコード数が 100 万を超える事例を除外）



今回扱ったデータ漏洩 / 侵害事例は全部で 855 件ですが、これまでと同じく、被害を受けた企業・組織の規模は様々です。被害にあったのは大半が小規模の企業・組織で、昨年の DBIR の分析結果と同じです。これは、どの業界でも「産業化」（大量生産）が起こるように、データ漏洩 / 侵害の分野でも「産業化」された攻撃が増えていることによります。つまり、多数の企業・組織に対して驚くほど短期間のうちに、ほとんど抵抗にもあわずデータ漏洩 / 侵害を成し遂げるという攻撃です。（抵抗とは、標的の企業・組織からの抵抗です。警察も目を光らせ、身構えています。「発見方法」の節の説明のほか付録 B も参照してください。）「産業化」された攻撃の理想的な標的は小規模企業であり、金銭が目当てで可能な限りリスクを避けたいサイバー犯罪者は、このことを十分に心得ています。このような理由から、小規模の企業・組織が被害に遭うケースが増加の一途を辿っています。

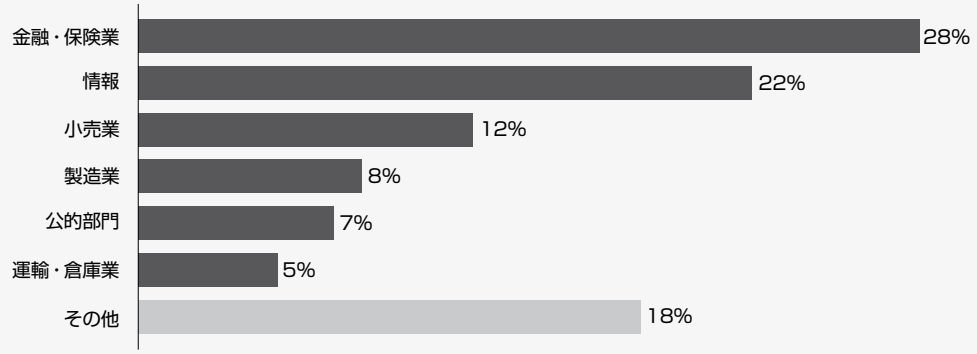
データ漏洩 / 侵害事例の中には企業・組織の規模が「不明」な事例もかなりあり、この情報は当然ながら必要です。本報告書の協力機関には、規模などの統計学上の情報も要請しているのですが、不明だったり、または分かっていても何らかの理由でこちらに伝えられないこともあります。攻撃の方法や特徴などは判明しているが、統計学上の情報はほとんど不明という事例でも、有効な事例として採用する場合もあります。これは理想的ではないものの、いわば許容範囲としなければなりません。結局、規模などの統計学上の情報がない事例でも無効なデータとして除外せず、欠落情報を「不明」としてデータを使用しています（表 2）。

前述したように、本報告書では小規模だけでなく大規模の企業・組織についても必要に応じて詳しく見ていきます。**ここで「大規模」とは、被害に遭った企業・組織のうち従業員が 1,000 人以上の企業・組織を指します。**本報告書は、このことを頭に置いて読み進めてください。図 6 は、全データ漏洩 / 侵害事例のうち大規模の企業・組織で発生したデータ漏洩 / 侵害事（60 件）だけを取り出し、業界別に分類したときのグラフです。

表 2. 規模（従業員数）別のデータ漏洩 / 侵害事例の数

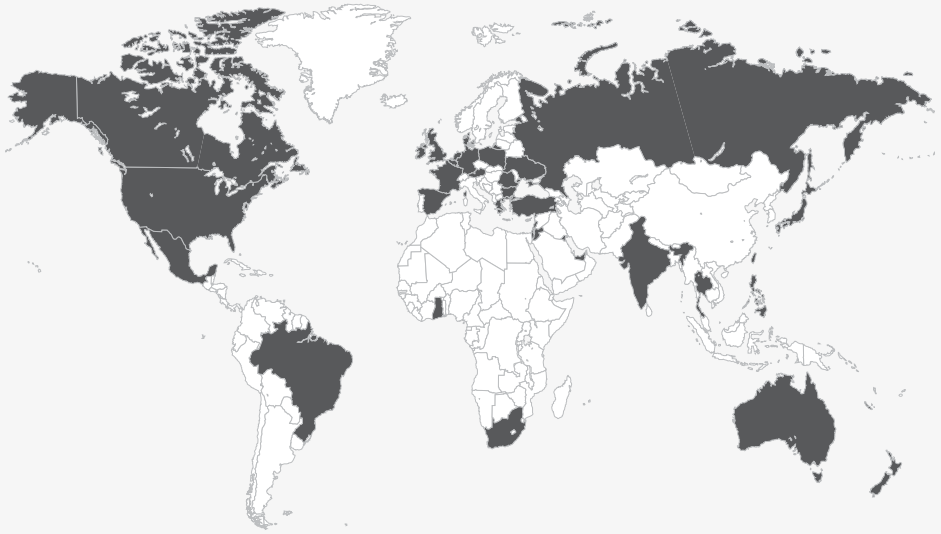
1 人から 10 人	42
11 人から 100 人	570
101 人から 1,000 人	48
1,001 人から 10,000 人	27
10,001 人から 100,000 人	23
100,000 人超	10
不明	135

図 6. 業界別のデータ漏洩 / 侵害事例の割合（大規模の企業・組織のみ）



例のごとく、被害に遭った企業・組織が存在する国を調査しても、それほどの意味はありません。データ漏洩 / 侵害を実行する場合、攻撃者は物理的にその国にいる必要はないからです。データ漏洩 / 侵害に遭遇した企業・組織の国は、2010 年には過去最高の 22 カ国に及びましたが、2011 年は、この記録が塗り替えられ 36 カ国に達しました。国が増えたのは、主に本報告書の各協力機関からの事例データ提供によるところが大きいのですが、いずれにしてもデータ漏洩 / 侵害はもはや一地域の問題でないことは明らかです。

図 7. 2011 年にデータ漏洩 / 侵害が発生した国（総合事例データ）



データ漏洩 / 侵害が確認された国

オーストラリア	フランス	ヨルダン	ポーランド	アラブ首長国連邦
オーストリア	ドイツ	クウェート	ルーマニア	ウクライナ
バハマ	ガーナ	レバノン	ロシア連邦	英国
ベルギー	ギリシャ	ルクセンブルグ	南アフリカ	米国
ブラジル	インド	メキシコ	スペイン	
ブルガリア	アイルランド	オランダ	台湾	
カナダ	イスラエル	ニュージーランド	タイ	
デンマーク	日本	フィリピン	トルコ	

データ漏洩 / 侵害に遭遇した企業・組織の国は、2010 年には過去最高の 22 カ国に及びましたが、2011 年は、この記録が塗り替えられ 36 カ国に達しました。

2011 年度データ漏洩 / 侵害調査報告書：脅威イベントの概要

昨年のデータ漏洩 / 侵害調査報告書で初めて、脅威イベント（VERIS で定義されている脅威イベント）の表を掲載しました。この脅威イベントの表は、各協力組織から提供される新たな事例データと同じく、本報告書の特徴の中でも高く評価されている特徴の一つです。本報告書では、データ漏洩 / 侵害事例を脅威因子、脅威アクション、資産、属性（A4 脅威モデルの 4 つの要素）を基準にして個別に分析していますが、この脅威イベントの表では 4 つの要素の相互関係を見ることができます。言い換えると、2011 年のデータ漏洩 / 侵害に関連している脅威イベント（データ漏洩 / 侵害の原因であるイベント）を確認できます。図 8（全企業・組織の事例）と図 9（大規模企業向け・組織の事例のみ）は、前述の図 1 をもとにして作成したものです。図 1 の場合、マス目の値は脅威イベント番号（TE#）ですが、図 8 と図 9 では、マス目の値は、その脅威イベント（他の脅威イベントも関係していることもあります）によって引き起こされたデータ漏洩 / 侵害の数です。[8] 図 8 と図 9 は今回の 855 件のデータ漏洩 / 侵害事例を集計した表であり、注目すべき点がいくつかあります。

図 8. VERIS の脅威イベントの表（マス目の値はデータ漏洩 / 侵害事例の数）

		マルウェア			ハッキング			ソーシャル			不正使用			物理的脅威			過失			環境面の脅威		
		外部	内部	パートナー	外部	内部	パートナー	外部	内部	パートナー	外部	内部	パートナー	外部	内部	パートナー	外部	内部	パートナー	外部	内部	パートナー
サーバー	機密性と所有	381			518		1				9	8	1					2	1			
	整合性と信憑性	397			422		1				6	1	1									
	可用性と有用性	2			6						5											
ネットワーク	機密性と所有										1											
	整合性と信憑性	1									1											
	可用性と有用性	1			1						1											
ユーザー機器	機密性と所有	356			419						1			86								
	整合性と信憑性	355			355						1	1		86								
	可用性と有用性										1			3								
オフラインデータ	機密性と所有											23							1			
	整合性と信憑性																					
	可用性と有用性																					
人間	機密性と所有							30	1													
	整合性と信憑性							59	2													
	可用性と有用性																					

全企業・組織の事例の表（図 8）を見てみると、315 種類の脅威イベントのうち値が 0 より大きい脅威イベント（実際にデータ漏洩 / 侵害を引き起こした脅威イベント）は 40 種類（13%）しかありません。この表で分かるように脅威イベントの中には発生しないものもあり、この点は理解しておく必要があります。また、本報告書は、ベライゾンと各協力機関のデータ漏洩 / 侵害事例を使って作成した報告書であることにも留意してください。つまり過去 1 年間、データ漏洩 / 侵害が発生した企業と協力し、データ漏洩 / 侵害に関する情報を VERIS に登録する作業を行いましたが、登録した情報を使って脅威イベントの表を作成し、上記の表と比較してみると面白いことが分かります。お気づきかもしれませんが、脅威アクションが過失または不正使用、属性が可用性である脅威イベントの値が大きく（つまりデータ漏洩 / 侵害事例の数が多い）、この点、上記の表とは異なります。

8 この表から、2011 年の 855 件のデータ漏洩 / 侵害事例のうち 381 件は、脅威因子が外部、脅威アクションがマルウェア、資産がサーバー、属性が機密性である脅威イベント（左上角のマス目）に関連した事例であることが分かります。

図 9. VERIS の脅威イベントの表（マス目の値はデータ漏洩 / 侵害事例の数）（大規模の企業・組織の事例のみ）

		マルウェア			ハッキング			ソーシャル			不正使用			物理的脅威			過失			環境面の脅威		
		外部	内部	パートナー	外部	内部	パートナー	外部	内部	パートナー	外部	内部	パートナー	外部	内部	パートナー	外部	内部	パートナー	外部	内部	パートナー
サーバー	機密性と所有	7			33						3							2	1			
	整合性と信憑性	10			18						1											
	可用性と有用性				1																	
ネットワーク	機密性と所有																					
	整合性と信憑性																					
	可用性と有用性	1			1																	
ユーザー機器	機密性と所有	3			6									10								
	整合性と信憑性	4			2									10								
	可用性と有用性													1								
オフラインデータ	機密性と所有											1							1			
	整合性と信憑性																					
	可用性と有用性																					
人間	機密性と所有							7														
	整合性と信憑性							11														
	可用性と有用性																					

VERIS の利用による「証拠に基づくリスク管理」

このタイトルは宣伝のように聞こえるかもしれませんが、そうではありません。VERIS を利用して、証拠に基づくリスク管理が可能です（しかもお金はかかりません）。自分が会社のリスク管理責任者であり、それまで会社で発生したセキュリティインシデントをすべて VERIS を使って記録しているとします（自社のインシデントの情報とあわせて、自社と似た会社で発生したインシデントの情報を記録すると参考データが増えます）。時間が経つにつれ、自分の会社で何がどのくらいの頻度で発生し、また何が起こらなかったが分かるようになります。不明なことが減り、不安も徐々に消えます。データが十分に蓄積されれば、社内のデータ処理スタッフにデータを渡し、図 9 のような脅威イベントの表を作るように依頼します。表は、会社の部門ごとに作成するのが効果的です。表ができれば、値（データ漏洩 / 侵害の数）が大きい脅威イベントに注目します。この種の脅威イベントが問題であり、その底にある病気を診断しなければなりません。続いて診断結果に基づき、脅威イベントの阻止や予防、検出のほか、再発した（または被害を受けた）脅威イベントからの回復に必要な治療方法を考え、治療の手順も決めます。ただし、これで終わりではありません。処方箋の有効性を確認する作業、つまり治療によってインシデントや情報漏洩が減少したかどうかを追跡することが必要です。正確な確認作業があってこそ、効果的な管理が可能です。同僚からは「リスクドクター」と呼ばれ、セキュリティに関する会議や打ち合わせでも自分の意見が俄に尊重されるようになります。悪くはない結果です。

もちろん、上の最後の部分は冗談ですが、この方法には確実にメリットがあります。この方法を「証拠に基づくリスク管理」（EBRM）と呼んでおり、この名称は「証拠に基づく医療」という用語に因んだものです。EBRM の基本的な目的は、実証的研究から得られた入手可能な最高の証拠を使用し、情報リスクの把握と管理を行うことにあります。セキュリティインシデントは、その規模の大小にかかわらず「入手可能な最高の証拠」の宝庫です。これが、セキュリティインシデントを詳しく丁寧に分析することこそメリットが大きい手法である、と日頃から主張している理由です。

脅威イベントの表の話に戻ります。全企業・組織の事例の脅威イベントの表（図 8）の内容は、昨年の報告書の結果とほぼ同じです。大きな違いは、本年は、不正使用と物理の脅威イベントの値（データ漏洩 / 侵害の数）が昨年より多少減少している一方、マルウェアとハッキングの脅威イベントの値が増えていることです。同様に上位 10 位までの脅威イベントも、本年は昨年とよく似ています。

全企業・組織の事例の脅威イベントの表（図 8）の内容は、昨年の報告書の結果とほぼ同じです。大きな違いは、本年は、不正使用と物理の脅威イベントの値（データ漏洩 / 侵害の数）が昨年より多少減少している一方、マルウェアとハッキングの脅威イベントの値が増えていることです。

表 3：上位 10 位までの脅威イベント

	脅威イベント	脅威イベント番号	合計
1	外部−ハッキング−サーバー−機密性	4	518
2	外部−ハッキング−サーバー−整合性	28	422
3	外部−ハッキング−ユーザー機器−機密性	130	419
4	外部−マルウェア−サーバー−整合性	22	397
5	外部−マルウェア−サーバー−機密性	1	381
6	外部−マルウェア−ユーザー機器−機密性	127	356
7	外部−マルウェア−ユーザー機器−整合性	148	355
8	外部−ハッキング−ユーザー機器−整合性	151	355
9	外部−物理−ユーザー機器−機密性	139	86
10	外部−物理−ユーザー機器−整合性	160	86

表 4：上位 10 位までの脅威イベント（大規模の企業・組織の事例のみ）

	脅威イベント	脅威イベント番号	合計
1	外部−ハッキング−サーバー−機密性	4	33
2	外部−ハッキング−サーバー−整合性	28	18
3	外部−ソーシャル−人−整合性	280	11
4	外部−マルウェア−サーバー−整合性	22	10
5	外部−物理−ユーザー機器−機密性	139	10
6	外部−物理−ユーザー機器−整合性	160	10
7	外部−マルウェア−サーバー−機密性	1	7
8	外部−ソーシャル−人−機密性	259	7
9	外部−ハッキング−ユーザー機器−機密性	130	6
10	外部−マルウェア−ユーザー機器−整合性	148	4

図 9 は大規模企業向け・組織の事例のみの場合の脅威イベントの表ですが、ここで注意点をいくつか簡単に紹介します。まず、お気づきかもしれませんが、図 9 は図 8（全企業・組織の事例）に比べて、値が 0 を超える脅威イベントの種類が少ないのです（315 種類の脅威イベントのうち 22 種類しかなく、割合にすると 7%です）。少ないのは、大規模企業向け・組織の場合、セキュリティ対策が堅固であるからと考える読者もいるでしょう。この理由はおそらく正しく、本報告書の分析結果と矛盾するものではありません。私どもの見解では、図 9 が図 8 に比べて脅威イベントの種類が少なく疎らなのは、大規模企業向け・組織のデータ漏洩 / 侵害事例が少ないこと（大規模企業向け・組織の事例は、全 855 件中の 60 件）が主な理由と思われます。また、脅威イベントの値の分布に注目すると、大規模企業向け・組織の事例の場合、侵入型の脅威イベントの値の分布が図 8 に比べてはるかに均等です（図 8 では脅威アクションがマルウェアまたはハッキングの脅威イベントの値は大きな開きがありますが、図 9 ではそれほど開きはありません）。最近、ソーシャルエンジニアリングによる攻撃が目立っていると報じられていることを考慮すると、これは不思議ではありません。

上記については、後続の各節で詳しく説明します。

脅威因子（データ漏洩 / 侵害の実行者）

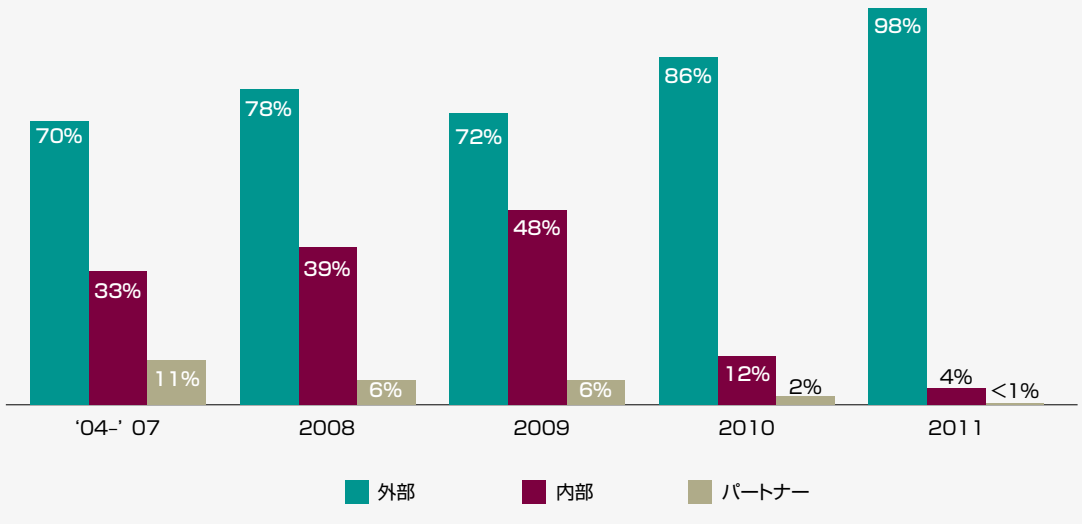
インシデント（ここではデータ漏洩 / 侵害事例）を引き起こし、またはインシデントの発生に寄与した要素を脅威因子と呼んでいます。インシデントには、当然のことながら複数の脅威因子が関わっていることがあります。脅威因子による行為には、悪意の有無、故意または偶然、その行為が直接の原因かどうかなどの側面があり、また動機も様々です（動機については、後述の脅威因子に関する節で詳しく説明します）。インシデントが発生した場合、そのインシデントに関連する脅威因子を特定することが何より重要であり、それで初めて具体的な対策を講じることができ、また今後の防御戦略に関する意思決定も可能になります。VERIS では、主な脅威因子として外部因子、内部因子、パートナーの 3 種類を定義しています。

- **外部因子**：企業・組織、また企業・組織のパートナーのネットワークの外部に存在する脅威因子です。外部因子としては、元従業員、ハッカー（個人）、組織犯罪グループ、政府機関などがあります。また、洪水や地震、停電といった環境事象も外部因子に含まれます。外部因子は通常、信用されておらず、また、権限も付与されていません。
- **内部因子**：企業・組織の内部に存在する脅威因子（部内者）です。例えば、役員、従業員、契約社員・契約会社、研修員･実習員などが内部因子で、そのほか内部インフラも内部因子です。部内者は、信頼され権限を持っています。（信頼や権限のレベルは部内者によって異なります）。
- **パートナー**：企業・組織と業務上の関係を有する第三者（ビジネスパートナー）です。パートナーの例としては、サプライヤー、ベンダー、ホスティングプロバイダー、IT サポートプロバイダーなどがあります。パートナーは、一定レベルの信頼を得て、権限が付与されているのが普通です。

VERIS の分類に関する注意：脅威因子の過失を原因としてデータ漏洩 / 侵害が発生し、その過失が寄与過失（寄与原因）である場合には、その脅威因子を脅威因子として扱わないことにしています。例えば、内部因子（部内者）が、意図せず（偶然）にアプリケーションの設定を誤り、そのため攻撃に対してアプリケーションが脆弱なままになっており、その後、その部内者以外の脅威因子を原因としてデータ漏洩 / 侵害が発生した場合、その部内者は、そのデータ漏洩 / 侵害の脅威因子ではありません。これに対して、部内者が故意にデータを盗む、または部内者の不適切な行為（ポリシー違反など）を原因としてデータ漏洩 / 侵害が発生した場合、その部内者は、そのデータ漏洩 / 侵害の脅威因子です。

図 10 は、全データ漏洩 / 侵害事例において、どの脅威因子がどの程度（%）関与していたかを示したグラフで、今回の結果のほかに過去の結果もすべて掲載してあります。このグラフでは、本年の結果だけでなく過去の結果の傾向も併せて見ることが大事です。使用した事例データについて言えば、当初の数年はベライゾンの事例データのみで、その後、USSS（2007 ～ 2011 年 ）、NHTCU（2006 ～ 2011 年 ）AFP（2011 年 ）、IRISSCERT（2011 年 ）、PCeU（2011 年）のデータが追加されました。したがってグラフを見る場合、脅威の状況の変化だけでなく、使用した事例データの変化も勘案する必要があります。

図 10. 各脅威因子のデータ漏洩 / 侵害件数の推移



2011 年も相変わらず、外部因子が関与したデータ漏洩 / 侵害事例が非常に多いという結果が出ています。外部因子によるデータ漏洩 / 侵害は以前から多かったのですが、これほど突出したのは過去にはありません。ただし、2009 年は例外です。この年に内部因子の割合が多いのは、主に USSS の事例データが追加されたことの副産物です（USSS の事例データの場合、内部因子が関与したデータ漏洩 / 侵害事例が多く、これは 2010 年度データ漏洩 / 侵害調査報告書[9] で説明してあります）。2009 年の後は内部因子関与のデータ漏洩 / 侵害は減り、外部因子の一人勝ちです。

USSS の事例データを含め、使用した事例データは年ごとに異なりますが、外部因子が増加する一方で内部因子とパートナーは減少するという傾向は明らかであり、その理由はいくつかあります。第一の理由は、2011 年度データ漏洩 / 侵害調査報告書[10] で述べてあるように、「産業化」された攻撃が増えていることです。「産業化」された攻撃とは、組織犯罪グループがインターネットに接続された POS システムや、物理的にアクセスが可能な ATM やガソリンスタンドの給油機からカード情報を盗んだ後、攻撃を仕掛け、一度の攻撃で何百人もの犠牲者が出るという手口です。いわばパターン化されているが拡張性に優れた攻撃方法であり、この攻撃方法が横行していることを考慮すると、外部因子の割合が増加した理由がよく分かります。一方、外部因子が増えた影響から、内部因子（部内者）の割合は減っています。

2011 年も相変わらず、外部因子が関与したデータ漏洩 / 侵害事例が非常に多いという結果が出ています。外部因子によるデータ漏洩 / 侵害は以前から多かったのですが、これほど突出したのは過去にはありません。

2011 年に外部因子の割合が増加したことのもうひとつの理由は、活動家グループの活動が勢いづいたことです。活動家グループによる攻撃は一般に「ハクティビズム」と呼ばれ、活動家グループは性質上、外部因子です。活動家グループによる攻撃は、主流のサイバー犯罪と比べると発生頻度は低いのですが（「一定」と呼ぶ人もいます）、後述のように被害が甚大に及ぶことがあります。

忘れないうちに触れておくと、2011 年のデータ漏洩 / 侵害事例の中には、内部因子がデータ漏洩 / 侵害の定義に合致しないものもありました。つまり、内部因子が仕事上、自分に与えられたアクセス権または機密情報を不正に使用した場合でも、内部因子がその情報を権限のない者に公開しなかったときには、機密性は失われません。[11] したがって、このような事例は本報告書の分析対象から除外しました。

2011 年の事例でもうひとつ興味深いのは、複数の種類の脅威因子が関わったデータ漏洩 / 侵害が大幅に減っていることです。例えば 2009 年を見てみると、複数の異なる脅威因子が関与したデータ漏洩 / 侵害事例が全事例の 4 分の 1 を超えています。このような事例は、刑事上の共謀もありますが、部外者が部内者を誘惑し何らかの形で犯罪に関与させるというほうが一般的です。2011 年の場合、このような事例の割合はわずか 2%でした。この減少も、上述した「攻撃の産業化」によるところが大きいと思われます。

パートナーによるデータ漏洩 / 侵害は、過去数年にわたって減少を続けており、今回も同様でした。[12] 今回、パートナーを原因とするデータ漏洩 / 侵害は 1%未満で、来年、これ以下になることは恐らくないでしょう。パートナーが減少したのは、内部因子の場合と同じく、外部因子が大幅に増加したことが理由のひとつですが、理由は他にもあります。パートナーの減少傾向は 2008 年に始まり、以後、外部因子による攻撃が大規模で拡張性の高いものへと大きく変化します。パートナーの割合が少ないことの理由については、過去の報告書で仮説をいくつか（データ漏洩 / 侵害に対する意識、規制、技術の進歩など）述べました。また、脅威因子を主原因（データ漏洩 / 侵害に直接関与）または寄与原因（データ漏洩 / 侵害に間接的に関与）のどちらとして定義するかによってパートナーの割合は変わってきます。つまり、パートナーがデータ漏洩 / 侵害に直接関与していなかった場合（寄与原因である場合）、そのパートナーは脅威因子とはみなさないため、そのような事例は「パートナー」の割合には含まれていません。パートナーの定義については、本報告書の「パートナー」と「過失」の節に詳しい説明があります。

また、部内者とパートナーの割合が少ないことの大きな理由として、部内者やパートナーが秘密裏に行動したために彼らの不正は発見されないことが考えられます。過去の報告書では、詐欺行為（例えばカード詐欺）が見つかって初めて、その詐欺行為に関連するデータ漏洩 / 侵害が発見されるケースが非常に多いことを指摘しました（本報告書の以降の節でも繰り返し指摘します）。ところが非財務データ（金銭とは直接関係のない情報）の場合、データ漏洩 / 侵害に遭っても発見する方法があまりないため、カード詐欺などと違って発見が難しいのが実情です。手元の事例データによれば、信頼されている者は、そうでない者と比べて知的財産やその他の（非財務）機密データを盗む確率がかなり高く、その一方、発見さ

9 http://www.verizonbusiness.com/resources/reports/rp_2010-data-breach-report_ja_xg.pdf
10 http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2011_ja_xg.pdf
11 例えば、銀行の行員がシステム権限を使って不正に金銭を引き出したり送金したりといった例がよく見られます。この行為は間違いなくセキュリティ侵害ですが、データ漏洩 / 侵害ではありません（データの機密性は失われていません）。
12 パートナーの割合は、過去の報告書では今回よりかなり大きかったことを思い出す読者もいるかもしれません。なお、過去の報告書ではベライゾンの事例データだけによる結果も別個に示しましたが、このグラフは各協力機関からの事例データを集計した場合の結果です。したがって、ベライゾンの事例データだけの場合、結果は異なります。

図 11. 脅威因子別のデータ漏洩 / 侵害事例の割合
（複数種類の脅威因子を原因とするデータ漏洩 / 侵害を別途分類）

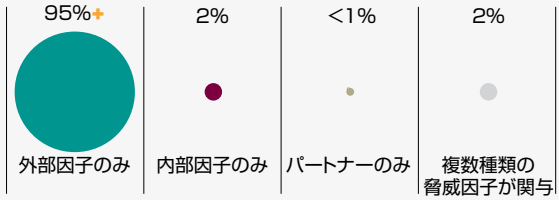
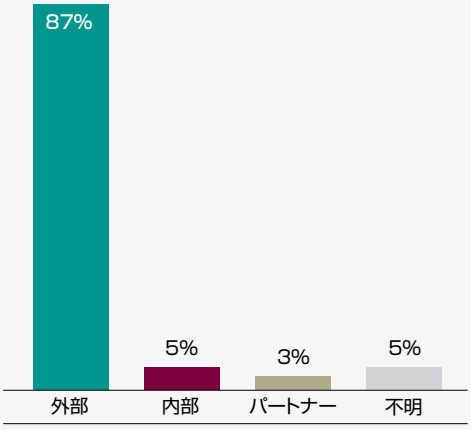


図 12. 脅威因子別のデータ漏洩 / 侵害事例の割合
（大規模の企業・組織の事例のみ）



れる確率は低いという結果が出ています。以上、部内者とパートナーの割合が少ないことの理由をいくつか列挙しましたが、これは本報告書の分析結果に偏りがあることを「弁解」したり、社会に対して不安や疑念、不信を煽ったりするのが目的ではなく、内部因子とパートナーの割合は図 10 よりも恐らく多いことを指摘することが目的です（もっとも、このような悪意のある内部因子やパートナーも大局的に見ると外部因子ではありません）。

大規模の企業・組織のデータ漏洩 / 侵害についても詳しく説明すると前述しましたが、図 12 は、その分析結果です。大規模の企業・組織では内部因子やパートナーによるデータ漏洩 / 侵害は少ないはずと予想していた読者は、この結果に失望するでしょう。（理論がデータに駆逐されて愉快と思う人はいません。）大規模の企業・組織の場合、内部因子（部内者）やパートナーによるデータ漏洩 / 侵害が比較的多いであろうということについて、極めて洞察に優れ道理にかなった理由を用意していたのですが、無駄になってしまいました。

脅威因子で分類した場合のデータ漏洩 / 侵害の規模

流出したレコードの数（侵害レコード数）でデータ漏洩 / 侵害の規模を測定するという方法では、そのデータ漏洩 / 侵害の影響を正確に把握できるとは限りませんが、指標としては実用的で有効です。また、データ漏洩 / 侵害に対する対応、ブランドへの損害、企業の評判、法律上の処罰などを考慮した場合、データ漏洩 / 侵害関連の情報として侵害レコード数を含めるのは至極妥当と思われます。このような理由から今回、本報告書に短い節を新たに設け、侵害レコードについて多少詳しく検討することにしました（この節は後半にあります）。ここでは侵害レコード数だけを紹介します。

図 13 は、2011 年の総合事例データをもとにして脅威因子別に侵害レコード数を分類したグラフで、侵害レコードの総数は約 1 億 7400 万でした。もちろん、内部因子とパートナーによって盗まれたレコードも含まれていますが、どちらも「泡沫」であり、実際にはほとんど全部のレコードが外部因子によって窃取されたといえます。図 13 と図 14（過去のすべての年の分析結果を集計したグラフ）を比較してみると、大きな違いはありません（図 14 の場合、内部因子とパートナーの点が大きいため色が見えます）。しかしながら内部因子とパートナーの侵害レコード数の割合が減っており、これはメガ（大規模）データ漏洩 / 侵害、つまり一度に何百万というレコードが盗まれる事例が増えていることによります（メガデータ漏洩 / 侵害の実行者は通常、外部因子です）。また、入手できる情報の量は少ないものの、多数の標的に攻撃を仕掛けるという外部因子が増加しており、これも内部因子とパートナーの侵害レコード数の割合が減っている原因のひとつです。

標的となる情報にはいろいろな種類があり、その種類と侵害レコード数の関係を理解することも重要です。例えば、カード情報や個人情報は一般に同じ場所に大量に保存されており、したがって盗まれる情報（レコード）も大量です。一方、知的財産や機密情報の場合、盗まれるのは単一の「レコード」であるのが普通です。前述したように、部内者はカード情報や個人情報より、知的財産や機密情報を好みます。

図 13. 脅威因子別の侵害レコード数（2011 年）

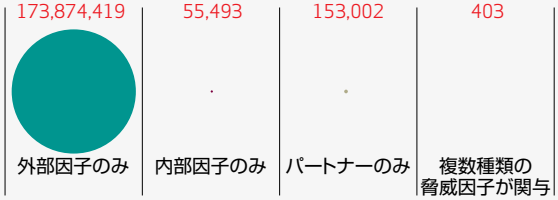
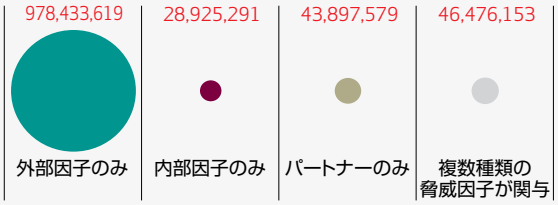


図 14. 脅威因子別の侵害レコード数（2004 年～ 2011 年）



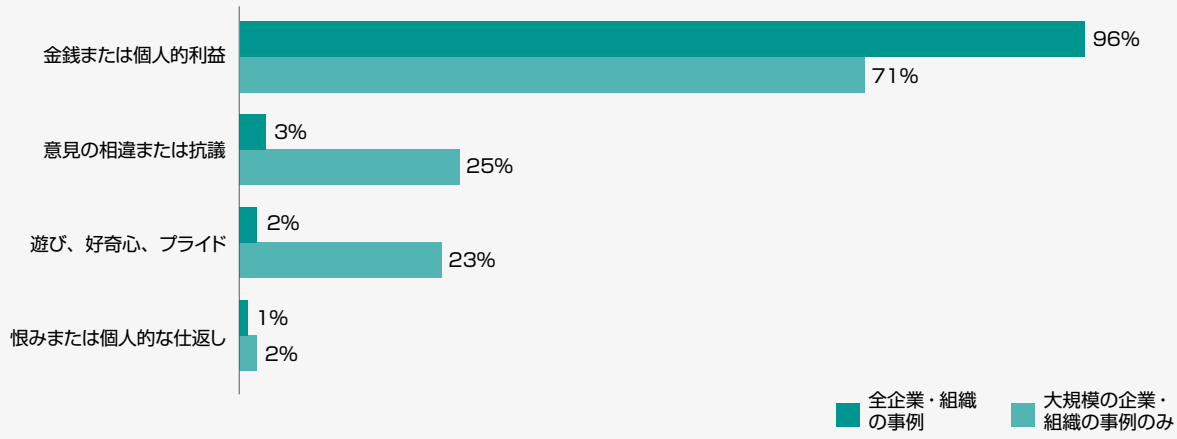
外部因子（全データ漏洩 / 侵害の 98%、全侵害レコードの 99%以上が外部因子によるもの）

これまでと同じく今回も、部内者とパートナーによるデータ漏洩 / 侵害事例より、外部因子によるデータ漏洩 / 侵害事例のほうが格段に多いという結果になりました。具体的には、全データ漏洩 / 侵害事例の 98%が外部因子によるものでした。外部因子の役割（直接関与または間接関与）、種類、動機については、今回も今までとほぼ同じでした。

結論を言えば、データ窃盗はほとんどがプロの犯罪者であり、換金できる情報を故意に盗むのが目的であるといえます。動機は金目当てで、これも以前と同じです。

直接関与し、意図的に悪意をもってデータ漏洩 / 侵害を行ったという外部因子（部外者）がほとんどでした。外部因子が間接的に関与して（寄与原因として）データ漏洩 / 侵害を実行、つまり誰かを誘惑またはそそのかし、もしくは手助けしてデータ漏洩 / 侵害を実行させるという事例はほんの 2%でした。外部因子のタイプとしては今回も組織犯罪グループが一番多く、この種のグループによるデータ漏洩 / 侵害事例は全事例の 83%を占めました。なぜデータ漏洩 / 侵害という犯罪に手を染めるのかと疑問に思う人もいるでしょう（私どもは疑問に思ったからこそ昨年から動機の分析を始めました）。答えはごく簡単で、金銭が目当てです（96%）。結論を言えば、データ窃盗はほとんどがプロの犯罪者であり、換金できる情報を故意に盗むのが目的であるといえます。動機は金目当てで、これも以前と同じです。

図 15. 外部因子の動機で分類した場合のデータ漏洩 / 侵害の割合（外部因子によるデータ漏洩 / 侵害事例のみ）



2011 年の外部因子の傾向や特徴は上記だけではありません。また、上記の傾向が最も重要というわけでもありません。外部因子の場合、2011 年で何よりも注目すべき変化は、「ハクティビズム」が台頭し、世界中の大規模企業・組織に攻撃を仕掛けているという事実です。実際、活動家グループによるデータ漏洩 / 侵害の件数を見ると、2011 年の件数は、本調査シリーズの最初の年から昨年までの合計件数を超えています。この傾向は、ベライゾンの事例データだけなく本報告書の各協力機関の事例データにも見られ、実際、各協力機関はハクティビスト（政治的ハッカー）の活動に対して多大な時間と労力を費やして対応や調査を行い、起訴も試みていました。各協力機関の事例データを集計し、活動家グループによるデータ漏洩 / 侵害と被害を世界的視点に立って分析するというのは非常に興味深い作業でした。活動家グループによるデータ漏洩 / 侵害事例の割合は全企業・組織の事例の 2%であり、これは少ないように見えます（ただし、今回扱ったデータ漏洩 / 侵害が 850 件を超えることを考えると決して少なくはありませんし、活動家グループに関連する動機の割合はこれより多く、さらにタイプが「不明」の外部因子の中には活動家グループも存在すると思われます）。いずれにしても、本年のデータ漏洩 / 侵害調査報告書において、活動家グループの台頭が恐らく最大かつ最も重要な変化といえます。

外部因子の傾向や特徴はこれだけではありません。また、上記の傾向が最も重要というわけでもありません。外部因子の場合、2011 年で何よりも注目すべき変化は、「ハクティビズム」が台頭し、世界中の大規模企業・組織に攻撃を仕掛けているという事実です。

といっても、ハクティビズムは以前から存在していました。ハクティビズムという語は、1990 年代遅くにカルト･オブ･ザ･デッド・カウ（Cult of the Dead Cow）と称するハッカー集団が作ったもので以後、巷間で使われています。[13] 当時、ハクティビズムの具体的内容は、主にウェブサイトの改変や協調型 DoS のほか、反対意思の表明、自慢や見せびらかし、「腹いせ」などでした。この傾向は 2011 年に大きく変わりました。活動家グループは上記のレパートリーにデータ漏洩 / 侵害を加え、しかも活動は以前より公然かつ頻繁になったのです。言い換えると、2011 年は「ところで、情報も全部盗むからね」という活動家グループの宣言によって、以前の古典的悪行とデータ漏洩 / 侵害が一体化した年ということになります。

表 5. 外部因子のタイプで分類した場合のデータ漏洩 / 侵害の割合と侵害レコード数の割合（外部因子によるデータ漏洩 / 侵害のみ）

	全企業・組織の事例		大規模の企業・組織の事例のみ	
組織犯罪グループ	83%	35%–	33%	36%
不明	10%	1%	31%	0%
組織やグループに属していない個人（一人または複数人）	4%	0%	10%	0%
活動家グループ	2%	58%+	21%	61%
元従業員（退社し、以後は接触なし）	1%	0%	6%	0%
従業員の親類や知人	0%	0%	2%	0%

話はまだあります。活動家グループによる 2011 年のデータ漏洩 / 侵害は、件数こそ多くはありませんが盗まれたレコードは 1 億を超えます。この 1 億超という侵害レコード数は、動機が「金銭または個人的利益」の外部因子の侵害レコード数のほぼ 2 倍に相当します。したがって、活動家グループによる攻撃の発生件数はそれほど多くはなかったが、被害は間違いなく甚大でした。

実際、侵害レコード数の割合を見ると（表 5）、活動家グループが一番多く、次がプロのサイバー犯罪者（組織犯罪グループ）です。この違いの理由は何でしょうか。分析によれば、金銭目当ての組織犯罪グループは今までと同じく、主に不特定多数の脆弱な標的を狙っているようです。この方法を使っているのは、近年はデータ漏洩 / 侵害で逮捕される確率が高く、恐らくそれを回避するためです。言い換えると、大きな（またリスクの高い）仕事は避け、攻撃者にとってリスクが少ない多数の小規模企業・組織から少量のデータを掠め取るという方法に頼っているのです。業務プロセスの合理化と言ってもいいでしょう。無防備で脆弱、動きの鈍い企業・組織を餌食にし、同じ攻撃を大々的に繰り返せというわけです。いわば「薄利多売」方式で、これが組織犯罪グループの一般的な手口になっており、その結果、組織犯罪グループの侵害レコード数は比較的少ないということになります。

活動家グループに関してもうひとつ大事なことがあり、それは活動家グループによって盗まれたデータは、ほとんど全部が大規模の企業･組織からのものだったという事実です。また、大規模の企業･組織の事例のみの場合、動機がハクティビズム関連（意見の相違または抗議）であるデータ漏洩 / 侵害の割合は 25%に達しています（図 15）。活動家グループは「有名ブランド」に惹かれる傾向があり、したがって、この結果は納得できます。

攻撃者はセキュリティの専門家と懸命に闘っていますが、それと同じく逮捕される危険性とも必死に闘っています。このような事情から、法執行機関がサイバー犯罪に挑む場合、犯罪者のオンライン上の情報から実際の身分をどう割り出すかが難問のひとつです。残念ながら、2011 年のデータ漏洩 / 侵害事例のうち、外部因子の身分（この場合はタイプ）を特定できなかった事例が 10%に上りました。理由はいくつかあります。まず、十分なログデータを保持していなかった企業・組織が多く、それでタイプが特定ができなかったことが最初の理由です。この種の作業はディスクフォレンジック解析だけでは無理なのが普通であり、ログデータが必要です。また、データ漏洩 / 侵害の封じ込めに成功した場合、さらに調査を進めることを希望する企業・組織は少なく、これが第二の理由です。そのほか、攻撃者が中間システムを多数用意し、データ漏洩 / 侵害の痕跡を消したり隠したりすると特定は不可能です。それに攻撃者をうまく特定できたと思っても、「チャックテスタの仕業」（注記：2011 年末に YouTube で流行した言葉” Nope! Chuck Testa”）ということも時折あります。

外部因子が存在する場所

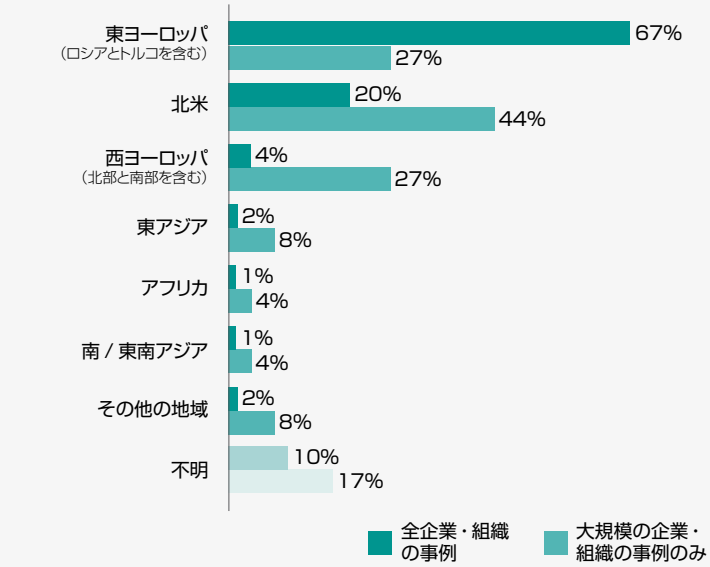
外部因子が地理的にどこに存在するかを特定するのは、IP アドレスだけでは困難です。ソース IP アドレスの国を特定できたとしても、攻撃者が常時、そこにいるとは限りません。その場所は、ボットネット上のホストか、もしくは外部因子が使っている「中継点」かもしれません。場合によっては、法執行機関からの情報やネットフロー分析ツールで得られ

13 http://www.wired.com/techbiz/it/news/2004/07/64193

た情報など、各種の情報を駆使することで攻撃者の本来の場所を特定できることもあります。いずれにしても、攻撃者の地理的な場所を調べることは、いろいろな面で有益です。

2011 年の場合も今までとほぼ同じで、外部因子による全データ漏洩 / 侵害事例のうち、その 3 分の 2 が東ヨーロッパに存在する外部因子によって実行されたものでした（図 16）。ただし、大規模の企業・組織の事例だけに絞ると、この割合は 27%に低下します。これは、小規模で防御が甘い企業・組織を狙う組織犯罪グループ（主に東ヨーロッパから攻撃を実行）が多いことを示しています。大規模の企業･組織の場合、東ヨーロッパだけでなく、世界の各地の攻撃者から攻撃される傾向が見られました。

図 16. 外部因子による攻撃の発生元とデータ漏洩 / 侵害の割合（外部因子によるデータ漏洩 / 侵害のみ）



内部因子（全データ漏洩 / 侵害の 4%、全侵害レコードの <1%が内部因子によるもの）

「脅威因子の概要」の節で述べたように、内部因子（部内者）によるデータ漏洩 / 侵害の件数は減少傾向にあり、これは部内者によるデータ漏洩 / 侵害自体が減ったというより、「産業化された攻撃」が引き続き増加していることに主な原因があります。なお、企業・組織の中には、部内者によるデータ漏洩 / 侵害に気がつかなかったり、気がついても経営・運営上の理由から、フォレンジック調査を依頼したり法執行機関に通報したりせずに内部で処理することにしたところも多く、したがって内部因子によるデータ漏洩 / 侵害の実際の件数は、この報告書の値より多いかもしれません。

部内者は、データ漏洩 / 侵害に直接関与する場合と間接的に関与する場合がありますが、どちらの場合も、その役割（故意かどうか、悪意があるどうかなどの別）にはいくつか種類があります。本報告書では便宜上、この役割を 3 種類に分類しています。「意図的かつ悪意あり」、「不適切（悪意なし）」、「非意図的」の 3 つです。2011 年の場合、内部因子によるデータ漏洩 / 侵害のうち「意図的かつ悪意あり」のデータ漏洩 / 侵害がほぼ全部を占め、これは 3 年連続です（毎年、約 90%を占めます）。なお、ベライゾンのデータ漏洩 / 侵害事例の中には、部内者の非意図的な過失によりデータが流出したケースがわずかにありました。例えば、従業員が機密情報とは知らずに、その情報をインターネットに誤って公開してしまったという事例が見られました。

企業･組織の中には、部内者によるデータ漏洩 / 侵害に気がつかなかったり、気がついても経営・運営上の理由から、フォレンジック調査を依頼したり法執行機関に通報したりせずに内部で処理することにしたところも多いはずです。

部内者が間接的にデータ漏洩 / 侵害に関与した場合[14]、通常は、その部内者を脅威因子とはみなさず、したがって本節では解説しません。ここで取り上げるのは、部内者が自社内で直接データ漏洩 / 侵害を行ったか、または主原因としてデータ漏洩 / 侵害に直接関わった事例です。

これまで「一般従業員 / エンドユーザー」の中にはレジ係、窓口係、ウェイターが入っていましたが、本年は分離して「レジ係 / 窓口係 / ウェイター」という分類項目を新設しました。この項目を作ったのは、いずれも金銭を扱う職であり、その点で企業の一般従業員とは異なるからです。以前は一般従業員によるデータ漏洩 / 侵害の割合が非常に大きかったのですが、この項目を設けたことで内訳が具体的に分かるようになりました。「レジ係 / 窓口係 / ウェイター」によるデータ漏洩 / 侵害は、内部因子による全データ漏洩 / 侵害事例の 65%を占めました。このような従業員は、外部の犯罪組織にそそのかされ、顧客のカード情報をスキミングするという行為に及ぶことがよくあります。スキミングは、携帯デバイスで磁気ストライプデータを読み取るという方法で行われます。スキミングされたデータは、所定の経路を通じて犯

14 部内者が間接的にデータ漏洩 / 侵害に関与した場合、どのような状況であれば、その部内者を脅威因子とはみなさないかについては、「パートナー」と「過失」の節に例と説明があります。

表 6. 内部因子のタイプで分類した場合のデータ漏洩 / 侵害の割合（内部因子によるデータ漏洩 / 侵害のみ）

レジ係 / 窓口係 / ウェイター	65%
管理職 / 監督者	15%
一般従業員 / エンドユーザー	12%
財務 / 会計スタッフ	6%
システム / ネットワーク管理者	6%
監査担当者	3%
経営幹部 / 上級管理職	3%
外部のシステムまたはサイト	3%
不明	3%

罪者に渡され、犯罪者は磁気ストライプエンコーダーを使って偽のカードを作ります。この種のデータ漏洩 / 侵害は、小規模の店舗や大手ブランドの地元フランチャイズ店で発生することが非常に多いのですが、これは上記のような事情によります。

一方、「一般従業員 / エンドユーザー」によるデータ漏洩 / 侵害（12%）は、「レジ係 / 窓口係 / ウェイター」によるデータ漏洩 / 侵害と内容的に大きく異なります。つまり、一般の従業員は大抵の場合、システムアクセス権などの特権を不正に使用し、機密情報を窃取するという方法を使います。また、部内者によるデータ漏洩 / 侵害の動機は十中八九、金銭または個人的利益です。

「管理職 / 監督者」と「経営幹部 / 上級管理職」によるデータ侵害も比較的多く、合計すると 18%に達します。管理職などは、一般従業員の場合と同じくシステムアクセス権などの特権を悪用し、個人的利益を得るという方法を用いています。「財務 / 会計スタッフ」は、3 年連続で減少しました。それでも、このようなスタッフは仕事柄、日常的に貴重な資産や情報を管理したり扱ったりしており、ほぼ自由にデータ漏洩 / 侵害を実行できる立場にあることは以前と同じです。部内者のタイプ別のデータ漏洩 / 侵害と規制の関係を見てみるとどうか、と思う読者もいるはずです。規制は、グラス・スティーガル法からグラム・リーチ・ブライリー法へ、さらにドッド・フランク法とめまぐるしく変わっています。規制の変化に応じて部内者によるデータ漏洩 / 侵害がどう変わっているかを確かめてみるのも、極めて興味深い作業です。

最後に「システム / ネットワーク管理者」についても触れなければ、職務怠慢となりかねません。システム / ネットワーク管理者は信頼の厚い「技術戦士」で、この戦士がいるからこそ IT 企業は世界を席巻でき、そのためシステム / ネットワーク管理者は「王国への鍵」を握っているとよく言われます。2011 年の場合、システム / ネットワーク管理者によるデータ漏洩 / 侵害は何件かありましたが、ほとんどレーダーに映し出される点ほどのものでしかなく、これは前年も同様でした。本報告書の冒頭より少し後の部分で、ある企業がデータ漏洩 / 侵害にあい、その企業と協力してデータ漏洩 / 侵害を分析したと述べました。この事例では管理者によるデータ漏洩 / 侵害がかなり発生していましたが、被害は機密性の喪失ではなく、大半が可用性の喪失とダウンタイムの発生でした。

パートナー（全データ漏洩 / 侵害の < 1%、全侵害レコードの < 1%がパートナーによるもの）

パートナーによるデータ漏洩 / 侵害は、2010 年はほんのわずかでしたが、2011 年も引き続き同じでした。実際、2011 年の総合事例データには、パートナーによるデータ漏洩 / 侵害は 3 件しかありませんでした（偶然と言えば偶然ですが昨年の報告書も 3 件でした）。そのうち 2 件は、主原因（直接関与）として過失により情報を公開したケース、具体的にはパートナーが誤って機密データをインターネット上の公開ウェブサイトに投稿したケースでした。残りの 1 件は、サードパーティによる意図的で悪意のある不正使用で、動機は金銭の入手でした。具体的には、サードパーティのデータベースデベロッパーが契約業務を行っている際に SQL の脆弱性を発見し、その脆弱性を悪用してデータ漏洩 / 侵害を実行したという事例でした。

なお、上記の 3 件は、パートナーを脅威因子（主原因）とみなしたときの結果です。このほか、パートナーが間接的に関与、つまりパートナーがデータ漏洩 / 侵害の周辺の環境に関係したデータ漏洩 / 侵害も多数ありましたが、そのような事例は除外しました。この区別は若干、厄介です。事実、データ漏洩 / 侵害調査報告書の読者や VERIS のユーザーから、どのような事例をパートナーによるデータ漏洩 / 侵害とすればいいか（部内者の場合も同じです）という質問を多数頂戴しています。上記の 3 件のパートナーによるデータ漏洩 / 侵害については、これ以上説明することはありませんので、ここでギアを切り替え、どのような場合にパートナーを脅威因子として定義すればいいかを説明することにします。もちろん、VERIS を使用しないか、不要と思えば読み飛ばして結構です。

パートナーの定義例：

1. パートナーの行為により直接、データ漏洩 / 侵害が発生した場合、そのパートナーを脅威因子とみなします。
2. パートナーが別の脅威因子の指示や決定に基づいて何らかの行為を行い、その行為によって何らかの状況または条件が生じ、その状況または条件によって脅威イベントが生じた場合には、そのパートナーを脅威因子とはみなしません。この場合、イベントは条件イベントであり、パートナーは寄与原因（つまり間接的に関与した）と考えることができます。この場合のパートナーの行為は、脅威に関係した行為ではなく、被害企業・組織のセキュリティまたは脆弱性に関係した行為でなければなりません。
3. 企業・組織の資産についてデータ漏洩 / 侵害が発生し、その資産をパートナーが所有し、ホストし、もしくは管理していた場合、そのパートナーを必ずしも脅威因子とみなす必要はありません。場合によっては脅威因子であることもありますが（そのパートナーの行為の結果、データ漏洩 / 侵害が発生した場合）、上記の状況だけでは脅威因子とみなすことはできません。

上の例 2 は、どうも合点がいかないという人が多いかもしれません。そこで分かりやすいように、具体例を使って説明することにします。パートナーが契約企業から、その企業のデバイスをインターネット経由でリモートアクセスかデスクトップサービスを使ってリモートから管理するように依頼された、とします。作業を進め設置も終わったのですが、セキュリティ設定を有効にするのを忘れたか、設定を誤ってした、とします（他には、管理者であれば絶対にしないこと、例えばデフォルトの認証情報を変更しなかったなど適宜、想像してください）。その後、こともあろうか、東ヨーロッパの組織犯罪グループがそのデバイスのユーザー名とパスワードの推測を開始し、30 秒も立たないうちに探し当ててしまいました。もちろん、これは架空の話であって、現実の世界では起こるはずもありません（ところがそうでもないのです）。この場合、脅威因子は組織犯罪グループであって、パートナーは脅威因子ではありません。このパートナーは（間接的）寄与原因であり、したがって VERIS で登録する場合、機能（役割）を「条件イベントに寄与」、脅威アクションを「過失」として記録します。この事例は結局、パートナーが脆弱性（条件イベント）を作り出し、その脆弱性が外部因子によって悪用されたデータ漏洩 / 侵害ということになります。

パートナーのセキュリティ管理体制が貧弱でガバナンスも甘いと（どちらも企業・組織では管理できず内容も不明なのが普通です）、一般にセキュリティインシデントの発生確率が上昇します。

以前にも述べたように、企業・組織が IT 管理やサポートをパートナーにアウトソーシングする場合、同時に相当程度の信頼もアウトソーシングすることになります。パートナーのセキュリティ管理体制が貧弱でガバナンスも甘いと（どちらも企業・組織では管理できず内容も不明なのが普通です）、一般にセキュリティインシデントの発生確率が上昇します。それでもアウトソーシングにはメリットが多く、アウトソーシングに伴うリスクを解消したい場合、パートナーのポリシーや契約内容、管理体制、その他の必要事項を十分に検討するのが最善策です。ひとつ注意しなければならないのは、業務はパートナーにアウトソーシングできるが、リスクと責任はアウトソーシングできないということです。どちらも企業・組織の仕事であり、これは当然ながら、データを所定の方法で正しく扱っているということを公に示し、信頼を得る必要があるからです。

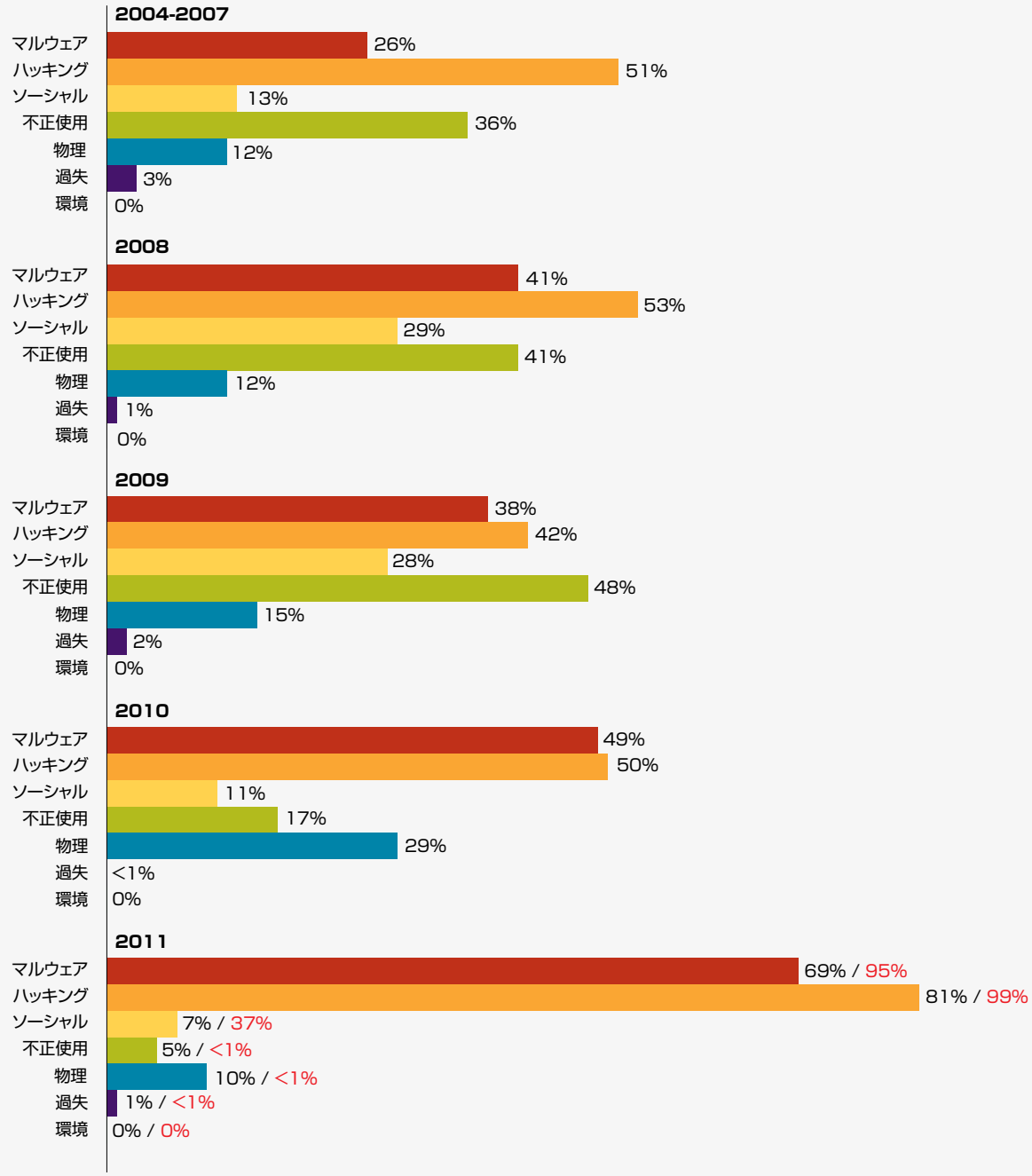
脅威アクション

脅威アクションとは、何らかの脅威因子による行為または活動であり、データ漏洩 / 侵害を引き起こし、もしくはその発生に寄与する行為または活動をいいます。同一のデータ漏洩 / 侵害には通常、複数の脅威アクションが関係しており、そのため脅威アクションを基準にデータ漏洩 / 侵害を分類すると、各脅威アクションの割合の合計は 100%を超えます。VERIS では、脅威アクションを 7 種類に分類しています（それぞれ後続の節で詳しく説明してあります）。

脅威アクションの中では、以前からハッキングとマルウェアが突出していましたが、今回はさらに突出し、「ハロー」と言いながらカメラの間近まで迫ってきたような勢いでした。本年の分析対象のデータ漏洩 / 侵害は全部で 855 件でしたが、その 81%がハッキング、69%がマルウェアによるものでした。また、ハッキングとマルウェアの両方が関係していたデータ漏洩 / 侵害は、全データ漏洩 / 侵害の 61%を占めました。複数の脅威アクションが関係していたデータ漏洩 / 侵害は 602 件あり、そのうちハッキングとマルウェアが関係していたデータ漏洩 / 侵害は 86%に上りました（データ漏洩 / 侵害あたりの脅威アクションの数については、付録 A に説明があります）。

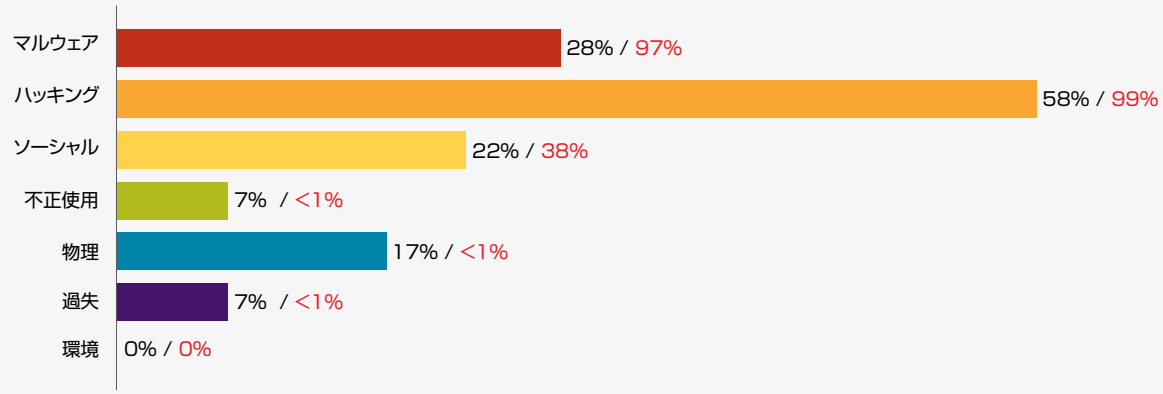
脅威アクションの中では、以前からハッキングとマルウェアが突出していましたが、今回はさらに突出し、「ハロー」と言いながらカメラの間近まで迫ってきたような勢いでした。

図 17. 脅威アクションのカテゴリー別のデータ漏洩 / 侵害事例の割合と侵害レコード数の割合（年別）



全体的に見ると、脅威アクションは年を追うごとに多少変化しています。不正使用とソーシャルは 2009 年に絶頂期を迎え、一方、物理的攻撃は翌年の 2010 年に勇姿を現しています。昨年、物理的攻撃は急激に落ち込み、これは世界各国の法執行機関がスキミングの犯人の逮捕に成功したことによるものと思われます。各国の法執行機関は、個々のスキミング事件ではなく事件の背後にいる犯罪組織を追跡することで逮捕にこぎ着け、最近、その成果が見え始めているようです。

図 18. 脅威アクションのカテゴリー別のデータ漏洩 / 侵害事例の割合と侵害レコード数の割合（大規模の企業・組織の事例のみ）



一方、大規模の企業・組織の事例だけを見てみると、
各脅威アクションの構成は全企業・組織の場合といささか異なります。
図 18 は、大規模の企業・組織の事例だけを使用して分類した結果ですが、
この結果には単純ながら一言の価値がある真実が隠されています。

見解はいろいろあるかもしれませんが、明らかなことがひとつあります。それは、全企業・組織を見た場合、各脅威アクションの構成は年にかかわらず総じて似通っているということです。

一方、大規模の企業・組織の事例だけを見てみると、各脅威アクションの構成は全企業・組織の場合といささか異なります。図 18 は、大規模の企業・組織の事例だけを使用して分類した結果ですが、この結果には単純ながら一言の価値がある真実が隠されています。それは、データ漏洩 / 侵害に関しては、小規模企業と大規模企業とでは問題の質や大きさが異なるということです。つまり、大規模企業の場合には自社の IT スタッフが低い位置に生っている果実（地面に落ち朽ちている果実と言ったほうが正確）に対して何らかの対策を講じているが、小規模企業ではそうではないのが普通です。なお、企業・組織のデータ漏洩 / 侵害に対する対策を考える場合、脅威アクションをさらに分類して検討する必要があり（細分項目をタイプと呼びます）、表 7 はその結果です。

表 7. 脅威アクションのタイプ（上位 10 位）で分類した場合のデータ漏洩 / 侵害件数と侵害レコード数

順位	タイプ	カテゴリー	漏洩 / 侵害	侵害レコード数
1	キーロガー / フォームグラバー / スパイウェア（ユーザーの操作を記録）	マルウェア	48%	35%
2	デフォルトまたは推測可能な認証情報の悪用	ハッキング	44%	1%
3	盗んだログイン情報の使用	ハッキング	32%	82%
4	外部のサイトや組織 / 個人にデータを送信	マルウェア	30%	<1%
5	ブルートフォース（総当たり攻撃）と辞書攻撃	ハッキング	23%	<1%
6	バックドア（リモートアクセス / 制御）	マルウェア	20%	49%
7	バックドアまたはコマンド&コントロールチャンネルの不正使用	ハッキング	20%	49%
8	セキュリティコントロールの無効化または妨害	マルウェア	18%	<1%
9	タンパリング	物理	10%	<1%
10	不十分な認証の悪用（ログイン不要など）	ハッキング	5%	<1%

企業の規模を問わず、ユーザーによる入力の捕捉を目的とした悪意のコード（一般にキーロガーと呼ばれます）によってデータが侵害された事例が多く、この事例が全データ漏洩 / 侵害のほぼ半分（48%）を占めました。悪意のコードで入手したログイン情報を使ってデータ漏洩 / 侵害を実行するケースが多く、そのため「盗んだログイン情報の使用」がデータ漏洩 / 侵害 3 件のうちほぼ 1 件を占めています。もうひとつ、大規模企業と小規模企業を問わず多いのがバックドアのインストールで、データ漏洩 / 侵害 5 件のうち 1 件がこの事例でした。表 7 は全企業・組織の事例による分析結果ですが、大規模企業の事例だけを使って分析すると脅威アクションの相違が分かります。表 8 は、大規模企業の事例だけを使用し、脅威アクションのタイプ（上位 10 位）を基準に分類した表です。

表 8. 脅威アクションのタイプ（上位 10 位）で分類した場合のデータ漏洩 / 侵害件数と侵害レコード数の割合（大規模の企業・組織の事例のみ）

順位	全企業・組織の事例での順位	タイプ	カテゴリー	漏洩 / 侵害	侵害レコード数
1	3	盗んだログイン情報の使用	ハッキング	30%	84%
2	6	バックドア（リモートアクセス / 制御）	マルウェア	18%	51%
3	7	バックドアまたはコマンド&コントロールチャンネルの不正使用	ハッキング	17%	51%
4	9	タンパリング	物理	17%	<1%
5	1	キーロガー / フォームグラバー / スパイウェア（ユーザーの操作を記録）	マルウェア	13%	36%
6	11	プリテキスティング（従来の一般的ソーシャルエンジニアリング）	ソーシャル	12%	<1%
7	5	ブルートフォース (総当たり攻撃) と辞書攻撃	ハッキング	8%	<1%
8	15	SQL インジェクション	ハッキング	8%	1%
9	20	フィッシング（各種）	ソーシャル	8%	38%
10	22	コマンド&コントロール（コマンドを待受し実行）	マルウェア	8%	36%

表 8 は事例データの量が少ないため、そのまま解釈するのは問題がありますが（データが少ないとサンプリング誤差の増大につながります）、それでも興味深い点をいくつか発見できます。まず気がつくのは、ソーシャル（プリテキスティング）が上位に来ていることです。具体的には、大規模の企業･組織だけの場合、データ漏洩 / 侵害の実に 12%がソーシャルによるものでした。大規模企業でソーシャルによるデータ漏洩 / 侵害が多いのは、データ漏洩 / 侵害に対する防御が固いこと（その結果、システムではなく人間が標的になることが多い）や、従業員同士の関係が複雑であること（従業員が多いため、信頼できる同僚とできない同僚の区別が難しい）が原因と考えられます。

表 8 でもう一点、面白いのは「デフォルトまたは推測可能な認証情報の悪用」が 10 位以内に入っていないことです。このタイプの脅威アクションは大規模の企業･組織の事例（60 件）のうち 2、3 例しかなく、そのせいで表から消えました。理由としては、大規模の企業・組織の場合、この種の認証情報は技術者が変更してあることが多いこと、またデフォルトのパスワードが複数あるため、攻撃者が容易に「王冠の宝石」に辿り着けないことなどがあげられます。このような理由から、大規模の企業・組織が標的の場合、攻撃者はログイン情報を盗みデータ漏洩 / 侵害を試みるという方法に頼ることになります。脅威アクションのタイプの説明はここまでとして、次に、2011 年のデータ漏洩 / 侵害で見られた脅威アクションと分析結果をカテゴリー別に詳しく見ていきます。

マルウェア（全データ漏洩 / 侵害の 69%、全侵害レコードの 95% がマルウェアによるもの）

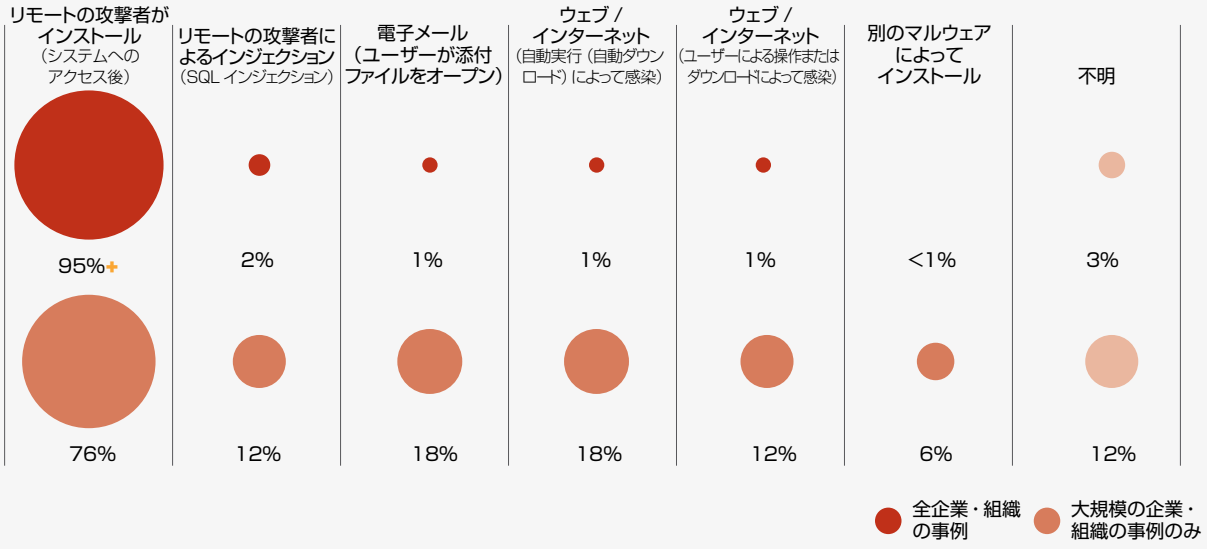
マルウェアとは、情報資産の所有者の同意を得ずに、その資産を侵害したり被害を及ぼすことを目的として開発された悪意のソフトウェアまたはスクリプト、もしくはコードをいいます。2011 年の場合、マルウェアが関係したデータ漏洩 / 侵害は全事例の 3 分の 2 を超え、また全侵害レコードの 95%にマルウェアが関係していました。ベライゾン RISK チームがデータ漏洩 / 侵害事例の調査を実施し、その事例がマルウェアによるものと判定した場合には通常、客観解析を行い、そのデータ漏洩 / 侵害事例を分析するとともに内容を特定します。また、RISK チームでは分析結果をもとに、被害を受けた企業・組織と協力してマルウェアの除去や封じ込め、被害からの復旧に努めます。マルウェアの分類方法は種々ありますが、VERIS フレームワークでは 2 次元手法を用いています。2 次元手法とは、マルウェアの感染経路と機能を基準にしてマルウェアを分析する方法です。マルウェアの感染経路と機能を理解することは、マルウェアの検出と防止に必要な対策を策定する上で重要です。

マルウェアの感染経路

今回、マルウェアの感染経路として一番よく見られたのは、これまでと同じく攻撃者によるリモートからのインストールやインジェクションという方法でした。例えば、攻撃者がリモートアクセスを介してシステムに侵入し、その後、ウェブアプリケーションの脆弱性を悪用してマルウェアをインストールしたり、コードをインジェクトするというのがこの方法に該当します。この感染経路は過去数年間、次第に増加する傾向にあります。具体的には、この感染経路によるマルウェアを原因として発生したデータ漏洩 / 侵害は、2009 年の場合は全データ漏洩 / 侵害の半分強、2010 年は約 80%で、昨年は実に 95%に達しました。この感染経路が「人気」が高いのは、システム（PC やサーバーなど）へのアクセス後、攻撃者がシステムを継続してコントロールできると同時に、リモートアクセスサービスを介して多数の標的に自動化された攻撃を実行できることが理由と思われます。金銭が目的のデータ漏洩 / 侵害事例（ペイメントカード情報の窃取など）でもこの感染経路がよく使われ、この場合、マルウェアが最初に使用されることはあまりなく、何らかの手段でアクセスした後、攻撃者がマルウェアをインストールするというのが普通の手順です。この手順は、攻撃手法によっては異なることもあります。例えば、知的財産の窃取の場合、ソーシャルエンジニアリング（フィッシング電子メールなど）が成功した後、マルウェアが使用されるのが一般的です。いずれにしても、アンチウイルスソフトウェアの使用だけでなく、堅固で多重の防御体制を敷くことによって攻撃者を水際で阻止することができます。

今回、マルウェアの感染経路として一番よく見られたのは、これまでと同じく攻撃者によるリモートからのインストールやインジェクションという方法でした。例えば、攻撃者がリモートアクセスを介してシステムに侵入し、その後、ウェブアプリケーションの脆弱性を悪用してマルウェアをインストールしたり、コードをインジェクトするというのがこの方法に該当します。

図 19. マルウェアの感染経路で分類した場合のデータ漏洩 / 侵害事例の割合（マルウェアによるデータ漏洩 / 侵害のみ）



昨年の状況を見ると、電子メールは、感染経路としてはそれほど一般的ではなくなっています。理由は、多くの企業・組織がアンチウイルスソフトウェアやフィルタリングメカニズムを導入し、インターネット上に存在している何百万種類というマルウェアの感染阻止と隔離に成功しているためです。このような対策が施されていなければ、電子メールは感染経路として未だによく使われているものと思われます。

電子メールと同じく、ウェブ / インターネットによる感染も減少しました。ウェブベースのマルウェアは、自動実行（自動ダウンロード）コードと、ユーザーが操作する必要があるソフトウェア（悪意のハイパーリンクをクリック）の 2 種類があります。ウェブベースのマルウェアによって感染した例は無数にありますが、データの窃取を確認できたのは氷山の一角にすぎないと考えられます。

ウェブベースのマルウェアの場合、通常、感染しているウェブサイトをユーザーが訪れる必要があります。この方法は、パスワード窃取を目的としたマルウェアであるゼウス（Zeus）などでは有効ですが、決済システムを装って大規模なデータ漏洩 / 侵害を実行するのには不向きです。感染したシステムのほとんどは数千というボットネットに接続され、DDoSなどの攻撃に利用されます。

大規模の企業・組織の場合、全企業・組織の場合に比べるとマルウェアの感染経路の差は大きくはありません。「電子メール」と「ウェブ / インターネット」（2 種類）の割合は大きく、逆に「リモートの攻撃者がインストール」の割合は小さく、全体的にそれほど不均衡ではありません。

大規模の企業・組織の場合、全企業・組織の場合に比べるとマルウェアの感染経路の差は大きくはありません。「電子メール」と「ウェブ / インターネット」（2 種類）の割合は大きく、逆に「リモートの攻撃者がインストール」の割合は小さく、全体的にそれほど不均衡ではありません。攻撃者は恐らく、大規模の企業・組織を真っ向から攻撃して防御を破るより、従業員にマルウェアをインストールさせるほうが簡単と考えており、これが電子メールとウェブ / インターネットの割合が大きい主な原因です。「不明」の割合が多い理由はいくつかあります。一番一般的な理由は、システムに証拠が残っていないことです（例えば、ログデータがない、攻撃者がアンチフォレンジックを行った、証拠を収集しないうちにシステムをクリーンアップしたなど）。このようなケースでは、マルウェアが存在していたことは分かっているものの、結局は感染経路の特定は不可能であり、したがって感染経路は「不明」です。

マルウェアの機能

マルウェアに感染した場合、マルウェアの機能が動作を開始することになりますが、この機能もマルウェアの感染経路と同様に重要です。ベライゾン RISK チームがマルウェアによるデータ漏洩 / 侵害を調査する際、もちろんマルウェアに注目しますが、作業中に企業・組織にとっては不要と思われ、かつ不審なファイルを発見することがよくあります。このようなファイルが見つかるのは、システムの管理が不十分であり、またセキュリティ対策が施されていない証拠であり、その意味では有益です。マルウェアは種々の方法でシステムに被害を及ぼしますが、データ漏洩 / 侵害の観点から見ると、マルウェアの機能は基本的には 3 つです。3 つとは、アクセスの確立または継続、データの捕捉、何らかの方法による攻撃の継続です。

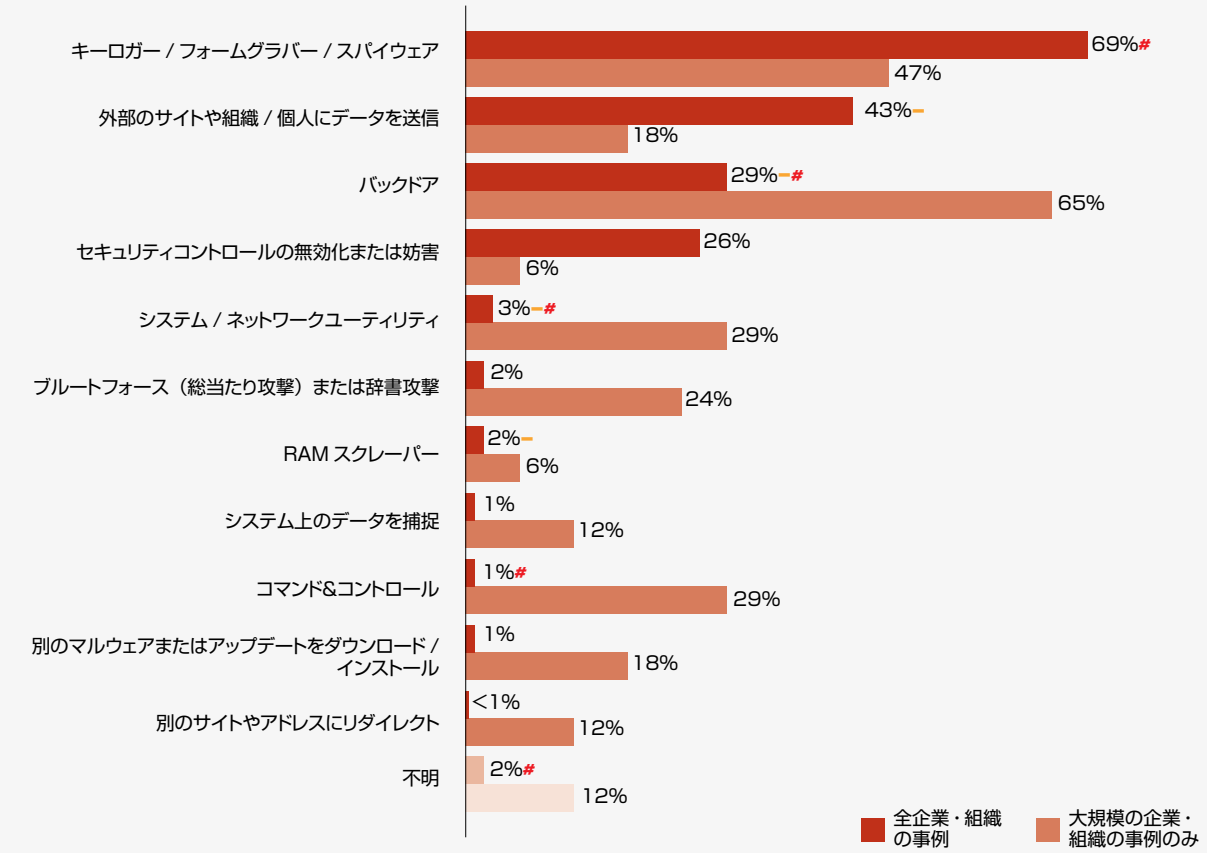
図 20 にあるように、マルウェアの機能の中でもっとも頻繁に見られた 3 つの機能はこれまでと同じく、キーストローク（その他の方法によるユーザーからの入力を含む）のロギング、外部の場所へのデータの送信、バックドアでした。ここで注意しなければならないのは、この 3 つの機能は必ずしも別個のものではなく、単一のマルウェアが 3 つの機能を兼ね備えていることも少なくないということです。

図に示されているように、キーロガーが使用されたデータ漏洩 / 侵害事例は、マルウェアが関係している全データ漏洩 / 侵害事例の 3 分の 2 以上を占めており、この事例は前年より多少増加しています。キーロガーは、ソフトウェアパッケージとして市販されているものがあり、インターネット上にダウンロード版もあります。さらに、その海賊版（フル機能）を P2P ネットワークやダウンロードサイトで入手できます。キーロガーの中には、攻撃者がリモートインストールパッケージを作成し、そのパッケージを標的のシステムにインストールできるという機能を備えたものもあります。キーロガーは、入手が容易、使いやすい、種類が豊富、アンチフォレンジック機能がある（ファイルリストに登録されず、プロセスとしても記録されないなど）などの理由から、攻撃者にとっては魅力的なツールです。

キーロガーの次に多かったのは、データの取り出し（外部のサイトや組織 / 個人にデータを送信）でした。一般的に言えば、攻撃者がデータの抽出を行う方法には二通りあります。ひとつは、侵入後、すぐに企業・組織からデータを外部に送信する方法です。この方法は、昨年の報告書ではトップでした（今回は 43%、昨年の報告書では 79%）。この方法の場合、リアルタイムで送信（データの捕捉と同時に送信）するほか、一定間隔または何らかの処理（プログラムの起動後）の後に送信するという処理も可能です。この機能は、ほとんどのキーロガーに搭載されています（付録 A を参照）。

もうひとつは、攻撃者がいったんネットワークから離れ、そのあと再度ネットワークに侵入してデータを抽出するという方法です。この場合、攻撃者は当初の感染経路から侵入することもできますし、バックドアを使ってリモートからデータを取り出すこともできます。また、データ抽出機能を備えたマルウェアには通常、侵害したシステムを制御する機能も搭載されています。例えば、別のマルウェアをインストールしたり、企業･組織の環境に常駐したり、侵害したシステムを使って別の攻撃を仕掛けたりといった操作が可能です。バックドアは、事例データによれば、標的の企業・組織からデータを抽出する方法として以前から継続して極めて頻繁に使われています。

図 20. マルウェアの機能で分類した場合のデータ漏洩 / 侵害事例の割合（マルウェアによるデータ漏洩 / 侵害のみ）



以上、2011 年の事例データをもとに攻撃者がデータを取り出す場合の方法を見てきましたが、この方法は企業・組織の規模によって相違があります。つまり、小規模の企業・組織の場合、「外部のサイトや組織 / 個人にデータを送信」がよく使われる傾向があります。前述のように近年、多数の小中規模企業を狙った自動化された攻撃が増えていますが、このような攻撃で使われるマルウェアには「外部のサイトや組織 / 個人にデータを送信」機能が搭載されており、これが上記の傾向の理由です。一方、大規模の企業･組織の場合、バックドアを利用してデータを抽出する攻撃者が主流です。大規模の企業・組織は、リモートサービスの認証やアクセス制御に関して厳格に管理を行っているのが普通です。この事情から、大規模の企業・組織のネットワークに侵入した後、バックドアを介して内部のシステムに足場を作るという方法を使う攻撃者が少なくありません。いったん足場ができれば、その足場を使ってバックドアをいくつもインストールし、その後、長期にわたってアクセスを続けます。

また、大規模の企業・組織の場合、「悪意のない」システム / ネットワークユーティリティ（SysInternals など）を使用する攻撃者が多いという傾向があります。このようなユーティリティはもちろん、システム / ネットワーク管理者がシステムのメンテナンスに使用するのが一般的です。しかしながら攻撃者は、このようなユーティリティを標的の企業・組織のシステムにインストールすることがあり、その場合、報告書ではマルウェアとして分類しています。このようなユーティリティは通常、アンチウイルスソフトウェアによってマルウェアと認識されることはありません。

過去の報告書でも説明しましたが、企業・組織には、システムを最低限の権限モードで使用すること、ネットワークの入口と出口の両方を監視すること、システムに不正な変更が加えられていないかを確認することを強く推奨しています。このような対策を励行することで、不正行為を発見できるとともに、データ漏洩 / 侵害や何らかのセキュリティインシデントが発生した場合でも被害を限定できる可能性が高くなります。上記に加えて、侵害の徴候、例えば不要な PsTools などのプロセス管理ツールがないかどうか、ZIP や RAR などのアーカイブファイルが増えていないかどうか、属性が「隠しファイル」や「読み取り専用」の新規ファイルがないかどうかを確認することも重要です。

アンチウイルスベンダーのアラートはどうも信用できないという方も多いかもしれませんが、それでもアンチウイルスソフトウェアからアラートが出たら、それなりの対応をとる必要があります。「火の無い所に煙は立たぬ」という諺がありますが、これはデータ漏洩 / 侵害の場合にも当てはまります。マルウェアの検出と対応は感染直後に開始しなければならず、そうでなければ全面的データ漏洩 / 侵害に発展します。実際、多数の調査で、企業・組織がアンチウイルスのアラートを真剣に捉え、迅速に対応していればデータ漏洩 / 侵害を阻止できていたことが証明されています。

マルウェアのカスタマイズ

本年の場合、カスタマイズされたマルウェアが使用された事例は、マルウェアが関係した全データ漏洩 / 侵害のうちの約 3 分の 1 で（ベライゾンのデータ漏洩 / 侵害事例のみ）、これは過去の報告書の結果とはかなり違います。ベライゾンの 2005 年から 2007 年までのデータ漏洩 / 侵害事例では、カスタマイズされたマルウェアが使用されていた事例は、これよりもずっと多いという結果が出ていました。カスタマイズされたマルウェアは、大規模の企業・組織に対して使用されることが多いのですが、かなり多いというわけではありません。マルウェアをカスタマイズする方法としては、攻撃者が初めから作成・開発する方法と既存のマルウェアを修正する方法の 2 種類があり、この傾向は、全企業・組織の場合も大規模の企業・組織だけの場合も同様です。カスタマイズされたマルウェアがあまり見られなくなったのは、「産業化された」攻撃では市販のアプリケーションが使用されることが主な理由です。つまり、非常に多数の企業・組織に対するデータ漏洩 / 侵害を目的とした攻撃の場合、「既製品」を使って数千という標的を効率よく攻撃できるため、マルウェアをわざわざカスタマイズする必要はないのです。

VERIS の分類に関する注意：ハッキングと不正使用は、どちらも脅威アクションの一カテゴリーです。経路はどちらも似ており、行為の結果も似ています。ただし、脅威因子のアクセス権は、不正使用の場合は脅威因子に正規に付与されたものですが（そのアクセス権を不正に使用）、ハッキングの場合、脅威因子が不法に入手したものです。

ハッキング（全データ漏洩 / 侵害の 81%、全侵害レコードの 99% がハッキングによるもの）

ハッキングは VERIS フレームワークで定義されている脅威アクション（のカテゴリー）のひとつで、論理セキュリティメカニズムを妨害もしくは無効化することにより、権限なしで（もしくは権限を超えて）、意図的に情報資産にアクセスし、または情報資産を侵害しようとする行為すべてを指します。ハッキングは、攻撃方法としては便利で有用であり、その理由はいくつかあります。まず、通常はリモートから実行するため、攻撃者にとって匿名性と攻撃の拡張性という利点があります。また、自動化ツールと基本的なスクリプト（第三者が書いたものを攻撃者が使用するのが普通）を使って、多種多様なハッキング行為を極めて簡単に実行でき、また非常に多数の標的に対して攻撃が可能です。

本節では、2011 年の総合事例データ（ベライゾンと各協力機関のデータ漏洩 / 侵害事例を合わせたもの）を使用し、ハッキングの手法と経路について見ていきます。

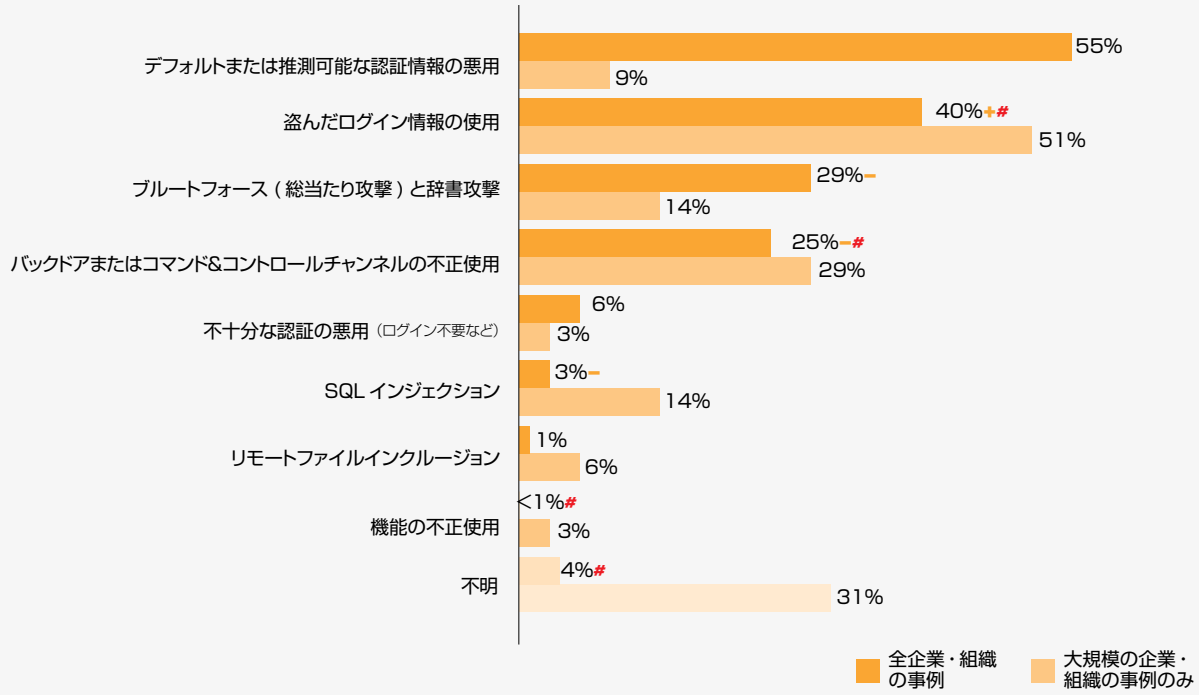
ハッキングのタイプ

次ページのグラフは、2011 年のデータ漏洩 / 侵害事例のうち、脅威アクション（カテゴリー）がハッキングだった事例を取り出し、ハッキングのタイプ（手法）で事例を分類したグラフです。以下、今回の傾向を説明しますが、データ漏洩 / 侵害調査報告書シリーズの常連読者であればお気づきかもしれません。例年と同様、今回もいくつかの手法が群を抜いて目立っています。ハッキングの手法は、総じて言えば認証に関する攻撃（ログイン情報の窃取、ブルートフォース、認証情報の推測など）と、認証を迂回または突破することを目的とした攻撃（SQL インジェクションやバックドアなど）に大きく分けられます。

例年と同様、今回もいくつかの手法が群を抜いて目立っています。ハッキングの手法は、総じて言えば認証に関する攻撃と、認証を迂回または突破することを目的とした攻撃に大きく分けられます。

また、本年は「メガデータ漏洩 / 侵害」が再出現したため、これまでのデータ漏洩 / 侵害の件数と侵害レコード数のバランスが崩れました。その結果、タイプの中には、データ漏洩 / 侵害事例の数はひとつ二つなのに侵害レコード数は多いというタイプ（「機能の不正使用」など）が見られました。「不明」もデータ漏洩 / 侵害の数は少ないのに侵害レコード数は多い手法で（全侵害レコード数の半分超）、データ漏洩 / 侵害のどこかでハッキング手法が使用され、その手法が不明だった場合、

図 21. ハッキングのタイプで分類した場合のデータ漏洩 / 侵害事例の割合（ハッキングによるデータ漏洩 / 侵害のみ）



ここに分類しました。ハッキング手法が不明だった理由としては、ログの欠落、攻撃者によるアンチフォレンジックの実行、依頼主による調査の中止の要請などがあります。

自動化された攻撃は引き続き盛んに使われており、この種の攻撃は技術的にはそれほど高度でなく、一回の攻撃あたりの侵害レコード数も多くはありません。自動化された攻撃の主な標的は、小売業やホテル・飲食業の小中規模企業です。また、小中規模企業に対するハッキングで使用される手法と、大規模企業のデータ漏洩 / 侵害に使われるハッキング手法ではいくつか異なる点があります。例えば、一般に大規模企業は、簡単で防御しやすい攻撃には強いと見られており、そのため「盗んだログイン情報の使用」は少ないようですが、実際には全侵害レコードの約 98%が「盗んだログイン情報の使用」によるものでした。

大規模企業は緑深き豊かな土地であり、攻撃者にとって魅力的な投資の対象です。緑深き豊かな土地を前にして、攻撃者は座ったままトンネルを掘ってバックドアを作り、やすやすと牧草地にたどり着きます。

小中規模企業の場合、攻撃者が入手できる情報の量は一般に多くないため、ハッカーはいわゆる「軍隊アリ」戦術を用いる傾向があります。「軍隊アリ」戦術とは、サーバーに存在するデータを何もかも根こそぎさらっていく方法で、この場合、サーバーを「居場所」にしようとはしません。一方、大規模企業は緑深き豊かな土地であり、攻撃者にとって魅力的な投資の対象です。緑深き豊かな土地を前にして、攻撃者は座ったままトンネルを掘ってバックドアを作り、やすやすと牧草地にたどり着きます。もっとも、このような攻撃には技術が必要ですが、分類上、特に「高度」な攻撃ではなく、また長期にわたってデータの入手が可能です。

「ブルートフォースと辞書攻撃」と「デフォルトまたは推測可能な認証情報の悪用」は昨年より減っていますが、小売業界とホテル・飲食業界（小中規模企業が多い）ではまだ頻繁に見られます。残念ながら、ベンダーのサイトに行って顧客リストを入手し、デフォルトのユーザー名とパスワード、もしくはユーザー名とパスワードを推測して入力すれば当たり、というのはよくあるようです。この手の攻撃は攻撃者にとって比較的簡単で、専門知識はほとんど必要なく工夫もほぼ不要です。通常、スクリプトが使われ、標的の数は多く、失敗すれば諦めるのが普通です。

実際、スクリプトを使ってデータをリモートサーバーに送った場合、そのリモートサーバーにアクセスして初めて何を盗んだかが分かるといったこともよくあります。この種の手法の場合、一回のデータ漏洩 / 侵害で窃取できるレコードの数は少ないため、攻撃者にとって個々の標的はそれほどの価値はありません。結局、標的の数が大事です。

ブルートフォース攻撃に関連して、「うっかり」攻撃者の例をひとつ紹介します。オンライン FTP サーバーの設定が不適切で匿名 FTP アクセスが可能になっており、このサーバーにブルートフォースツールによる攻撃が実行されました（ほとんどのオンラインシステムが、この攻撃を受けます）。この攻撃では、定石通り多数のユーザー名 / パスワードが試されていました。ただし、匿名アクセスは試されませんでした（匿名アクセスで簡単に入れたのです）。

大規模企業は幸い、認証とアクセスを厳格に管理していることが多く、またセキュリティポリシーを自社の従業員とベンダーの両方に周知させています。このことは、大規模の企業・組織の分析結果に示されています。具体的には「ブルートフォースと辞書攻撃」は大規模の企業・組織の事例の 14%（全企業・組織の場合は 29%）、「デフォルトまたは推測可能な認証情報の悪用」は 10%未満（侵害レコード数は <1%）でした。パッチで修正可能な脆弱性を突く攻撃とゼロデイ攻撃（脆弱性の発表前の攻撃）は、ほとんど見られませんでした。「不十分な認証の悪用（ログイン不要など）」は未だに比較的多く、この傾向は続くかもしれません。

ハッキングの経路

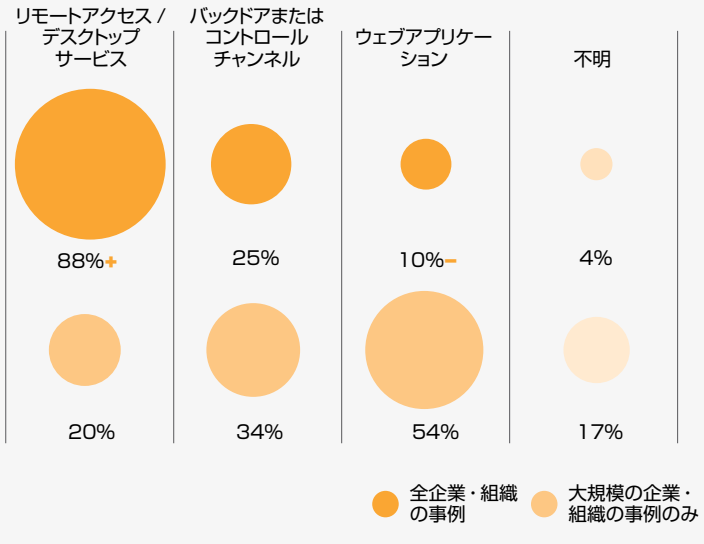
図 22 はハッキングの経路を示した図で、過去数年の結果とほぼ同じです。リモートアクセスサービス（VNC、RDP など）は引き続き増加傾向にあり、ハッキングが関係していた全データ漏洩 / 侵害の 88%を占めており、順位はトップです。リモートアクセスサービスはインターネット上からアクセスでき、このリモートアクセスサービスと「デフォルトまたは推測可能な認証情報」や「盗んだログイン情報」を併用した攻撃が現在も多く、主に小売業界やホテル・飲食業の小中規模企業がこの攻撃の犠牲になっています。ソフトウェアベンダーやサポートベンダーの顧客企業が標的で、そのため複数の顧客企業が犠牲になるのが普通です。この攻撃の場合、まずスクリプトを使って標的のリモートアクセスポート（TCP 3389、RDP、VNC）を探し、ベンダーが使っているデフォルトの認証情報を送信して標的に侵入し、その後、自動化された攻撃で効率よくデータ漏洩 / 侵害を実行するというのが基本的な手順です。

「バックドアまたはコントロールチャンネル」もハッキングの経路としては前年と同様、よく見られました（バックドアのインストールと利用について前述しました）。昨年は、ハッキングが関係していた全データ漏洩 / 侵害の 4 分の 1 でバックドアが経路として使用され、言い換えると、データ漏洩 / 侵害の一連のイベントのどこかで（通常は侵入後）デバイスにバックドアがインストールされたことになります。また、侵害レコード（確認済み）の 90%超がバックドアを利用した攻撃によって侵害されたレコードでした。

「ウェブアプリケーション」は前年と同じく経路としては 3 番目に多く、データ漏洩 / 侵害の件数は減ったものの、侵害レコードの 3 分の 1 超がこの経路を通じて侵害されました。インターネット上で利用できるウェブアプリケーションは需要があり、数も増えていることから必然的に標的になります。ウェブアプリケーションを介して企業のデータベースに侵入できるため、攻撃者にとっては魅力的です。

大規模の企業・組織の場合、ハッキングの経路は、全企業・組織の場合と比べて相違点がいくつかあります。一番の違いは、経路がリモートアクセスサービスであるデータ漏洩 / 侵害事例がわずか 20%であることです。これは、大規模の企業・組織の場合、セキュリティ体制が堅固なためリモートアクセス

図 22. ハッキングの経路で分類した場合のデータ漏洩 / 侵害事例の割合（ハッキングによるデータ漏洩 / 侵害のみ）



サービスによるアクセスを制限でき、また認証制御も強力であることによります。また、バックドアは全企業・組織の事例に比べるとがいくぶん多く、この経路を通じて侵害されたレコードは、ハッキングが関係した侵害レコードのほぼ全部を占めています。さらに、大規模の企業・組織ではウェブアプリケーションが非常に多く（全事例の 54%）、侵害レコード数も多い（全事例の 39%）という結果になっています。理由は、大規模企業は、前述のようにインターネット経由の攻撃に対する防御が固く、攻撃者にとっては使えるもの（ウェブアプリケーション）を狙うか、マルウェア（バックドアやコントロールチャンネル）でセキュリティを迂回するかのいずれかしかないためです。

大規模の企業・組織ではウェブアプリケーションが非常に多く（全事例の 54%）侵害レコード数も多い（全事例の 39%）という結果になっています。

ソーシャル・エンジニアリング（全データ漏洩 / 侵害の 7%、全レコードの 37%がソーシャル・エンジニアリングによるもの）

何世紀もわたって犯罪目的で権謀術数が繰り広げられてきましたが、今や情報セキュリティの世界もその舞台となっています。情報資産の「守護神」（ユーザー）は、策略やごまかし、脅迫といった悪質な対人テクニック（ソーシャルエンジニアリング）に極めて弱く、賢明な攻撃者はその弱点を利用する術を心得ています。人間は地球上のどの生物より複雑な生物ですが、裏をかいたり知恵を逆手にとってまんまとデータの窃取する犯罪者は少なくありません。2011 年の場合、ソーシャルエンジニアリングが関係していたデータ漏洩 / 侵害は前年より多少減った一方（前年は 11%）、盗まれたデータの量（侵害レコード数）は前年の 1%から 37%から激増しました。これは、データ漏洩 / 侵害調査報告書シリーズでは最高記録でした（なお、前述したように今回は「メガデータ漏洩 / 侵害」がいくつかあり、そのひとつがソーシャルエンジニアリングによるデータ漏洩 / 侵害だったことが激増の主な原因であることに注意）。

図 23. ソーシャルエンジニアリングのタイプで分類した場合のデータ漏洩 / 侵害事例の割合（ソーシャルエンジニアリングによるデータ漏洩 / 侵害のみ）

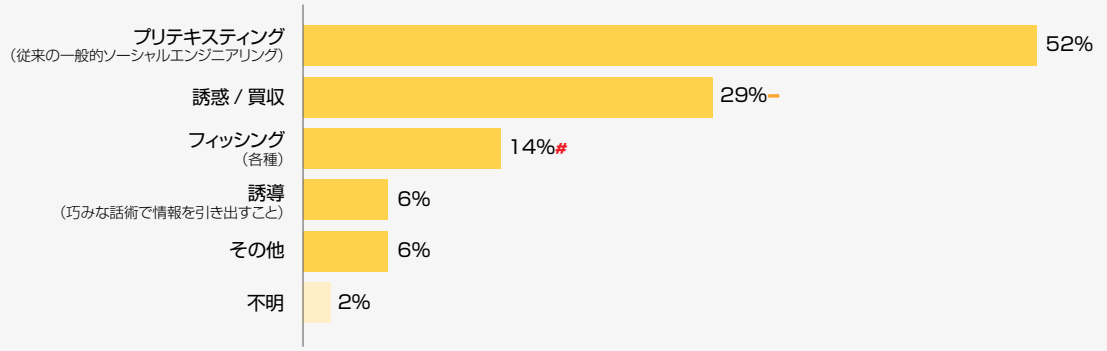


図 23 にあるように、今回はプリテキスティング（従来からある一般的ソーシャルエンジニアリング、一般的なだまし）が本報告書シリーズの開始以来、初めてトップの座につきました。想像力に富み、人的・物的リソースも豊かな攻撃者であればプリテキスティングの手法は無限ですが、2011 年に一番よく見られたテクニックは、小規模企業のオーナーに電話をかけ、大手カード会社のサービス員を装って詐欺を働くという手口でした。一方、「誘惑 / 買収」の場合、2010 年はソーシャルエンジニアリングが関係していたデータ漏洩 / 侵害の 74%が「誘惑 / 買収」によるものだったのに対して、2011 年は 29%に大幅に減少しました。これは、2011 年の場合、銀行の職員を誘惑して情報を窃取したという事例はいずれも小規模であり、組織的で大規模なものが少なかったことが第一の理由です。また、昨年は、このような銀行関連のデータ漏洩 / 侵害に関係している犯罪組織のうち大きな犯罪組織がいくつか摘発され、多数の犯人が逮捕されました。このことも「誘惑 / 買収」が減った原因のひとつです。

情報資産の「守護神」（ユーザー）は、策略やごまかし、脅迫といった悪質な対人テクニック（ソーシャルエンジニアリング）に極めて弱く、賢明な攻撃者はその弱点を利用する業を心得ています。

「フィッシング」は、昨年は前年と比べてそれほどの変化はなく、具体的に言えば 2010 年の 11%からいくぶん増加しました。ただし、大規模の企業・組織だけを見ると、フィッシングが一因となっているデータ漏洩 / 侵害の発生割合はかなり高いという結果が出ています。最近、擬似餌としてマルウェアがくっついている「ルアー」が大手・有名企業に向かって投げられているという報道が多いことを思い出すと、この結果はかなり興味深いといえます。このマルウェア付きの「ルアー」は、大規模企業の堅固なセキュリティ対策を迂回することを目的とした攻撃者の戦略と思われます。フィッシングの場合、企業・組織をチェックして攻撃方法や脆弱性を探す必要はありません。どの企業・組織でもフィッシングに弱い人間がいるからです。必要なのは、何も疑わずにクリックしてくれる好奇心旺盛なユーザーだけであり、このようなユーザーは決して珍しくはありません（疑い深い読者は、こちら[15] をご覧ください）。

図 24. ソーシャルエンジニアリングの経路で分類した場合のデータ漏洩 / 侵害事例の割合（ソーシャルエンジニアリングによるデータ漏洩 / 侵害のみ）

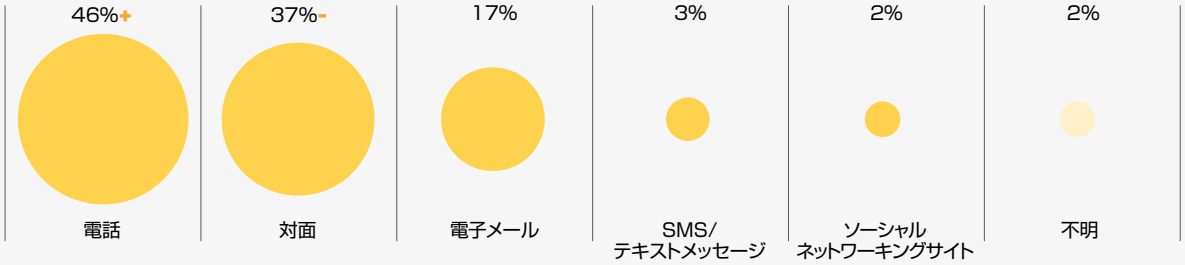


図 24 にあるように、ソーシャルエンジニアリングの上位 3 位までの経路は、順位は入れ替わっていますが前年と同じです。今回、懐かしい「電話」が返り咲き、ソーシャルエンジニアリングが関係したデータ漏洩 / 侵害事例のほぼ半分近くが電話によるものでした。電話が返り咲いたのは、上述したように、プリテキスティングによる情報の窃取がトップに躍り出たことと符合しています（プリテキスティングでは通常、電話が使われます）。第 2 位は「対面」（直に会って話をして騙すこと）で、主に小規模企業（飲食店など）のウェイターやレジ係を標的にする場合に使われます。

大規模の企業・組織の場合、ソーシャルエンジニアリングに使われる経路として「電子メール」と「電話」がトップを分け合っており、これはタイプとしてプリテキスティングとフィッシングが上位であることと関係しています。また、2011 年の場合、大手企業（または有名企業）の従業員の電子メールアドレスを盗み、その後の攻撃やフィッシングに用いるという事例が見られました。中には、電子メールアドレスの窃取後、その電子メールアドレスを使ってすぐに攻撃を開始したというケースがありました。協力機関の事例データの中には、別の攻撃者から注文が入っており、その攻撃者に電子メールアドレスを渡したという事例のほか、自分で電子メールアドレスを直接使って攻撃したというケースも見られました。

表 9. ソーシャルエンジニアリングの標的で分類した場合のデータ漏洩 / 侵害事例の割合（ソーシャルエンジニアリングによるデータ漏洩 / 侵害のみ）

一般従業員 / エンドユーザー	43%
レジ係 / 窓口係 / ウェイター	33%
コールセンターのスタッフ	8%
財務 / 会計スタッフ	6%-
システム / ネットワーク管理者	5%
経営幹部 / 上級管理職	3%
ヘルプデスクスタッフ	3%
顧客（企業の顧客）	2%
人事部門スタッフ	2%-
不明	6%

ソーシャルエンジニアリングの標的については、本年はそれほどの変化はありません（表 9）。ご想像のように、一般従業員と「金銭に触れる機会のある職」が前年に続いて主な標的です。ポリシーや手順を策定し、訓練を行い、技術的に高度な防御体制を築くという方法で従業員を罠から守るのは確かに良策ですが、それでも完璧な人間はいないものです。事例の中に、スパムフィルターにフィッシングメールが捕捉されたものの、その後、従業員が取り出し、まんまと引っかかったという例がありました（ニャンキャットが夜空に虹をかけながら駆けていれば、クリックしない人はいないでしょう）。残念なことに、この災いのクリックによってデータ漏洩 / 侵害が始まり、結果的に大量のデータが流出し、大勢の顧客が混乱に巻き込まれることになりました。このような事例は、企業・組織が「人間管理」をコツコツ続けても何かと災禍が生じるものであることの教訓です。とはいっても、何も手を打たなければ事態はさらに悪

15 http://www.youreereallynotlisteningortryingveryhardareyouwhyonearthwouldyouclickthis/haventyoureadanythingwevesaid.com

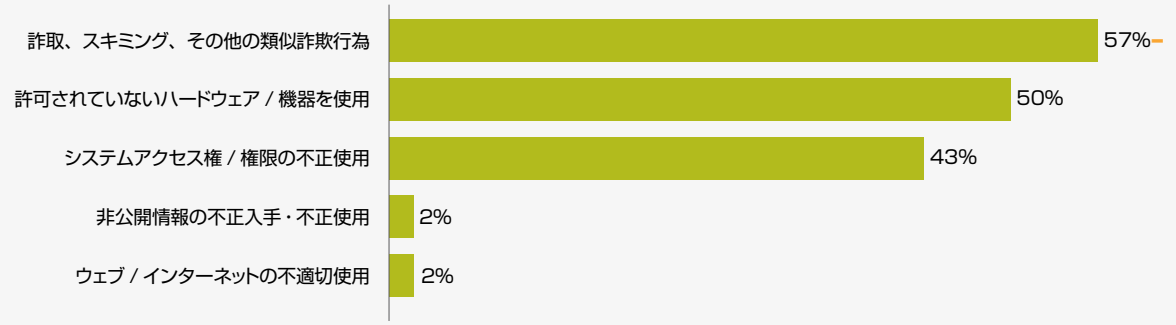
化します。これまで同じく、よく練り上げられた対策を効率よく従業員に伝え、ソーシャルエンジニアリングに対する意識を高めるという方法が効果的です。

不正使用（全データ漏洩 / 侵害の 5%、全侵害レコードの＜1%が不正使用によるもの）

不正使用とは、企業・組織のリソースや権限を、そのリソースや権限の本来の目的または用途に反して使用する行為をいいます。性質上、不正使用は悪意のあるものと悪意のないものに分類できます。また、内部因子（部内者）やパートナーなど、企業・組織から一定の信頼を得ている者が不正使用を行った場合に限って不正使用と呼びます。2009 年の場合、不正使用は脅威アクションの中で最多でしたが、2010 年には大幅に減少しました（48%から 17%）。2011 年も、不正使用が関係していたデータ漏洩 / 侵害の割合は減少しました。具体的には（総合事例データ）、不正使用が関与していた全事例の 5%にすぎず、侵害レコード数は 1%未満でした。

不正使用は、データ漏洩 / 侵害の件数は大きく減っていますが、そのタイプは前年とほとんど同じです。つまり、不正使用が関係していたデータ漏洩 / 侵害の件数では、今回も「詐取、スキミング、その他の類似詐欺行為」がトップで、全データ漏洩 / 侵害の 57%を占めました。このタイプの場合、データ漏洩 / 侵害の割合は比較的多いのですが侵害レコード数はほとんどゼロでした。第 2 位は「許可されていないハードウェア / 機器を使用」で、データ漏洩 / 侵害の割合は 50%でした。このタイプの場合、ペイメントカードを扱える従業員（レジ係やレストランの従業員）が小型の携帯型スキミング装置を使ってデータを盗んだという事例がほとんどでした（これ以外の機器のよるデータ窃取事例もありました）。第 3 位は「システムアクセス権 / 権限の不正使用」で、不正使用が関係していた全データ漏洩 / 侵害事例のうち 43%がこのタイプでした。記憶にある方もおられるかもしれませんが、この上位 3 位までのタイプは順位の違いはあるものの、ここ 2 年間同じでした（昨年は、「詐取、スキミング、その他の類似詐欺行為」が 75%、「システムアクセス権 / 権限の不正使用」が 49%、「許可されていないハードウェア / 機器を使用」が 39%）。この 3 種類のタイプは、金銭の入手を目的とした部内者が情報資産に直接または間接的に接触するという行為であり、その性質から今後も同じ傾向が続くと思われます。

図 25. 不正使用のタイプで分類した場合のデータ漏洩 / 侵害事例の割合（不正使用によるデータ漏洩 / 侵害のみ）



不正使用の経路については今まで説明しなかったのですが、本年から始めることにしました。なお、今回は 1 年間の限られた数の事例を分析するだけなので正確な結果は得られないとは思いますが、年を経るごとに改善されるはずです。不正使用の経路を検討する目的は、攻撃者がどこでどのようにしてデータ漏洩 / 侵害を行ったかを分析し、その結果をもとに防御対策を考え、また実際に講じることにあります。事例データによれば、不正使用によるデータ漏洩 / 侵害の半分が、企業の施設に物理的に侵入するという方法で実行されていました。これは、すぐに理解できることであり、またタイプとして「詐取、スキミング、その他の類似詐欺行為」が首位だったことと深く関連しています。面白いことに、内部のネットワークを使ったデータ漏洩 / 侵害とリモートアクセス（VPN など）を使ったデータ漏洩 / 侵害の割合が同じ（21%）でした。つまり、一般に外部からデータ漏洩 / 侵害を試みるほうが会社内部でデータ漏洩 / 侵害を実行するより多いと考えられていますが、この結果から、そうでもないことが分かります。このような分析結果が今後、どう変わるかが楽しみです。

私ども、また業界関係者が警戒を呼びかけているにもかかわらず、退職した従業員が恨みや腹いせでデータを盗むという事例はいまだに多いのが実情です。VERIS では、この種の従業員は外部因子として分類しています（退職し、部内者ではないからです）。ただし、退職後も権限が取り消されず有効のままとなっており、その状態でデータ漏洩 / 侵害が実行された場合、部内者による不正使用として分類しています。繰り返しになりますが、従業員が退職した場合、会社のシステムについてその従業員に付与されていたアクセス権を直ちに無効にする必要があります。

物理（全データ漏洩 / 侵害の 10%、全侵害レコードの <1%が物理によるもの）

この脅威アクションは、人間による物理的行為によって、または人間が物理的に近づくことによって実行される物理的攻撃（物理的行為）を指します。物理的攻撃は、2009 年までは脅威アクションの中でもデータ漏洩 / 侵害の件数が少なく、被害も少なかった脅威アクションでした。少なかった理由は、物理的攻撃の性質、つまりデータは「リスクに曝されている」もののデータが実際に盗まれたかどうかは一般に不明であるから（例えばユーザー機器の窃盗の場合）と思われます。また、部内者が自分の通常の業務の一部として何らかの機器を直接操作してデータ侵害を行った場合、VERIS では、その脅威アクションを物理ではなく不正使用として分類しており、このことも物理的攻撃が少なかった理由のひとつです（「不正使用」の節、また詐取に関する説明を参照）。

ところが、2010 年になると ATM やガソリンスタンドの給油機でスキミングが多発するようになり、このため物理的攻撃の割合が急増し（29%）、侵害レコード数も増えました（10%）。この種のスキミングは組織犯罪グループが行うことが多く、「派手」な事例では複数の場所で同時多発的に発生したこともあります。このような事例は、一般にベライゾンが調査を行うことはなく、当然ながら USSS などの法執行機関の管轄です。

データ漏洩 / 侵害の件数ですが、2011 年に世界で発生したペイメントカードスキミング事件は減っておらず、実際、この種の犯罪の犯人が多数逮捕されました。逮捕は「ナイトクローン」作戦によるもので、この逮捕によりスキミング犯罪グループが世界各国で暗躍していることが分かります。

2011 年はスキミングなどの物理的攻撃によるデータ侵害は減少し、全事例の 10%にすぎませんでした。ここで、「では 2010 年は異常だったのか」という疑問がわきます。答えは、「恐らくそうではない」です。本報告書の統計では、物理的攻撃が関係していたデータ漏洩 / 侵害と侵害レコードの割合は減少しましたが実際には減っておらず、以下、その理由を説明します。

まず、データ漏洩 / 侵害の件数ですが、2011 年に世界で発生したペイメントカードスキミング事件は減っておらず、実際、この種の犯罪の犯人が多数逮捕されました。逮捕は「ナイトクローン」作戦によるもので、この逮捕によりスキミング犯罪グループが世界各国で暗躍していることが分かります。「ナイトクローン」は世界各国の法執行機関による共同捜査の一環として実施され、2011 年 7 月、この作戦を通じて少なくても 5 カ国で 60 人以上が逮捕されました。[16] 2011 年の事例データの中にも、米国を含め世界各地でスキミング犯罪グループによるデータ漏洩 / 侵害が多数見られ、結局、被害に遭った企業・組織は本報告書の分析結果より多いものと思われます。

また、侵害レコード数の減少については、ペイメントカードのスキミングによる侵害レコード数を特定するのが難しいことが関係しています。つまり、スキミングの場合、標的は保管されているデータではなく（保管されているデータであれば量は分かります）、またカードが不正に使用されて初めてスキミングが判明します（不正使用されなければ不明です）。2011 年の事例データではスキミング事例は多かったのですが、上の事情により、どのくらいの数のカード情報が窃取されたかは不明で、これが侵害レコード数の減少の理由のひとつです。ただし、2011 年の全事例データの侵害レコード数（物理的攻撃以外の脅威アクションによるもの）は非常に多く、それと比較すると少ないように見えるということが物理的攻撃による侵害レコード数の減少の最大の理由です。

昨年の物理的攻撃のタイプは、タンパリング、盗み見、窃盗の 3 種類にほぼ限られ、これ以外はほとんど見られませんでした。タンパリングとは、資産の通常の状態または機能を無許可で改ざんまたは阻害する物理的行為をいいます。昨年の場合、物理的攻撃によるデータ漏洩 / 侵害のほとんど全部が何らかのタンパリングでした。タンパリングとしては例えばスキミング装置の取り付けがあり、この行為は非常によく見られました。もうひとつのタンパリングの形態は、組織犯罪グループが既存の PIN（暗証番号）入力装置やポイントオブセール（POS）システムを「新品」、つまり偽物と

16 https://www.europol.europa.eu/content/press/major-international-network-payment-card-fraudsters-dismantled-1001

取り替えるという行為です。このような偽物は、外観は瓜二つで機能も同じですが、ペイメントカードの情報を取得できるようになっています。つまり、スワイプリーダーや PIN 入力キーパッドで入力された情報を秘密裏に収集するという機能が搭載されています。タンパリングの次に多かったタイプは、盗み見でした。「盗み見」の定義は様々ありますが、本報告書では、隠しカメラなどを取り付け、顧客が入力した PIN や ATM で入力された PIN を捕捉し送信することと定義しています。盗み見ではカメラのほかにスキミング装置が使われることも多く、このタイプによるデータ漏洩 / 侵害は物理的攻撃による全データ漏洩 / 侵害の 35%を占め、これは前年（17%）の倍です。一方、窃盗（3%）とは、物理的に何らかの装置を盗むことをいいます。もちろん、報告書のデータ漏洩 / 侵害事例はいずれも「窃盗」といえますが、ここでは具体的な物理的窃盗を指しています。つまり、屋内または屋外の公の場所に設置されている装置、ご推察のように ATM やガソリンスタンドの給油機などを物理的に盗む行為を指します。

過失（全データ漏洩 / 侵害の＜1%、全侵害レコードの＜1%が過失によるもの）

VERIS を使ってセキュリティインシデントを分類する場合、脅威アクションのカテゴリーの中では「過失」の扱いが一番厄介で、これは定義が難しいことによります。過失の定義を広げすぎると、どのインシデントも何らかの過失によるものということになります。逆に絞りすぎると、レイヤー 8 テクノロジーの傾向と状況が見えなくなります（7 層 OSI 参照モデルに加え、第 8 層は人間です）。本報告書では「過失」を比較的広く解釈しており、つまり、誤ってまたは不注意で何らかの行為を行うこと（または行わないこと）を過失と定義しています。ただし、口で言うのは簡単です。データ漏洩 / 侵害を構成する一連のイベントの中で誰がどのような過失を冒したかについては人によって見解が異なり、そのため現実問題としては少し複雑です。

VERIS では過失をどのように定義しているか、ここでもう一度見てみます。会社の担当者が「当社と契約しているベンダーは、ソース IP アドレスによるサーバーアクセス制御とデフォルトのパスワードの変更を行うことになっているが、今回、どういうわけかそうなっていない」とベンダーに伝えたとします。ベンダーがこの設定を行っていない場合、VERIS では、これを寄与過失として分類します。一方、ベンダーが「えっ、パスワードの変更と IP アドレスによるアクセス制限のことは何も言われていませんよ」という返答したとします。この手の言い方をする人は多いようですが、いずれにしても、この場合はベンダーの過失（寄与過失）ではありません。

過失の定義については、本報告書シリーズでは毎年、過失の定義を徐々に狭めています。従来、判断の誤りや不適切な行為、勘違いなどが「過失」に相当するかどうかという方法で分析してきましたが、過失がデータ漏洩 / 侵害の主原因であるか、もしくは寄与原因であるかどうかに着目するという方法に次第に移行しています（つまり、過失を脆弱性というより脅威として捉えるようにしました）。また、過失は、企業･組織の防御体制とも関係があります。具体的に言えば、過失によってデータ漏洩 / 侵害が発生したと思われる場合でも、それが実際に「過失」によるものか、あるいはセキュリティ体制が弱いことによるものかが不明なこともあります。

以上、いろいろ検討してきましたが、本報告書では結局、データ流出の主原因となった過失だけを過失として取り上げました。

今回、855 件のデータ漏洩 / 侵害事例のうち、主原因の過失による事例は 4 件だけでした。いずれの事例もサーバー上の機密データが盗まれ、過失は、誤ってデータを公開してしまったこと、または設定が不適切だったことの 2 種類でした。そのほか、寄与過失によるデータ漏洩 / 侵害が 12 件ありました。昨年の報告書では、寄与過失によるデータ漏洩 / 侵害は 200 件を優に超えていました。あいにく、この減少は、企業・組織がセキュリティ対策を強化したことによるものではありません。前述のように過失の定義を狭め、デフォルトの認証情報をそのまま使用することなど、セキュリティの面で安全ではない行為を正規の「過失」から除外したことによります。

従来、判断の誤りや不適切な行為、
勘違いなどが「過失」に相当するかどうかという方法で分析してきましたが、
過失がデータ漏洩 / 侵害の主原因であるか、もしくは寄与原因であるかどうかに着目するという方法に次第に移行しています（つまり、過失を脆弱性というより脅威として捉えるようにしました）。

環境（全データ漏洩 / 侵害の 0%、全侵害レコードの 0%が環境によるもの）

脅威アクションのカテゴリーのひとつである環境には、地震や洪水などの自然事象のほか、資産が置かれている環境（インフラ）に関連する危険事象も含まれます。このような危険事象としては、停電、電気的干渉、配管の漏れ、大気条件などがあります。過去数年と同じく、2011 年も環境（自然事象と危険事象）によるデータ漏洩 / 侵害はひとつもありませんでした。ただし、機密性と可用性の両方の喪失に関連する事例がひとつありました。

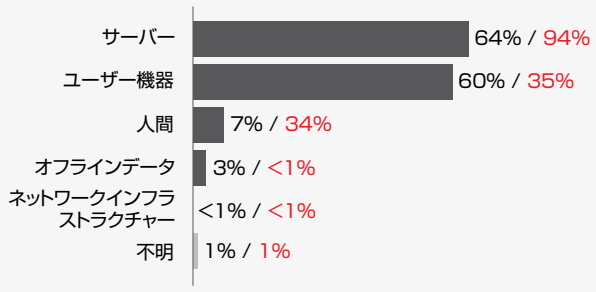
それは、2011 年 5 月にミズーリ州のジョプリンを襲った竜巻 EF5 でした。[17] この竜巻の通り道にセントジョーンズ地域医療センターがあり、大きな損害を受けました。医療記録と X 線データを含め書類や資料がまき散らされ、はるか約 100 キロ先まで飛ばされたものもありました。[18] センターでは電子カルテを遠隔地のバックアップサイトに保存する方針をとっており、復旧には、この方針が大いに功を奏したようです。

漏洩 / 侵害の対象となった資産

以下、2011 年にデータ漏洩 / 侵害を受けた情報資産について説明します。情報資産は A[4] 脅威モデルの要素のひとつであり、また脅威因子と脅威アクションの対象であることから重要です。今まで「攻撃者は誰で何をしているか」という「外部」の話をしてきましたが、ここから「防御に必要なものとして何を持っているか、防御に失敗するとどんな被害を被るか」という「内部」の話に切り替わります。

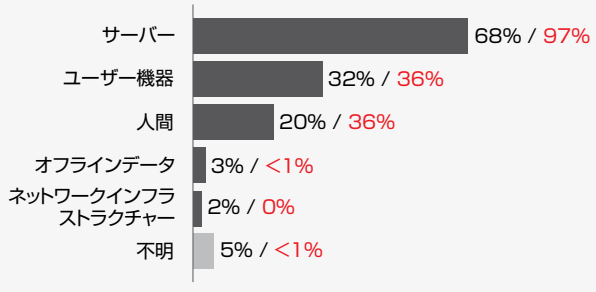
昨年の報告書では、「被害にあった資産のトップはサーバーで 2 位がユーザー機器だが、2011 年はユーザー機器が勝利を収めるかどうか」と書きました。結局、サーバーが Pwnie 賞（最も優れたセキュリティバグに贈られる賞）を受賞しました。具体的には、ユーザーの機器と 4%の僅差でサーバーが今回も勝利を収めました（2010 年は、今回よりはるかに僅差の 1%の差でトップでした）。ユーザー機器に関しては、ユーザー機器のうち被害が多かったのは、POS 端末（35%）、デスクトップ（18%）、ATM（8%）の 3 種類でした。ノートパソコンは最下位で、割合は 1%でした。結局、デスクトップパソコンとノートブックは合計しても、侵害された資産の 19%にすぎませんでした。統計と同じく、物語はつながりと展開が大事です。今回はユーザー機器のファンは残念でしたが（恐らく皆さんファンでしょう）、落胆は無用です。なかなかの健闘を見せており、それに来年という年が来なかった試しはありません。

図 26. 漏洩 / 侵害の対象となった資産のカテゴリーで分類した場合のデータ漏洩 / 侵害事例の割合と侵害レコード数の割合



まじめな話に戻ると、サーバーがトップの座に居すわっていますが、これはデータ漏洩 / 侵害の標的となる資産の種類を考えると、それほど不思議なことではありません（サーバーはデータの宝庫です）。

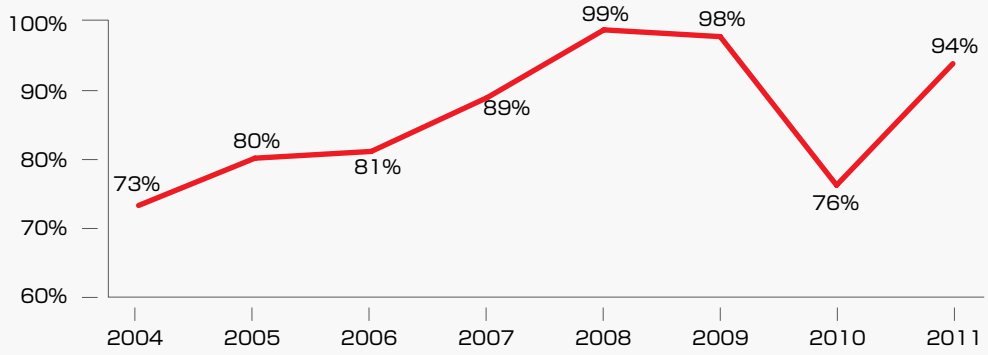
図 27. 漏洩 / 侵害の対象となった資産のカテゴリーで分類した場合のデータ漏洩 / 侵害事例の割合と侵害レコード数の割合（大規模の企業・組織の事例のみ）



資産にはデータの塊が保存されており、データは窃取されますが、この事実が失われることはありません。サーバーは本来、データを保存するための資産であり、その理由から盗まれたデータの量が他の資産よりも多いのは当然です。図 28 は、サーバーに対する攻撃によって侵害されたレコード（割合）の推移を示したグラフです。2010 年は割合が落ち込んでおり不思議と思われるかもしれませんが、これは、この年に「メガデータ漏洩 / 侵害」がなかったことが主な原因です（この辺の事情につ

17 http://en.wikipedia.org/wiki/2011_Joplin_tornado
18 http://www.news-leader.com/article/20110523/NEWS11/110523001/Missouri-officials-say-tornado-killed-least-89

図 28. サーバーに対するデータ漏洩 / 侵害で侵害されたレコード（割合）の推移



いては、2011 年度データ漏洩 / 侵害調査報告書に詳細があります）。侵害されたデータの量が非常に多いデータ漏洩 / 侵害事例は、ほぼ例外なくサーバーが標的です。2010 年にはこのようなデータ漏洩 / 侵害事例はなかったため、割合は低くなっています。「漏洩 / 侵害の対象となったデータ」の節の図 35 は毎年の侵害レコード数の推移を示したグラフですが、このグラフは上記の事実を裏付けており、また図 28 と非常によく似ています。

当然ながら、データはユーザー機器にも保存されています。また、ほとんどの企業・組織ではサーバーよりユーザー機器のほうが数が多く、各部門・部署にあり移動も容易で、使用上の制約もゆるいのが普通です。しかも、恐らく見逃せないことは、エンドユーザーがそれぞれユーザー機器を管理しているということです（これを聞くと管理者は背筋が寒くなるはずです）。理由は他にもありますが、主に上記の理由から、ユーザー機器は何らかの形でデータ漏洩 / 侵害の標的となり、結果的に大量のデータが流出することになります。サーバーと同じくユーザー機器からはデータが窃取されますが、それよりも企業・組織への「足場」としてユーザー機器が使われることが少なくありません。攻撃者は、この足場を使って次の攻撃を仕掛けます。よくある例としては、これは特に大規模の企業・組織に多いのですが、ワークステーションやノートブックにキーロガーをインストールし、内部アプリケーションサーバーのユーザー名とパスワードを盗むという事例があります。

このほか、資産としては人間、オフラインデータ、ネットワークインフラがあり、順に説明します。どうして「人間」が情報資産なのかと聞く人もおり、この質問には、頭が空っぽのため情報資産を保存できず処理もできない抜け殻ゾンビが従業員なら生産性はどうなりますか、と答えることにしています。人間はゾンビと違って、どのような情報を公開してはいけないか、また情報の公開（もしくは何らかの被害）につながるようなことを（他人や資産に対して）してはならないことを知っており、だから保護しなければなりません。図 27 を見ると分かるように、大規模の企業・組織の事例だけの場合、資産が人間だったデータ漏洩 / 侵害事例は全体の 20%、侵害レコード数は 36%を占めています。続いてオフラインデータですが、この資産が絡んだデー

表 10. 侵害された資産のタイプで分類した場合のデータ漏洩 / 侵害事例の割合と侵害レコード数の割合 *

タイプ	カテゴリー	全企業・組織の事例		大規模の企業・組織の事例のみ	
POS サーバー（店舗情報制御装置）	サーバー	50%	1%	2%	<1%
POS 端末	ユーザー機器	35%	<1%	2%	<1%
デスクトップ / ワークステーション	ユーザー機器	18%	34%	12%	36%
ATM（現金自動預入支払機）	ユーザー機器	8%	<1%	13%	<1%
ウェブ / アプリケーションサーバー	サーバー	6%	80%	33%	82%
データベースサーバー	サーバー	6%	96%	33%	98%
一般従業員 / エンドユーザー	人間	3%	1%	5%	<1%
メールサーバー	サーバー	3%	2%	10%	2%
ペイメントカード（クレジットカード、デビットカードなど）	オフラインデータ	3%	<1%	0%	<1%
レジ係 / 窓口係 / ウェイター	人間	2%	<1%	2%	<1%
カード対応の給油機	ユーザー機器	2%	<1%	0%	<1%
ファイルサーバー	サーバー	1%	<1%	5%	<1%
ノートブック / ネットブック	ユーザー機器	1%	<1%	5%	<1%
リモートアクセスサーバー	サーバー	1%	<1%	7%	<1%
コールセンターのスタッフ	人間	1%	<1%	7%	<1%

* データ漏洩 / 侵害事例が全データ漏洩 / 侵害事例の 1%未満の資産は、割愛してあります。

タ漏洩 / 侵害の割合は 3 年連続して減少しています（25%から 12%へ、さらに 3%に減少）。オフラインデータの減少の理由は、同じ時期に部内者の過失によるデータ漏洩 / 侵害が減少していることと関係があると思われます。つまり、この種のデータ漏洩 / 侵害の場合、一般に文書やメディアなど職場に無造作に置かれている物（オフラインデータ）が標的です。オフラインデータの減少の原因を「グリーンイニシアティブ」（環境保護運動）とするのは、恐らく行き過ぎです。しかしながら、おかげで印刷物が減ると文書泥棒も減るということが分かり（もちろん、データベースが紙文書より安全かどうかという問題がありますが、それはさておき）、結果的に地球は今より明るく幸せな惑星になる可能性があります。最後に、「ネットワーク（インフラストラクチャー）」から情報が窃取されたデータ漏洩 / 侵害がほとんどなかった理由について説明します。まず、大半のデータ漏洩 / 侵害で、ネットワークへの侵入が発生したことは間違いありません。ただし、ここでいうネットワークインフラストラクチャーとは、ルーターやスイッチ、ケーブルなどの機器を指します。データ漏洩 / 侵害の際、トラフィックはこのよう機器を通過するかもしれませんが、機器自体が侵害されることはありません。これが、ネットワーク絡みのデータ漏洩 / 侵害がほとんど見られなかった理由です。

表 10 は、今回の 850 件以上のデータ漏洩 / 侵害事例をもとに、データ漏洩 / 侵害を資産のタイプでさらに細かく分類した結果です。この表では、特に大規模の企業・組織の事例だけの結果が参考になります。例えば POS サーバーと POS 端末は、全企業・組織の事例の場合は相当な割合を占めていますが、大規模の企業・組織の事例のみの場合、割合は僅少です。ウェブアプリケーションとデータベースは大規模の企業・組織でデータ漏洩 / 侵害が多発しており、これの説明は不要です。

表 10 にはモバイル機器デバイス（タブレット端末やスマートフォンなど）がなく、これを不思議に思う読者もおられるかもしれません。正直なところ、モバイル機器のデータ漏洩 / 侵害がかなりの割合で出現すると思っていたのですが、今のところそうではありません。念のため、モバイル機器のフォレンジック調査を行いましたが（マルウェア、不正使用、タンパリングなどの証拠の調査）、モバイル機器から情報が盗まれたことを確認できたデータ漏洩 / 侵害はほとんどありませんでした。ただし、モバイルユーザーやモバイルアプリケーション、モバイル決済サービスが爆発的な普及を見せていることを考慮すると、今後、台頭してくる可能性は大と思われます。

「クラウド」は今のところ決まった定義がないため、クラウドからデータが窃取されたデータ漏洩 / 侵害がどの程度あるのかという質問に答えるのは簡単ではありません。

所有者、ホスティング、管理

ここで、IT・セキュリティ関係者にとって最近、非常に気になる 2 つの話題、つまりクラウドコンピューティングと BYOD (Bring-Your-Own-Device) について少し説明します。後者の BYOD は読んで字のごとしで、従業員が個人で所有する機器を業務に活用することです。この形態は、魅力的でもあり恐怖でもあります。従業員はお金のほか、機器をいくつも使わなければならない手間を節約できるため幸福度が増しますが、機器や使用方法が企業のセキュリティポリシーに準拠していないときには、企業のデータやシステムがリスクに曝されることになります（いずれにしても従業員にとってはありがたいことです）。2011 年は BYOD 周りが賑やかになってきたことから、VERIS の分類項目としてデータ漏洩 / 侵害を受けた資産の所有者を追加しました。その分類結果は、図 31 に示してあります。

「クラウド」は今のところ決まった定義がないため、クラウドからデータが窃取されたデータ漏洩 / 侵害がどの程度あるのかという質問に答えるのは簡単ではありません。例えば、被害を受けた企業・組織が管理していない外部ホスティング環境（クラウドを含む）で、データ漏洩 / 侵害がよく発生したかと質問されればどうでしょう。答えは、イエスです。では、一般ユーザー環境のハイパーバイザー（ソフトウェアによる仮想化マシン）に対する攻撃が成功しているかという質問はどうでしょう。それほどはない、というのが答えです。以前にも述べましたが、ここで繰り返します。クラウドに問題があるとすれば、それはクラウドの技術というより資産やデータの管理を十分に行っていない（したがって資産やデータに関するリスクの管理も十分ではない）という事実に関する問題なのです。

答えるのは難しいと前段で書きましたが、これは質問や回答を避けるための口実ではありません。クラウドに関連するデータ漏洩 / 侵害を分析する場合、通常、クラウドに置かれている資産の特徴を特定し、その特徴がデータ漏洩 / 侵害とどのように関係しているかを考察するという方法を使っています。クラウドに置かれている資産の特徴とは、単純化しすぎという方もおられるでしょうが、所有者、ホスティング、管理の 3 つです。この観点から言えば、クラウド（雲）の中にある資産は、本来の所有者以外の者が所有し、外部の施設でホスティングされ、第三者が管理・運営している（もしくはいずれか 2 つの組み合わせ）という形式が一般的です。

図 29. 資産の場所を基準に分類した場合のデータ漏洩 / 侵害の割合 *

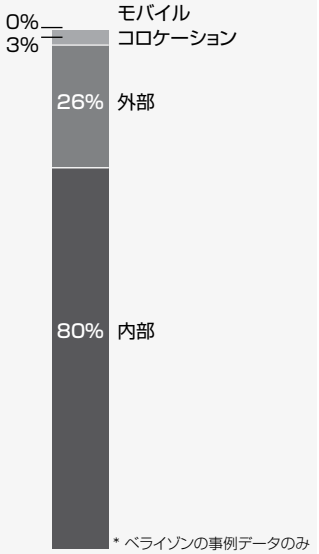


図 30. 資産の管理方式を基準に分類した場合のデータ漏洩 / 侵害の割合 *

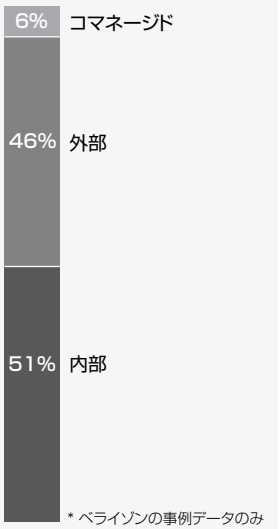


図 31. 資産の所有者を基準に分類した場合のデータ漏洩 / 侵害の割合 *

相関と因果関係は必ずしも同じではないものの、両者のパターン間に関係があることもあります。このことを頭に置いて、図 29、30、31 を見てみます。それぞれ、資産の場所（ホスティング）、資産の管理方式、資産の所有者を基準にデータ漏洩 / 侵害事例を分類したグラフです（ベライゾンの事例データのみ）。手元のデータだけでは、各グラフのパターンの間に相互関係があるかどうかは明瞭ではありませんが、注目すべき点はいくつかあります。まず、場所が「外部」の資産のデータ漏洩 / 侵害、また管理方式が「外部」の資産のデータ漏洩 / 侵害がどちらも、過去 3 年間にわたって増加している点があげられます。これは重要なポイントです。特に、サードパーティの POS ベンダーの中にはアクセスコントロールリストの設定が不十分だったり、デフォルトの認証情報を変更せずにそのまま使用しているベンダーが多いことを勘案すると重要です。また、大規模の企業・組織の場合、場所が「内部」の資産、また管理方式が「内部」の資産についてデータ漏洩 / 侵害が多いことも注目すべき点です（両者とも約 80%を占めています）。従業員が所有する機器については、この種の機器から情報が窃取された事例は今回ははほとんどありませんが、BYOD が普及すれば増加するはずです。

漏洩 / 侵害の対象となったデータ

ここ数年、侵害レコード数を追跡調査することに意味があるかどうかについて読者から意見や提案をいろいろと頂戴しています。詰まるところ、問題はレコードのタイプ（種類）のようです。言い換えると、本報告書シリーズでは、名前と電子メールしか入っていないデータも 1 レコード、ソフトウェア開発会社の主要製品のソースコードも 1 レコードとして数えており、これは問題ではないかということです。実際、これは憂慮すべきことであって、本報告書の侵害レコード数を利用したり自分の仕事に応用するときには注意するように読者にお願いしています。とはいえ、侵害レコード数を追跡することはやはり価値があります。第一の理由は、本報告書の侵害レコード数を必要としている企業があり（ペイメントカード会社など）、また、どのようなレコードがどのくらい流出したかを知ることは企業にとって有益だからです。2 番目の理由は、データ漏洩 / 侵害で流出したレコードの数とデータ漏洩 / 侵害の影響（被害）との間には関連性があり（この関連性は、特定のタイプのデータでは顕著です）、流出したレコードの数を計算しなければ影響は不明で、影響に関する質問にも答えられないためです。最後の理由としては、侵害レコード数の計算は「濡れた指を宙にかざして風の動きを探る」有効な方法であるだけでなく、流出したデータのタイプと量を知ることによって攻撃者の動機と行動をよく理解できることがあげられます。

侵害されたデータに関して端的に言えば、一年間の休暇を取った「メガデータ漏洩 / 侵害」が舞い戻ってきて、それも今回は脅威因子と動機が変ったということなります。以下、恐ろしいほど大量の侵害レコード数（1 億 7400 万）はさておき、データ漏洩 / 侵害の件数と侵害レコード数をデータのタイプごとに比較するという作業から始めます。その後、侵害レコードの分布、侵害レコードの定量評価、過去のデータとの比較の順で説明を進めます。

侵害されたデータのタイプ

データ漏洩 / 侵害の件数に関しては、今回はペイメントカード情報が流出した事例がトップで（48%）、ただし前年と違って一人勝ちではありませんでした。次いで、小差で認証情報が 2 位に入りました（42%）。今回もペイメントカード情報が「最も盗まれた情報」賞を受賞しました。3 位は前年と同じく「個人情報」（名前、電子メールアドレス、国民番号など）でしたが、今回は割合がグンと減っています。なお、個人情報が流出したデータ漏洩 / 侵害事例の割合はたったの 4%でしたが、侵害レコード数は全侵害レコード数の 95%を占めています。個人情報の侵害レコード数の割合は、2009 年は 4%、2010 年は 1%でしたから、この 95%という結果は驚異的な変化です。

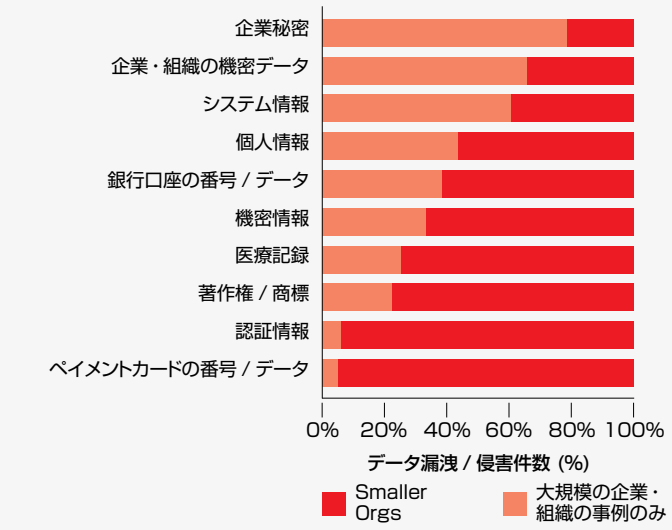
表 11. 侵害されたデータのタイプで分類した場合のデータ漏洩 / 侵害事例の割合と侵害レコード数の割合

		全企業・組織の事例		大規模の企業・組織の事例のみ	
タイプ	図 32 の名称	漏洩 / 侵害	侵害レコード数	漏洩 / 侵害	侵害レコード数
ペイメントカードの番号 / データ	カードデータ	48%	3%	33%	1%
認証情報（ユーザー名、パスワードなど）	認証情報	42%	1%	35%	1%
個人情報（名前、社会保障番号、住所など）	個人情報	4%	95%	27%	98%
企業・組織の機密データ（報告書、計画書など）	企業・組織の機密データ	2%	<1%	22%	<1%
銀行口座の番号 / データ	銀行データ	2%	1%	10%	1%
システム情報（設定、サービス、スイッチなど）	システム情報	2%	<1%	15%	<1%
著作権 / 商標	著作権	1%	1%	3%	<1%
企業秘密	企業秘密	1%	<1%	12%	<1%
機密情報	機密情報	<1%	<1%	2%	<1%
医療記録	医療記録	<1%	<1%	2%	<1%
不明（具体的なタイプ不明）	不明	44%	<1%	2%	<1%

2011 年は、意外なことに組織犯罪グループだけでなく活動家グループによっても個人情報が大量に盗まれましたが、両者の動機は異なります。活動家（ハクティビスト）グループの場合、個人情報を盗むのは「声明」のため、つまり被害者を困らせること、言い換えると一種の意趣返しが目的です。したがって、データの金銭的価値よりもデータ漏洩 / 侵害の規模、データの機密度、盗んだデータの公開の方法が重要です。

図 32. 侵害されたデータのタイプで分類した場合のデータ漏洩 / 侵害数と侵害レコード数

図 33. 侵害されたデータのタイプと企業・組織の規模



一方、組織犯罪グループの場合、データの価値が関心の的です。組織犯罪グループにとって大事なのは、個人情報を大量に盗むこと、また盗んだ後のデータの処理です。厳密に言えば、情報自体の価値より、その情報が詐欺などの犯罪に利用できるかどうかが重要です。

実際、データ漏洩 / 侵害事例データを通じて、犯人が個人情報を使ってフィッシングやアイデンティティ窃盗など、各種各様の詐欺行為に及ぶ場面を見てきました。犯人によって手口は多少違うかもしれませんが、最終的には金が目的です。

上記のほか、表 11 で注目すべきなのは「不明」の割合です。この割合は、データが建物から出て行ったのは明らかだが、何が出て行ったか分からない（または部分的にしか分からない）というデータ漏洩 / 侵害事例が全データ漏洩 / 侵害のほぼ半分を占めることを示しています。この結果については、本節で後ほど詳しく説明します。

（中略）そのせいで犯罪コミュニティは、目立った動きをするのを控えています。
大きな仕事をやり遂げれば名声と財産が手に入るかもしれませんが、
無用な視線を浴びることにもなるからです。

-2011 年度データ漏洩 / 侵害報告書

図 33 は、企業・組織の規模（全企業・組織と大規模の企業・組織）によって、どのタイプのデータの侵害事例が多いかを示したグラフです。ここでは両極端のタイプ、つまり上端と下端のタイプに注目して解説します。まず下端を見ると、「ペイメントカードの番号 / データ」のデータ漏洩 / 侵害事例は、そのほとんどが全企業・組織で発生し、大規模の企業・組織での発生件数は非常に少なかったことが分かります。この傾向は昨年の報告書でも見られました。ペイメントカードを標的にした攻撃は、大規模の企業・組織から小規模の企業・組織に移行する傾向があり、これは主に小規模の企業・組織のほうがリスクが低いことによります。一方、上端を見ると、大規模の企業・組織の場合、企業秘密や企業・組織の機密データが盗まれるケースが非常に多かったことが分かります。

侵害レコードの分布

表 12 は、インシデント（データ漏洩 / 侵害）当たりの侵害レコード数を基準にデータ漏洩 / 侵害事例を 5 つのカテゴリーに分類したものです。昨年と同様、侵害レコード数が少ない事例が大半を占めていますが、注意しなければならないのは大量流出の可能性も見え隠れしていることです。今回、侵害レコード数が数百ないし数千のデータ漏洩 / 侵害が主で、数百万のレコードが流出したという新聞の見出しに踊るような事例は希でしたが、それでも多少はありました。

具体的には、流出したレコードが 10,000 未満のデータ漏洩 / 侵害事例が 4 分の 3 以上を占めていますが、その一方、流出レコードが百万を超えたという事例が 855 件中 7 件ありました。[19] メガデータ漏洩 / 侵害が復活の兆しを見せており、その標的は、お気づきのように大規模

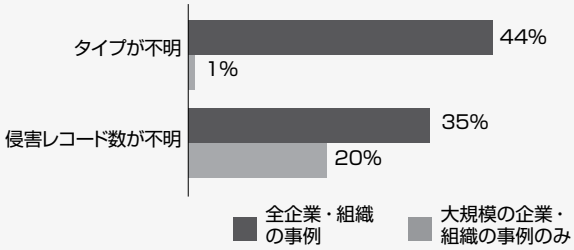
表 12. 侵害レコード数の分布とデータ漏洩 / 侵害事例の割合

	全企業・組織の事例	大規模の企業・組織の事例のみ
1,000 未満	39%	62%
1,000 ～ 1 万	44%	15%
1 万～ 10 万	11%	5%
10 万～ 100 万	3%	5%
100 万超	2%	13%

19 RISK チームの OB であるアレックス・ハットンは、大規模データ漏洩 / 侵害を好んで「ブラックスワン（黒鳥）」と呼びますが、その言い方はタレブの理論の応用としては間違っているとよく助言しています（これは冗談ですが、何となく皮肉を言いたい気持ちです。いつか詳しく聞いてみます）。

の企業・組織です。大規模の企業・組織にはデータが大量に存在するため、メガデータ漏洩 / 侵害の標的になるのは不思議ではありません。本報告書の事例データによれば、侵害レコード数が 1,000 万超のデータ漏洩 / 侵害はすべて、従業員が 1,000 人を超す企業・組織で発生しました。また、侵害レコード数が 100 万超のデータ漏洩 / 侵害の 3 分の 2 以上が、この種の企業・組織で発生しました。

図 34. タイプまたは侵害レコード数が不明のデータ漏洩 / 侵害の割合



侵害レコードの定量評価

ここでは、侵害されたレコード全体（全侵害レコード）の検討、言い換えるとセキュリティインシデントの結果全体の定量評価を行います。この定量評価では、「免責事項」がいくつかあります。ひとつ目は、ここでは全侵害レコードについて分析しますが、分析結果は、セキュリティインシデントの被害を測定する上でのひとつの指標にすぎないということです。つまり、データのタイプと価値は企業・組織によって異なるため、ここでの分析結果はあくまで概要です。データのタイプについては前述しましたが、ここで再度触れます。

もうひとつの免責事項は、定量評価が非常に難しい場合があるという事実です。

窃取されたレコードの数の特定という作業は難しく、理由としては、攻撃手法が複雑、データのタイプの性質から特定が困難、被害企業・組織にログがなかったなどがあります。実際、ベライゾン（それに各協力機関）の事例データの中には、侵害が発生したことは明らかでデータが盗まれた証拠も見つかった（例えば、暗号化ペイロードファイルがあった）のに、レコードのタイプと数の特定は困難もしくは不可能という事例が多数ありました。また、ペイメントカード情報が窃取された場合、その後、不正に使用されたカードの数は判明するものの、盗まれたカードの総数は不明というケースもよく見られました。さらに、データのタイプによっては（企業秘密など）、その性質上、窃取されたデータの数の特定が難しい場合もあります。窃取されたデータによっては後日の不正が発覚することが少なく、したがって被害企業・組織に通知されることも希で、結局はデータ漏洩 / 侵害の発見が困難というケースもあります。そのほか、法執行機関は攻撃者の追跡と逮捕に集中するのが普通であり、窃取されたレコードの正確な数を割り出すという作業にはあまり関心を示しません。話は変わりますが、レコードのタイプが不明だったデータ漏洩 / 侵害事例は、ほぼ全部が小中規模の企業・組織（従業員数が 1,000 人未満）で発生しており、そうでない事例はたった 1 件でした。

以上、侵害レコード数の特定が簡単でないことを縷々述べましたが、続いて、昨年（2011 年）は過去 7 年と比較して侵害レコード数がどう変わったかを見てみます。

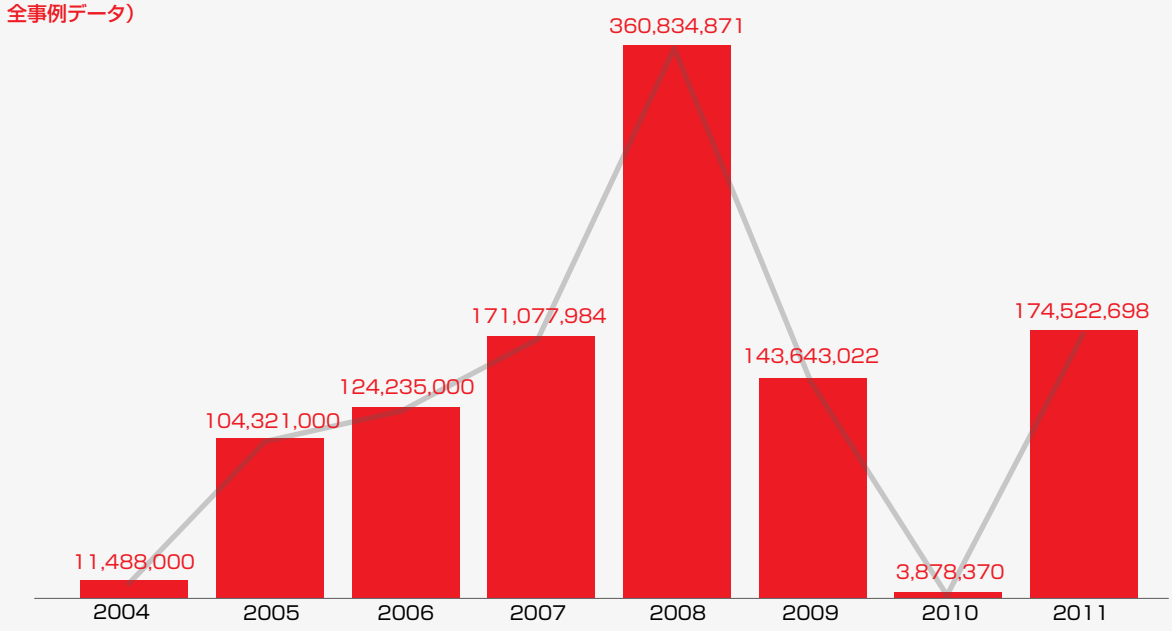
図 35 で分かるように、攻撃者はその悪辣非道ぶりを復活させたようです（こちらでは、攻撃者を怒らせるようなことは何もしていません）。2011 年は、侵害レコード数は急激な増加を見せ、本シリーズ開始以来 2 位を記録しました。ただし、ここでは 2010 年の落ち込みについて再度、見てみることにします。この落ち込みの理由はすでにいくつか指摘しており、いずれも今でも妥当と考えています。第一の理由は、金銭を目的とする犯罪者グループが、派手で単発のデータ窃盗から自動化された攻撃に移行しているというものでした。事実、2010 年は小中規模の企業・組織のデータ漏洩 / 侵害が増え、この傾向は昨年も続いています。このことは、攻撃者ができるだけ抵抗を回避しながら、多数の標的から少しずつデータを着実に盗むという方法を選択し使

表 13. 侵害レコード数の記述統計（2004 年～ 2011 年）

	2011 年	全期間（2004 年～ 2011 年）
合計レコード数	174,522,698	1,081,495,508
平均	548,814	801,108
中央値	1,270	1,270
標準偏差	5,632,140	8,221,338
パーセンタイル（百分位数）		
10	12	10
25	100	45
50	1,270	1,270
75	3,500	10,559
90	35,219	153,978
99	2,830,000	10,000,001

用していることを示しています。なお、昨年の大規模データ漏洩 / 侵害事例（侵害レコード数が 100 万超）は 1 件を除いてすべて活動家グループによるもので、これは、例年は主に金銭目当ての攻撃者が実行者であることと大きく異なります。この傾向は、組織犯罪グループが密かに防御の甘い小規模の標的を攻撃しているのに対して、活動家グループは「衝撃と畏怖」作戦に打って出ているという見方を裏付けています。

図 35. 毎年の侵害レコード数の推移（本報告書シリーズの全事例データ）



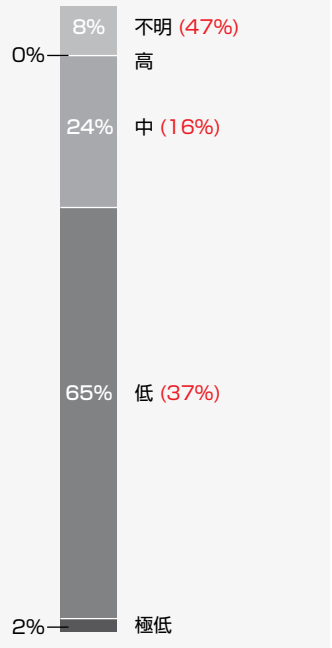
統計に明るい読者のため（もちろん全員がそうでしょう）、表 13 に戻ります。全期間の値と比較すると、本年の平均侵害レコード数は 550,000 弱に低下し、中央値は 1,270 にわずかに上昇、また標準偏差は約 560 万でした。最初の報告書から本報告書までの合計侵害レコード数は、10 億を超えます。切れのいい数字ですからシャンパンを開けて祝いたいところですが、そういうわけにはいきません。代わりに、11 億にならないことを祈って乾杯するならいいでしょう。

攻撃の難しさ

どんなデータ漏洩 / 侵害が一番いいかというと、侵害に遭わないのがいいに決まっています。それでも侵害に遭遇した場合、最初の段階で食い止めることが被害を最小限に抑える方法であることは明らかです。とはいっても、セキュリティ対策は多種多様で、ごく簡単なものから非常に複雑で高コストのものまで様々です。どのようなセキュリティ対策を施せばいいかを決定する場合、攻撃者の「圧力」を理解する必要があり、その圧力はデータ漏洩 / 侵害の進行とともに増加するのが普通です。

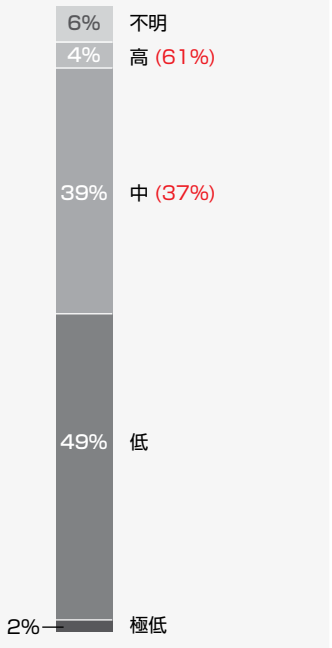
本年は、圧力がデータ漏洩 / 侵害の進行とともに増加するという考えに注目し、攻撃の難しさ（攻撃者の攻撃の技術レベル）の評価方法を一部変更することにしました。具体的には、データ漏洩 / 侵害を最初の侵害と侵害後のアクションの 2 種類に分けて評価するという方法を採用することにしました。最初の侵害とは攻撃者が資産に不正にアクセスすることをいい、侵害後のアクションとは最初の侵害の後に実行されたあらゆる行為や操作、処理を指し、実際のデータの侵害行為のほかデータの取り出し（窃取）も含まれます。侵害後のアクションは複雑で評価も難しいのですが、その分析と評価は以前からの念願でした。分析結果を紹介する前に、評価に使った基準について説明します。

図 36. 最初の侵害の難しさで分類した場合のデータ漏洩 / 侵害事例の割合と侵害レコード数の割合 *



* ベライゾンの事例データのみ

図 37. 侵害後のアクションの難しさで分類した場合のデータ漏洩 / 侵害事例の割合と侵害レコード数の割合 *



* ベライゾンの事例データのみ

攻撃の難しさを評価する場合、ある程度は主観が入ります。それでも、企業の資産の侵害に攻撃者がどのくらいの労力とコストを必要としたかを示す指標として有効です。現在使用している攻撃の難度は次の 4 種類です。この基準を使って事例データを分類しました。[20]

- **極低レベル**：攻撃者は、技術やリソースは特に必要なし。平均的なコンピュータユーザーであれば可能な攻撃。
- **低レベル**：基本的な攻撃。攻撃者は、攻撃のカスタマイズは不要だが多少のリソースは必要。自動化ツールとスクリプトによる攻撃。
- **中レベル**：一定の技術を用いた攻撃。攻撃者は、ある程度のカスタマイズとかなりのリソース、もしくはいずれかが必要。
- **高レベル**：高度な技術を用いた攻撃。攻撃者は、相当程度のカスタマイズと非常に豊富なリソース、もしくはいずれかが必要。

上記の各レベルの説明を頭に置いて、図 36 と図 37 を見てください。上でも触れましたが、難しさのレベルは、最初の侵害より侵害後のアクションのほうが高いことが分かります。例えば、最初の侵害（アクセス）の場合、レベルが「中」の事例は 4 分の 1 弱（24%）ですが、侵害後のアクションではレベルが「中」の事例は 39%です。なお、レベルが「不明」の事例も一定程度はありました。ログがあまり残っていなかったり攻撃に使われた手法が明らかでなく、そのためレベルが不明だった事例はここに分類しました。

図 21（ハッキングのタイプで分類した場合の事例の割合）を併せて見てみると、最初の侵害のレベルが低いことがよく分かります。つまり、図 21 のハッキングのタイプの多く（いずれも主に最初の侵害で使用されます）、とりわけアクセスに関連するものは、技術的にそれほど高度ではありません。一般的なデータ漏洩 / 侵害の場合、最初の侵入より、そのあとに起こる事のほうが「面白い」のが普通です。例えば、攻撃者は最初の侵入後、各種のマルウェア（ある程度カスタマイズされています）をインストールしたり、上位の権限を入手したりします。また、リモートエントリ / コントロールメカニズムを仕掛ける、企業・組織のネットワークに入って「品物」のありかを探すといった行為も見られます。結局、やりたい放題です。図 37 で分かるように、レベルが「中」と「高」のデータ漏洩 / 侵害事例で盗まれたレコードが全侵害レコードの実に 99%を占めており、これは、いくら攻撃者でも侵入後にレコードを窃取するには相応の苦労が必要であることを示しています。以前から、最初の不正アクセスを阻止することが何より重要であると語ってきましたが、上の分析結果は、このことを裏付けています。

以上は全事例の分析結果ですが、大規模の企業・組織の場合はどうでしょうか。攻撃者にとって、大規模の企業・組織に侵入するのは小規模の企業・組織よりはるかに難しいと考えがちですが、果たしてそ

大規模の企業・組織の場合はどうでしょうか。攻撃者にとって、大規模の企業・組織に侵入するのは小規模の企業・組織よりはるかに難しいと考えがちですが、果たしてそうでしょうか。残念ながら、事例データによるとそうではありません。大規模の企業・組織の場合、小中規模の企業・組織に比べてよほど精を出さなければ侵害に成功しない、ということはないようです。

20 攻撃の難しさは VERIS フレームワークの分類項目ではなく、そのため各協力機関では、この項目を VERIS には入力していません。したがって、本節の分析結果はすべてベライゾンの 2011 年のデータによるものです。

うでしょうか。残念ながら、事例データによるとそうではありません。大規模の企業・組織の場合、小中規模の企業・組織に比べてよほど精を出さなければ侵害に成功しない、ということはないようです。

一方、侵害後のアクションは最初の侵害よりも攻撃のレベルが上で、図で分かるようにレベルが「中」と「高」の事例が合計で約半分を占めます。侵害後のアクションのレベルが高いのは多分、標的となる資産の種類が多く企業・組織の防御体制も堅固で、さらに攻撃に対する企業・組織の検出・対応能力も高いため（そうでない場合もあります）、攻撃者側も腕を磨かなければならないことの結果です。

本節の冒頭で述べたように、攻撃の難度の評価にはある程度は主観が混じります。それでも難度の評価は、脅威因子（攻撃者）の攻撃能力を測る尺度として、また攻撃に対してどのような対策を講じなければならないかを決定するための尺度として有効です。攻撃を阻止したい場合、効果と効率の両面で最善の方法は、とにかく攻撃者を「家」の中に入れないことです。オポチュニスティック型の攻撃の場合（次の節で説明しますが大半の攻撃がこのタイプ）、標的の情報の価値がほぼ同じであれば、攻撃者は防御の甘い標的を狙うのがほとんどで、防御が堅固な標的をわざわざリソースを費やして攻撃することはありません。一方、攻撃者が何らかの情報に目を付け、その情報に執着しているときには、基本的な防御体制では（その体制が必要最低限の能力を備えていても）一般に不十分です。このような場合、周到に考慮され、準備万端の防御体制を構築する必要があり、そのためには攻撃者の動機（目的）や技術、方法を理解することが重要です。

攻撃の標的選定

情報セキュリティ業界では、攻撃者の攻撃をオポチュニスティック（無作為）型と単一標的型の 2 種類に分類するのが一般的です。この 2 種類の攻撃は、違いは多数ありますが簡潔にまとめれば次のように定義できます。

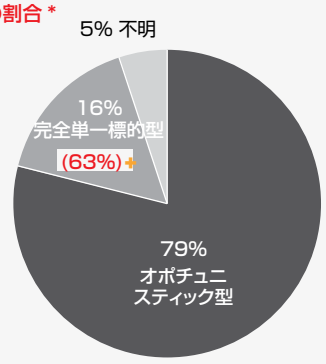
- **オポチュニスティック型**：標的を限定しないで攻撃。多数の標的を物色し、利用可能な弱点があればその弱点を突いて攻撃します。
- **完全単一標的型**：標的をひとつに絞って攻撃。標的を選定した後、弱点を調べ、その弱点を利用して攻撃します。

言えることは、名前が売れたり、価値のある資産を所有していることが知られたりすると、攻撃の標的となる可能性が高くなるということです。

2011 年のオポチュニスティック型と完全単一標的型の比率は（図 38）、前年とほぼ同じでした。ただし今回、オポチュニスティック型に関して興味深い点を 2 つ発見しました。ひとつは、オポチュニスティック型の攻撃の 85%が従業員が 1,000 人未満の企業・組織を標的していること、もうひとつは、オポチュニスティック型の攻撃の 4 分の 3 近くが小売業とホテル・飲食業で発生していることです。この 2 点はそれぞれ本報告書の各所で指摘している 2 つの点、つまり最近、自動化された攻撃によって不特定多数の小中規模企業が攻撃を受けていること、また POS システムが頻繁に攻撃されていることを裏付けていると思われます。

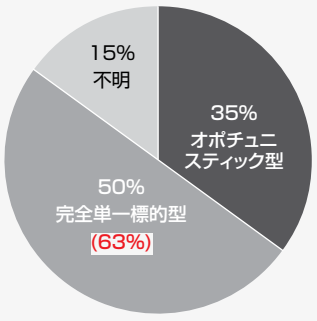
一方、完全単一標的型は、オポチュニスティック型と大きく異なります。完全単一標的型の場合、金融・保険業界と情報業界が標的になることが多く、また大規模の企業・組織を狙うことが少なくありません。事実、完全単一標的型の攻撃によるデータ漏洩 / 侵害は、10 件のうちほぼ 7 件が大規模の企業・組織で発生しています。また、大規模の企業・組織に対する完全単一標的型の攻撃は（図 39）、全企業・組織の事例（図 38）と比較すると 2 倍を大きく超えています。

図 38. 攻撃の種類で分類した場合のデータ漏洩 / 侵害事例の割合と侵害レコード数の割合 *



* ベライゾンの事例データのみ

図 39. 攻撃の種類で分類した場合のデータ漏洩 / 侵害事例の割合と侵害レコード数の割合（大規模の企業・組織の事例のみ）*



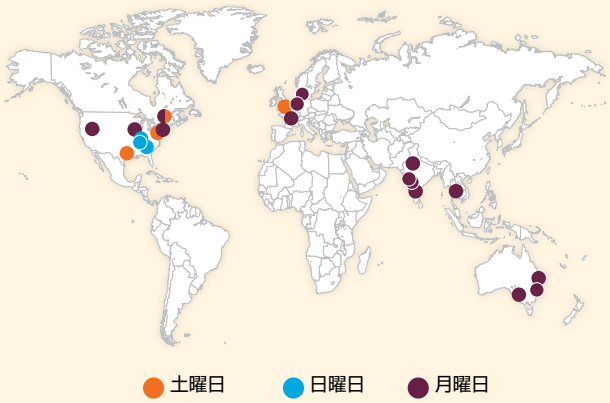
* ベライゾンの事例データのみ

あいにく、オポチュニスティック型と完全単一標的型についてはこれ以上説明することはなく、今後の傾向も不明です（。オポチュニスティック型と完全単一標的型の割合が小中規模と大規模の企業・組織でどうして違うかについては、はっきりした理由は分からず、この相違が今後も続くかどうかも分かりません。ただ言えることは、名前が売れたり、価値のある資産を所有していることが知られたりすると、攻撃の標的となる可能性が高くなるということです。とりわけ、前述したように活動家グループが台頭しており、その熱い視線を浴びる恐れがあります。小中規模の企業・組織の場合、インターネットに接続されている資産に重大な弱点があることが多く、また弱点の解消に必要な知識とリソースが不足しているのが普通であり、その結果、オポチュニスティック型の攻撃を受けやすいという傾向があります。一方、大規模の企業・組織は一般にセキュリティ問題の扱いは慣れているものの、資産が多く、方々に置かれており管理も複雑であることから、小中規模の企業・組織ほどではないにしてもオポチュニスティック型の攻撃を受けることになります。結局、小中規模の企業・組織も大規模の企業・組織もオポチュニスティック型に対する「免疫」はなく、そのため攻撃者志望者の絶好の攻撃として対象としてデータ漏洩・侵害の被害を被ります。

全体的に見ると、企業・組織では大規模企業、業界では金融業界と情報業界に対する攻撃が増えています。したがって、この条件に該当する企業・組織は、オポチュニスティック型または完全単一標的型、もしくは両方の攻撃に対する防御体制を強化するのが妥当と思われます。いずれにしても、基本原則は変わりません。つまり、企業・組織によっては何をしても標的になることもありますが、ほとんどの企業・組織は、何をするか（または何をしないか）によって標的になるかどうかが決まります。

週 3 日労働

本報告書のデータを VERIS で記録する際、協力機関のひとつからリストが渡されました。東ヨーロッパの小さい組織犯罪グループが関与したインシデントの一覧で、日付と場所も記載されていました。リストは、その組織犯罪グループの約 6 ヶ月間の活動記録でしたので、内容を分析することにしました。分析したのは、「産業化」、「速攻」、「大規模」、「オポチュニスティック型」など、本報告書で使用している用語の意味を把握する上で有益と考えたからです。

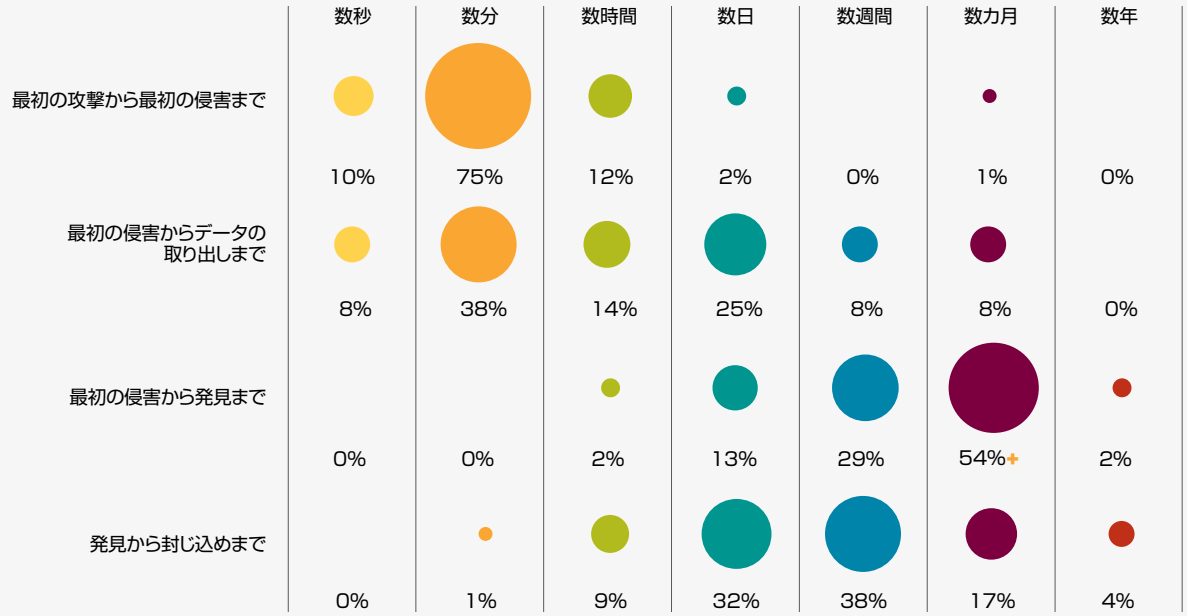


記録を分析したところ、組織犯罪グループの「労働日」は特に決まっておらず、また、平均すると週 3 日労働であることが分かりました。労働日としては、土曜日、日曜日、月曜日が一般的でした。累計してみると、土曜日、日曜日、月曜日に全部で 9 カ国、22 の企業・組織でデータ漏洩 / 侵害を実行していました。特に月曜日は「生産性」が高く、月曜日に行ったデータ漏洩 / 侵害は 15 件に及んでいます（紫のマーク）。「うまく手に入れば、それはお手柄」というジャズソングをネタによく冗談を言いますが、監獄に行くことになれば決して「お手柄」ではありません。

データ侵害の時間的段階

過去のデータ漏洩 / 侵害調査報告書でも述べたように、インシデントを時間で追って捉えることにより、脅威の種類や内容を正確に把握できるとともに、脅威の能力の評価も正確に行えます。データ漏洩 / 侵害は一般に多種のイベントで構成され、イベントとイベントの時間的間隔は多数の要素によって大きく左右されますが、このことはベテランのインシデント対応担当者であれば十分に承知しています。いずれの科学でも同じですが、上記のような要素は、研究を重ねることによって要素の理解に必要なモデルを進化させることができ、また要素自体に対する理解も深まります。これまでのデータ漏洩 / 侵害調査報告書では、データ漏洩 / 侵害を構成するイベントを 3 つの時間的段階に分割しており、一般的なインシデントに対応する場合にはこの方式で十分と考えていましたし、現在も同じです。それでも今回、3 つの時間的段階に多少手を加えることにしした。具体的には、以前の「開始から侵害まで」という段階を「最初の攻撃から最初の侵害まで」と「最初の侵害からデータの取り出し（窃取）まで」の 2 つに分割しました。図 40 は、4 つの時間的段階と、各段階の時間の長さを基準にデータ漏洩 / 侵害事例を分類したときの結果です。以下、各段階について順に説明します。

図 40. 各時間的段階の時間の長さで分類した場合のデータ漏洩 / 侵害事例の割合

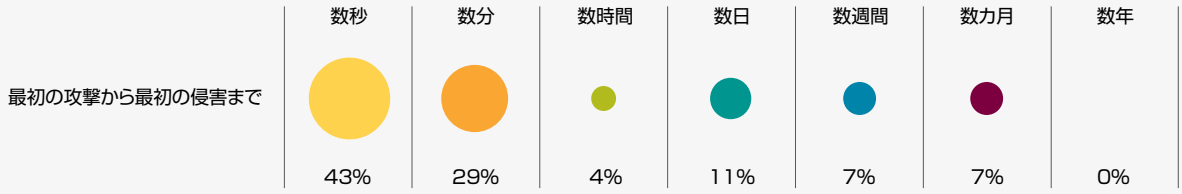


最初の攻撃から最初の侵害まで

この段階は 4 つの時間的段階の中の最初の段階で、悪意のアクションが初めて企業・組織に対して実行されたときから、情報資産のセキュリティ属性（機密性など）が悪影響を受けた（セキュリティが侵害された）ときまでの段階です。この段階は、一般にインシデントの「頂点」でありません。通常、攻撃者が最初のアクションを開始してから、ネットワークへの侵入に成功したときまでを指します。なお、ひとつ注意ですが、この段階は、資産に対するアクセス権または権限を持っていない脅威因子が故意に悪意のあるアクションを実行した場合に限って該当します（それ以外の場合は使用しません）。

2011 年の場合、非常に短い時間（数分以下）でこの段階を完了していたデータ漏洩 / 侵害が大半（85%）を占めています。なお、今回は以前の「開始から侵害まで」を 2 つに分割したため、前年の「開始から侵害まで」の結果を比較検討することはできません。攻撃者が不正アクセスに成功するまでの時間を調べることで主な攻撃のスピードが正確に分かりますが、2011 年は、このスピードが非常に速くなっています。これは昨年、小中規模の企業・組織に対する「速攻」の自動化された攻撃が多かったことに主な原因があります（原因はほかにもあります）。例えば、既知のユーザー名とパスワードのスクリプトリストを使うことで、短時間で POS システムに侵入できます。

図 41.「最初の攻撃から最初の侵害まで」のデータ漏洩 / 侵害の割合（大規模の企業・組織の事例のみ）



大規模の企業・組織の読者の中には、上記のような「速攻」の侵害には強いと考えておられる方も多いかもしれませんので、ここで参考までに統計をお見せします。図にあるように、データ漏洩 / 侵害事例の 71%が、この段階を数分以内に完了しています。もちろん、侵害に使用された脅威アクション（SQL インジェクションなど）は事例によって異なるかもしれませんが、終わってしまったことを今更とやかく言っても始まりません。

大規模の企業・組織の読者の中には、上記のような「速攻」の侵害には強いと考えておられる方も多いかもしれませんので、ここで参考までに統計をお見せします。図にあるように、データ漏洩 / 侵害事例の 71%が、この段階を数分以内に完了しています。もちろん、侵害に使用された脅威アクション（SQL インジェクションなど）は事例によって異なるかもしれませんが、終わってしまったことを今更とやかく言っても始まりません。

最初の侵害からデータの取り出しまで

2 番目の段階である「最初の侵害からデータの取り出しまで」は、情報資産のセキュリティ属性が悪影響を受けたときから、非公開データが企業・組織から取り出された（窃取された）時点までをいいます。なお、この段階の統計（図 40 の「最初の侵害からデータの取り出しまで」）は、ベライゾンの 2011 年の事例データだけを使って作成したものです。図 40 を見ると、攻撃者は「家」に侵入するのも素早かったのですが（最初の段階）、獲物（データ）を手中にするのも速かったことが分かります。事実、最初の侵害から数時間以内に企業・組織のデータを窃取したという事例が、優に半分を超えています。この割合は大規模の企業・組織では 25%に落ちますが、それでも大規模の企業・組織を「よくやった」と手放しで褒めるわけには行きません。25%だったのは、データ保護の装甲が厚かったというより、攻撃者が獲物を探すのにもう少し調査（つまり時間）が必要だったからというのが、妥当な理由と思われるからです。

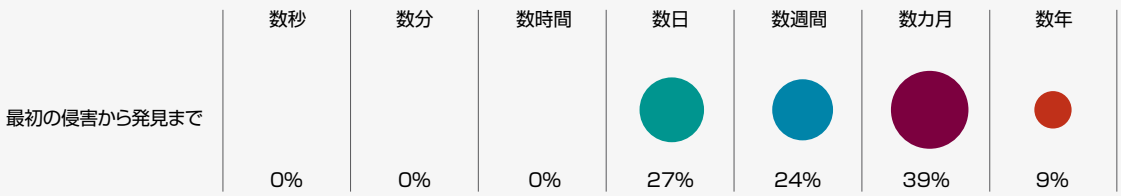
この段階の分析結果について何か為になることはないかと聞かれれば、ひとつあります。それは、データの場所の特定と窃取に 1 日以上要している事例が、全事例の 40%を超えているということです。これはとりもなおさず、攻撃者が企業・組織からデータを持ち出すまでにはある程度の時間があり、その間にインシデントを発見し、阻止できる可能性があることを示しています。

最初の侵害から発見まで

この段階は、情報資産のセキュリティ属性が悪影響を受けたときから、インシデント（データ漏洩 / 侵害）が発生したという事実を企業・組織が発見したときまでをいいます。残念ながら、丸木舟で世界一周してからようやく（世界一周ではなくバイユーから?そういう歌がありました）インシデントを発見するという企業・組織が未だに多いという事実を報告しなければなりません。分析結果では、データ漏洩 / 侵害の発見まで数カ月（場合によっては数年）を要したという事例が半数を超えていました。数カ月もしくは数年間、顧客情報や知的財産などの機密情報が犯人の意のままになり、しかも情報の持ち主はその事実を知らないというのは、何とも長すぎます。

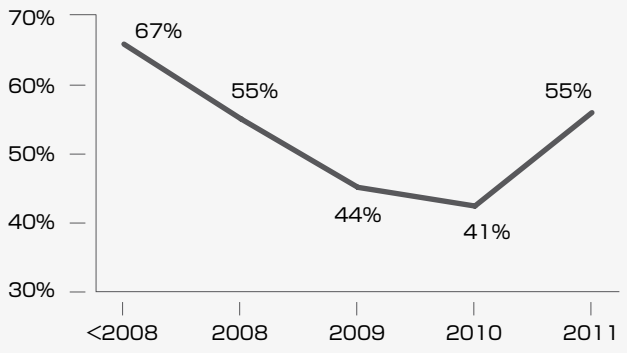
この事実は甚だ大事であるため（それと PowerPoint 風のグラフにも興味があります）、図 42 を作成しました。大規模の企業・組織の場合の分析結果です。大規模の企業・組織の場合、少しはましですがファンファーレを鳴らすほどではありません。丸木舟を小型バッテリー駆動モーター付きボートに変えれば、もう少し速く世界一周から帰って来られるかもしれません。

図 42.「最初の侵害から発見まで」のデータ漏洩 / 侵害の割合（大規模の企業・組織の事例のみ）



この段階については、過去と比較して事実上、何の改善も見られません。本報告書で使用した事例データに偏りがあったという証拠はなく、したがって改善が見られないことが偏りによるものとも思われません。毎年、データ漏洩 / 侵害の発生元と事例が増えますが、映画「恋はデジャブ」のビル・マーレイの目覚まし時計と同じく、歌（傾向）は変わらないのです。さて、この辺で厳しい現実から離れ、少し明るい話に視線を向けることにします。「ここには大したものはないよ」ということです。

図 43. 数カ月以上にわたって発見されなかったデータ漏洩 / 侵害事例の割合



発見から封じ込め・復旧まで

最後の段階は、企業・組織がインシデント発生を発見したときから、インシデントを封じ込めたとき（「情報流出」を止めたとき）まで、または侵害されたシステムが復旧したとき（システムの機能が正常に戻ったとき）までです。

封じ込めまでの時間は前年と比較するといくぶん短縮された、と多少楽観的な言い方をしていいようです。例えば 2010 年の場合、数日以内に封じ込められた事例は全事例の 34％でしたが、2011 年は 42%でした。上にあるように「いくぶん」ですが、それでも真っ当な方向に進んでいることは確かです。この調子で行きましょう。

インシデントに対応する場合、スピードと実行の両方が等しく重要であり、これを記憶に留めておくことが大事です。ただし、スピードを重視し、あまりにも拙速に行動すると誤りを冒すリスクが増し、その結果、コストがかさんだり、その後のインシデントの軽減作業に余計な時間がかかるといったことも起こります。本報告書で「効果的なインシデント対応」と言う場合、それはインシデント対応担当者の「数」を増やすことではありません。インシデント対応に必要なメカニズムを用意し、そのメカニズムを介して対応を開始するとともにインシデントを分類し、また時機を見計らって外部の支援を要請したり法執行機関に連絡したりすることをいいます。また、ネットワーク図など、実用的な資料を作成しておくこと、もしくは必要な場合に作成できるようにしておくことも「効果的なインシデント対応」の一要素です。さらに、関係者全員と協力しながら、インシデントの封じ込めという共通の目標に向かって進むことも必要です。いずれも常識のように聞こえますが、常識にはそれなりの理由があります。とはいっても、腕をまくってインシデントの解決に当たる代わりに、インシデントに対応したときの失敗や予想外の結果を恐れ、対応に二の足を踏む企業・組織が多いのも事実です。

漏洩 / 侵害の発見方法

上述の時間的段階とは違って、データ漏洩 / 侵害の発見方法の分析結果は、本報告書の分析結果の中でも特に興味がそそられ、また注目すべき結果の部類に入ります。侵害が発見されるまでの時間は通常、侵害の発見方法によってそれぞれ異なり、したがって両者間には密接な関連があります。とはいえ、どちらも企業・組織が脅威を検出し、対応する能力を示す指標、言い換えると企業・組織のセキュリティ体制の成熟度を表す優れた指標です。残念なことに、過去数年間、被害を受けた企業・組織自体より第三者がデータ漏洩 / 侵害を発見したというケースがはるかに多いという結果が出ています。

ベライゾン RISK チームでは現在、データ漏洩 / 侵害の発見方法の主な分類項目として「外部」と「内部」の 2 種類を使っています。「外部」は、外部の者がデータ漏洩 / 侵害を発見し、被害を受けた企業・組織に通知したという発見方法を指します。

「内部」は、さらに「能動的」（発見を目的として設計・配置されている機器やツールなどによる発見）と「受動的」（一般にセキュリティの専門家でない人が徴候などを発見）に分類してあります。

図 44. 発見者で分類した場合のデータ漏洩 / 侵害事例の割合（簡易版）

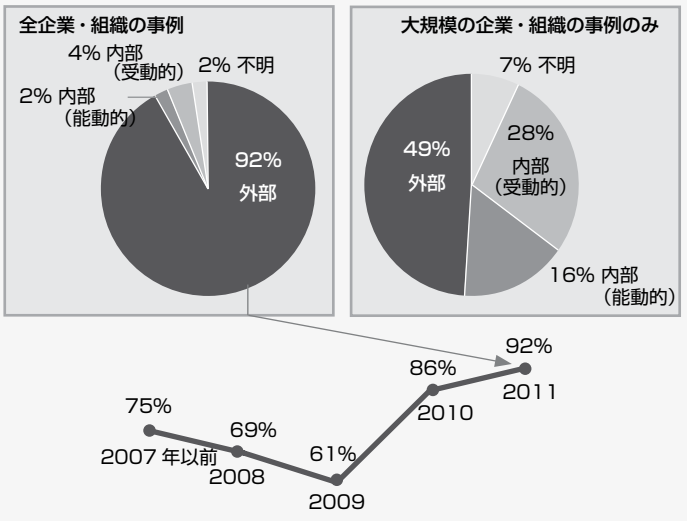
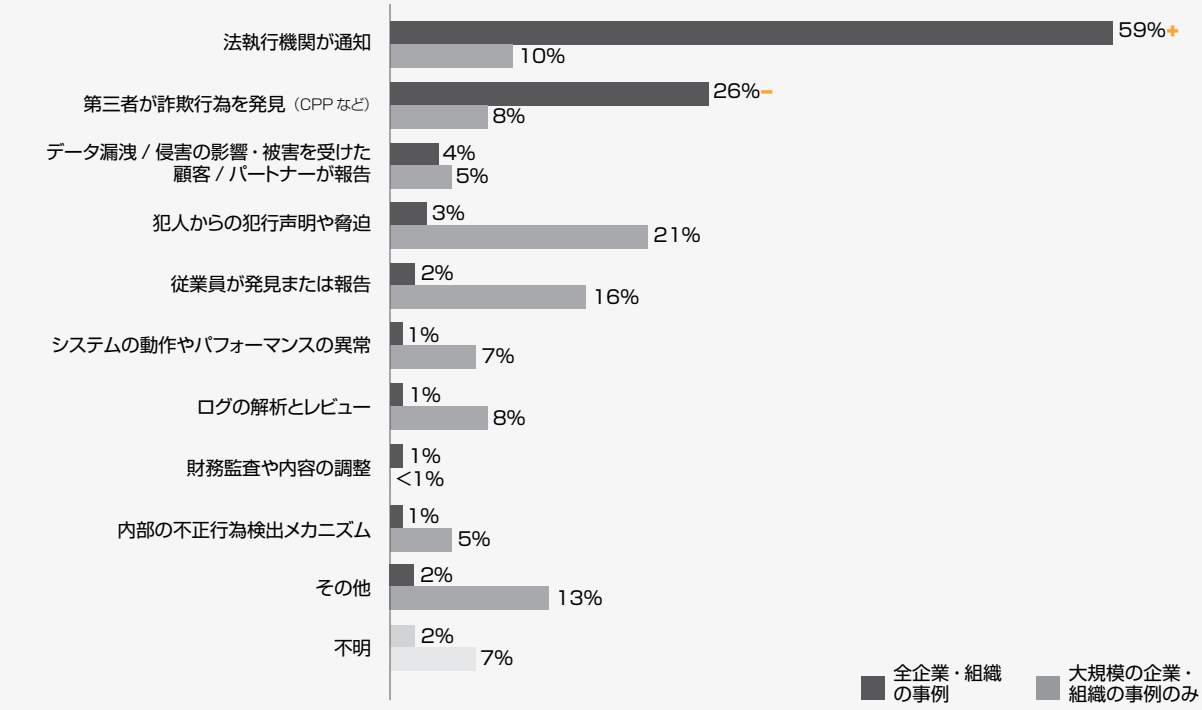


図 44 ですぐ分かるように、今回は外部の者によって発見された事例の割合が過去最高を記録しています。理由は二つあり、今回使用した事例データの性質が主な理由です（2 番目の理由）。最初の理由は、小規模の企業・組織の場合、一般にセキュリティイベントの監視に必要な専門知識と技術が不足していることです。それに、「壊れてないものは直すな」（触らぬ神に祟りなし）という金言に則って日常の業務に当たっています。さらに正確に言うなら、そもそも壊れているかどうか分からないのだから直しようがない、ということかもしれません。2 番目の理由は、最初の理由（小規模の企業・組織）と今回の各協力機関の事例データの「副産物」を加えたものです。上記の理由については、次の「外部」の節で詳しく説明します。

全企業・組織の結果と大規模の企業・組織のみの結果を比較してみると、大きな相違があります。つまり図 44 で分かるように、「外部」は大規模の企業・組織のほうが格段に少なく（49%）、また、「内部」（受動的と能動的の合計）は逆に大規模の企業・組織のほうがはるかに多い（44%）という結果になっています。以前にも説明したように、大規模の企業・組織の場合、専門知識や能力、リソースを利用してセキュリティ侵害を効率よく発見でき（もちろん活用すればの話です）、これが上記の結果の理由です。このことについては、次の節でもう少し掘り下げて検討します。勉強になることがいくつかあります。

図 45. 侵害の発見方法で分類した場合のデータ漏洩 / 侵害事例の割合



もうひとつ CPP の注意点として、CPP では分析できないような方法で詐欺行為が行われれば効果がないということがあげられます。一方、企業・組織の機密データ（知的財産など）の侵害事例の中には、データの窃取後もその事実がまったく発覚しないというケースもあります。

外部

今回、データ漏洩 / 侵害の発見方法として再度、「法執行機関が通知」が主な方法の部類に入りました。というより今回、常連チャンピオンである「第三者が詐欺行為を発見」を押さえてトップに返り咲きました。その理由のひとつとして、近年、法執行機関が犯人グループとその悪行の追跡に一層尽力していることがあげられます。つまり、法執行機関は捜査を通じて、攻撃やデータ漏洩 / 侵害が発生したことを把握し、被害を受けた企業・組織に連絡することができます。この連絡は、CPP（Common Point of Purchase: 共通の購入場所）分析で詐欺行為（カードの不正使用）が発見される前に行われることも少なくありません。

CPP との関連で言えば、今回も「第三者が詐欺行為を発見」が引き続き有効な発見方法のひとつであることに注目しなければなりません。CPP の利点は、広い地域に散在する多数の企業・組織を対象にして、被害を受けた企業・組織を探せることにあり、したがって特定の企業・組織を起点に調査を展開するという方法より格段に効率的です。ただし CPP はあくまで事後検出手法、つまりデータ流出や詐欺行為を事前に防止するのではなく、データ流出後に詐欺行為が行われて初めて、被害を受けた企業・組織を特定できる手法であり、その点では限界があります。もうひとつ CPP の注意点として、CPP では分析できないような方法で詐欺行為が行われれば効果がないということがあげられます。一方、企業・組織の機密データ（知的財産など）の侵害事例の中には、データの窃取後もその事実がまったく発覚しないというケースもあります。この種のデータ（ペイメントカード情報以外の情報）の場合、CPP のような検出方法が存在しないことから、実際のデータ漏洩 / 侵害事例の件数は一般に公表されているよりはるかに多いと思われます。

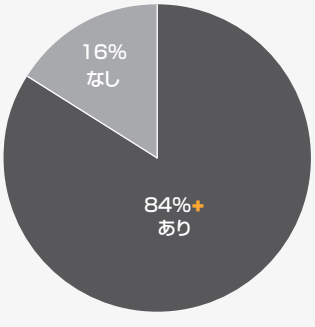
大規模の企業・組織の事例のみの場合、「外部」の発見方法の割合は、全企業・組織の事例の場合と大きく異なります。まず、大規模の企業・組織の場合は「法執行機関が通知」が 2 番目に多いのですが（10%）、これは全企業・組織の割合と比べるとわずかです。また、大規模の企業・組織では「犯人からの犯行声明や脅迫」がトップ、つまり犯人が何らかの形でデータの窃取を公表した時点で気がついたというケースが最多でした。この状況を考えると、来年のデータ漏洩 / 侵害調査報告書では「YouTube」「Pastebin」、「Twitter」という分類項目を作ったほうがいいかもしれません。（もちろん冗談ですが（半分本気です）、最近ではソーシャルネットワークがデータ漏洩 / 侵害の発見に貢献していること、それと残念なことに、攻撃の中にはソーシャルネットワークを使って開始されるものもあり、この現実を理解することが大事です。この辺の事情については、頃合いを見てブログで補足します。）次に、企業・組織では「内部」でどのような方法を使ってデータ漏洩 / 侵害を発見しているか（またはしていないか）を見ることにします。ただし、残念ながら「内部で発見」したことを示す証拠はあまり見つかりませんでした。

内部（能動的）

「内部（能動的）」とは、IDS、IPS、HIPS、ログ解析、アンチウイルスなど、企業・組織が一般にデータ漏洩 / 侵害の防止や検出、対応に使用している技術やツールによってデータ漏洩 / 侵害を発見することをいいます。残念ながら、上述したように小規模な企業・組織の場合、意識や姿勢、資金、技術が十分でないことからデータ漏洩 / 侵害の防止、検出、対応は容易ではなく、特に攻撃のスピードが速かったり技術レベルが高かった場合はそう言えます。

一方、大規模の企業・組織は、上のような技術の活用に関しては小中規模の企業・組織よりは巧者ではあるものの、状況が好転するまでには至っていません。例えば、大規模の企業・組織の場合、「内部（能動的）」の中では「ログの解析とレビュー」がトップですが、それでも大規模の企業・組織の全事例のうちの 8%にすぎません。お気づきかもしれませんが、「ログの解析とレビュー」は毎年、私どもが推奨している発見方法のひとつであり、また、ほとんど他のどの発見方法よりも効果的であると考えています。どうしてでしょうか。調査を行う場合、ログを読み分析することで発見できるケースが非常に多いからです（図 46）。また、ログの中の針を探すのではなく干し草の山に注目せよと以前から主張しています。針と干し草の山については、次ページの別枠記事に詳細がありますのでお読みください。

図 46. フォレンジック分析でデータ漏洩 / 侵害の証拠があった事例となかった事例の割合 *



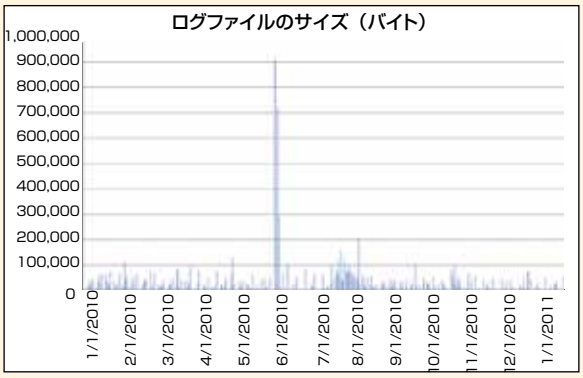
* ベライゾンの事例データのみ

ログの中の針と干し草の山（その二）

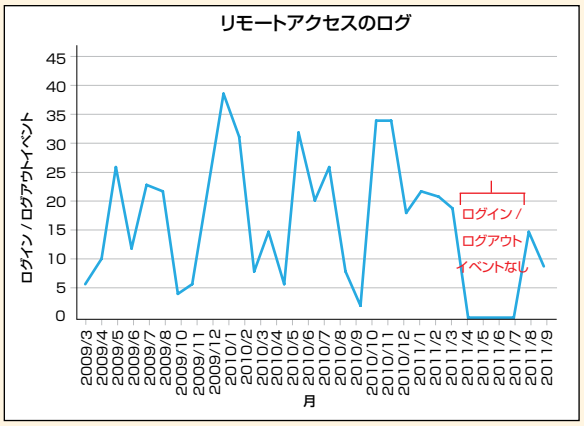
読者の中には、2010 年度データ漏洩 / 侵害報告書（P.50）の「ログの中の針と干し草の山」という別枠記事を覚えている方もおられるでしょう。本年は、その続編を書くのに向いていると考え、書き下ろしてここに掲載しました。

データ漏洩 / 侵害の発見方法として「セサミストリート」法を使うことがよくあり、これは独自に考案した方法です。自分の子供、自分が子供だった頃、友人･知人の子供など、誰でもいいですので自分が子供になったと想像し、セサミストリートの「この中でどれが違う」という題名の歌を思い出してください。調査を行う場合、この方法でセキュリティイベントの証拠を探すことが少なくありません。体を使うのもいいですが、やはり頭脳です。つまり、多大な労力を投じて針を探す代わりに干し草の山に注目します。具体的には、いくつもの干し草の山の中に「他と違う干し草の山」があれば、そこで針探しを始めます。まだ抽象的なので、現実世界の例を使って説明します。

セミナーなどを開いたときには、下のグラフを紹介し、「このグラフで、何か変わったところは見当たりませんか」と尋ねることがよくあります。笑い声がやんだら、郵便切手ほどに縮小できることも説明します（これは、さほど大事なことではありません）。いずれにしても、「この中でどれが違う」の答えはすぐに分かります。下は、各ログファイルのサイズを使って作成したグラフですが、そのほか色々なデータを使って作成できます。



例えばデータ漏洩 / 侵害の発見に有効なデータとしては、ログファイルのカウント、ログファイルの行の長さ（特に SQL インジェクションの発見に有効）、特定のタイプのトラフィック量（ssh、FTP、DNS など、企業・組織で通常は使用していないタイプのトラフィック）、イベントの数、IP 接続（必要な場合はプロトコル別）の発生元の国、使用されている帯域幅、送受信された電子メールなどがあります。このほかにも多数あり、想像力次第です。この「この中でどれが違う」発見方法の面白い点は、有効な方法なのにお金がかからないことです。実際、Linux や Windows のコマンドをいくつか使えば簡単にできます。



イベントの数を示したグラフを見る場合、注意しなければならないことがあります。それは、急激に増加している部分だけが怪しいわけでなく、イベントが減っている場所も懸念部分であり、したがって要注意ということです。このグラフにはリモートアクセスのログイン / ログアウトイベントの数が示されており、イベントが多い月もありますが、右側にイベントが発生していない部分もあります。ここでデータ漏洩 / 侵害が発生していました。

もちろん、以上は全部「栄光の後知恵」によって明らかになったことですが、このような方法は他では見られないはずです。

内部（受動的）

「内部（受動的）」とは、セキュリティを専門としていない人間（または物）がインシデントの徴候や痕跡を発見することをいいます。例えば、従業員が日常の業務を行っているときに奇妙な出来事（システムの動作が遅いなど）に気がついたというのが代表的な例です。なお、おかしな出来事に気がつくことも大切ですが、その出来事に気がついたときに直ちに行動することがそれ以上に重要です。しかしながら、調査に行って聞き取りを行うと、システム（PC など）の動作が変だったことには気がついたが、そのあと何もしなかったし、上司にも報告もしなかったという回答が少なくないのです。どうしていいか分からなかった、または大したことではないと思ったというのがその理由でした。企業・組織では、研修などを通じて、従業員にセキュリティインシデントの徴候の見つけ方や対処方法を十分に教えることが重要であり、うまく行けば「インシデント探検隊」を手に入れたも同然です。昨年の報告書では、従業員に対してインシデント教育を行っている企業・組織を称えましたが、本年は称えるだけでなくワインを振る舞うことにします。

<ここから>ワインの振る舞い先は、分析結果によれば大規模の企業･組織になるようです。大規模の企業･組織の場合、データ漏洩 / 侵害事例の実に 16%が従業員によって発見されています（図 44）。大規模の企業・組織では通常、各種の規制に準拠するため従業員のセキュリティ意識を高める必要があり、また研修も定期的に実施されていることを考えると、この結果は納得できます。これに対して、小売店舗の従業員は、不審な出来事や異常にはあまり気がつかないのが普通です（Facebook で「ビジュエルド」ゲームをしている最中に動作がおかしくなれば当然、気がつきます）。企業・組織が従業員に研修を行っても、差出人が不明の電子メールのリンクをクリックしたり、添付ファイルを開ける従業員は中にはいるでしょう。それでも、セキュリティインシデントの徴候を見つけたり迅速に対応できるようになり、結果的に企業・組織ではセキュリティインシデントの発生を早期に発見できます。

アンチフォレンジック

攻撃者によるアンチフォレンジック（セキュリティ侵害の証拠消し）に関しては、問題があります。アンチフォレンジックが巧みであれば、それだけ発見が難しいという問題です。それでも、調査員が現場でアンチフォレンジックテクニックを見つけることも珍しくありません。アンチフォレンジックを見つけた場合には記録し、分析に回します。

2011 年の場合、アンチフォレンジックは、ベライゾンのデータ漏洩 / 侵害事例の 3 分の 1 に見られました（この傾向は過去数年間、同じです）。なお、この数字は非常に控えめな推定値で、実際にはもっと多いと思われます。当然ながら、アンチフォレンジックの手法は性質も目的も千差万別ですが、基本的にはデータの消去、隠蔽、破壊の 3 種類に絞られます。よくあるテクニックの具体例としては、ログのワイピング（削除）やタンパリング（改ざん）、窃取したデータの暗号化などがあります。目的は、後日の調査を妨害したり、犯罪現場を掃除してピーコック婦人がマスタード大佐を燭台で殺害したことを分からなくするためです（眠くなったかと思い、ちょっと目覚ましです）。

攻撃者によるアンチフォレンジック（セキュリティ侵害の証拠消し）に関しては、問題があります。当然ながら、アンチフォレンジックの手法は性質も目的も千差万別ですが、基本的にはデータの消去、隠蔽、破壊の 3 種類に絞られます。

少し不思議なのは、アンチフォレンジックが行われた事例の割合が小中規模の企業・組織と大規模の企業・組織でそれほど違わないように見えることです。それでも、今までの記録によれば、攻撃者は企業・組織の規模に関係なくアンチフォレンジックテクニックを使用しているようで、そういうことなのでしょう。APT は証拠が残らないことが多く、これはスケアウェア（ユーザーの恐怖心を煽り金銭や情報を奪おうとするマルウェア）も同様です。タイムストンピング（ファイルの日付・時刻を修正）、パッキング（EXE ファイルを圧縮）、暗号化もよく見られるテクニックです。

タイムストンピングについて

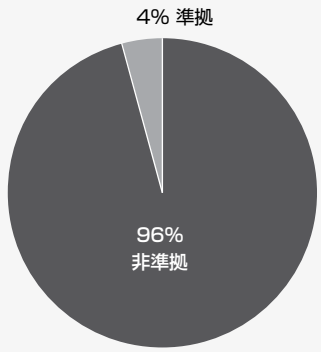
フォレンジック調査員の主要業務のひとつとして、システムイベントのタイムライン（時系列）解析があります。非常によく見られるアンチフォレンジックテクニックのひとつとしてタイムストンピングがあり、その機能はタイムスタンプ（日付 / 時刻）をストンピングする（踏みつける）というものです。タイムスタンプが攻撃者により修正または操作されていたり、もしくは新規に作成されていた場合、それが通常の形式であれば問題なく分かります。しかしながら、NTFS ファイルシステムの場合、各ファイルにそれぞれタイムスタンプが複数あり、これがタイムストンピングが行われているかどうかの判別を難しくしています。この理由から、NTFS ファイルシステムのタイムスタンプの仕組みを理解しておくことは、タイムストンピングが行われたかどうかを判別する上で有用です（NTFS の場合）。

NTFS のファイルは、内容的には属性の集合で、各属性のインデックスがマスターファイルテーブル（MFT）に記録されています。一般にタイムスタンプと呼ばれるタイムスタンプは、$STANDARD_INFORMATION 属性に記録されています。そのほか、ここには 4 つ目のタイムスタンプ（MFT エントリモディファイドタイムスタンプ）も記録されています。全部で 4 つのタイムスタンプはいずれも、Windows API の NtQueryInformationFile を使ってアクセスできます。また、この 4 つのタイムスタンプはコードを使ってストンピングでき、ストンピングするには NtSetInformationFile（設定）を使用します。

NTFS のファイルの属性としては、そのほか $FILE_NAME 属性もあります。この属性はファイルのハードリンクに関する属性で、それぞれ専用の 4 つのタイムスタンプ（4 つでワンセット）があります。この 4 つのタイムスタンプは、Windows API ではアクセス（または修正）できません。

つまり、攻撃者は、十分な権限を持っていれば標準の Windows API を使って NTFS のファイルのタイムスタンプを変更でき、したがってタイムライン解析を実質上、無意味にすることができます。現実世界で言えば、ハリケーンが犯罪現場を通過したのと同等です。タイムストンピングは、ベテランの調査員にとって一巻の終わりというわけではありませんが、それでも作業する上で支障になるのは確かです。

図 47. PCI DSS への準拠状況（直前の PCI DSS 評価による）*



* ベライゾンの事例データのみ。準拠状況は、主に企業・組織の自己申告によるもの（証明は求めませんでした）。

PCI DSS

ペイメントカードカード業界データセキュリティ基準（PCI DSS）は複数の要件で構成されており、要件はいずれもカード所有者の情報の保護を目的としています。毎年そうですが、ベライゾンの事例データの中には、PCI DSS への準拠義務がある企業・組織の事例も多数見られます。ここで問題となるのは、このような企業・組織が PCI DSS に準拠していたかどうかです。PCI DSS への準拠は重要であり、本節では、事例と PCI DSS への準拠との関係について検討します。

PCI DSS に関する分析結果を見る場合、検証とはどういうものかについて考えてみる必要があります。まず、自分が自分の生活（のレベル）をどのようにして「検証」しているかを想像してください。この場合、他人（同僚や隣人、またセレブでも結構です）の生活を思い浮かべ、それを自分の生活と比較するという方法で検証する人がほとんどのはずです。これは、個人の生活だけでなくビジネスの世界でも同様です。例えば、会社で PCI DSS への準拠が話題に上った場合、「ウチの準拠状況は、XYZ 会社に比べてどうだい」や「業界の中では、準拠レベルはいいほうかな」という言い方をよく聞きます。表面上は世間話のようにも聞こえますが、おそらく真剣です。

ただし、このように比較によって自社の準拠状況を検証するという方法には重大な欠点があります。それは、自社の準拠状況が他社より少しでも良ければ、セキュリティも他社より優れていると思い込んでしまう傾向があることです。

この「思い込み」を「良い」、「比較的良い」、「最高」の 3 段階評価で表すと次のようになります。

- 良い－「我が社のセキュリティは他の多数の企業より優れているが、まだ準拠すべき要件を満たすには至っていない…」
- 比較的良い－「我が社のセキュリティは他の大半の企業より優れており、また準拠すべき要件を「字句」の上で満たしている・・・」
- 最高－「我が社のセキュリティは他の大半の企業より優れており、また準拠すべき要件を「精神」の上で満たしている。さらに、常時変化する脅威環境に応じてセキュリティを強化している・・・」

では、上の評価（思い込み）と PCI DSS はどんな関係があるでしょうか。図 47 で分かるように、データ漏洩 / 侵害を受けた企業・組織（PCI DSS の準拠義務がある企業・組織）のうち、今までの最後の評価（PCI DSS に準拠しているかどうかの検証）で PCI DSS に準拠していないと判定された企業・組織の割合は 96%に達しています（この中には、評価の経験が一度もない企業・組織も含まれています）。つまり、一般にセキュリティが「良い」と考えている企業が多いようですが、実際には大半の企業が該当していなかったことになります。割合については、この 96%という数値は今までの報告書の中で最高の値です。見方は色々あるかもしれませんが、結局、被害を受けた企業・組織の中には、実際に「比較的良い」や「最高」に該当する企業・組織はほとんどなかったということになります。

一般にセキュリティが「良い」と考えている企業が多いようですが、実際には大半の企業が該当していなかったことになります。

では、これだけ侵害事例が多いということは、PCI DSS がデータ漏洩 / 侵害に対して有効ではないということでしょうか。そうは思われません。PCI DSS が有効でないのであれば、「比較的良い」や「最高」の企業（準拠すべき要件を満たしている企業）がデータ漏洩 / 侵害を受けた事例はもっと多かったはずであり、また PCI DSS に準拠していたのに侵害を受けた企業・組織の割合（今回は 4%）も多かったと思われます。PCI DSS に準拠していなかった企業・組織（96%）の内訳を見ると小規模企業（レベル 4 加盟店）が多く、その割合が増える傾向が続いています。このような小規模企業の場合、PCI DSS の（自己）評価を行っていなかったり、PCI DSS の要件のいくつかに準拠していなかったという例がよく見られました。ここで注意しなければならないのは、小規模企業（加盟店）が自己評価を行っていないこと、または PCI DSS に準拠していないことと、PCI DSS が有効でないこととは全く異なるということです。また、ベライゾンでは大規模の企業・組織のデータ漏洩 / 侵害事例を多数調査しましたが、その中の多くが、ペイメントカード情報に

関連したデータ漏洩 / 侵害ではなかったこと（言い換えると、大規模の企業・組織のデータ漏洩 / 侵害事例が必ずしも大量のペイメントカード情報が窃取された事例ではないこと）を知っておくことも大事です。

表 14 は PCI DSS で準拠すべきとされている要件（PCI DSS 要件）を示したものですが、この表で、12 の要件のうち 8 つが全期間（2008 年～ 2011 年）の 3 分の 2 以上で「非準拠」であることが分かります。このことは、PCI DSS に準拠している企業･組織が極めて少ないという上記の説明を裏付けるものです。因果関係はそれぞれ異なり、その全部を証明するのは困難です。それでも、非常に多数の企業・組織がデータ漏洩 / 侵害を受けた主な要因は PCI DSS（それと業界の多数の基準）からの大きな偏差（非準拠）にあり、この事実は、ほぼすべての事例に当てはまると断言できます。

表 14. データ漏洩 / 侵害を受けた企業･組織が各 PCI DSS 要件に準拠していたかどうかをベライゾンの IR チームが分析した結果（数値は、要件に準拠していた企業・組織の割合）*

				2011	
	2008	2009	2010	全企業・組織の事例	大規模の企業・組織の事例のみ
安全なネットワークの構築と維持					
要件 1：カード会員データを保護するために、ファイアウォールをインストールして構成を維持する	30%	**35%**	18%	29%	71%
要件 2：システムパスワードおよびその他のセキュリティパラメータにベンダー提供のデフォルト値を使用しない	**49%**	30%	33%	42%	86%
カード会員データの保護					
要件 3：保存されるカード会員データの保護	11%	**30%**	21%	18%	14%
要件 4：オープンな公共ネットワーク経由でカード会員データを伝送する場合、暗号化する	68%	**90%**	89%	89%	86%
脆弱性管理プログラムの整備					
要件 5：アンチウイルスソフトウェアを使用し、定期的に更新する	**62%**	53%	47%	23%	86%
要件 6：安全性の高いシステムとアプリケーションを開発し、保守する	5%	**21%**	19%	20%	57%
強固なアクセス制御手法の導入					
要件 7：カード会員データへのアクセスを、業務上必要な範囲内に制限する	24%	30%	33%	**36%**	29%
要件 8：コンピュータにアクセスできる各ユーザーに一意の ID を割り当てる	19%	**35%**	26%	20%	57%
要件 9：カード会員データへの物理アクセスを制限する	43%	58%	65%	**73%**	100%
ネットワークの定期的な監視およびテスト					
要件 10：ネットワークリソースおよびカード会員データへのすべてのアクセスを追跡および監視する	5%	**30%**	11%	11%	43%
要件 11：セキュリティシステムおよびプロセスを定期的にテストする	14%	**25%**	19%	6%	33%
情報セキュリティポリシーの整備					
要件 12：情報セキュリティポリシーを整備する	14%	**40%**	16%	16%	83%

また、PCI DSS に準拠していなかった企業・組織（96%）を（a）従業員が 1,000 人未満、（b）従業員が 1,000 人以上という基準を使って分類してみましたが、この分析により PCI DSS への準拠に関して両者に大きな違いがあることが分かりました。まず、1,000 人未満の場合、前述のレベル 4 加盟店が大多数を占めていました。一方、従業員が 1,000 人以上（大規模の企業･組織）の場合、「非準拠」の要件は 3 つしかありませんでした（表 14）。これに対して、全企業･組織の場合は 12 の要件のうち 8 つが「非準拠」でした。この事実から、どんなことが推測できるでしょうか。

恐らく、大規模の企業・組織は基準への準拠を進めており（セキュリティ確保に必要な基本対策を実施しており）、そのためデータ漏洩 / 侵害のリスクに曝されたり実際に侵害を受けることが少ないと言って問題はありません。ペイメントカード業界では、大規模加盟店の PCI DSS 準拠状況について資料を提供していますが、上記は、この資料の内容とも符合します。

もうひとつ、PCI DSS に準拠していたのに侵害を受けた企業・組織（4%）について見てみます。このような企業・組織からは、例のごとく「PCI DSS に準拠しているのに、どうしてウチがやられるんだ。」というぼやきが聞こえます。このような場合、準拠はセキュリティの強化には間違いなく有効だが、準拠と完璧なセキュリティは別物、と繰り返すしか方法がありません。また、この種のデータ漏洩 / 侵害では、犯人の哲学は同じです。つまり、これは検察官からよく聞く話ですが、犯人はハッキング対象の企業・組織を知らないまま行動に出ることが非常に多いといいます。そのため、不正アクセスに成功して初めて相手が誰かが分かる、というのがほとんどのようです。

PCI DSS 評価は「任意の時点」での評価であるため、直前（データ漏洩 / 侵害発生の前）の PCI DSS 評価で準拠していると判定されていても、データ漏洩 / 侵害の発生時には準拠していなかったということもありえます。また、準拠の判定は、評価担当者によって甘い、厳しいが少しはあります。

要件を全体的に見ると、企業・組織は規模を問わず、3、7、10、11 の 4 つの要件に悪戦苦闘しているようです。4 年間の変化（改善、悪化、同じ）をまとめると、次のようになります。

- 改善（5 つ）— 要件 1、2、6、7、9
- 悪化（4 つ）— 要件 3、5、8、11
- 同じ（3 つ）— 要件 4、10、12

上の結果を見てみると、改善した要件の数が悪化した要件の数を上回っています。ただし、総合改善値（32%）と総合悪化値（-46%）を比較すると、その差は -14%です。改善が一番顕著だったのは要件 1（+11%）、「カード会員データを保護するために、ファイアウォールをインストールして構成を維持する」でした。一方、一番悪化したのは要件 5（-24%）、「アンチウイルスソフトウェアを使用し、定期的に更新する」でした。

このような企業・組織からは、例のごとく「PCI DSS に準拠しているのに、どうしてウチがやられるんだ。」というぼやきが聞こえます。このような場合、準拠はセキュリティの強化には間違いなく有効だが、準拠と完璧なセキュリティは別物、と繰り返すしか方法がありません。

以上、PCI DSS 関連の分析結果について説明しましたが、最後に PCI DSS の効果を考えてみます。一般的に言えば、PCI DSS は、カード所有者の情報の保護に必要な基本的要件をまとめたものです。本節では、PCI DSS への準拠義務がある企業・組織のデータ漏洩 / 侵害事例について見てきましたが、そのほとんど全部が、企業・組織が PCI DSS の要件を確実に遵守していれば防止できたと思われる事例でした。もちろん、PCI DSS に準拠している企業・組織の防御が極めて固く、どんな新手の作戦を使ってもハッカーが突破できなかったという例もあったでしょう。とはいっても、上で見たように PCI DSS の要件に準拠していない企業・組織は非常に多く、この状況が続く限り、ハッカーが脆弱性（最小抵抗経路など）を突いて不正にアクセスしようとする傾向は続きます。このような背景から、企業・組織はできるだけ強固なセキュリティ体制を構築しなければならず、同時にその努力を続ける必要があります。上記のようなセキュリティ体制を構築する場合、大半の企業・組織にとって、PCI DSS はその進捗状況を確認する上で妥当（かつ必要）な基準であり、その役割は今後も続くはずです。

データ漏洩 / 侵害の影響

データ漏洩 / 侵害調査報告書にはデータ漏洩 / 侵害の影響（被害）や結果に関する情報が少ない、という意見が毎年必ず寄せられます。「全員をいつも喜ばせておくことはとてもできない」という格言がありますが、当たっています。といっても、このご意見はごもっともですし、読者の横に立って一緒に「もっと被害に関する情報を出してくれ」と叫びたいところです。本報告書シリーズはリスク管理には有益であり、このことは多大な時間と相当な紙幅を費やして説明してきました。ただし報告書では、リスクの 2 つの要素、つまり頻度と規模のうち、後者の規模に関する情報はほとんど紹介してきませんでした。[21]

21 情報リスク要因分析（FAIR）は、情報に関するリスクを「将来の喪失の推定頻度と推定規模」の観点から分析する手法です。詳しくは、「情報リスク要因分析（FAIR）の概要」（Risk Management Insight LLC、2006 年 11 月）を参照してください。本報告書に記載されている統計は、ほとんどがロスイベント（喪失事象）の頻度に関するものです。

データ漏洩 / 侵害の被害やその規模に関する情報が少ないのは、何も怠慢のせいではなく、そのような情報を入手できない理由がいくつかあるからです。第一の理由は、データ漏洩 / 侵害に遭遇すると大抵の企業・組織は「火消し」に奔走し、できるだけ早く「元の状態」に戻ろうとすることに関係しています。つまり、費用とリソースをどこにどれだけつぎ込んだかを記録するという作業はあくまで二の次で、結局、記録は残りません。それに火が消えた後も、企業・組織はどういうわけか、被害や損害に関するデータを集めようとはしません。2 番目の理由としては、調査では一般に侵害の証拠（または反証）の収集、データ流出の評価、侵害の封じ込めが重視され、被害にはあまり目が向けられないことがあげられます。また、企業・組織がこうむった金銭的被害の分析と定量化は、私どもの本来の仕事ではありません。時折、被害に関する情報を入手することもありますが、その情報量はパズルを完成できるほどではありません。そのほか、侵害後、その事例を長期にわたって追跡し、結果を調査することはないのも理由のひとつです。

データ漏洩 / 侵害の場合、脅威因子や脅威アクション、データ流出だけでなく、金銭的損害に関する情報も「聖杯」であることは心得ています。そこで、「被害に関するデータは報告書には掲載しない」という当初の決定を覆し、被害に関する情報をできるだけ集めることにしました。この作業は、調査中と調査後の両方で行いました。

被害に関するデータは、収集して報告書に掲載することもできますが、最終的にはしないことにしました。データ漏洩 / 侵害調査報告書の特徴のひとつは（他の調査報告書もそうだと思います）、最初から最後まで客観的で信頼性が高く、しかも事実に基づく情報だけを掲載してあることです。被害に関しては、上記の基準に見合ったデータを調査で収集しておらず、したがって報告書に掲載するべきではないと考えました。

とはいっても、被害に関するデータを収集して報告書に掲載したいのは山々であり、読者の中には見てみたいと思っている方もいるはずです。データ漏洩 / 侵害の場合、脅威因子や脅威アクション、データ流出だけでなく、金銭的損害に関する情報も「聖杯」であることは心得ています。そこで、「被害に関するデータは報告書には掲載しない」という当初の決定を覆し、被害に関する情報をできるだけ集めることにしました。この作業は、調査中と調査後の両方で行いました。情報収集作業では、何も得られないこともありましたし、貴重な情報が手に入ったこともあります。2011 年の被害に関する情報は十分ではないため、ここでは統計を記載することはできませんが、注目すべき点をいくつか紹介します。

2011 年の場合、データ漏洩 / 侵害事例の中には被害が何億ドルにも及ぶと思われる大きな事例も何件かはありましたが、ほとんどの場合、目立った被害は見られませんでした。というより、大多数の事例では、データ漏洩 / 侵害による被害は比較的軽微で済みました。中には、何日かは業務に支障が出た企業・組織もあったかもしれませんが、正常の業務に戻るまでにはそれほど長くはかかりませんでした。

まず、2011 年のデータ漏洩 / 侵害による損害の中で明らかなのは、対応と復旧（フォレンジックを含む）に企業・組織が支払った費用です。もちろん、ベライゾンの調査チームの作業は一般に有料であるためこの費用がかかりますが、公的な調査・捜査機関の場合はそうではありません。この種の費用は、大規模の企業・組織の場合はそれほど問題にはなりませんが、小中規模の企業・組織にとっては痛手です。また、詐欺（カードの不正使用など）による損害も多く、ペイメントカードと個人情報を標的にしたデータ漏洩 / 侵害が多発したことを考えると、このことは納得がいきます。詐欺による被害金額は、数ドルから 1 億ドル超まで様々です。

あまり一般的ではありませんが（ただし金額は少なくありません）、規制や法律に関連して発生した費用もあり（パブリックドメイン情報の場合に多い）、このケースのデータ漏洩 / 侵害事例がいくつかありました。この費用は、実際に支払われたかどうか不明な場合もありますが、集団訴訟などでは相当な額の預託金を支払うのが普通です。

また、データ漏洩 / 侵害の発生後、「そうなったらどうしよう」恐怖症候群にかかる企業幹部も多いのですが、その主な症状として、ブランドイメージの低下、株の値下がり、競争力の低下があります。ただし、かなり深刻と思われるものも含め、ほとんどのデータ漏洩 / 侵害では、このような心配は無用です。株価が下がり、その状態が長期にわたって続くということは一般的にはないようです。

上記のように 2011 年は、損害は比較的軽微でしたが例外もいくつかありました。例えば、データ漏洩 / 侵害が直接または間接の原因となり、結果的に営業を停止せざるを得なくなった企業が少なくても 4 社ありました。この中の一社は、インシデントの最中に顧客向けのシステムが被害を受け、そのシステムの復旧ができなかったため営業を継続できなくなりました。もう一社は、本業に相当なダメージを受け、結局は店舗を閉めました。もう一社は小規模な「クリックアンドモルタル」（店頭販売とオンライン販売の両方を行う会社）で、「クリック」部門が侵害を受け、その部門（E コマース）を廃止しました。そのほか、顧客からの抗議や苦情、B2B 関係の悪化、政府機関による調査など、あまり経験したくない結果も見られました。幸い、このような結果は希ですが、それでも「必ず一定間隔で起こる」と皆さんに注意しておくのが義務です。

また、実際にはデータ漏洩 / 侵害に遭っていない企業・組織でも、そのデータ漏洩 / 侵害による被害を受けることがよくあります。例えば、ペイメントカードのデータ漏洩 / 侵害では、窃取されたカード情報が不正に使用された場合、カードの発行者（顧客にカードを発行した銀行）が大きな損害を受けることがあります。データ漏洩 / 侵害の被害や結果を検討する場合、このような「下流効果」は無視されるのが普通です。

本節は、この辺で終了しますが（来年は分量を増やす予定です）、最後に「インシデントの影響の評価は、価値ある作業である」という信条をここに記します。データ漏洩 / 侵害の発生後、ほとんどの企業・組織は「正常な状態に戻る」ことを求め、侵害の結果（被害）に注目することはあまりありません。しかしながら、データ漏洩 / 侵害に遭ったということは、貴重な学習機会を得たということに他なりません。この機会を活用することで、発生したデータ漏洩 / 侵害の理解が進むだけでなく、そこで得られたデータを今後のリスク分析や意思決定に利用できます。

ご存じのように、VERIS ではデータ漏洩 / 侵害の影響分析も行えます。データ漏洩 / 侵害の影響に関する入力項目がいくつかあり、簡単に始められます。結果が返送されますので、参考資料としてご利用いただけます。

今は法律の時代です。ベライゾンの E ディスカバリー（電子情報開示）チームで業務に当たっている調査員によると、データ漏洩 / 侵害の発生後、ほとんど時を置かずに訴訟が始まるのが普通といいます。企業がデータ漏洩 / 侵害を受け、訴訟を検討している場合、直ちに法的保留通知を発行するのが実務上、最善策とされています。ただし、データ漏洩 / 侵害の性質と種類によっては、データ漏洩 / 侵害の後、すぐに法的保留通知を発行するより開示対応プロセスを開始するほうが適切なケースもあります。その場合、開示対応プロセスを開始し、続いてデータ管理者とデータ保管場所を決め、その後、法的保留通知を発行し、最後に各種プロセスを開始するという手順で作業を進めます。

開示プロセスにおける E ディスカバリーの重要性は近年、いっそう増しています。このような状況の中、企業のリーガルチームと IT チームは、自社の訴訟能力や法的な調査について十分に理解しておく必要があります。開示対応プロセスは信頼性と完成度の両方に優れていなければならず、このような開示対応プロセスを用いることで、開示要請に関連するコストや時間、リスクが軽減されるとともに、インシデントに対応する際のリスクも低くなります。また、開示対応プロセスが優れていれば、顧問弁護士は、インシデントと開示の両方に対応するという複雑な作業を体系的かつ効果的に推進できます。

現在、定義（文書化）済みの E ディスカバリープロセスが（ひとつも）なく、トレーニングもほとんど行っておらず、利用できる IT 技術も少なく、さらに経営幹部の支援がないため（この支援が何より重要です）、開示要請に効果的かつ効率的に対応できないという企業があまりにも多すぎます。企業は、サイクルタイムやコスト、リスクなどの軽減を真剣に考えているのであれば、完成度の高い開示対応プログラム（開示対応計画と開示対応チームに関する事項も含む）を用意し、いつでも使用できるようにしておく必要があります。ただし、このような開示対応プログラムを作成する前に、開示対応関連のスタッフやプロセス、IT 技術を総合的かつ客観的に評価することが不可欠であり、それで初めて既存のリソースを活用できるとともに、どこに見逃しや欠点があるかを理解できます。

データ漏洩 / 侵害報告書に関するご意見、ご質問は、大いに歓迎します。
ご意見やご質問は dbir@verizon.com までお寄せください。Facebook や Twitter（hashtag #dbir）もご利用いただけます。

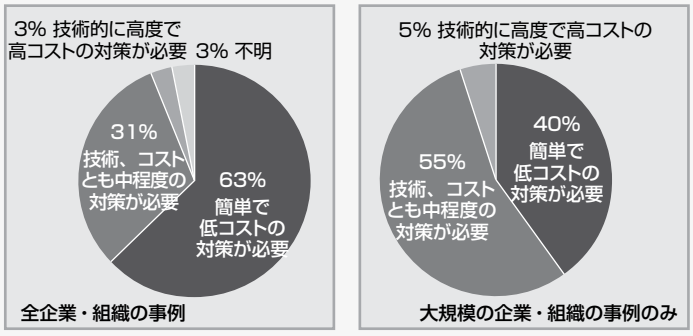
2012 年データ漏洩 / 侵害調査報告書：結論と推奨事項

本年は、新たな推奨事項をご紹介します。なお、環境保護グループとしては、リソースを大切にする義務があります。そのため、新作を紹介する前に昨年の「序文」を再利用し、下に掲載します。

> *「本調査報告書（DBIR）には推奨項目を記載してありますが、実効性の高いものを考案するのは年々難しくなってきています。考えてみればレポートの分析結果は、年ごとに徐々に変化し進化しますが、まったく新しくなったり一変したりすることは稀と言えるでしょう。推奨は、分析結果に基づいているのですから、分析結果が変わらなければ推奨措置も変わらないのは当然です。必要であれば、多数の推奨事項を盛り込んだリストを作り、提供することもできますが、このようなリストは他からも入手できるでしょう。弊社の関心は、数ではなくメリットにあります。」*

新たな推奨事項の後、「2009 年データ漏洩 / 侵害調査報告書（補足版）」の推奨事項を「再利用」して掲載します。内容と形式は、分かりやすくするため多少変更してあります。新作の説明は、二酸化炭素排出量（ページ数）が少なくなるようにできるだけ簡潔にしました。加えて本年は、調査員の出張費や証拠の発送費、無駄なコンピュータ処理も節約しました。ですから、本年は「環境保護バッジ」を頂戴する資格が十分あります。

図 48. 推奨される予防対策の種類で分類した場合のデータ漏洩 / 侵害の割合 *



* ベライゾンの事例データのみ

では、「新作」（新たな推奨事項）について説明します。本報告書では多数の企業・組織の状況を見ていきましたが、セキュリティに関するメッセージを受け取った企業・組織は多くはないようです。特に POS システムが一つ（またはいくつか）しかない小中規模の企業・組織が、このケースに該当します。次ページに保存用の切り抜き記事を用意しています。これは、中小規模の企業・組織向けに作成したものです。読者の皆様にお願いですが、このメッセージを切り抜いて POS を利用している行きつけのレストランや小売店舗、ホテルなどにお持ちいただき、配布いただくことが可能です。このメッセージはレストランなどが必要としているもので、読者の皆様の協力を通じてメッセージを普及させることができます。もちろん、レストランや小売店舗などだけでなく、ほかの企業・組織にとっても傾聴の価値があるメッセージです。メッセージの内容はシンプルですが、記載されていることが実践されれば、小中規模企業が遭遇している問題の大半が解決されるはずであり、これは手元の証拠が示しています。

「新作」の後に「再利用」の推奨事項を記載してあります。いずれも、大規模の企業・組織向けの推奨事項です（ただし小中規模の企業・組織にも有効です）。本報告書で見てきたように、データ漏洩 / 侵害に関して大規模の企業・組織が抱えている問題は、小中規模の企業・組織が抱えている問題と色々な点で異なります。したがって、当然ながら問題解決の方法も両者で異なります。本節では、小中規模の企業・組織用の対策（メッセージ）と大規模の企業・組織用の対策（後掲の表の対策）を分けて掲載してありますが、これは上記の理由によるものです。

次ページに保存用の切り抜き記事を用意しています。これは、
中小規模の企業・組織向けに作成したものです。読者の皆様にお願いですが、
このメッセージを切り抜いて POS を利用している行きつけのレストランや
小売店舗、ホテルなどにお持ちいただき、配布いただくことが可能です。

POS のセキュリティと対策

このカードは、貴店がお客様の顧客情報やクレジットカードなどのペイメント（決済）カード情報を守るための対策、特に POS のセキュリティと対策についてお知らせするものです。貴店がハッカーからこれらの情報を守秘されることを心から願っております。

「ハッカーに情報を盗まれるようなことは絶対にない」ということは事実ではなく、ほとんどの攻撃が小規模な店舗や企業を狙ったものなのです。しかし、大半の攻撃は、比較的簡単な対策をいくつか講じるだけで防止できます。お客様の支払いを POS システムで処理しているお店は、データ漏洩 / 侵害を受けることが非常に多く、ベライゾンは今までそのような事例を数千件、調査してきました。下記は、その調査結果や専門的な経験をもとにして弊社が独自に考案した対策です。セキュリティご担当者、または経営者様にこの対策をお伝えください。

✓ **すべての POS システムの管理者パスワードを変更しましょう。**
- ハッカーはインターネット上で常時、簡単に解読できるパスワードを探しています。

✓ **ファイアウォールをインストール、またはリモートアクセスサービスにアクセスコントロールリストを設置しましょう。**
- 上の対策によりハッカーはお店のシステムに侵入できなくなり、その結果、簡単に情報が盗まれることはなくなります。

以上に加えて、次の対策も実施するとさらに効果的です。
- POS システムを使ってウェブを閲覧することはやめてください（インターネット上で閲覧と同様の操作をすることも控えます）。
- POS 環境が PCI DSS に準拠しているかどうか確認してください（POS のベンダーにお聞きください）。

POS システムの管理をサードパーティベンダーに依頼している場合、上記の対策が実施されているかを確認します。また、できれば対策を文書化したものを入手してください。以上の比較的簡単な対策を講じることで、データ漏洩 / 侵害が発生した場合の金銭的損害や時間の浪費、その他、お店とお客様が遭遇する可能性のある問題を事前に防止できます。

詳細については、www.verizonbusiness.com/jp/Products/security/dbir/ をご覧ください（なお、POS からアクセスするのは危険ですので控えてください）。

もう忘れてしまったという読者のために付記すると、「2009 年データ漏洩 / 侵害調査報告書（補足版）」には、当時の主な脅威アクションについて詳しく書かれていました。具体的には、脅威アクションの概要のほか、その脅威アクションに関連する脅威因子や資産、特徴、徴候、対策、具体的事例などが記載されていました。以下、本年の推奨事項を紹介しますが、本年は主に大規模企業向け・組織向けの推奨事項を記載する関係から、上記の事項を「徴候」と「対策」の 2 つに絞りました。

- **徴候**:脅威アクションが現在発生していること、もしくは既に発生したことを示す徴候、またはその徴候を検出できるツールや方法。
- **対策**：脅威アクションの防止や予防、または脅威アクションの発生後の復旧・対応（封じ込め）に有効な措置、手段。

以下、本年の推奨事項を列挙します。記載してある脅威アクション（タイプ）は本報告書の「脅威アクション」の節の表 7 と 8 から選択したもので、いずれも大規模企業向け・組織の事例のみの場合の上位 10 位までのタイプ（攻撃手法）です。また、脅威アクションの攻撃手法をすべて記載することはやめ、紙幅の節約のため代表的な脅威アクションだけに整理しました。結局、次の 7 種類について推奨事項を掲載しました。

- キーロガー、盗んだログイン情報の使用
- バックドアとコマンド コントロール
- タンパリング
- プリテキスティング
- フィッシング
- ブルートフォース
- SQL インジェクション

ハッキング：盗んだログイン情報の使用	
概要	攻撃者が、盗んだログイン情報（有効な認証情報）を使って、保護されているコンピュータや機器にアクセスすること。
徴候	システムにマルウェアがないかどうかのチェック、ユーザーの行動の異常に関する分析（たとえば、通常とは異なる場所で、または通常とは異なる時間にログオンを行っていないか）、「直前のログオン」バナーの利用（不正アクセスの検出が可能）、権限が必要な管理作業（サードパーティによる管理作業も含む）の監視により徴候を発見できます。
対策	2 要素認証を使用します。盗まれた可能性があると思われるパスワードを変更します。機器を利用できる時間を制限します。IP ブラックリスティングを行います（業務に直接関係のないアドレスが多い場合、IP ブラックリスティングで一括してアドレスをブロックします）。管理者による接続を制限します（内部の特定の場所からのみ接続できるようにします）。認証情報の盗難の防止については、「キーロガーとスパイウェア」、「プリテキスティング」、「フィッシング」の説明を参照してください。

マルウェア：バックドア、コマンド&コントロール ハッキング：バックドアまたはコマンド&コントロールチャンネルの不正使用	
概要	コンピュータウィルスに感染したコンピュータに外部からアクセス、またはコンピュータを制御することを目的とした攻撃手法。バックドアプログラムとコマンド／コントロールプログラムはどちらも、コンピュータ上の通常の認証メカニズムやセキュリティコントロールを迂回する機能があり、また秘密裏に動作するように設計されています。
徴候	コンピュータの動作やパフォーマンスが異常になり（マウスを触っていないのに勝手にカーソルが動いてファイルを操作しているように見える）、またネットワークの動作も異常になります。徴候のチェック方法としては、IDS/IPS（非カスタマイズバージョン）の使用、レジストリの監視、プロセスの監視、定期的ログ監視、コンピュータ上にマルウェアが存在しないかどうかの確認、アンチウィルスが無効になっていないかのチェックなどがあります。 調査対応チームがマルウェアの調査を行う場合、通常、アクティブのプロセスをチェックします。また、コンピュータの全内容を作成日または修正日を基準にしてソートした後、リストを出力します。この作業により、Windows¥system32 ディレクトリやユーザーの暫定ディレクトリに悪意のファイルが見つかることがよくあります。
対策	出口フィルタリング（この攻撃手法の場合、通常とは異なるポートやプロトコル、サービスを介してデータが送信されるのが一般的です）、アウトバウンドトラフィックに対するプロキシの使用、IP ブラックリスティング（業務に直接関係のないアドレスが多い場合、IP ブラックリスティングで一括してアドレスをブロックします）、ホスト IDS（HIDS）、整合性監視、管理者権限を持つユーザーの数の制限、パーソナルファイアウォール、データ漏洩防止ツール（DLP）、アンチウィルスとアンチスパイウェア（アンチウィルスは、カスタマイズすると効果が弱くなります。アンチウィルスベンダー 40 社の製品を試してみましたが、バックドアの検出に成功したのは、その中の 1 つだけでした）、ウェブ閲覧ポリシーの強化。

物理：タンパリング	
概要	タンパリングとは、資産の通常の状態または機能を無許可で改ざんまたは阻害することをいいます。ソフトウェアやシステム設定の改ざんではなく、機器などを物理的に改ざんすることです。
徴候	予定がないのに機器の保守点検が行われている。傷がある、接着剤を使った跡がある、カメラに穴があいている、キーパッドの上に何かのせられているなど。タンパリングは発見が困難です（オーバーレイスキーマーは機器の上に乗せられているため注意すれば発見できますが、内部タンパリングは一般に外部からは見えません）。タンパリング防止シールが破れている。心当たりのないブルートゥース信号が長い間、続くのも徴候の一つです。 ATM やガソリンスタンドに取り付けられたスキマーは、通常は数時間後に取り外されます。数日や数週間、設置されたままになっていることはありません。

物理：タンパリング	
対策	タンパリングを発見するように従業員を指導し、顧客にも注意を呼びかけます。定期的に（勤務交代の際など）、タンパリングの対象となる機器を点検します。カードと PIN（暗唱番号）が必要な機器の場合、通常は両方が標的になります（「徴候」を参照）。チェックを行うときは、その点（スキマーが 2 つないかどうかなど）に注意します。 スタッフ全員に研修を行い、保守点検作業について詳しく説明します。保守点検作業のスケジュールのほか、保守員や保守ベンダーの入館許可についても説明します。 機器を購入する際、機器にタンパリング防止技術・機能を搭載するようにベンダーに依頼するか、タンパリング防止装置（例えばタンパースイッチ。プラスチックで覆われた電子機器で、メモリーの初期化が可能）付きの POS 装置や PIN 入力装置だけを購入します。

キーロガー / フォームグラバー / スパイウェア	
概要	いずれもマルウェアで、ユーザーが行う操作の監視やログ、また入力したデータの収集を目的として設計されています。大規模な攻撃に先立ち、ユーザー名やパスワードの収集に使用されるのが普通です。また、侵害した POS 機器からペイメントカード情報を盗むのにも使われます。ほとんどの場合、秘密裏に実行されるため、ユーザーは気がつきません。
徴候	通常、コンピュータの動作やパフォーマンス、ネットワーク動作が異常になります。徴候のチェック方法としては、IDS/IPS（非カスタマイズバージョン用）の使用、レジストリの監視、プロセスの監視、定期的ログ監視、コンピュータ上にマルウェアが存在しないかどうかのチェック、物理的改ざんがないか（見慣れない機器が取り付けられていないか）の確認などがあります。認証（ログイン）情報の不正使用のチェックについては、「盗んだログイン情報による不正アクセス」の説明を参照してください。 調査対応チームがマルウェアの調査を行う場合、通常、アクティブのプロセスをチェックします。また、コンピュータの全内容を作成日または修正日を基準にしてソートした後、リストを出力します。この作業により、Windows¥system32 ディレクトリやユーザーの暫定ディレクトリに悪意のファイルが見つかることがよくあります。
対策	管理者権限を持つユーザーの数を最小限にします。防御対策としては、コードサイニング、ライブブート CD、ワンタイムパスワード、アンチウィルスとアンチスパイウェア、パーソナルファイアウォール、ウェブコンテンツフィルタリング、ブラックリスティング、出口フィルタリング（この攻撃手法の場合、通常とは異なるポートやプロトコル、サービスを介してデータが送信されるのが一般的です）、ホスト IDS（HIDS）の使用・適用のほか、整合性監視、ウェブ閲覧ポリシーの強化、セキュリティ意識強化トレーニングの実施、ネットワークのセグメント化などがあります。

プリテキスティング（ソーシャルエンジニアリング）	
概要	ソーシャルエンジニアリングとは、攻撃者が何らかの状況を用意し、目標（人間）を説得したり巧みに操ったり、もしくは策謀し何らかの行為を行わせたり、情報を漏洩させる行為です。「ヒューマンハードウェアのバグ」を悪用した脅威アクションで、残念ながらパッチは存在しません。
徴候	この攻撃手法は、人間の弱さを悪用し、技術的な警戒メカニズムを迂回するという発想を基礎としているため、発見は非常に難しいというのが現状です。おかしな話を持ちかけられたり、一般的な作業から逸脱した作業を要求されたり、情報の提供や何らかの行為の実行を求められ、それが会社のポリシーに違反するような場合が、この攻撃手法の徴候です。電話や訪問者、電子メールの記録のチェックも徴候を発見するのに有効です。

プリテキスティング（ソーシャルエンジニアリング）	
対策	セキュリティ意識強化トレーニングを実施し、また明瞭なポリシーと規則を策定します。ポリシーに違反する行為があった場合、すぐに指摘し、ポリシーを厳格に遵守するように指導します。ソーシャルエンジニアリングに注意し、その疑いがあったには、必ず報告するように指導します。普通でない依頼や要請を受けた場合、信頼できる社員や部署に相談するように指示しておきます。社員名簿（その他、類似の情報の記録）を公開しないようにします。

ブルートフォース（総当たり）攻撃	
概要	認証が成功するまで、異なるユーザー名とパスワードの組み合わせを何度も繰り返す自動化プロセス。
徴候	定期的ログ監視、また、何回も失敗しているログイン試行がないかどうか（とくにユーザー名やパスワードを変えて繰り返しログインを試行していないか）をチェックすることで徴候を確認できます。何回かログインを試したがログインできないという電話がサポート窓口にかかってくるのも徴候です。
対策	ユーザーが使用できるパスワードを強固なものに限定します（パスワードの最低長を指定したり、簡単なパスワードを受け付けないようにしたり、またパスワードの入力可能回数を少なくします）。パスワード閉鎖時間（ログインが何回か続けて失敗した後、再度パスワードを入力してログインを試行できるまでの時間）を長くします。パスワード破りテストを行います。アクセス制御リストを強固にします。管理作業のためのログインを制限します（内部の特定のコンピュータからのみ、管理作業のログインが可能なようにします）。2 要素認証を使用します。CAPTCHA（画像の中の文字を入力を要求）を使用します。

SQL インジェクション	
概要	SQL インジェクションは、ウェブページとバックエンドデータベースとの間の通信を利用する攻撃手法です。攻撃者は、ウェブページの入力フィールドを使って、データベースに対してコマンド（特殊な SQL 文）を実行します。
徴候	定期的ログ監視（とくにウェブサーバーとデータベースの監視）と IDS/IPS で徴候を発見できます。
対策	高度なセキュリティ環境での開発、入力の検証（エスケープ、ホワイトリスティングなど）、パラメータ化プロシージャやストアドプロシージャの使用、データベースアカウントの権限の制限・最小化、不要なサービスの削除、システムバードニング、データベースエラーメッセージのクライアントへの出力の無効化、アプリケーションの脆弱性のチェック、侵入テストの実施、ウェブアプリケーションファイアウォールの設置などが対策として有効です。

デフォルトの認証情報を使った不正アクセス	
概要	既定（初期設定）のユーザー名とパスワード（第三者が入手できるようなユーザー名とパスワード）によって保護されているコンピュータや機器に、攻撃者が不正にアクセスすること。
徴候	ユーザーの行動の分析（たとえば、通常とは異なる時間や場所からログオンしていないか）、権限が必要な管理作業（サードパーティによる管理作業も含む）の監視、「直前のログオン」バナーの利用（不正アクセスの検出が可能）により徴候を確認できます。
対策	既定の認証情報の変更（アプリケーションなどの導入前）、既定のアカウントの削除または無効化、既定のパスワードが使用されていないかのチェック（導入後）、パスワードの定期的切り替え（既定のパスワードの強制変更に有効）、リモート管理サービス（とくにサードパーティが使用しているリモート管理サービス）のインベントリーの作成を行います。サードパーティに業務を委託する場合、契約書（パスワードに関する事項を記載）や共同管理作業に関する取り決めを作成し、また、サードパーティが既定のパスワード（サードパーティがサポートしている資産のパスワード）を使用していないかをチェックします。

フィッシング（類似のバリエーションを含む）	
概要	フィッシングは、ソーシャルエンジニアリングの一種で、電子通信手段（電子メールが一般的）を使って相手をだまし情報を不正に入手しようとする手法です。ほとんどの場合、電子メールなどの差出人は信頼できそうな人間や会社、団体で、内容もまともに見えます。詐欺ウェブサイトや「おとり」があるのがごく普通です。
徴候	フィッシングは、その性質上、人間の弱さを利用する手法であるため、発見は簡単ではありません。普段は滅多に来ないような不要な電子メールや手紙、情報の提供を含め会社のポリシーに反した行為の要求、通常とは異なる作業の要求、辻褄の合わない話、偽の緊急通報・連絡はいずれもフィッシングの徴候です。電子メールのログのチェックも徴候の確認に有効です。
対策	セキュリティ意識強化トレーニングを実施し、明瞭なポリシーと規則を策定します。ポリシーに違反する行為があった場合、すぐに指摘し、ポリシーを厳格に遵守するように指導します。電子メールの管理や設定に関する規則（パスワードの変更手順など）を作ります。フィッシングと思われるような電子メールなどを受け取ったら必ず、報告するように指導します。普通でない依頼や要請を受けた場合、信頼できる社員や部署に相談するように指示しておきます。HTML メールをテキストメールで受信するように電子メールクライアントプログラムを設定します。アンチスパムツールを使用します。電子メールの添付ファイルにウイルスが存在しないかどうかチェックし、またフィルタリングを行います。

データ漏洩 / 侵害報告書に関するご意見、ご質問は、大いに歓迎します。
ご意見やご質問は dbir@verizon.com までお寄せください。Facebook や Twitter（hashtag #dbir）もご利用いただけます。

付録 A：各脅威アクションの比較検討

本年は、ここで少し時間を割いて脅威アクションをさらに掘り下げて検討することにします。本報告書では、表 7 に上位 10 位までの脅威アクション（タイプ）、表 8 には大規模の企業･組織を対象に同様の脅威アクションを記載しましたが、この部分をもう少し深く見てみます。具体的には、2011 年のデータ漏洩 / 侵害事例で見られた各脅威アクションを比較しながら、詳しく検討することにします。

脅威アクションをよく分析してみると、脅威因子は、最小限の労力と経費で最大限の見返りを得ようとしているようです（これは誰でも同じです）。脅威因子は知的で順応性もありますが、データを分析してみると、必要な範囲でのみ知的であり順応性があるということが分かりました。

本報告書の図 18 には 7 種類のカテゴリーの脅威アクション（ハッキング、マルウェア、ソーシャルなど）を記載してあり、カテゴリーにはそれぞれタイプがいくつかあります（VERIS で入力できます）。インシデント（データ漏洩 / 侵害）にはいずれも脅威アクションが少なくても 1 つ関与していますが、複数の脅威アクションが関与しているインシデントも少なくありません。図 49 はインシデント当たりの脅威アクションの数を示したもので、この図を見ると複数の脅威アクションが関与しているインシデントが多いことが分かります。

図 49. データ漏洩 / 侵害当たりの脅威アクションの数

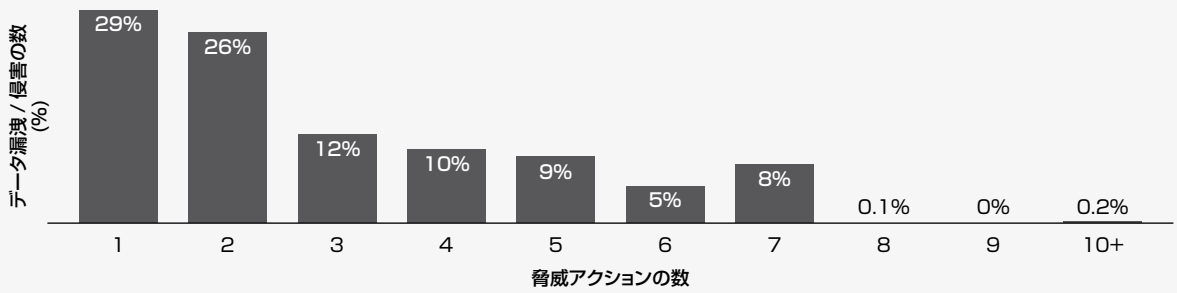


図 49 にあるように、脅威アクションが 1 つのデータ漏洩 / 侵害は全データ漏洩 / 侵害の 29%、脅威アクションが 2 つのデータ漏洩 / 侵害は 26%を占めています。この図により、脅威アクションが 1 つまたは 2 つのデータ漏洩 / 侵害事例が全事例の半分以上を占めていることが分かります。データ漏洩 / 侵害当たりの脅威アクション数の平均は 2.9 で、大規模の企業・組織の事例のみの場合、平均は 2.75 です。これは検討に値する数値ですが、ここでは先を急ぎ、脅威因子に順応能力がどの程度あるか（またはないか）を見ていくことにします。

脅威アクションが 1 つのデータ漏洩 / 侵害

表 15 は、脅威アクションが 1 つのデータ漏洩 / 侵害だけを対象にしたときの分析結果ですが、この結果は、通常のデータ漏洩 / 侵害（脅威アクションの数は考慮せず）の場合（表 7）とは異なります。脅威アクションが 1 つのデータ漏洩 / 侵害とは、攻撃者と標的のデータの間にある「壁」（通常は複数）のうちひとつだけが突破されたインシデントをいい、このようなインシデントをシングルイベントインシデントと呼んでいます。例えば 2011 年の場合、SQL インジェクションが関係したデータ漏洩 / 侵害事例のうち、その 60%がシングルイベントインシデント、つまり最初の SQL インジェクションでデータが窃取され（場合によっては侵入だけで窃取はなし）、その時点で侵害が終了したインシデントでした。シングルイベントインシデントは数秒で終了することが多く、早いときには数ミリ秒で終了することもあります。

注意していただきたいのは、表 15 に記載されている 11 種類の脅威アクション（タイプ）は、全データ漏洩 / 侵害事例を対象としたときの上位 11 位ではないということです。この表は、全事例の中から脅威アクションが 1 つのデータ漏洩 / 侵害事例を抽出し、その中で使用頻度の多かった脅威アクションを上から順に並べたものです。VERIS では全部で 150 種類以上の脅威アクション（タイプ）が定義されていますが、脅威アクションが 1 つのデータ漏洩 / 侵害事例（240 件）の場合、脅威アクションは 11 種類にすぎないことが表 15 で分かります。また、表 15 では、上位 5 位までの脅威アクションのデータ漏洩 / 侵害が全体の 89%を占めていることが見て取れます。

表 15. 脅威アクションが 1 つのデータ漏洩 / 侵害で使われていた主な脅威アクション

順位	脅威アクション（タイプ）	カテゴリー	全企業・組織の事例	大規模の企業・組織の事例のみ
1	デフォルトまたは推測可能な認証情報の悪用	ハッキング	104	0
2	タンパリング	物理的脅威	52	5
3	プリテキスティング（従来の一般的ソーシャルエンジニアリング）	ソーシャル	24	3
4	ブルートフォース (総当たり攻撃) と辞書攻撃	ハッキング	21	0
5	SQL インジェクション	ハッキング	12	1
6	システムアクセス権 / 権限の不正使用	ハッキング	12	3
7	盗んだログイン情報の使用	ハッキング	5	2
8	不十分な認証の悪用（ログイン不要など）	ハッキング	5	0
9	情報の公開に関する過失	過失	3	3
10	設定ミス	過失	1	1
11	詐取、スキミング、その他の類似詐欺行為	不正使用	1	0

脅威アクションが 2 つ以上のデータ漏洩 / 侵害

続いて、脅威アクションが 2 つ以上のデータ漏洩 / 侵害に目を移すと、面白い傾向がいくつか見えてきます。「森の中の木」を見るため、脅威アクションが 2 つ以上のデータ漏洩 / 侵害事例についてそれぞれ、脅威アクションの対（ペア）を作りました（例えば、脅威アクションが 2 つのデータ漏洩 / 侵害では対は 1 つ、脅威アクションが 3 つのデータ漏洩 / 侵害では対は 3 つ、脅威アクションが 4 つのデータ漏洩 / 侵害では対は 6 つできます）。結局、脅威アクションの対は 4000 ほどでき、そのうちの 281 がユニーク（ほかに同じものがない対）でした。このような対をもとに作成したのが図 51 で、この図では、脅威アクションが 2 つ以上のデータ漏洩 / 侵害で、どのような脅威アクションの対が使用されたかを見ることができます。

図は見にくいかもしれませんが、黄色の小さい四角形が脅威アクションの対で、灰色の部分はその場所の対がなかったことを表し、これが全体の 96%を占めています。また、橙色と赤の四角形（数が多かった対）がいくつか見られます。この図は何らかの傾向があることを示しており、詳細に分析してみる必要があります。以下、検討を始めますが、ここでは紙幅の関係から目の保養程度に留め、詳細は後日にブログで説明することにします。

図 50. 脅威アクションの対の累積分布

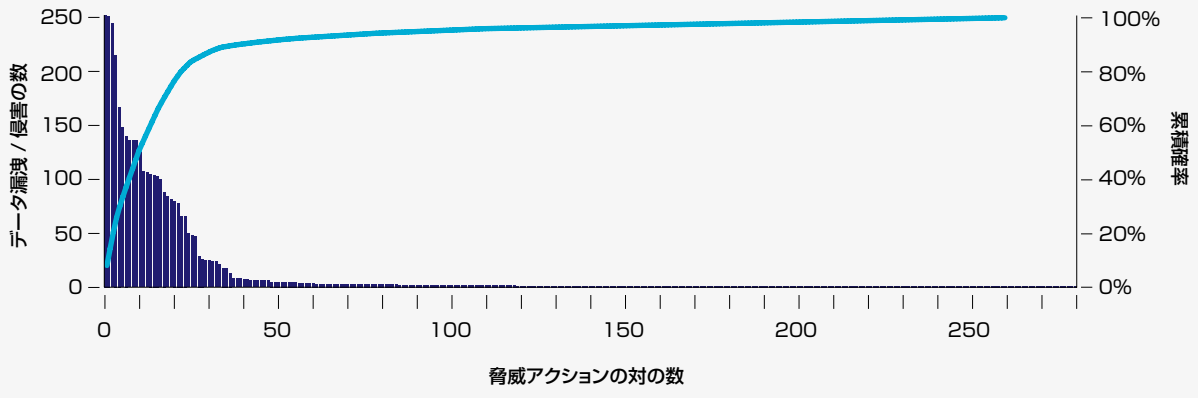


図 51. 脅威アクションの対

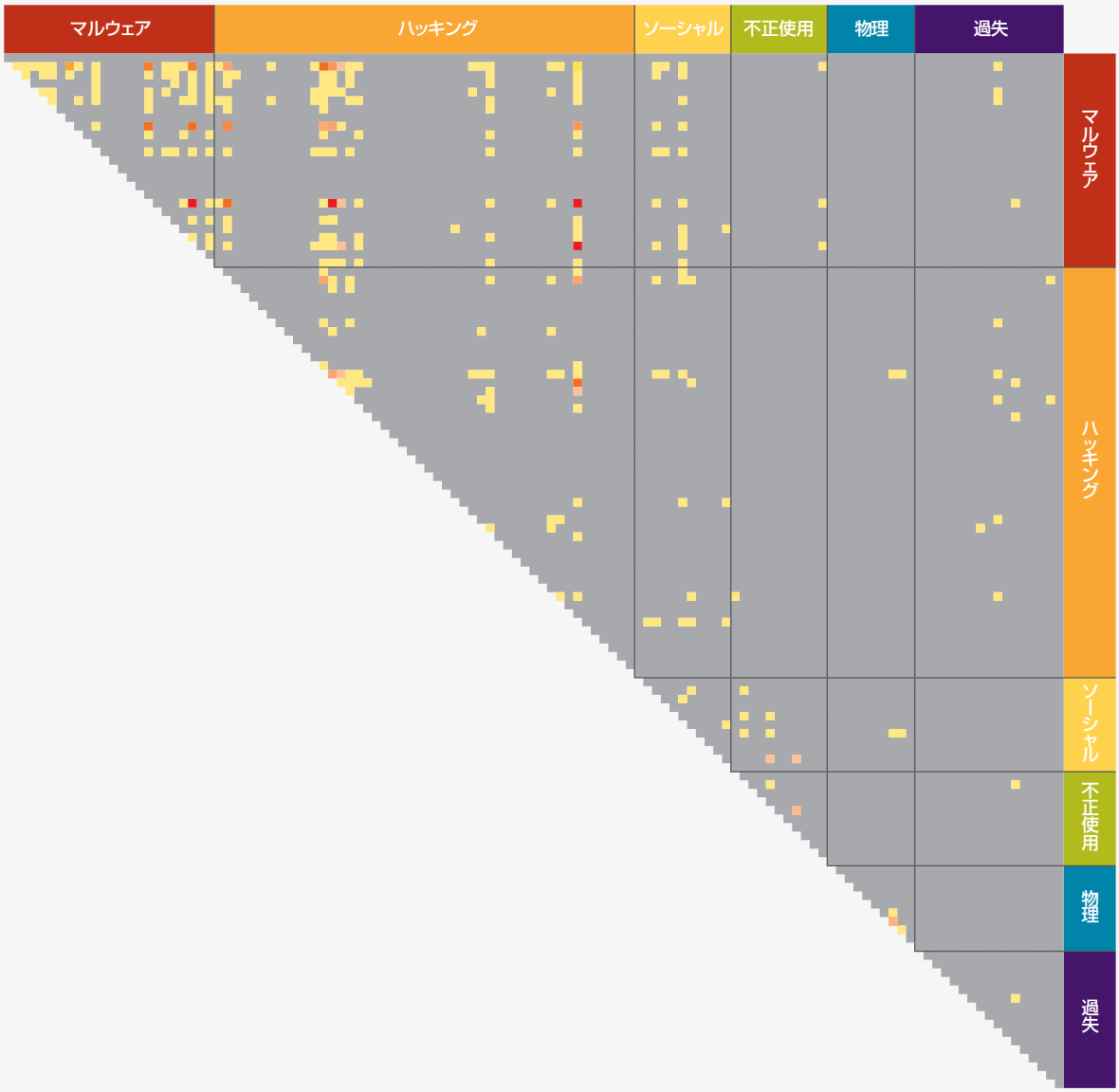


図 50 の紺色の縦棒はそれぞれ、何らかの脅威アクションの対が使用されたデータ漏洩 / 侵害の数を表しています。例えば、2011 年の場合、マルウェアの「キーロガー」（タイプ）とハッキングの「盗んだログイン情報の使用」（タイプ）の対がもっとも使用頻度が高く、この対は全データ漏洩 / 侵害事例の中の 252 事例で使用されていました。図の左端の紺色の縦棒がこの対を示しており（252 事例）、その右には他の脅威アクションの対が順に並び、対が使用された事例の数（縦棒）は次第に少なくなっています。図 50 の水色の曲線は、対の累積確率を表しています（格好よく言えば「累積分布関数」）。水色の曲線は 25 番目の対の付近で水平に移行しており、したがって上位 25 位までの対に的を絞って検討するのが「セキュリティ的にお買い得」ということでしょう。

（以下の説明は、「なるほど」とうなずきながら読んでいただくと光栄です。）

表 16. 上位 25 位までの対に見られた脅威アクションの種類（タイプ）

マルウェア	キーロガー / フォームグラバー / スパイウェア（ユーザーの操作を記録）
マルウェア	外部のサイトや組織 / 個人にデータを送信
マルウェア	バックドア（リモートアクセス / 制御）
マルウェア	セキュリティコントロールの無効化または妨害
ハッキング	デフォルトまたは推測可能な認証情報の悪用
ハッキング	バックドアまたはコマンド&コントロールチャンネルの不正使用
ハッキング	ブルートフォース（総当たり攻撃）と辞書攻撃
ハッキング	盗んだログイン情報の使用

上位 25 位までの対を詳しく見てみると（上位 25 位までの対が非常に多く、約 4000 の対の 81%を占めています）、対を構成する脅威アクションは全部で 8 種類しかありません（表 16）。したがって 2011 年は、ほとんどの攻撃者が主にこの 8 種類の脅威アクションを使ったということになります。

言い換えると、何種類かの基本的な脅威アクション（例えば、ハッキングの基本的なタイプとマルウェアの基本的なタイプ）を組み合わせて攻撃を行った攻撃者が大半だったといえます。もちろん、複雑なマルウェアや高度なハッキング手法が使用された事例もありましたが、多かれ少なかれ、攻撃者の知性と順応性は、自分たちが必要とする範囲に限定されていました。これは言い方を若干変えて、「攻撃者の知性と順応性は、こちらが容認する範囲に限定されていた」と表現したほうが正鵠を得ているかもしれません。もちろん、攻撃者を容認し、その「本領」を発揮させるような事態にならないように注意しなければなりません。

大規模の企業・組織の場合、脅威アクションの対の傾向にはいくつか異なる点があります（なお、大規模の企業・組織の事例は非常に少なく、その点に留意して分析結果をお読みください）。まず、大規模の企業・組織では、マルウェアに属する脅威アクションが極めて多く、実際、マルウェアの対（どちらのタイプもマルウェア）が使われた事例は大規模の企業・組織の事例の 40%を占めていました。二つ目の相違は、フィッシングの対（マルウェアのタイプとの組み合わせ）が上位 25 位までに入り（対の種類は 3 つ）、また、ソーシャルのタイプが関連する対が使われた事例が大規模の企業・組織の事例の 84%を占めていたことです。最後に、大規模の企業・組織の場合、脅威アクションの対の種類が多く、内容（対を構成する 2 つの要素）が同じ対は 36%しかなかった点が異なります（全企業・組織の場合、内容が同じ対が 93%を占めます）。上記の 3 つの相違は、攻撃者が大規模の企業・組織に対して全力を尽くしていないことが原因とも考えられますが、それより、小中規模の企業・組織に対して繰り返し自動化された攻撃を仕掛けるという傾向が顕著になっていることが主な原因と思われます。

以上、脅威アクションの対について検討してきましたが、見るべき点がもう少しあります。具体的には、何らかの脅威アクションのタイプがどのような頻度で使用され、また、そのタイプが別の脅威アクションのタイプとどのような頻度で併用されたかを分析し、その結果を下に順に記載しました。酒席で同僚をなるほどと言わせたい、異性との話を盛り上げたい、エレベーターで経営幹部と乗り合わせ、間が持たないときの話のネタがほしいという方は、じっくりお読みください。

マルウェアを使ってデータが窃取されたデータ漏洩 / 侵害事例のうち（対の一方が何らかのマルウェア）、対のもう一方がキーロガーだった事例が 98%を占めました。これは、ほとんどのキーロガーが、収集したデータを送信するように設定（送信機能を搭載）されていたことを表しています。対の一方がキーロガーである対によってデータが窃取された事例は 251 件ありましたが、8 件を除いて他の事例はいずれも、対のもう一方は「盗んだログイン情報の使用」でした（これは、脅威アクションが 2 つの事例に加えて、脅威アクションが 3 つの事例も使って分析した結果です）。

対の一方がバックドアのインストール（マルウェア）のデータ漏洩 / 侵害事例のうち、対のもう一方がバックドアの使用（ハッキング）だった事例が 98%を占めていました。本報告書ではデータ窃取が確認されたデータ漏洩 / 侵害だけを扱っていることを考慮すると、この割合はもっと多いかもしれません。いずれにしても、この割合は非常に大きく、たまたまインストールされているというより、そこら辺中バックドアだらけというのが実情のようです。そのせいで、バックドアに慣れてしまったのかもしれません（ネットワークをチェックする場合、このことに注意しなければなりません）。

統計に関する説明を読み、たとえ統計が完璧だとしても、その説明を信じる人は 73.6%です。過去の報告書では、そうだったかもしれません。ただし、本報告書の統計は出色の出来と言えます。

対の一方が「盗んだログイン情報の使用」のデータ漏洩 / 侵害事例は 276 件あり、そのうち、対のもう一方がキーロガーだった事例は 91%に及びました。キーロガーと盗んだログイン情報の使用の組み合わせが非常に多いことは、

上の最初の説明でも触れました。なお、本報告書では確認済みのデータ漏洩 / 侵害だけを扱っているため、この割合はさらに多い可能性があります。いずれにしても「衝撃と畏怖」の事実であり、学ぶべきことは少なくありません。

「デフォルトまたは推測可能な認証情報の悪用」が使われた事例（379 件）のうち、キーロガーがインストールされていた事例は 57%、またバックドアが存在した事例は 47%でした。なお、脅威アクションが「デフォルトまたは推測可能な認証情報の悪用」だけだった事例は、104 件ありました。

バックドアがインストールされていた事例は 174 件あり、そのうちの 61%でキーロガーが使われていました。これは驚天動地とまでは行きませんが、マルウェアが色々な用途に使われていることを示しており、注目すべき点のひとつです。

以上をまとめると、上の分析は想像の域を出ませんが、それでも今後の研究の基本資料として重要な事項もいくつかあります。例えば、攻撃者の攻撃のコストを引き上げるような対策をとることが大事である、と今まで何度も指摘してきました。ところが、上述の分析結果は、攻撃のコストは今や大半のデータ漏洩 / 侵害事例で決して高くないことを示しています。このような状況を変え、再度、攻撃のコストを引き上げるような努力が必要です。もうひとつ考慮しなければならないのは、パターン認識を使ってインシデントを検出する技術です。ヒューリスティックやパターンマッチングを利用した監視技術も一部では使用されていますが、インシデントの検出は、ほとんどの場合、一次元痕跡（単純証拠）に依存しているのが現状です。攻撃の手順や内容、関係、依存性などを今以上に理解する必要があり、理解の度合いが深まるほど、眼前で発生しているデータ漏洩 / 侵害を正確に認識できるようになります。

上記のような分析については、ブログ（verizon.com/enterprise/securityblog）で更に詳しく説明する予定です。また、この種の分析は、今後も機会を見ながら続けようと考えています。

データ漏洩 / 侵害報告書に関するご意見、ご質問は、大いに歓迎します。
ご意見やご質問は dbir@verizon.com までお寄せください。Facebook や Twitter（hashtag #dbir）もご利用いただけます。

付録 B：USSS の事例データに見られた大規模「産業化」サイバー犯罪

2008 年 4 月、ある銀行で詐欺の調査に当たっていた捜査官から、アメリカ合衆国シークレットサービスに状況報告が入りました。報告によると、その銀行のデビットカードの情報が多数盗まれ、盗まれた場所はニューイングランドのフランチャイズレストランということでした。この事件の後、カード情報を使った詐欺行為がヨーロッパで発生し、手口は白いプラスチックカード（偽造カード）を使って ATM などで取引をするというものでした。

シークレットサービスの捜査官が何人かフランチャイズレストランに赴き、オーナーや支配人のほか、従業員から聞き取り調査を行い、レストランではカードによる支払いをどのように処理しているか、また誰が支払い処理を担当しているかなどを確認しました。この調査より、POS サーバーがファイアウォールなしでインターネットに接続されており、アンチウイルスもインストールされていないことが分かりました。また、レストランの従業員は、システムを使ってインターネットにアクセスし、自分のウェブメールをチェックすることを許可されていました。POS サーバーを調べたところ、キーロギングプログラム（キーロガー）が発見され、このプログラムによってペイメントカードの情報が捕捉されていました。捕捉されたカード情報は、フロリダのウェブホスティング会社が所有し、その会社に設置されているサーバーのひとつに送られていました。残念なことに、そのウェブホスティング会社はログの記録と保管はあまり丁寧に行っておらず、そのためログは助けにはなりませんでした。

その後、あるクレジットカードプロバイダーからシークレットサービスに連絡が入り、連絡によるとカード詐欺が発生しているということでした。今回の詐欺の発生場所は、トルコやブルガリア、オーストリアなど、ヨーロッパの国々でした。カード情報が盗まれた場所は、最初に侵害が発生したレストランではなく、フランチャイズは同じだが別のレストランのようだということです。捜査官がそのレストランに行き POS サーバーを調べたところ、今回もキーロガーが見つかり、そのほかピアツーピアプログラムとパスワード解析ツールも発見されました。POS サーバーをさらに詳しく調べてみると、ログイン情報は、上記のウェブホスティング会社が使用しているものであることが分かりました。

一方、ある会社で同じような POS 侵入事件が発生し、その会社をシークレットサービスの捜査官が捜査した結果、上記のウェブホスティング会社のサーバーにカード情報が送られており、ログイン情報も同じでした。この証拠をもとに、そのサーバーの連邦捜査令状をとって捜査してみると、このフランチャイズに属する米国中のレストランでデータ漏洩 / 侵害が発生していることが明らかになりました。

その後、フロリダのウェブホスティング会社からシークレットサービスに連絡が入りました。この会社は、フランチャイズの各レストランのペイメントカードの処理を一手に引き受けていました。ウェブホスティング会社の話によると、フロリダのあるレストランで POS 侵入事件が発生したため自分で調べたところ、そのレストランで捕捉されたカード情報は、そのウェブホスティング会社にあるサーバーに送られていたということでした。調査の結果、最初に侵害が発生したレストランのほか、そのフランチャイズの 25 軒のレストランがデータ漏洩 / 侵害を受け、また攻撃者は同じでログ情報も今まで使われていたものと似ていることが分かりました。

シークレットサービスでは、フランチャイズの本部と連携してデータ漏洩 / 侵害の経路と広がりを調査しました。調査の結果、フランチャイズの企業ネットワークには侵入されていないことが分かりました。したがって、攻撃者はリモート管理サービスを使用し、インターネットを介して各レストランにそれぞれ別個に侵入したものと思われます。また、攻撃者は、アクセスに成功すると直ちにキーロギングプログラムをインストールし、ペイメントカード情報を捕捉していることが判明しました。

結局、フランチャイズの約 50 軒のレストランがデータ漏洩 / 侵害を受け、またウェブホスティング会社にある数台の FTP サーバーはいずれもログイン情報が類似していました。数台の FTP サーバーを調べて行くうちに、このフランチャイズ以外の会社でも POS 侵入が発生していることが次第に分かってきました。

一方、カーネギーメロン大学の CERT でも分析を進めており、その結果、東ヨーロッパの某国から不審な処理が実行されていることが判明しました。CERT ではまた、キーロガーファイルの取り出しに使われている IP アドレスが某民間企業のサーバーの IP アドレスであることを突き止めました。シークレットサービスは、その民間企業の同意を取り付け、そのサーバー（侵害されたサーバー）の監視を行いました。監視の結果、そのサーバーを通じて別の数台の FTP サーバーが見つかり、FTP サーバーはいずれもフロリダのウェブホスティング会社にある FTP サーバーでした。また、数台の FTP サーバーで受信されたトラフィックは、最初に侵害が発見された同社の FTP サーバー（最初に侵害されたレス

トランからカード情報が送信された FTP サーバー）で受信されたトラフィックと類似しており、ログイン情報も似ていました。この数台の FTP サーバー、また民間企業のサーバー（侵害されたサーバー）で受信されたトラフィックを調べてみると、いずれの FTP サーバーからも東ヨーロッパの某国（CERT の分析で判明した国）に対して頻繁に接続が実行されていることが分かりました。さらに FTP サーバーを分析したところ、50 軒の加盟店が侵害されていることが判明しましたが、いずれの加盟店も最初に侵害が発見されたレストランのフランチャイズとは無関係でした。

また、上記の民間企業のサーバーのトラフィックを分析したところ、単なる中継サーバーではなく、それ以上の役目を果たしていたことが分かりました。つまり、このサーバーから収集した証拠を分析した結果、POS システムへの侵入に使われたツールや手法、窃取されたデータのほか攻撃者（複数）を特定でき、また標的は米国中の POS システムでした。ツールの中にはリモートデスクトッププロトコル（RDP）ツールもありました。攻撃者は、この RDP ツールを使って一定範囲の IP アドレスを自動的にスキャンし、RDP ポートがオープンしているコンピュータを発見しようとしていたようです。RDP ポートがオープンしているコンピュータが見つかると、可能性のあるユーザー名とパスワードを入力し、またはパスワード解析ツールを使用して POS システムへの侵入を試みていました。ハッキングツールのほか、ICQ 番号も見つかりました。リモートデスクトップサービスを介してサーバーにログインし、ICQ チャットクライアントを開始するという操作を行っていたのです。ウェブメールアカウントにログインし、ICQ でチャットしたり FTP サーバーからファイルを取り出すという処理も行っていました。

シークレットサービスの捜査官は、ウェブメールアカウントをいくつか割り出し、また容疑者の ICQ チャット記録も発見しました。その後、ウェブメールアカウントの捜査に必要な令状を取り、攻撃者グループの逮捕に乗り出しました。シークレットサービスでは、攻撃者グループが民間企業のサーバーに接続したときのデータとウェブメールアカウントを分析し、その結果、東ヨーロッパの某国（CERT の分析で判明した国）が浮かび上がりました。また、ペイメントカード情報の送信先の FTP サーバーを監視したり、ウェブメールアカウントの調査で侵害が明らかになったカードを追跡したりといった作業を行った結果、被害を受けた企業が徐々に明らかになってきました。

シークレットサービスは、東ヨーロッパにある支部や外国の法執行機関の協力の下で証拠を収集し、最終的に攻撃者の居住場所と実名を特定しました。攻撃者の中には、「コンピュータ犯罪」の犯人として自国で捜査を受けた経緯があり、また法執行機関にも知られていた者も何人かいました。

捜査の結果、レストランフランチャイズの店舗のうち 163 軒が侵害され、合計で 112,000 を超えるペイメントカードの情報が盗まれたことが分かりました。その後、ホテル、映画館、医療施設、ホームサーバー事業者、ピザ店、パン販売店、喫茶店などの小規模企業が標的となり、結局は 800 台以上の小売取引処理コンピュータシステムが侵害されたことが判明しました。損害は、現在のところ 2000 万ドルを超えています。

2011 年 5 月、連邦大審問は、4 人の東ヨーロッパ人をコンピュータ関連詐欺共謀罪、有線通信不正行為共謀罪、アクセスデバイス関連詐欺共謀罪で起訴しました。

その後、東ヨーロッパの法執行機関の協力により、容疑者のうち 3 人が逮捕されました。そのうち 2 人は、米国に入国しようとしたときにシークレットサービスの捜査官によって逮捕されました。残りの 1 人は、米司法省が発行した仮逮捕令状にしたがって東ヨーロッパの法執行機関が逮捕し、現在、米国への送還待ちです。

データ漏洩 / 侵害報告書に関するご意見、ご質問は、大いに歓迎します。
ご意見やご質問は dbir@verizon.com までお寄せください。Facebook や Twitter（hashtag #dbir）もご利用いただけます。

2012 年データ漏洩 / 侵害報告書における協力機関について

ベライゾン RISK チーム

ベライゾン RISK チームは、常に変化する RISK 環境の研究（R）、あらゆる形態のセキュリティイベントに対する調査と対応（I）、信頼性の高いデータと分析に基づくソリューションの開発（S）、知識の蓄積（K）を目的とするチームで、ベライゾン内部だけでなくお客様やセキュリティコミュニティとも連携して活動を行います。RISK チームには豊富な経験と専門知識があり、過去 10 年間に行ったインシデント対応業務は 1,000 件を超えます。中には、最大規模の侵害事件（報告済みの事件）の多くも含まれています。チームでは調査中、世界各国の政府・行政機関や法執行機関の関係者と定期的に接触し、チームが収集した事件の証拠を当該機関などに提供しました。提出した証拠は、起訴に持ち込むため準備資料として有用です。また、チームの調査で収集されたデータは非常に多く、このようなデータからはコンピュータ犯罪とデータ漏洩 / 侵害に関する興味深い傾向を窺い知ることができます。

オーストラリア連邦警察

オーストラリア連邦警察（AFP）サイバー犯罪オペレーション（CCO）調査チームの目的は、1995 年刑法典（Criminal Code Act 1995）第 10.7 条および第 10.8 条に規定されている犯罪行為の調査です。この種の犯罪行為としては、コンピュータへの侵入（悪意のハッキングなど）、悪意のソフトウェア（ウイルス、ワーム、トロイの木馬など）の作成と配布のほか、個人の財務情報を不正に取得したり扱ったりすること（アイデンティティ窃盗を含む）などがあります。上記の犯罪行為に関連するオーストラリア連邦警察（AFP）の活動は、主に次の 2 つです。

1. オーストラリア政府のシステムの保護
2. 国家の重要なシステムの保護（主に銀行・財務に関するシステム）

サイバー犯罪オペレーション（CCO）調査チームは、業界や政府の組織・機関と連携して作業を進めます。通常、サイバーセキュリティオペレーションセンター（CSOC）を介してオーストラリアインテリジェントコミュニティと協力して活動し、一方、攻撃が国際的な場合には国際法執行機関と連携して犯人の特定と攻撃の影響を軽減に努めます。

CSOC は政府に近い機関で、サイバー攻撃の脅威のほか、政府専用ネットワークや国家の重要なネットワークのセキュリティ状況の監視と確認を行います。また、高度なサイバー攻撃の特定と分析を行い、その結果に基づいて対応方法や必要な情報を政府に提供します。政府や民間部門のシステムやインフラがサイバー攻撃を受けた場合、その対応の支援も業務の一部です。

サイバー犯罪を調査する場合、一般に多数の課題に直面します。特に法律関連の問題は難しく、しかも裁判所に持ち込まれる起訴案件は増えており、法律の解釈と適用も徐々に変化しているため尚更です。サイバー犯罪オペレーション（CCO）調査チームでは、法曹界向けの研修プログラムを作成し、実施していますが、これまでの評判は上々です。

オランダハイテク犯罪ユニット

オランダハイテク犯罪ユニット（NHTCU）はオランダ国家警察の一部門で、技術的に高度なサイバー犯罪の捜査を専門としています。NHTCU の目標は、オランダをサイバー犯罪から守ることです。国民の保護のほか、オランダのインフラが犯罪に利用されないようにすることも任務のひとつです。

NHTCU は、独創的な手法やテクニックを駆使し、犯罪の首謀者や実行犯を追跡するという捜査活動を得意としています。北米や東西ヨーロッパに連絡窓口を有しており、このような連絡窓口を介して、各国のハイテク犯罪ユニット間の橋渡し役を果たすことも少なくありません。

NHTCU の成功要因のひとつとして、他の公的機関や民間企業とパートナーシップを組み、緊密に連携して活動するという点が挙げられます。この方法の場合、豊富な情報を入手できるとともに、共同戦略の下で活動できるという利点もあります。このような連携による捜査の成功例として、Bredolab ボットネットの閉鎖があります。NHTCU では最近、電子犯罪タスクフォースを立ち上げました。電子犯罪タスクフォースは、金融分野などの公的機関や民間企業とパートナーシップを構築し、共同でサイバー犯罪の撲滅に尽力することを目的としています。

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ーサービス

アイルランドは、過去 10 年間に急激な経済成長を遂げましたが、これは情報テクノロジーによるところが少なくありません。アイルランドでは、消費者も企業も情報テクノロジーとインターネット恩恵を受けています。例えば、サービスの利用と提供が便利になり、新たな市場が創出され利用できるようになったほか、情報交換の迅速化と情報処理の効率化も達成されました。その一方、情報テクノロジーへの依存が強まり、結果としてリスクと脅威が増加しました。このようなリスクと脅威に的確に対応しなければ、企業や個人、ひいては国家経済に重大な悪影響が及ぶ可能性があります。企業や消費者はインターネットを合法的に使用していますが、犯罪や非合法活動、テロのほか、企業や国家による不正・スパイ活動などにインターネットが利用されることも少なくありません。

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ーサービス（IRISSCERT）は、アイルランドの初めてのコンピュータ緊急対応チームです。IRISSCERT は独立系非営利組織で、保証契約の下で 2008 年に設立されました。その目的は、情報セキュリティに関する高品質なサービスを提供することにより、アイルランドの企業と消費者を支援し、結果的に情報テクノロジー関連の設備とサービスのセキュリティを向上させることにあります。主なサービスとしては、現在または将来の脅威を含め、情報セキュリティ上の脅威に関する警告サービス、情報セキュリティに関する問題の予防や対応、軽減のための方針を策定する際の支援サービス、コンピュータセキュリティインシデントの対応・管理サービスがあり、国内企業だけでなく国際企業にもサービスを提供しています。

このようなサービスは、情報テクノロジー専門家グループが中心となって提供しており、主な対象はアイルランドのインターネット利用者で、サービスは無料です。この結果、企業の情報システムは保護され、ユーザーはアイルランドのインターネット空間を安全な環境として利用できます。

詳しくは、https://www.iriss.ie/iriss/RFC_2350.htm をご覧ください。インシデントを報告したい場合、内容をメールに書き e-mail info@iriss.ie までお送りください。

ロンドン警視庁サイバー犯罪合同捜査本部

ロンドン警視庁サイバー犯罪合同捜査本部（PCeU）は 2008 年 9 月、ロンドン警視庁コンピュータ犯罪ユニットの外郭組織として設立されました。主な業務は重大なサイバー犯罪を国家レベルで調査することで、また目的は「安全でセキュリティが確保されたオンライン・ネットワークコンピューティング環境を構築することにより、イギリスが生活とビジネスの両面で安全な場所であるという信頼をさらに強化する」ことにあります。

サイバー犯罪の場合、仮想タスクフォースを活用し、関係機関と連携しながら迅速に対応することがサイバー犯罪に効率よく取り組むとともに被害を抑える上で不可欠です。このことは、PCeU の今までの活動の成功例が証明しています。

イギリス政府は 2010 年 10 月に「戦略防衛安全保障見直し」を実施し、以後、サイバー犯罪は「ティア 1 脅威」とみなされるようになりました。国家電子犯罪プログラムと PCeU は予算の増額が認められ、イングランド、ウェールズ、北アイルランドの警察力をそれぞれ強化することで、電子犯罪に対する警察の対応能力を改善するという作業に取り組んでいます。

PCeU は、これまで多数の捜査や活動に成功してきました。規模も大きくなり評価も高まり、今では、サイバー犯罪と闘う強力な法執行機関に成長しました。PCeU は時宜を見計らった活動とパートナーとの連携を通じて、イギリスの財務的損害の縮小に貢献しており、サイバー犯罪の減少によって節約された金額は 2011 年の 4 月から 10 月までで 1 億 4000 万ポンドに上ります。

国家電子犯罪プログラムは、地方にもサイバー犯罪の専門家を配置する計画を進めており、この計画にしたがって 2012 年 2 月、PCeU の地域支部が 3 つ設立されました。本年の夏には、関係機関と連携して、ロンドンオリンピックを標的とするサイバー犯罪を防止するという業務に当たります。

アメリカ合衆国シークレットサービス

アメリカ合衆国シークレットサービス（USSS）は、米国の決済支払いシステムの保護を目的とする機関として初めて創設され、これまで長期にわたって米国の消費者や産業界、金融機関を詐欺や不正行為から保護するための活動を続けてきました。その歴史は 145 年以上に及び、その間に任務の数は増え対象範囲も広がり、さらに捜査権限も強化されました。USSS は現在、金銭サイバー詐欺の発見、調査、防止に関する実績と経験、また斬新な捜査手法において、世界中で認められる存在となっています。

グローバル経済の発達により、商取引は企業と消費者の双方にとって簡便になりました。金融機関の口座や情報処理システムには、世界のどこからでもアクセスできます。金銭詐欺師やサイバー犯罪者も、この取引のグローバル化という新たな状況に自らを順応させながら、情報技術への依存傾向を悪用しようと画策しています。その結果、サイバー犯罪者は今では、システムに保存されているデータ、転送中のデータ、暗号化されたデータのいずれについても盗みのエキスパートとなっています。その犯罪行為は、長年の信頼関係にある犯罪者仲間と共同で実行され、また厚いベールの下で確実に実行されるのが普通です。さらにサイバー犯罪者の世界は過去 10 年間に進化を遂げ、現在ではいわば本拠地も国境もない世界であり、しかも流動的で隠密性も高いため、踏み入るのはほぼ不可能です。

このような新たな脅威に対抗するため、USSS は「多面手法」を用いてサイバー犯罪やコンピュータ関連の犯罪に積極的に取り組んでいます。具体的には、32 の電子犯罪タスクフォース（ECTF）で構成されるネットワークを構築し、捜査に活用しています。2 つの国際 ECTF（イタリアのローマとイギリスのロンドン）、38 の金融犯罪タスクフォース（FCTF）、サイバー調査部門も、このネットワークの一部となっています。この手法は、米国の最重要インフラや決済支払いシステムに対するサイバー攻撃を含め、電子犯罪の検出や抑止、さらに徹底した捜査に極めて有効です。

データ漏洩 / 侵害に関する詳しい情報、またデータ漏洩 / 侵害を USSS に通知・報告する方法などについては、最寄りの USSS オフィスにお問い合わせください（www.secretservice.gov）。

データ漏洩 / 侵害報告書に関するご意見、ご質問は、大いに歓迎します。
ご意見やご質問は dbir@verizon.com までお寄せください。Facebook や Twitter（hashtag #dbir）もご利用いただけます。

2012年データ漏洩/侵害調査報告書

ベライゾンRISKチームによる調査。協力は、オーストラリア連邦警察、オランダハイテク犯罪ユニット、
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ーサービス（IRISSCERT）、
ロンドン警視庁サイバー犯罪合同捜査本部、アメリカ合衆国シークレットサービスの各機関。

verizon.com/enterprise/jp