Verizon Business リスクチームによる分析と研究

2009 年データ漏洩侵害調査報告書

verizon business

2009 年データ漏洩 / 侵害調査報告書

Verizon Business リスクチームによる分析と研究

追加の更新および解説についてはhttp://securityblog.verizonbusiness.com（英語のみ）をご覧ください。

執筆

ウェード・H・ベイカー
アレックス・ハットン
C・デービッド・ハイレンダー
クリストファー・ノバック
クリストファー・ポーター
ブライアン・サーティン
ピーター・ティペット、医学博士
J・アンドリュー・ヴァレンタイン

寄稿・協力

タイス・ボスハールト
エリック・ブローム
カルビン・チャン
ロン・ドルミド
K・エリック・ジェントリー
マーク・グーディー
リッキー・ホー
スタン・S・カン
ウェイン・リー
イェーレ・ニーマンス
ヴェルドリート
デービッド・オスターターク
マイケル・ローゼン
エンリコ・テレマック
マティス・ファンデルウェル
ベン・ファンエルク
リスクチームのメンバー
ICSA ラボ

特別協力

ジャネット・ブルームフィールド
カール・グライギール
ハンター・モンゴメリー

目次

2009 年データ漏洩 / 侵害調査報告書

Verizon Business リスクチームによる分析と研究

エグゼクティブサマリー

2008 年は、企業と消費者のどちらにとっても波乱の一年として記憶されることでしょう。世界の金融市場は不安、不確実性、疑念に覆いつくされました。名だたる巨大企業が、次々と驚くほどあっけなく姿を消しました。かつて豊かな生活を送っていた多くの人が、日々の糧を得ることすら困難な状況に陥りました。不況を伝える数々の見出しが躍る中、過去最大級のデータ漏洩 / 侵害についての報道がいくつか飛び込んできました。これらは、市場だけでなく情報の安全とセキュリティも頼りにできなくなったことを思い起こさせる出来事となりました。

2009 年版のデータ漏洩 / 侵害調査報告書（DBIR）は、「犯罪科学捜査官」の観点から、この歴史的な混沌の時期に焦点を当てます。2008 年の調査対象全事例のうち、確認された 90 件の漏洩 / 侵害事例だけで、実に 2 億 8500 万件ものレコードが漏洩 / 侵害の被害を受けました。これらのレコードには重要な内容が含まれており、本報告書ではそれらについて言及しています。本調査の目的は前年と同様、本報告書で提示するデータと分析が、読者の企業や組織におけるプランニングおよびセキュリティ対策の一助となることです。以下は報告書の要点をいくつか抜粋したものです。

データ漏洩 / 侵害の背後にいるのは誰か?

- **74%** が外部原因によるもの (+1%)
- **20%** がインサイダーによるもの (+2%)
- **32%** がビジネスパートナーによるもの (-7%)
- **39%** が複数の実行者が関与 (+9%)

2008 年の報告書の統計とほぼ同じ数字で、ほとんどのデータ漏洩 / 侵害はやはり外部の原因から発生しています。まだサンプルの 3 分の 1 を占めるとはいえ、ビジネスパートナーが関係する漏洩 / 侵害の割合は数年ぶりに低下しました。被害の平均規模ではインサイダーを原因とする漏洩 / 侵害が首位のままですが、被害に遭ったレコード数の総計ではアウトサイダーを原因とする侵害が上回りました。漏洩 / 侵害の被害に遭った全レコードの 91%に、組織犯罪グループが関係していました。

漏洩 / 侵害はどのようにして発生するか?

- **67%** が重大な過失によって助長 (<>)
- **64%** がハッキング (+5%)
- **38%** がマルウェアを利用 (+7%)
- **22%** が権限の不正使用によるもの (+7%)
- **9%** が物理的攻撃を介して発生 (+7%)

より成功した漏洩 / 侵害では、アタッカーは被害者が犯したミスにつけ込み、ハッキングによってネットワークに侵入し、データを収集するためのマルウェアをシステムにインストールしていました。侵害を受けた全レコード中の 98%には、これらの属性のうち少なくとも 1 つが含まれていました。デフォルトの認証情報による不正アクセス（通常は第三者によるリモートアクセス）と、（Web アプリケーションに対する）SQL インジェクションが、ハッキングの種類の上位を占めました。カスタマイズされたマルウェアがこれらの攻撃に用いられる割合は、2008 年に 2 倍以上になりました。権限の不正使用はそれなりに多く発生しましたが、物理的攻撃による漏洩 / 侵害は 2008 年にはそれほど多く確認されませんでした。

どのような共通点があるか?

69% が第三者によって発見 (-6%)

81% の被害者がクレジットカード業界（PCI）のセキュリティ基準に非準拠

83% の攻撃は、発見や対応がそれほど難しくない (<>)

87% の侵害は、初歩または中級レベルの統制を実施していれば回避できたと考えられる (<>)

99.9% のレコードはサーバーとアプリケーションから漏洩 / 侵害の被害を受けていた

難易度の高い攻撃に分類されたのは全攻撃中の 17%にすぎませんが、侵害を受けたレコード全体のうち 95%の被害はそのような攻撃によってもたらされたものでした。このことは、ハッカーは防御の薄い標的を好む一方で、その気になれば、圧力をかけるのに最も効果的な場所をよく研究していることを示唆します。これらのインシデントのほとんどは、実施が難しい、またはコストが高くつく予防的統制を導入せずとも防げるものです。ミスや見落としは、リソース不足にもましてセキュリティ対策を阻害する要因です。PCI DSS に準拠することが望ましい組織のうち 81%は、実際に漏洩 / 侵害を受けるまで準拠していませんでした。2008 年に被害が記録されたほぼすべてのレコードが、オンライン資産から漏洩 / 侵害の被害を受けていました。前年の報告書と同様に、過半数の漏洩 / 侵害は第三者によって発見されました。

軽減（解決）対策で重点を置くべき領域は?

これらの 5 つの推奨事項のうち 3 つは、前年の報告書でも挙げられていたことに気づいた読者もいるでしょう。これは意図的なものです。単なる繰り返し以上の意味があります。実際、これらは新しい視点からの見直しとさらなる検討を加えた上での結果です。

データ漏洩 / 侵害に対する最良の防御策は理屈としてはごく単純で、データを保持しないことです。これは多くの組織にとって非現実的なため、次善の策として、業務上または法務上の理由で必要なデータのみを保持し、データがどこに格納され、どこに流れているかを把握し、細心の注意を払ってデータを保護するように努めます。

過半数の漏洩 / 侵害の発生原因は、前年までと同様、基本的な統制が敷かれていなかったこと、または、統制は敷かれていたが組織全体で一貫して実施されるには至っていなかった、というものでした。明白な弱点をむき出しのまま放置すれば、その弱点を利用する隙をアタッカーに与えます。弱点を容易に発見できない場合に、アタッカーがよりいっそうの時間と労力を費やす可能性はそれほど高くありません。

以上の論点の延長として、2008 年の事例データに基づいた、実証済みで真に有効な統制をいくつか提言することが必要だという考えに至りました。非常に多くの割合のアタッカーが、デフォルトの認証情報、共有されたアクセス情報、または盗まれたアクセス情報を用いて企業ネットワークへにアクセスします。その上、多くの組織ではこの問題の深刻性がほとんど認識されていないように見受けられます。最初の段階でそのようなインシデントを防げれば確かに最善ですが、アカウント情報をレビューすることによって悪用または異常の兆候を見つけることは第 2 の防衛線となります。SQL インジェクションも昨年、企業のデータを侵害する手段として頻繁に用いられました。セキュア開発、コードレビュー、アプリケーションテストなどはすべて、このような弱点の発見という観点から有効であると考えられます。

攻撃の高度さや威力を問わず、発生した漏洩 / 侵害を早急に検知できる能力は、ほとんどの組織にとって大きな挑戦となります。技術力またはプロセスのどちらが不足しているにせよ、結果は同じです。過去 5 年間に、被害を受けた企業や組織が自らの手で漏洩 / 侵害を発見した例はごくわずかでした。漏洩 / 侵害を迅速に発見できた例に至ってはさらに少数です。

- ✔ 企業全体にわたって必要不可欠な統制を構築する
- ✔ データの場所を把握・追跡し、リスクを評価する
- ✔ イベントログを収集および監視する
- ✔ ユーザーアカウントとアクセス情報を監査する
- ✔ Web アプリケーションをテストおよびレビューする

メソドロジー

この報告書で使用している基本的なメソドロジーは、前年までと同様です。すべての結果は、2004 年から 2008 年にかけて Verizon Business が実施したデータ漏洩 / 侵害調査の期間中に直接的に収集された証拠に基づいています。報告書では、主に 2008 年の調査対象事例に焦点を当てて分析を行っていますが、データの範囲全体を徹底的に、また細部に至るまで参照しています。調査対応（IR）チームはさまざまな事例を扱いますが、この調査データには侵害が確認された漏洩 / 侵害に関する事例だけが含まれています。入力する情報の確実性と一貫性を保証するために、すべての調査担当者は標準化された同じツールを使用して、事例データおよびその他の関連事項を記録します。その後、記録された情報がリスクチームの他のメンバーに提出され、より詳細な検証と分析が行われます。

2009 年のデータ漏洩 / 侵害調査報告書には、上記以外にもいくつかの注意すべき相違点と追加事項があります。2008 年の報告書では、1 回の大規模なデータ収集作業を行った際に、4 年間の事例全体をさかのぼって分析を加えていました。一方、今回の調査データは年間を通して定期的に収集されたものです。調査担当者は事例が終結した段階で、事例についての記憶が新しいうちに情報を入力することができました。このように、「歴史を紐解く」形式から継続的なやり方にデータ収集の方針を転換したことにより、既存のデータポイントについてより詳細な情報が手に入るようになり、新しい研究領域への門戸が開かれました。これらの追加により、研究および実務に携わる方々にとっての、この報告書の価値と有用性がさらに高まることを願っています。

この報告書で提示するほとんどの統計は、事例の割合、侵害を受けたレコードの割合、または単なる事例件数に言及します。「レコードの割合」は今年新しく導入された統計で、場合によっては他の統計と異なる一方で常に洞察に満ちたデータの解釈を提示します。小規模なサンプルに割合の概念を当てはめると誤解を生じやすいため、調査対象の全事例の部分的サンプルを話題にするときは常に、事例の件数そのものを使用します。たとえば、38%の事例でマルウェアの証拠が見つかったという記述に続いて、マルウェアによる攻撃のみに言及したその後の数ページでは、すべての数値は整数で示されています。図表のキャプションと凡例も適切な解釈に役立つはずです。

2008 年の報告書では、一回の大規模なデータ収集作業を行った際に、
4 年間の事例全体をさかのぼって分析を加えていました。
一方、今回の調査データは年間を通して定期的に収集されたものです。
このように、「歴史を紐解く」形式から継続的なやり方にデータ収集の
方針を転換したことにより、既存のデータポイントについてより詳細な
情報が手に入るようになり、新しい研究領域への門戸が開かれました。

ここで重ねて述べておきたいのは、この報告書の調査結果は、すべての組織で常に起きているすべてのデータ漏洩 / 侵害を代表したものではない、ということです。これらの統計は今回の調査対象事例のみに基づいており、この報告書で提示するすべての結論または推論はこのサンプルから導き出されたものです。これらの結果の多くは一般的なものとして論じても適切であると考えられますが、ある程度の偏りが存在することは否定できません。それでもなお、この報告書にはデータ漏洩 / 侵害に関する情報が豊富に記載されており、企業にとって参考になる統計データも多数含まれています。いずれにしても、他の研究や報告と同様に、どのような情報や結果を採用するかは最終的には読者の判断に任される、ということです。

最後に大事なことですが、Verizon Business ではフォレンジックス調査を行った企業のプライバシーを厳格に守り、また名前をいっさい公表しないことを方針とし、また厳格に遵守しています。具体的には、調査の内容を記録し、必要な場合には法執行機関などに情報を提出した後、その情報を整理し、記録から顧客企業の名前を削除しています。したがってデータ漏洩 / 侵害に関する情報レポジトリーには、企業名を特定できるような情報はいっさい含まれていません。また、本報告書の統計データはすべて集計後のデータとして提供されており、個別のデータが分析の目的となることは決してありません。

2009年時点のサイバー犯罪の概況

2009 年版の報告書で提示する統計と分析を詳細に検討する前に、2008 年版の DBIR の「サイバー犯罪への誘惑」の内容を更新することが望ましいと考えました。この短い節では、データ関連の事情に論点を置き、世界中で起きているサイバー犯罪の巧妙化という重要な側面に光を当てることを試みます。わずか 1 年の間にサイバー犯罪市場にそれほど大きな変化が起きたのか、と疑わしく思う読者もいるでしょうが、2008 年に世界の金融市場を巻き込 んだ激変を思い起こせば、いかなる市場システムも（時として急速に）変わりうるということを容易に理解できるでしょう。サイバー犯罪の市場が発展するにつれて、アタッカー、標的、そして技術も進化や変貌を遂げます。

サイバー犯罪でデータを盗んでも、そのデータの市場、つまり情報闇市場がなければ、犯人にとってサイバー犯罪を犯す意味はありません。あらゆる正当な市場システムと同様に、商品とサービスの単価は需要と供給に応じて変動します。近年発生した磁気ストライプデータの大規模な漏洩（今回の調査対象事例に含まれるだけでも数億レコード）により、情報の闇市場は実質的に氾濫状態となり、市場には偽造を働くのに十分な「ごみの山」、つまりクレジットカードの磁気ストライプが大量に溢れ返りました。この市場飽和により、磁気ストライプ情報の価格相場は無価値に近い水準にまで下落しました。盗難に遭ったクレジットカードデータの販売価格は、2007 年半ばの 1 レコードあたり 10 ～ 16 ドルから、現在では 1 レコードあたり 0.50 ドルにまで下落しています。*

供給が増加して価格が下落するにつれて、犯罪者は収益性を維持するために、犯行のプロセスを見直して自らの「商品」を差別化する必要に迫られました。2008 年に入ると、データが集中した場所を標的にし、より価値の高い一連の消費者情報を入手するという形で、この目標が達成されるようになりました。

供給が増加して価格が下落するにつれて、犯罪者は収益性を維持するために、犯行のプロセスを見直して自らの「商品」を差別化する必要に迫られました。2008 年に入ると、データが集中した場所を標的にし、より価値の高い一連の消費者情報を入手するという形で、この目標が達成されるようになりました。現在では、一攫千金を目論む犯罪者は、個人識別番号（PIN）情報とそれに付随する銀行口座やクレジットカードの情報を盗み出します。実際、PIN データを狙った攻撃の爆発的増加は前年にも確認されました。これらの PIN ベースの攻撃は、署名ベースの典型的な偽造攻撃よりもずっと深刻な被害を消費者に与えます。その理由は、PIN 詐欺は一般に、顧客の口座（当座預金口座、普通預金口座、証券口座など）から直接現金が引き出されることにつながるからです。さらに、PIN 詐欺が発生した場合、行われた取引が実際には詐欺であることを証明するために、被害者の側も多大な負担を強いられるのが一般的です。このことから、失われた資産を取り戻すことは標準的なクレジット詐欺犯罪の場合よりも困難です。

より高い価値を持つ PIN データに攻撃の対象が移ったことに伴い、攻撃の手口も次々と高度化していきました。犯罪者はこの貴重なお宝を盗み出すために犯行のプロセスを再設計し、メモリ・スクレイピング（メモリ内容の重要箇所を読み取る）マルウェアなどの新しいツールを開発しました。このことは、かつては机上の空論としか考えられていなかった複雑な攻撃戦略の実行成功に結びつきました。結果として、2008 年の調査対象事例はこれらの傾向を反映したものになっています。これらの事例に含まれるサイバー犯罪攻撃は、それまでの数年間に見られたものよりも単一の標的を狙う傾向が強く、最先端の技術を駆使し、より複雑で巧妙なものになっています。

*Verizon Business の地下諜報活動の一環として収集されたデータに基づく図。

結果と分析

Verizon Business の調査対応チーム（IR チーム）は 2008 年、150 件のフォレンジックス調査に従事しました。そのうち 90 件は、侵害が確認されたデータ漏洩 / 侵害の調査でした。これらの調査の中には、非常に大規模で長期間に及ぶものが数多くありました。その結果として、今年の事例数は平均を下回りました。事例数こそ 90 件に減少したものの、2008 年の調査対象事例全体で侵害を受けたレコードの総数（2 億 8500 万超）は、2004 年から 2007 年の 4 年間を合計した数字を上回りました。

この報告書の執筆時点で、IR チームが前年に調査した漏洩 / 侵害の約 3 分の 1 は公表されています。とくに年末にかけて、公表件数はさらに増えると見込まれます。公表されなかった侵害は法務上の開示要件に該当していないと考えられ、おそらく今後も世間の目に触れることはないでしょう。

2008 年の事例の約 20%には複数の漏洩 / 侵害が関係していました。言い換えれば、1 件の事例の中で、複数の独立したエンティティまたは場所が個別に漏洩 / 侵害を受けていました。驚くべきことに、調査対象事例の半数近くは、相互に関係したインシデントの異なる集合で構成されていました。同じ犯人が攻撃を実行する例も非常に多く見られました。漏洩 / 侵害を経験した被害者と一般の第三者の間で、（文字通り）接続を共有していたこともありました。さらには、何らかの種類の共通アプリケーション、同一の攻撃パターンなどを通じて被害者どうしがリンクしていたこともありました。

2004 年から 2007 年にかけて扱った事例にこれら 90 件の事例を加えたものが、この報告書のすべての結果と分析の基礎になっています。

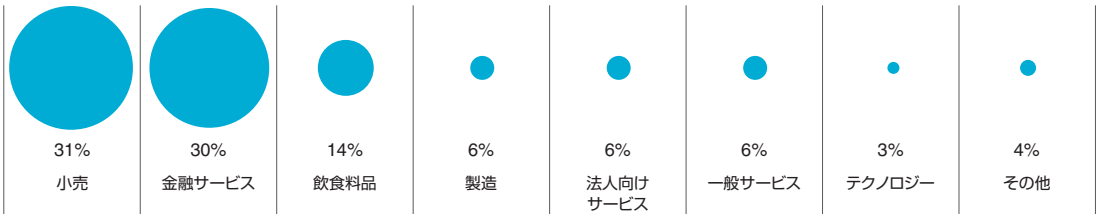
業界別と企業の規模別の統計

注）各表や図では 2 つ以上の複合要因によるものが有るために統計合計数が 100% より多くなっている場合があります。

前年の報告書と同様に、データ漏洩 / 侵害は 2008 年も多くの組織に影響を及ぼしました。図 1 は、発生した漏洩 / 侵害を業種グループ別に分類したものです。小売業界はすべての漏洩 / 侵害の 3 分の 1 近くを占め、前年と同じく最も多くの被害を受けた業界となっています。飲食料品業界は、2004 年から 2007 年にかけての調査データでは 2 位の割合でしたが、2008 年は 20%から 14%に割合を落とし、順位も 3 位に低下しました。2008 年に大きな伸びを見せたのは金融サービス業界で、調査対象事例に占める割合は 30%に倍増しました。

金融セクターのデータ漏洩 / 侵害の増加は、「サイバー犯罪の概況」の節で強調したサイバー犯罪活動の最近の傾向を示唆しています。この報告書全体で議論するように、金融サービス企業は狙い撃ちにされ、2008 年に発生した、非常に強い意志を持って実行され、非常に洗練された、そして不運にも華々しい成功を収めた何件かの攻撃の犠牲になりました。侵害を受けた 2 億 8500 万超のレコードの

図 1. 業種別の漏洩 / 侵害件数に占める割合

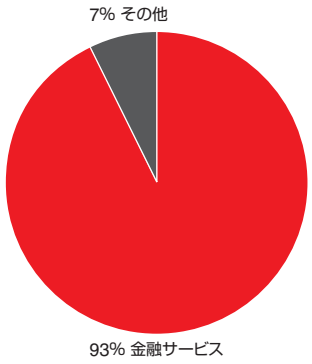


このページ内容に関するコメントまたは質問をお寄せください（英語のみ）

http://securityblog.verizonbusiness.com/category/2009dbir/ にアクセスし、
「Demographics」のページから英語でコメントを投稿できます。

うち、この業界で発生した漏洩 / 侵害によるものは 93%に上ります。この調査結果は、IR チームが前年に調査した数件の非常に大規模な漏洩 / 侵害を反映したものです。件数こそ少ないものの、そのような漏洩 / 侵害は、この報告書全体で議論するすべてのレコード統計で高い割合を占めています。

図 2. 業種別のレコード数に占める割合



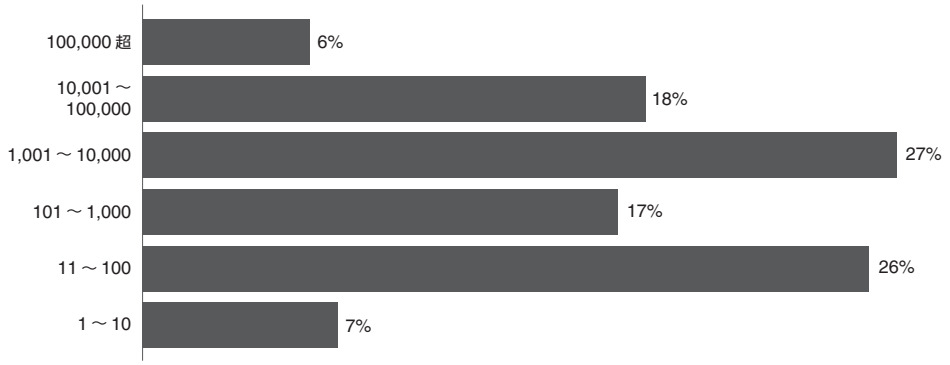
これらの上位 3 つを除いた他の業種グループで、残り 4 分の 1 の事例を少しずつ分け合う形になっています。製造、法人向けサービス（いくつかのメディア、マーケティング、コンサルティング、法律事務所を含む）、一般サービスの各業種はそれぞれ調査対象事例の 6%を占めました。2004 年から 2007 年にかけての事例では 13%を占めたテクノロジー企業は、2008 年に大きく割合を下げました。この変化は、一般的な傾向よりも本調査のサンプルをより強く反映していると考えられます。

IR チームが扱った米国外の事例の調査件数は、2008 年の調査対象事例の 3 分の 1 を超えるまでに増加しました。米国全域での大規模な調査に加えて、多くの漏洩 / 侵害がカナダとヨーロッパの企業や組織を襲った一方で、ブラジル、インドネシア、フィリピン、日本、オーストラリアの各地域でも事例調査の需要が伸び続けました。アタッカーは攻撃しやすい標的を世界中で探し続けており、新興市場国においても、とくに消費者データに関連した懸念が今後高まっていくと見込まれます。

組織規模の分布は前回の調査データに非常に近いものになっています。図 3 に示すように、データ窃盗犯は小規模な事業所や組織から巨大企業までをまんべんなく標的にしているように見受けられます。常にそうとは限りませんが、犯罪者は通常、規模などの被害者特性ではなく、標的のデータが持っている価値と、標的に対する攻撃のしやすさを判断材料にして攻撃を開始します。

この節を締めくくる前に、1 つの重要な点について言及しておく必要があります。2008 年に新しく追加された調査項目によると、調査対象の事例に関係する企業または組織の 13%が最近、合併または買収を経験しています。この統計から結論を引き出す、または

図 3. 企業または組織の規模（従業員数）と漏洩 / 侵害に占める割合



この統計に何らかの意義を与えることは困難ですが、漏洩 / 侵害の発生率にそのような変化が影響を及ぼす可能性については検討してみる価値があります。

合併と買収に際しては、それまで別個の存在であった複数の組織の従業員と製品が統合されるだけでなく、それらの組織の技術環境も統合されます。統合が一夜にして、また何の滞りもなく完了することはまずありません。業務上の便益のために、それまで採用されていた技術標準が破棄される場合があります。IT 運用環境にもたらされるそのような変化により、漏洩 / 侵害のリスクが高まる可能性があります。さらに、売却が決まっている事業については、売却時点のバランスシートを改善するための便利な手段として、営業費用（IT およびセキュリティ関連の費用を含む）の削減が図られる場合があります。最後に、所有者が変わることで、買収された組織の情報リスクに対する許容度が（命令または文化によって）変わる場合があります。

もちろん、これらはすべて推測にすぎず、追加の情報がなければ証明も反証も（仮説考証さえも）不可能です。合併と買収に関する統計を事例の評価指標に加えたのは、より重要な何らかの発見がこの統計からいずれ明らかになる可能性があるという考えに基づいたものであり、この統計の記録と報告は今後も継続していく予定です。

データ漏洩 / 侵害の原因

通常の犯罪捜査と同様、コンピュータ分野でのフォレンジックス調査の主な目的の一つは、犯罪に関与した人物の特定です。犯人が犯行現場に戻って来ることはよくあるため、漏洩 / 侵害の原因を知ることが防犯につながる可能性があります。大きく分けて、セキュリティインシデントには以下のいずれか 1 つ、または複数の要因が重なって発生します。

外部：データ漏洩 / 侵害の原因は、企業の外部にあると考えられています。このような外部原因としては、ハッカー、犯罪組織、行政機関などがありますが、異常気象や地震などの天災も外部原因となります。通常、企業と外部実体との間には信頼や権限などの関係は存在しません。

内部：内部原因とは、企業の内部の原因をいいます。たとえば、企業の幹部や従業員、インターンといった人的資産（インサイダー、内部関係者）のほか、設備や情報システムなどの物理資産などが内部原因となります。インサイダーは、会社から一定程度の信頼を得ており、中でも IT 管理者は、相当のアクセス権や特権を所有しています。

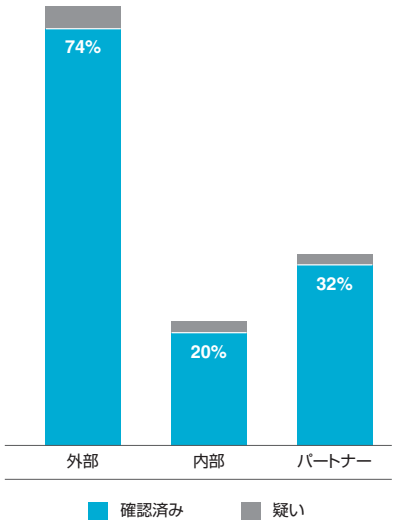
パートナー：企業と業務提携関係のあるサードパーティなどが含まれます。パートナー、ベンダー、サプライヤー、契約企業、顧客のバリューチェーンは、エクステンディドエンタープライズと呼ばれます。エクステンディドエンタープライズにとって情報はいわば活力源であり、そのため、企業とビジネスパートナー、また各ビジネスパートナーの間には通常、一定程度の信頼関係と権限が存在します。

5 年間の 600 件のインシデントから得られた結果は、ほとんどの漏洩 / 侵害の背後にはインサイダーがいるという、長きにわたって強く支持されている考えをいっそう裏付けるものです。

このページ内容に関するコメントまたは質問をお寄せください（英語のみ）

http://securityblog.verizonbusiness.com/category/2009dbir/ にアクセスし、
「Sources of Data Breaches」のページから英語でコメントを投稿できます。

図 4. 各原因が漏洩 / 侵害に占める割合



上記のいずれかの原因が漏洩 / 侵害において重要かつ積極的な役割を果たしたことが証拠から明白な場合、漏洩 / 侵害の原因として認定されます。「重要かつ積極的」の解釈には多少の幅がありますが、調査担当者は一貫性のある一連のガイドラインにしたがいます。たとえば、働いている企業から故意に機密情報を盗み出すインサイダーは明らかに「内部」の漏洩 / 侵害です。また、たとえ意図しないものであっても、インサイダーの行為が直接的に漏洩 / 侵害を引き起こしたり漏洩 / 侵害を助長した場合、そのインサイダーは漏洩 / 侵害の責任の一部を負うものと見なされます。Web サイトの閲覧中に意図せずマルウェアをコンピュータに取り込んでしまい、外部のアタッカーがあとからそのマルウェアを利用して不正にアクセス情報を入手するようなケースがその例です。インサイダーの不作為（見落とし、手順の励行を徹底しない、特定のセキュリティ対策を実装しないなど）が漏洩 / 侵害を可能にするか助長する場合、その行為は内部原因とは見なされません。図 4 は、2008 年の漏洩 / 侵害原因の分布を示したものです。この結果は、2004 年から 2007 年にかけての調査データの結果にきわめて似通っており、セキュリティ分野のコミュニティのデータ漏洩 / 侵害の発生源に関する主要な見解を覆しつつあります。

これらの結果についての議論を進める前に、混乱を招きかねない 2 つのポイントを明確にする必要があります。まず、多くの漏洩 / 侵害には複数の当事者が関係するため、図 4 で数値の合計が 100%を超えているのは誤りではありません。図 5 では、この事実を強調するために漏洩 / 侵害原因の分布を示しています。次に、これらの調査結果は、調査対象事例中のデータ漏洩 / 侵害につながるセキュリティ侵害の発生（または発生の可能性）に特に関係するものであり、攻撃、影響、一般的なセキュリティインシデント、リスクのどれにも関係しないことを明記しておきます。前年の報告書の公表後、この調査結果に対してやや強い反応が寄せられました。少なくとも一部の議論については、実際の結果よりも用語に関連したものでした。

過半数のデータ漏洩 / 侵害の原因は、前年までと同様、被害に遭った企業や組織の外部にあると考えられます。Verizon Business の 2008 年の調査では、漏洩 / 侵害の 74%が外部原因によるものと確認されましたが、これは 2004 年から 2007 年までの調査の平均値とほぼ同じ数字でした。また、5 年間の調査期間中、この統計値はそれほど大きく変化していません。こうした結果を踏まえれば、アウトサイダーがもたらす脅威を軽視できないことがわかります。

図 5. 単一および複数の原因が漏洩 / 侵害に占める割合

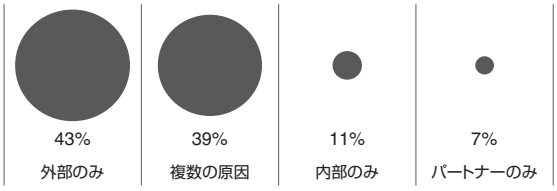
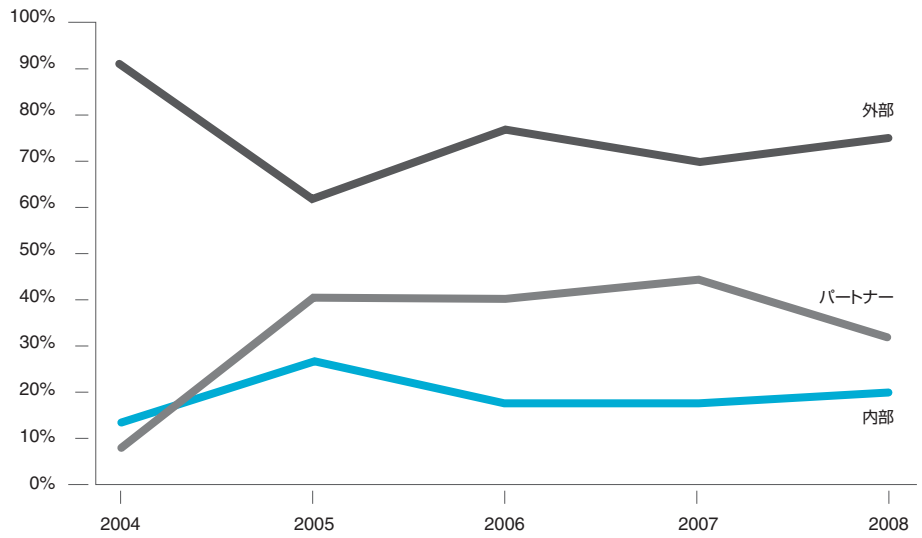


図 6. 各原因が漏洩 / 侵害に占める割合の推移



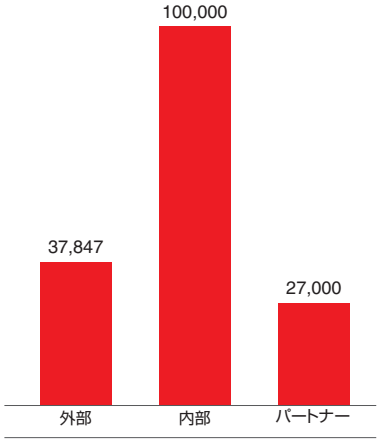
その一方で、インサイダーが原因の漏洩 / 侵害は 20%にとどまり、調査対象事例に対する割合では 4 年連続で最下位となっています。図 5 に示すように、インサイダーの単独犯による漏洩 / 侵害はそのうちの約半分（すべての漏洩 / 侵害の 11%）にすぎません。インサイダーが原因とされた残りの漏洩 / 侵害のほとんどは、過失やポリシー違反を通じて無意識のうちに犯罪に加担する形で、従業員が関与したものでした。これらの結果の基になった調査対象事例は消費者のデータが占める割合が大きく、結果はすべてのデータ漏洩 / 侵害を反映していない可能性があることは事実です。インサイダーは知的財産など、その他の種類のデータを標的とする傾向があるかもしれません。物質的な損害を発生させる漏洩 / 侵害は最終的にはすべて発覚すると考えられがちですが、発覚しないまま終わるインサイダー犯罪が数多くあることも事実です。インサイダーによる犯罪は内々で処理されやすい、という仮説も説得力があります。ともあれ、5 年間の 600 件のインシデントから得られた結果は、ほとんどの漏洩 / 侵害の背後にはインサイダーがいるという、長きにわたって強く支持されている考えをいっそう裏付けるものです。

ビジネスパートナーが原因の漏洩 / 侵害の件数は外部原因と内部原因の中間を保っていますが、2008 年に 12%低下しました。パートナー関連のリスクを減らすための対策が 1 年間で大きく進歩したとは考えにくいため、この下落の解釈は困難です。どちらかといえば、2008 年の調査対象事例のうち、飲食料品業界と小売業界で発生した事例の割合が低下したことのほうが関係が深そうです。前年の補足報告書の読者は、その 2 つの業界が、パートナー関連の漏洩 / 侵害で高い割合（とくに飲食料品業界は 70%以上）を示していたことを覚えているかもしれません。対照的に、2008 年の結果は、より見返りの大きい標的を犯罪者が直接狙っていることを示唆するものになっています。信頼されたパートナーのインフラストラクチャを介した「エンドアラウンド」計略は、これらの攻撃で選択される経路ではなさそうです。とはいえ、パートナーが関与した漏洩 / 侵害が多く発生していることに変わりはなく、確認された事例と疑わしい事例を両方ともカウントした場合、事例全体に占める割合は 3 分の 1 を超えます。調査対象事例の構成によって説明がつかない、過去のデータとのその他の相違はすべて、統計上のささいな変動と考えられます。

原因別の漏洩 / 侵害の規模

図 7 は、漏洩 / 侵害の被害を受けた、イベント 1 件あたりのレコード数の中央値 * を脅威の原因別に示したものです。注意点として、開示されたレコード数は漏洩 / 侵害のすべての結果を表しているわけではありません。ここでは単に全体的な影響を測定するための指標として、この統計を使用しています。

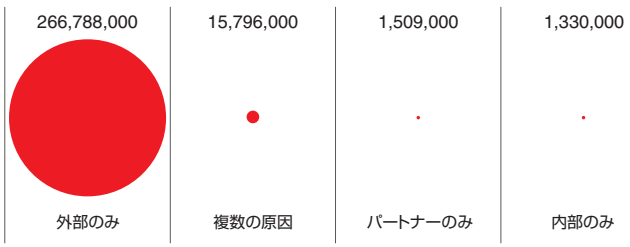
図 7. 漏洩 / 侵害の事例 1 件につき被害に遭ったレコード数の中央値



インサイダーによる漏洩 / 侵害（個別）は引き続き、他の原因による漏洩 / 侵害よりも損害が大きいことを示しています。ただし、ここで示された原因別の数値の差は、2004 年から 2007 年にかけての調査対象事例に見られたほどには大きくありません。より興味深い変化の 1 つは、アウトサイダーによる漏洩 / 侵害のほうが、パートナーによるものよりもインシデントあたりの被害レコード数が多くなった点です。この変化は、2008 年の調査対象に、アウトサイダーによって引き起こされたきわめて大規模な漏洩 / 侵害が複数含まれていたことが原因と考えられます。右のグラフに示された中央値（37,847）と平均値 **（5,651,067）を比較してみると、外部原因の漏洩 / 侵害の規模に関して、調査データに著しい偏りが存在していることを理解できます。このことは、これらのインシデントを分析する際に、優先する代表値として中央値を使用する理由の 1 つでもあります。図 8 は、昨年発生した外部原因による漏洩 / 侵害の規模と偏りについての印象的な見方を提供します。

この時点で、前回の報告書での疑似リスク計算（可能性 × 影響）とその結果をよく知っている読者は、今年の計算は違った結果になるのではと感じているかもしれません。実に的確な直感です。2008 年の事例結果では、アウトサイダーがデータ漏洩 / 侵害にとっての最大のリスクであり、インサイダーが僅差で続き、パートナーは最下位となっています。これは、2004 年から 2007 年にかけての調査データとは正反対のパターンです。このことは、情報リスクの根本的な性質が昨年 1 年間で大きく変わったことを意味するのでしょうか。必ずしもそうとはいえません。リスクは確率的なものであり、複数の測定結果を用いて長期的に判断するのが最も適切であることに留意してください。件数こそ少ないものの、複数の大規模な漏洩 / 侵害は、2008 年の調査でアウトサイダーが最もリスクの大きい原因となるのに十分な要因でした。

図 8. 漏洩 / 侵害の被害を受けたレコード数合計と原因



* 昇順に並べた一連のレコード数の中央値

** 一連のレコード数の平均値

表 1. 疑似リスク計算

原因	可能性	影響（レコード数）	リスク（疑似）
外部	**74%**	37,847	28,175
内部	20%	**100,000**	20,000
パートナー	32%	27,000	8,700

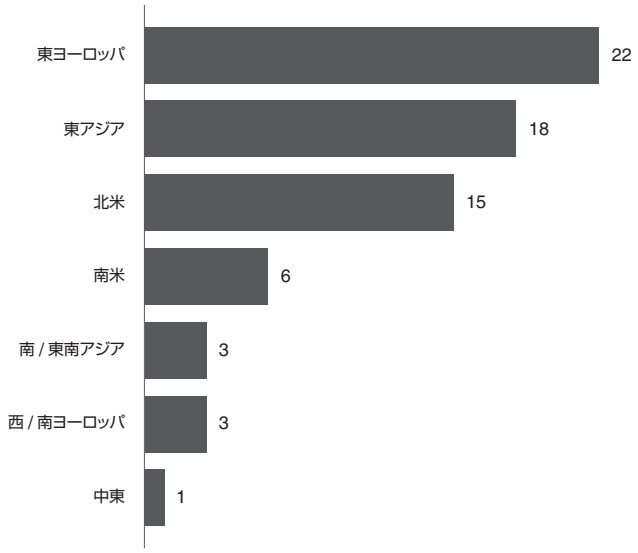
外部原因による漏洩 / 侵害

攻撃の地理的な起点を正確かつ確実に特定することは困難です。この決定はソース IP アドレスに基づきますが、多くの場合、さまざまな理由で信頼できません。それでも、事例間の共通要素、詐欺の相関パターン、Verizon Business の他の部門から提供される情報、捜査当局の協力を通じて追加の検証が可能です。データ漏洩 / 侵害の外部原因の地理的分布を図 9 に示します。

順位に多少の変動はありますが、東ヨーロッパ、東アジア、北米は 2008 年も上位に位置しています。実際、これらの地域は前年よりもさらに比率を高め、すべての外部攻撃の 82%を占めています。2004 年から 2007 年にかけての漏洩 / 侵害のうち、これらの地域を起点としていたものは 59%でした。変動の主な要因は東アジア（15%増）と東ヨーロッパ（9%増）です。

アジアからの攻撃には国家的な支援が絡んでいるのではと邪推する向きもありますが、各国政府がサイバー犯罪の有力なエージェントであるという見解を支持する証拠は見当たりません。東ヨーロッパからの悪意ある活動が犯罪組織の仕業であるという証拠は数多く揃っています。このことは、地域別ではなく一般的な種類別に外部エンティティを分類した図 10 を見ればさらによく理解できます。

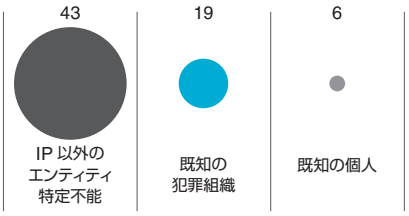
図 9. アタッカーの IP アドレスの地域と漏洩 / 侵害件数



3 分の 2 近くの事例が「IP 以外のエンティティ特定不能」になっているのは、いくつかの要因の結果です。まず、単純にそのような追跡が不可能な場合があります。追加の時間と費用を投じる価値がない、と被害者が判断する場合もあります。ほとんどの場合、IP アドレスの特定は、攻撃元のエンティティを一掃することではなく、侵害を封じ込めることを直接の目的として行われます。それらの事例で、IP アドレスの追跡によって攻撃元エンティティの特定を試みるときは、捜査当局の担当官の協力を仰ぎます。図に示すように、追跡によって既知の犯罪組織のメンバーが特定されることはよくあります。図 10 から読み取れないのは、

2008 年に漏洩 / 侵害の被害を受けた全レコードの 91%について、組織的犯罪活動が原因だったという驚くべき統計です。明るい話題として、捜査当局の協力を得たこれらの取り組みが、2008 年に少なくとも 15 件の事例（および集計）で検挙に結びついたことを報告できるのは喜ばしいことです。

図 10. 漏洩 / 侵害の外部原因の分類と漏洩 / 侵害件数



内部原因による漏洩 / 侵害

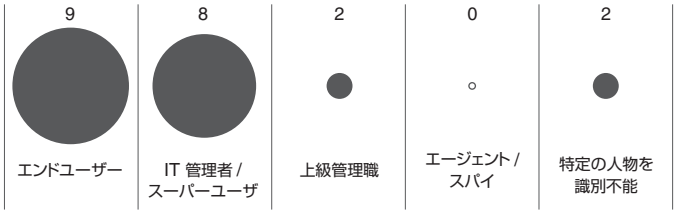
図 11 は、職務に応じたインサイダーの分類と、それぞれの職務のインサイダーが原因となったインシデントの割合を示した図です。2008 年の結果は、2004 年から 2007 年の調査データに類似しています。以前の調査と同様、ほとんどの漏洩 / 侵害にエンドユーザーと IT 管理者が容疑者として関わっています。IT 管理者に関しては、この調査結果は驚くべきものではありません。権限が高ければ高いほど、その悪用を促す機会と誘惑も大きくなるからです。同時に、エンドユーザーによって引き起こされたインシデントに関する結果は、内部原因による漏洩 / 侵害が、権限または管理用のアクセス情報のみに依存しないことを思い出させる役割を果たします。今回の調査の評価指標にはパートタイムと派遣労働者の項目も含まれていますが、それらの当事者が関係した事例はありません。

調査担当者は、2008 年のすべてのインサイダー事例のうち約 3 分の 2 が計画的な行為の結果で、残りは意図的なものではなかったと判定しました。管理者がエンドユーザーや他の従業員よりも計画的に、悪意を持って行動したと推論するのは容易ですが、証拠はそのような結論を支持しません。両者が事例に占める割合はほぼ同じでした。上級管理職が関与した両方の事例が、その人物が解雇された後に実行された計画的な行動の結果だったことは注目に値します。また、直近に解雇された従業員によって引き起こされた漏洩 / 侵害がほかにも数件、調査対象事例に含まれていたことが判明しました。過半数は管理者でしたが、いくつかの事例にはエンドユーザーも関与していました。直近に解雇された従業員によって引き起こされた漏洩 / 侵害に関しては、次の 2 つのシナリオが観察されました。

- 従業員が解雇され、その人物のアカウントが直ちに無効にされなかった。
- 従業員は解雇通知を受けたが、監視のない状態で、通常のアクセス権 / 権限を与えられたまま「その日の業務を終える」ことを許された。

このことは明らかに、適切な時期を定め、すべてのアクセス領域（アカウントの破棄、権限の無効化、解雇された従業員の残務整理）を網羅した解雇プランの必要性を示唆しています。

図 11. 漏洩 / 侵害の内部原因の分類と漏洩 / 侵害件数



パートナーによる漏洩 / 侵害

ビジネスパートナーが関与した漏洩 / 侵害の過半数は、第三者の情報資産および接続が侵害され、被害者のシステムを攻撃するために利用されたことの結果でした。この統計値は 2008 年に大きく増加しました（参考までに、2004 年から 2007 年にかけては事例の半数を少し上回る程度でした）。大多数の事例では、第三者のセキュリティ対策が手薄だったことにより攻撃が可能になっていました。パートナーがアクセスするシステムを監視し、責任を持って管理するための手段を組織が往々にして備えていないのは驚くべきことではありません。

図 12. 漏洩 / 侵害の原因となったパートナーの分類と漏洩 / 侵害件数

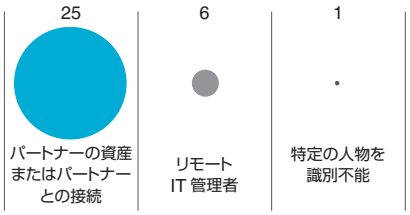


図 12 のように、第三者がパートナーを経由して企業、とくにエクステンディドエンタープライズのシステムに対してデータ漏洩 / 侵害を実行するケースが半分以上を占めていますが、パートナーが直接、データ漏洩 / 侵害に関与することもあります。第三者のリモート管理者による計画的で悪意のある行為は 6 件の事例が確認され、その割合は昨年わずかに上昇しました。これらの行為を働いた人物の 1 人は、直近に解雇されていました。

前年の報告書の公表後、被害者（クライアント）とパートナー間の関係が持つ性質について多くの調査を行ってきました。2008 年の調査の間、この情報の把握に努めました。この新しい情報により、これらの漏洩 / 侵害のほとんどに、被害者側の資産を管理するパートナーが関与していたことが判明しました。飲食料品業界の組織については、そのほとんどが、ポイントオブセールス（POS）システムをサポートするベンダーでした。パートナーが被害者のシステムへのユーザーレベルアクセス権を持っていた、または被害者と定期的にデータを交換していたいくつかの事例にも注目しました。被害者の資産を物理的に取り扱う、または輸送するパートナーが関与していた事例は 1 件だけでした。興味深いことに、調査対象事例には、パートナーが被害者のシステムをホストしていた事例は 1 件も含まれていませんでした。

大多数の事例では、第三者のセキュリティ対策が手薄だったことにより攻撃が可能になっていました。パートナーがアクセスするシステムを監視し、責任を持って管理するための手段を組織が備えていないというケースがよくあります。

脅威と攻撃の分類

企業情報資産の保護に携わる人なら誰でも、機密情報が不適切な人物の手に渡る経路は数え切れないほど存在することを知っています。ごく単純な構造のこともありますが、データ漏洩 / 侵害は多くの場合、互いに絡み合い、組み合わさった一連の出来事の結果です。これらのシナリオに関連した頻度と傾向の検証は保護対策にとって必要不可欠であり、この節の目的でもあります。

このページ内容に関するコメントまたは質問をお寄せください（英語のみ）

http://securityblog.verizonbusiness.com/category/2009dbir/ にアクセスし、「Threat and Attack Categories」のページから英語でコメントを投稿できます。

個別の攻撃の詳細については追って言及しますが、起こりうるすべての攻撃は、次の図に示した 7 つのトップレベル脅威分類のどれかに適合します。図 13 は、Verizon Business が 2008 年に調査したデータ漏洩 / 侵害について、直接的または間接的に原因となった脅威の分布を記録したものです。ほとんどのインシデントには複数の種類に分類されるイベントが関与することから、割合の合計は 100%を大きく上回っています。漏洩 / 侵害の被害を受けた全レコードのうち、それぞれの分類に属すると判定されたレコードの割合も赤色のバーで示しています。

2008 年の事例の結果は、2004 年から 2007 年にかけての調査データの結果に似通っています（これらの結果を時系列で表したグラフについては図 14 を参照）。詐欺と物理的攻撃の順位は入れ替わりましたが、それ以外の脅威の順位は変動していません。また、ハッキングとマルウェアは調査対象事例の中で大きな割合を占め続けています。過失が漏洩 / 侵害の直接原因であることはめったにありませんが、攻撃の成功を助長、または可能にしている要因であるケースは非常に多く見られます。図 13 から、典型的な漏洩 / 侵害のシナリオを推定することができます。アタッカーは被害者の何らかの過失につけ込み、ハッキングによってネットワークに侵入し、システムにマルウェアをインストールしてデータを収集します。図 13 の赤いバーで示されているように、このことは大規模な漏洩 / 侵害に特に当てはまります。以降の各節では、脅威の各分類をより詳細に検証していきます。

図 13. 各脅威分類に該当する漏洩 / 侵害の割合（黒）および各脅威とレコードとの関連性（赤）

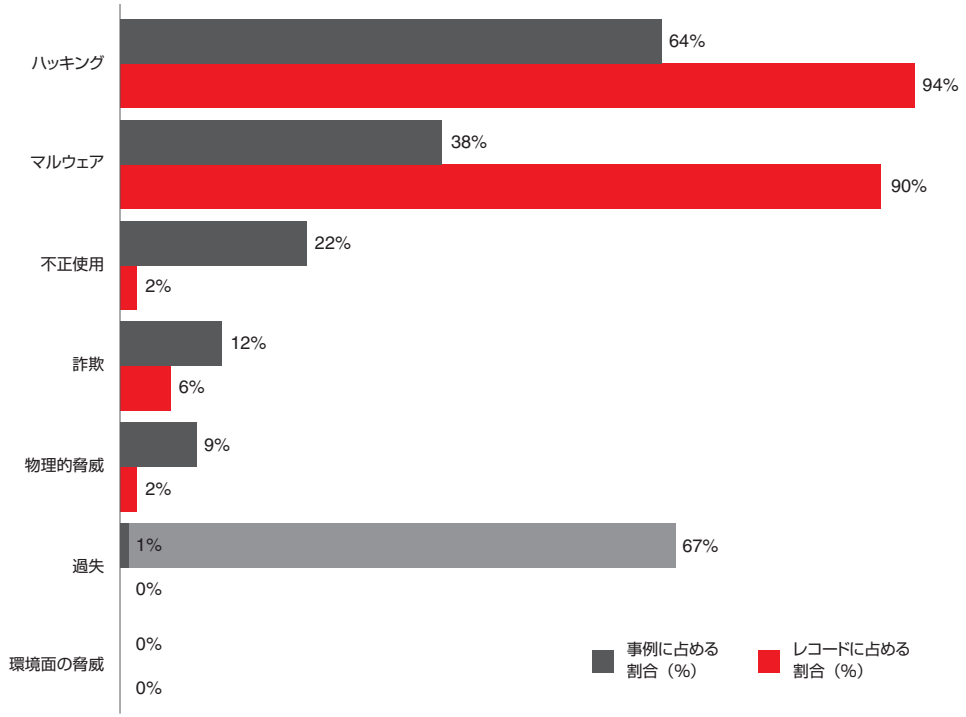
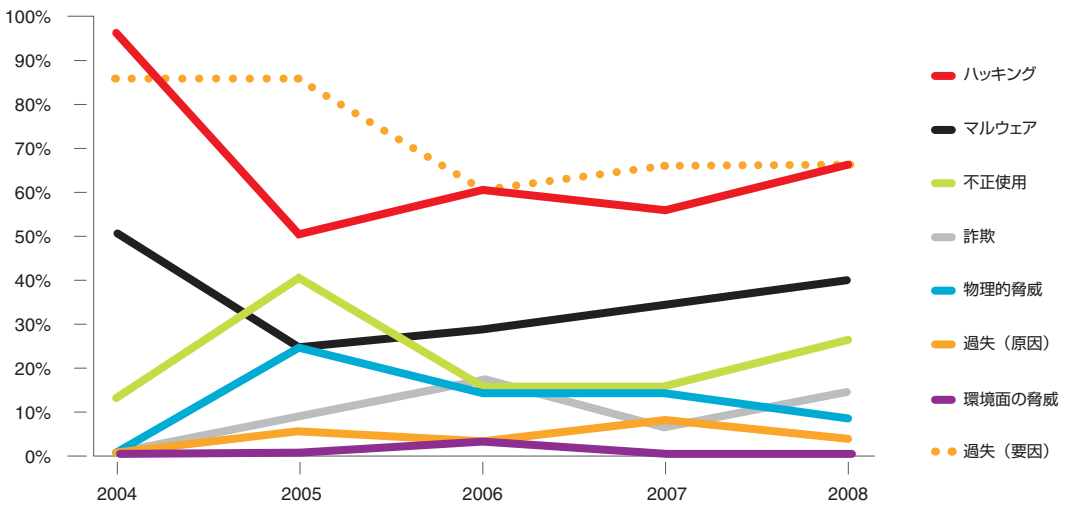


図 14. 各脅威分類に該当する漏洩 / 侵害の割合の推移



ハッキングと侵入

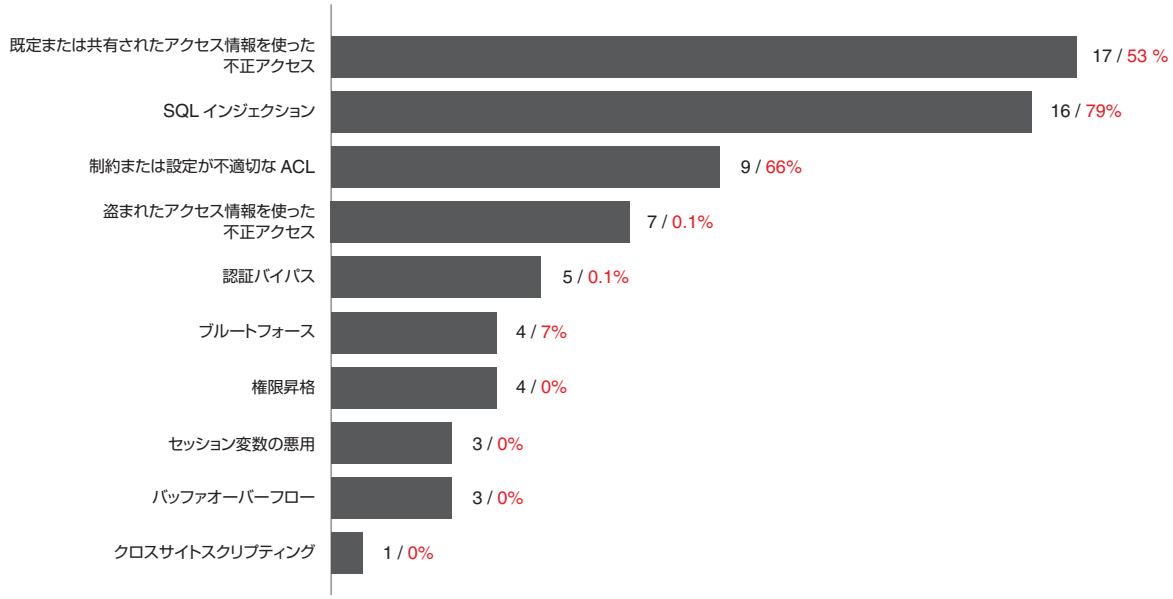
情報システムに対する悪意のある行為に関しては、5 年連続でハッキングがデータ漏洩 / 侵害の原因として首位でした。ハッキングは他の攻撃方法が受けるような制約（物理的な接近、人間との接触、特殊な権限などの必要性）をそれほど受けないため、これは意外ではありません。また、ツールが多数出回っており、このようなツールを使って攻撃プロセスを自動化したり高速化したりできるため、犯罪者にとっての攻撃のコストは比較的低く抑えられたままです。攻撃分類メソドロジーに精通している読者であれば、ハッキングおよび侵入のテクニックには実に多種多様なものがあることはご存じでしょう。2008 年の調査では、広く知られていて有効なこの脅威分類をさらに詳細化するために、調査対応（IR）事例の評価指標を拡張しました。図 15 は、昨年の漏洩 / 侵害調査中に Verizon Business によって確認されたハッキングの種類を示したものです。

グラフから明らかなように、多くの侵入は基本的なアイデンティティ管理（の不備）につけ込んだものです。デフォルトの認証情報、共有されたアクセス情報、または盗まれたアクセス情報を使っての不正アクセスは、件数では「ハッキング」の分類全体の 3 分の 1 を上回り、漏洩 / 侵害を受けた全レコードに占める割合では 50%を超えています。とくに憂慮すべきなのは、これらの攻撃は比較的容易に防ぐことができたにもかかわらず、デフォルトの認証情報または共有されたアクセス情報が利用された大規模な漏洩 / 侵害があまりにも多く発生していたことです。これらの分類は 2 つの異なった問題を表しているように思われることから、デフォルトの認証情報と共有されたアクセス情報がひとまとめに扱われるのを疑問に思った読者もいるかもしれません。その疑問に対する答えは、これらの問題が近い時期に相次いで見つかることが多かった、というものです。今回、同じ業界に属する複数の企業がすべて、きわめて短い期間のうちに漏洩 / 侵害の被害を受けた一連の事例について、その全体を対象とした調査を行いました。ほどなくして、各企業が社内システムのリモート管理を同じサードパーティベンダーに委託していたことが判明しました。さらに悪いことに、そのベンダーは既定のユーザー名とパスワードの変更を怠り、複数のクライアントに対して同じアクセス情報を使用していました。

憂慮すべきもう 1 つの問題は、それらの漏洩 / 侵害（および、被害を受けたレコードのかなりの割合）が、アクセス制御リスト（ACL）の不適切な設定に起因していたことです。かなりの数の事例で、ACL の設定が誤っていたせいでアタッカーに対して広く門戸が開かれ、やすやすと通過できる状態だったことが判明しました。最も抵抗が少ない経路を犯罪者が選択することが当然である以上、自由なアクセスを許す弱点につけ込まれたのも当然のことです。

なんとかしてアクセス権を不正に入手する必要があるハッカーにとって、SQL インジェクションは疑いなく最も都合の良いテクニックだと考えられます。2008 年の調査では、SQL インジェクション攻撃は漏洩 / 侵害に利用された件数では 2 位（16 件）、被害を及ぼしたレコード数では 1 位でした（総計 2 億 8500 万レコードの 79%）。最も初歩的な SQL インジェクション攻撃は、ユーザー入力の検証が適切に行われない弱点を利用します。この攻撃でとくに頻繁に標的とされるのは、カスタム開発アプリケーションと Web フロントエンドです。サードパーティの OS やプラットホームに固有の脆弱性を見つけられない場合、犯罪者はアプリケーション開発プロセスに潜む弱点を探し出して利用します。SQL インジェクションについての認識はもう何年も前からセキュリティ業界に浸透しており、この攻撃による被害がいまだに蔓延していることに驚く読者もいるかもしれません。とはいえ、アプリケーションの脆弱性の修正には高度な技術、高いコスト、そして多大な時間が必要となる可能性があり、それらの要因はすべて、この種の大規模な攻撃が長きにわたって観測されることの原因です。また、とくにデータ漏洩 / 侵害に利用されるものに関して、SQL インジェクション攻撃はますます高度なものに進化を遂げています。この攻撃は多くの場合、システムのより深くへとアクセスしてゆき、悪意のあるソフトウェアを仕掛ける目的で使用されます。ハッキングのテクニックに関連して、バッファオーバーフロー、セッション変数の悪用、権限昇格などのより一般的に知られたハッキングテクニックが、今回の調査データではそれほど多く確認されていないことも注目に値します。

図 15. ハッキングの種類別の漏洩 / 侵害件数（黒）および全レコードに占める割合（赤）



脆弱性の利用

構成上の弱点または機能性を利用した攻撃とは対照的に、パッチ適用可能な脆弱性を利用した攻撃の減少傾向は 2008 年も続きました。確認された漏洩 / 侵害のうち、パッチ適用可能な脆弱性を利用した攻撃によって引き起こされたのは 6 件だけでした。ここで使用している「パッチ適用可能な」という表現は、セキュリティに携わるすべての人々にとってこの脆弱性が同じ意味を持つとは限らないことに配慮して慎重に選ばれたものです。プログラミングエラーや不適切な設定･構成も広義の脆弱性には含まれますが、質の低いコードを常にパッチ適用によって修正できるとは限らず、管理上の不手際もパッチで修正することはできません。その上、多くのカスタム開発アプリケーションまたはプロプライエタリアプリケーションには、パッチの定期的な作成または配布のスケジュールがそもそも存在しません。

表 2 は、パッチが提供済みだった脆弱性を利用された 6 件の漏洩 / 侵害について、パッチが公開されてから被害が発生するまでの期間を示したものです。結果は前回の報告書と同様で、パッチがリリースされてから、脆弱性が利用されてデータ漏洩 / 侵害が発生するまでに 1 年以上の期間があったケースがほとんどです。脆弱性は確かにデータ漏洩 / 侵害に結びつく問題ですが、より早急なパッチ適用は解決策ではありません。今年の調査結果も前年までと同様、計画を立てて戦略的にパッチを実装するのがデータ漏洩 / 侵害を防止する上で有効である、という考えを支持する結果になっています。この方法は、パッチが出るたびにシステムに適用するという「火消し」式の方法より格段に効果的です。

表 2. パッチ公開から漏洩 / 侵害までの期間

1 ヵ月未満	0
1 ～ 3 ヵ月	0
3 ～ 6 ヵ月	0
6 ～ 12 ヵ月	1
1 年超	5

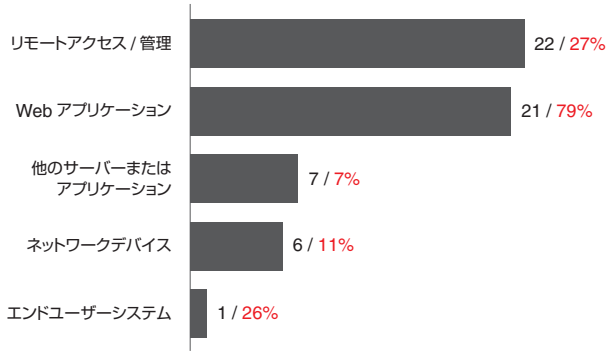
攻撃のベクトル

ハッキング活動をより深く調査すると、大部分の攻撃が、実行基盤のオペレーティングシステムまたはプラットフォームではなく、アプリケーションおよびサービスを標的とし続けていることは明白です。これらのうち、リモートアクセスサービスと Web アプリケーションは、大半の事例でアタッカーが企業システムへのアクセス権を獲得するために利用したベクトルでした。ネットワークデバイスが攻撃の手段として利用される場合もあ りますが、2008 年に起きたそのような攻撃の頻度はかなり低いものでした。

ハッキングが関与した漏洩 / 侵害の約 4 割で、アタッカーは何らかのリモートアクセス / 管理ソフトウェアを使って企業のシステムに不正にアクセスしました。これらの接続のほとんどは、企業内では使用されず、リモートからのシステム管理を委託した第三者企業（パートナー）に供給されていました。今回および前回の報告書でたびたび述べているように、パートナーによる攻撃も確かに存在しますが、攻撃の真の黒幕はパートナーではないのが一般的です。それよりも多いのは、外部の人間や組織がパートナーのシステムやネットワークに侵入し、信頼された接続を使って被害者企業のシステムにアクセスする手口です。被害者からはアタッカーが正規の第三者、たとえばリモート管理を請け負っているベンダーのように見えることから、このようなデータ漏洩 / 侵害はとくに対応が困難です。信頼されたアクセスにデフォルトの認証情報が使われていたような場合、対応はなおいっそう困難です。

Web アプリケーションに対する攻撃は、リモートアクセスサービスに対する攻撃に比べると件数こそ少ないものの、被害を及ぼしたレコード数では全体の 79%とはるかに上回っています。以前の議論を踏まえれば、Web アプリケーションを対象とした攻撃では SQL インジェクションが多数を占めることを容易に推測できます。興味深いことに、SQL インジェクションがこれほど多用される理由は、先述したリモートアクセス / 管理ソフトウェアにまつわるシナリオに関連します。Web アプリケーションとバックエンドデータベースを適切に機能させるためには、両者間に信頼関係を設定する必要があります。この状況では、アプリケーションからの要求は特権を持つ管理

図 16. 攻撃の侵入経路と漏洩 / 侵害件数（黒）および全レコードに占める割合（赤）



者からの要求に近いものになります。データベースはアプリケーションによって要求された情報をその通りに出力し、コマンドが有効なものか、それとも外部のアタッカーによって不正な文字列が渡された結果であるのかを検証しません。これは、システムの物理的な窃盗または制御を伴わない攻撃の防止に、データベースの暗号化が限られた有効性しか持たないことの主な理由の 1 つです。

ルーター、スイッチ、その他のネットワークデバイスを標的としたハッキングの割合は大きく低下しました。これには無線ネットワークも含まれていますが、無線ネットワークは、データ漏洩 / 侵害を狙った攻撃の標的になりにくい傾向が続いています。2008 年の調査対象事例全体で見ても、無線ネットワークが不正にアクセスされた事例は 1 件だけであり、それに伴って被害を受けたレコード数は 2008 年に被害を受けた全レコードの 0.01%にすぎません。2007 年も同じ件数でした。さらに比較すると、2004 年から 2006 年にかけて調査された事例のうち、無線ネットワークが関係していたのは 13%でした。ちなみに、被害を受けたのはすべて合法的な企業内無線 LAN であり、必要な認可を得ずに配備された違法デバイスではありませんでした。この減少には多くの理由がありますが、初期設定状態のセキュリティの向上、暗号化の使用の広がり、攻撃実行のための接近の必要性などは理由の一部にすぎません。Web ベースのアプリケーションやリモートアクセスツールは、その運用上の性質そのものにより、企業ネットワークへの侵入経路を探している外部の人間や組織にとってはるかに目に留まりやすく、アクセスも容易です。

ルーター、スイッチ、その他のネットワークデバイスを標的としたハッキングの割合は大きく低下しました。2008 年の調査対象事例全体で見ても、無線ネットワークが不正にアクセスされた事例は 1 件だけです。

マルウェア

Verizon Business の独立部門である ICSA ラボは、情報セキュリティ業界内で高い信頼を得ている、サードパーティ製品のテストおよび認定サービスを提供しています。IR チームのメンバーによって調査中に発見された悪意のあるソフトウェア（マルウェア）は、分析のために ICSA ラボに送られます。調査担当者はこの分析結果を活用して、攻撃の封じ込め、マルウェアの除去、被害の回復などを支援する、よりきめ細かなサービスを顧客に提供します。以下に示す情報は、こうした協力によって実現された調査に基づくものです。

マルウェアは、2008 年の 1 年間に調査された事例の 3 分の 1 超に関与し、漏洩 / 侵害の被害を受けた全レコードに対する寄与度では 9 割に達しています。数年前まで、マルウェアの配布形態として一般的だったのは自己複製形式の電子メールウイルスやネットワークワームでした。これらは迅速かつ広範な拡散を主な目標としており、システムの可用性が損なわれたり、大がかりなクリーンアップ作業が必要になったりする結果をしばしば招いていました。過去 5 年間でこれらの目標は変質しました。マルウェアは今や、ほぼすべての大規模なデータ漏洩 / 侵害事例の不可欠な構成要素です。システムの内側に犯罪者を導き入れるハッキングに対して、マルウェアはデータを取ってきて犯罪者のもとに届けます。マルウェアを仕掛けることに成功した犯罪者が、できるだけ多くのデータを盗み出すために、発覚の可能性を最小限に抑えたいと考えるのは当然のことです。そのような理由から、マルウェアは目標選択型の性質をますます強め、精巧さや発覚しにくさも格段に向上しています。

マルウェアの配布方法としては、アタッカーがシステムに侵入し、リモートからそのシステムにマルウェアをインストールする手口が最も多く利用され、2 位以下に大差を付けました。より重要なのはおそらく、この方法によって配布されたマルウェアによる被害が、2008 年に漏洩 / 侵害の被害を受けた全レコードの 89%にも及んでいることです。7 件の感染は Web サイト経由で発生し、そのうち 4 件はユーザーの対話処理を必要としない「自動」ダウンロードでした。それ以外の 3 件は、従業員によって明示的にダウンロードされ、インストールされました。2008 年の事例のうち、パッチ適用可能な脆弱性を利用するマルウェアが関与していたのは 4 件だけでした。これらすべての事例で、感染を防ぐために必要なパッチは 1 年以上前から提供されていました。

感染経路についての重要な推論は、被害者の環境内に仕掛けられた後でマルウェアがどのような動作をするかです。以前の報告書では、ほとんどのマルウェアの動作は、データを収集してローカルに保存する、データを収集してリモートの人間や組織に送信する、感染したシステムへのリモートアクセスまたはそのシステムの制御を可能にする、のいずれかだと述べました。また、これら 3 つの機能を実行する割合はほぼ同等であると述べていました。図 18 に示すように、2008 年に確認されたマルウェアも同様の結果を示します。

図 17. マルウェア感染経路と漏洩 / 侵害件数

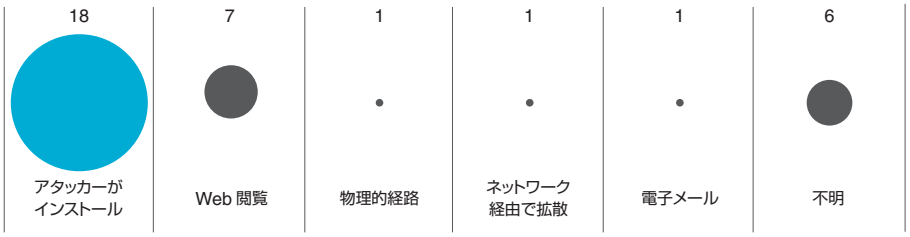
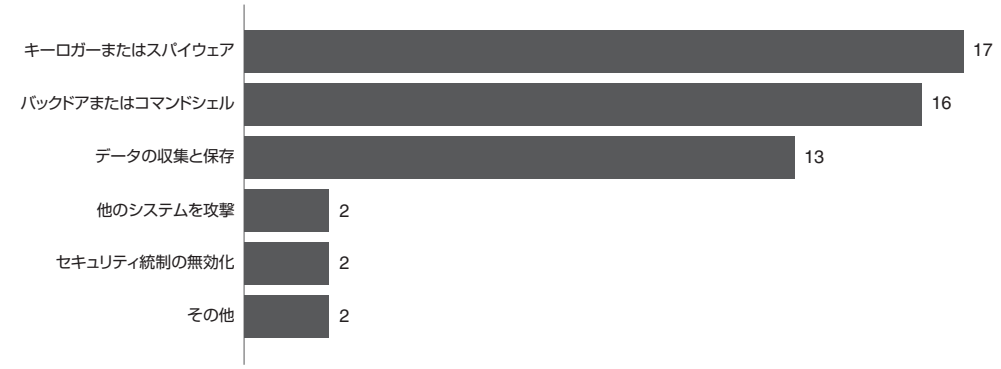


図 18. マルウェアの機能と漏洩 / 侵害件数



最も多く利用されたマルウェアの機能は、キーボードロガーまたはスパイウェアでした。これらの機能は一般に、認証情報を収集する目的で利用されます。収集された情報はリモートのアタッカーに送信される場合がほとんどで、ローカルに保存して後で取得するという使われ方はまれです。その理由は、情報を含んだパケットのサイズが小さく、検知されずに外部に送信できる可能性が高いためと考えられます。犯罪者はしばしば、これらのアクセス情報を、企業システムに対する後続の攻撃やより高度な攻撃に使用します。

2008 年に漏洩 / 侵害の被害を受けた全レコードの 82%に関係し、大量の機密データを盗み出すのに最も効果的なマルウェアは「収集して保存する」種類です。一般的に、このような機能を持ったマルウェアをアタッカーが好んで使用するのは、クレジットカードのデータや個人識別情報(PII)を盗み出すことが目的の場合です。なぜなら、多数のレコード情報を含んだ巨大なファイルを頻繁にエクスポートしていたのでは、犯行が発覚する可能性が高くなるからです。もちろん、盗み出した情報を被害者のシステムに置いておくという方法にも、特にその情報をどうやって持ち出すか、という点で課題があります。この問題を解決するためにアタッカーがよく用いる方法は、見つかることなくシステムに再び侵入するためのバックドアを、犯行が発覚するまでの間（一般的には数ヵ月程度）開けたままにしておくというものです。2008 年の事例では、マルウェアがデータを収集しローカルファイルに保存していたすべての事例で、調査担当者はバックドアツールまたはコマンドシェルツールを発見しました。

最近のデータ漏洩 / 侵害事例で、上記のような機能を持ったマルウェアの利用が増加している現象は、この報告書で前にも述べたサイバー犯罪市場のプレッシャーに由来するものですが、そのような現象は、コンプライアンスに関する各種の標準および要件の採用が広く普及したことに対する直接的な反応でもあります。各組織は、コンプライアンスを達成して維持するために必要な形式および程度をもって、規定された統制対策の実装を進めています。共通した弱点への対処も（着実ながらも確実に）進んでいることから、これは全体としては、各組織の内部でのデータ保護にとってよい傾向です。たとえば、それほど機密性の高くないデータは通常の業務活動の中でそのまま保存し、長く保持するデータについては暗号化する、といった取り組みが各組織で始まっています。パブリックネットワークやプライベートネットワーク上を流れる、暗号化されていない情報の量は減っています。ただ残念なことに、犯罪者は、チャンスが失われビジネスモデルが行き詰まったことを嘆きながら無為に過ごしているわけではありません。新たな状況への適応を日々模索しています。

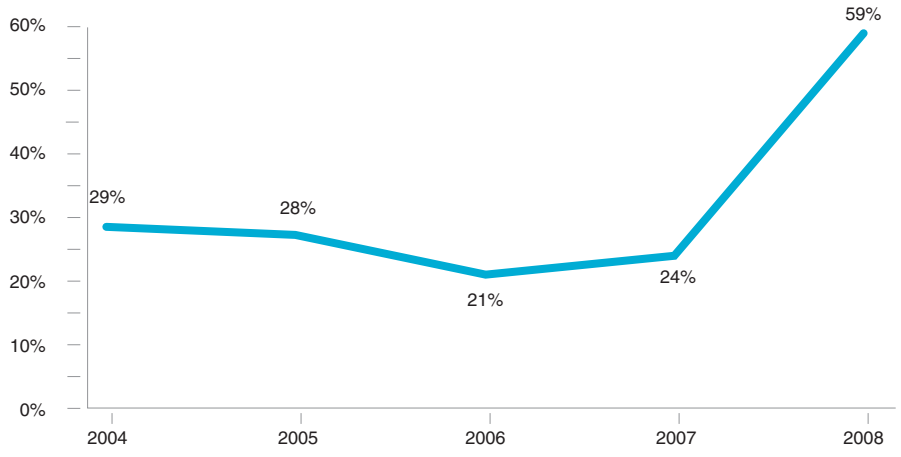
各組織が規制要件への適合を目指して動き始める中、そのコンプライアンスプロセスの一環として実装された特定の統制を回避するように設計された攻撃の明らかな増加が確認されました。より新しく、より精巧なマルウェアユーティリティは、既存のデータ統制や暗号化の網をかいくぐり、被害者の環境から後日入手できる脆弱なデータストアを実質的に作り出します。この手法の例としては、メモリスクレーパー、高度なパケットキャプチャユーティリティ、そしてマルウェアを使用し、割り当て解除されたディスク領域の内部で、またページファイルから特定のデータシーケンスを識別して収集する、というものがあります。

ただ残念なことに、犯罪者は、チャンスが失われビジネスモデルが行き詰まったことを嘆きながら無為に過ごしているわけではありません。新たな状況への適応を日々模索しています。

「保存されたデータ」という用語は従来、一時的でない項目（具体的には、ハードディスク、CD、またはバックアップテープ上のログファイル内またはデータベース内部の項目）を指していました。ただし、システムの RAM の内部にある一時的な情報記憶域は、通常はこれに含まれません。ほとんどのアプリケーションベンダーはメモリ内のデータを暗号化せず、長年にわたって RAM は安全であると考えてきました。しかしながら、システムの RAM をリアルタイムで解析し、機密情報を見つけることのできるマルウェアの登場により、これはデータセキュリティの防御上の弱点になりました。

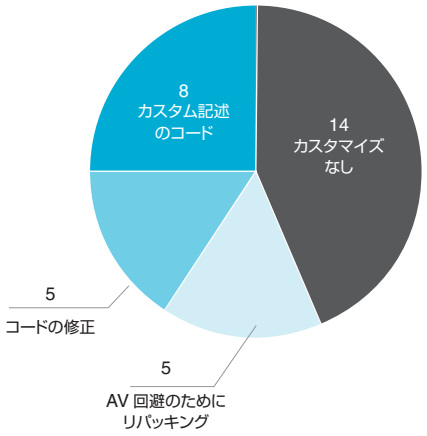
この拡張された機能はもちろん、魔法のように働くのではありません。悪意のあるプログラムをまた新しく作成したり、既存のプログラムを大幅に修正したりする必要があります。これは相当な時間、費用、そして専門知識を要する作業であり、そのような投資を積極的に行う、または行う準備ができている犯罪者はそれほど多くはありません。ただし、そのような投資が行われているとした場合、それは組織犯罪の豊富な資金の援助を受けているか、または貴重なデータという大きな獲物の期待に駆られてのものです。2008 年はこの傾向が顕著でした。この期間中、カスタマイズされたマルウェアの割合は 2 倍以上に上昇し、調査対象の全サンプルの 59% に達しました。

図 19. マルウェアのカスタマイズ（マルウェアが関与した漏洩 / 侵害に占める割合の推移）



これらの事例で、カスタマイズの程度や種類は実にさまざまでした。図 20 はこれを一般的に表したものです。一部のアタッカーは、単に既存のマルウェアをリパッキングすることで、そのシグネチャがウイルス対策ソフトウェア（AV）スキャナーによって検出されないようにしました。既存の悪意のあるコードを修正して機能を追加したり、被害者の環境に合わせてコードをカスタマイズしたりして利用したアタッカーもいました。ただし、2008 年に最も多かったのは、攻撃のために（見かけ上は）完全にゼロから作成されたマルウェアでした。やや控えめな統計によると、2008 年に漏洩 / 侵害の被害を受けた 2 億 8500 万レコードのうちの 85%は、カスタム作成のマルウェアによって収集されました。以前から存在していたコードが ICSA ラボの専門家とツールによって認識されなくなった可能性はありますが、このことは全体的な論点にはほとんど影響しません。

図 20. マルウェアのカスタマイズ（漏洩 / 侵害件数順）



より重要なのは、マルウェアの性能および適応性の向上もさることながら、データを侵害する目的に使用されるほとんどのマルウェアは最新の AV によって検出できないという点です。都合の悪いことに、多くの組織では、マルウェアの予防および検出のための主要な手段として AV に頼っています。AV は確かに基盤となる統制ですが、マルウェアの絶え間ない進化を考えれば、マルウェアへの対抗手段を AV のみに依拠するセキュリティ態勢は不安定なものになります。

不正使用と悪用

脅威としての不正使用とは、企業や組織のリソースや権限を、そのリソースや権限の本来の意図または目的に反して使用することをいいます。インサイダーやパートナーはある程度まで企業から信頼されていることが多く、そのため、不正使用はとくにインサイダーやパートナーに関連する脅威といえます。

全体としては、漏洩 / 侵害の 22%が何らかの形の不正使用によって引き起こされました（図 13 を参照）。システム権限の悪用を伴った漏洩 / 侵害のほうが通常はかなり大きな被害につながることから、インサイダーおよびパートナーによる不正使用が、2008 年に漏洩 /

より新しく、より精巧なマルウェアユーティリティは、既存のデータ統制や暗号化の網をかいくぐり、被害者の環境から後日入手できる脆弱なデータストアを実質的に作り出します。

侵害の被害を受けた全レコードの 2%にしか関与していないという事実は意外に思われます。ただし、2008 年はやや通常と異なる傾向が見られた年でした。また、この調査結果は、内部原因による漏洩 / 侵害に関して以前に示した結果と完全に符合します。さらに、そのような攻撃はより集中的に行われる（利用するつもりのものだけを盗む）傾向があり、レコード数の指標を使って判断するのには適さない種類のデータを標的としています。数百万件のクレジットカード番号に埋もれてしまう場合がありますが、1 つの IP アドレスの「レコード」のほうが被害の大きさという面でずっと大きな意味を持つことがありえます。

表 3 は、これらの事例で確認された不正使用の種類を示したものです。驚くようなことではありませんが、多かったのはシステムのアクセス権と権限の悪用でした。これらのほとんどは管理者権限を持つインサイダーによって犯されたもので、性質的には計画的で悪質です。悪意のないポリシー違反は、データの漏洩や消失の原因になることもありますが、その程度は大きくありません（ただし、セキュリティインシデント全体で見れば、このような違反は間違いなく、漏洩 / 侵害に限定されたこれらの数値が反映するよりもずっと多く発生しています）。そのような活動が、組織にマルウェアが入り込む経路になっているケースが非常に多くなっています。横領の事例も 2 件確認されました。

表 4 のデータは、従業員が不正使用に関与する場合に、より大規模なデータレポジトリーが狙われる傾向があることを示しています。ワークステーションとノートパソコンが関係するインシデントがポリシー違反に関連付けられていた一方で、サーバー関連の漏洩 / 侵害の大半は権限の悪用が原因でした。他の調査ではポータブルメディアがデータ漏洩 / 侵害の主な原因であることが示されたにもかかわらず、この種のデバイスが使用された事例が 1 件しか確認されなかったことは、興味深く注目に値します。その上に、この特定の事例では、ポータブルメディアの使用は漏洩 / 侵害の成否を分ける要因ではありませんでした。データ移動のための便利な手段として USB メディアが使われたにすぎません（そのようなデータ移動は、仮に USB メディアが使えなかったとしても他の手段で実行できたでしょう）。

詐欺攻撃とソーシャル攻撃

この分類には、詐欺または虚偽表示の使用が含まれます。それらの行為の目的は、人を騙したり、セキュリティ対策や手順の隙を突いたり、データ漏洩 / 侵害の目標達成を促進するその他のあらゆる手段を利用することです。これらの行為は、技術的手段と非技術的手段のどちらによっても実行できます。詐欺の一般的な例には、ソーシャルエンジニアリングとフィッシング詐欺があります。2008 年の調査データでは、その両方が確認されました。詐欺が明白であったのは事例の 12%にとどまり、これらの行為は全レコードの 6%の漏洩 / 侵害に関係していました。

表 3. 不正使用の種類と漏洩 / 侵害件数

システムアクセス / 権限の悪用	15
その他のセキュリティポリシー違反	6
PC/ 電子メール /Web 使用ポリシーの違反	5
横領	2

表 4. 不正使用された資産の種類と漏洩 / 侵害件数

データベースサーバー	6
アプリケーションサーバー	5
ノートパソコン	5
ファイルサーバー	3
公共キオスク端末	2
POS システム	2
ワークステーション	2
ポータブルメディア	1

表 5. 詐欺およびソーシャル攻撃の経路と漏洩 / 侵害件数

電子メール	5
対面	4
Web/ インターネット	3
電話	1
メディアまたは新聞	1
インスタントメッセージ	0

表 6. 詐欺およびソーシャル攻撃の標的と漏洩 / 侵害件数

エンドユーザー	8
パートナーまたは顧客	2
人事担当	1
IT 管理者またはスーパーユーザー	0
ヘルプデスク	0
上級管理職	0

表 7. 物理的攻撃の種類と漏洩 / 侵害件数

資産の盗難	5
システムアクセス（キーボードによる）	2
装置またはシステムの不正操作	2
資産の紛失または移動	0
盗聴	0
観察またはショルダーサーフィン	0
強要または脅迫	0

詐欺活動の大半は電子メールやインターネットを通じて実行されました。ただし、すべての詐欺が対人以外の手段で実行されたわけではありません。ソーシャルエンジニアリングのいくつかの事例では、対面または電話による手口も確認されています。Web と電子メールは、フィッシングや、詐欺に分類されるその他の攻撃の媒介として機能しました。

詐欺を用いた攻撃の主な標的はエンドユーザーでした。そのような攻撃には、この報告書の他の調査結果に加えて、エンドユーザーレベルでのより効果的なセキュリティ認識プログラムによる対処が必要です。

物理的攻撃

物理的攻撃に起因するデータ漏洩 / 侵害は下位にとどまり続けています。この調査結果は、漏洩 / 侵害統計の一般的な情報源と整合性が取れていないように思われる読者もいるでしょう。これにはいくつかの正当な理由があり、すべての原因は今回の調査対象事例に関係します。まず、ノートパソコンの紛失や盗難など、多くの物理的インシデントはデータ漏洩 / 侵害を引き起こすことはないものの、一部の規制ではそのインシデントの公表が義務づけられています。一方、今回の調査データは、実際の漏洩 / 侵害が発生したインシデントのみで構成されています。このことが結果に大きく影響しています。次に、物理的なイベントという性質上、検証可能なフォレンジックス証拠が残りにくいことから、第三者による調査が不可能になります。

2008 年に起きた漏洩 / 侵害のうち、物理的攻撃が関係していたのは 8 件だけでした。表 7 にその分類を示します（1 件の事例で 2 つの行為が関係していたため、数値の合計が 9 になっています）。窃盗の事例にはワークステーション、文書、バックアップテープが関係していた一方で（ノートパソコンは含まれません）、システムアクセスはオンラインデータレポジトリーに関連していました。不正操作の事例は 2 件とも、小売店の POS システムに接続された PIN 入力デバイスが関係したものです。

物理的攻撃の種類に加えて、調査担当者はこれらの漏洩 / 侵害が発生した場所にも注目しました。ここでも、漏洩 / 侵害の件数より数値が多くなっています。これは、1 件の精巧な犯行が複数の場所にまたがって実行されたことによるものです。主な観察結果としては、被害者にとっての外部の場所と内部の場所の比率がほぼ半々になっています。

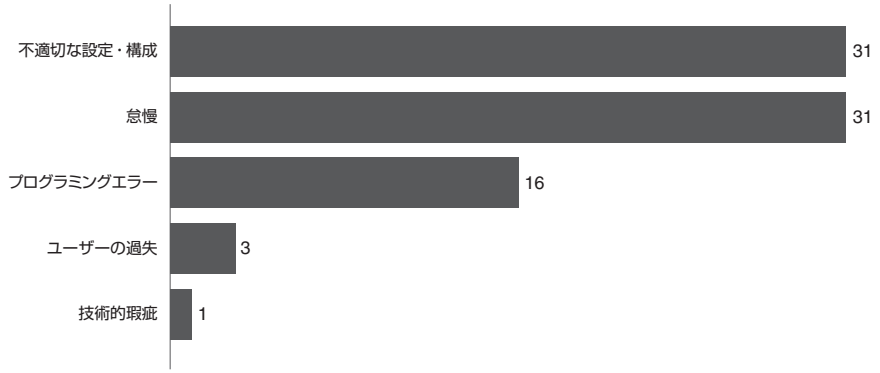
表 8. 物理的攻撃の場所と漏洩 / 侵害件数

被害者側の場所 : 社内、部外者が立ち入り可能なエリア（ロビー、荷物搬入所など）	3
外部の場所 : 店舗、レストランなど	2
外部の場所 : 従業員の自宅または自家用車内	2
外部の場所 : 空港、駅、地下鉄など	1
外部の場所 : ビジネスパートナーの施設	1
被害者側の場所 : 社内のワークスペース（キュービクル、オフィスなど）	1
被害者側の場所 : 社内の高セキュリティエリア（サーバールーム、研究開発施設など）	1
被害者側の場所 : 屋外の会社敷地（駐車場など）	0

過失と怠慢

広い意味では、データ漏洩 / 侵害を発生させる要因（脅威）は、ほとんど全部が過失といってもいいかもしれません。ここで過失とは、不適切な意思決定、コンプライアンス非準拠、システムの不適切な設定·構成、不適切な手順などを指し、このような過失が重なってインシデントにつながります。過失はきわめて多いことから、今回の報告書では、漏洩 / 侵害を直接引き起こした、または大きな影響を与えた過失だけを調査対象としました。図 13 では、「直接原因」（脅威）としての過失と「寄与要因」（防御の失敗）としての過失の違いを考慮して、過失を示すバーを色の濃い部分（原因）と薄い部分（要因）に分けています。過失がデータ漏洩 / 侵害の直接原因である割合は、過失が漏洩 / 侵害の発生につながる複数の要因のうちの 1 つである割合に比べてずっと低いことが明らかです。直接原因と寄与要因に加えて、図 21 に示す種類に過失をさらに分類することにします。この図は、過失が確認された 2008 年の事例全体における各過失の相対的な分布を表します。

図 21. 過失の種類と漏洩 / 侵害件数



「怠慢」と「不適切な設定・構成」を使用することで、ある程度論点が明確になります。「怠慢」は、組織で策定されたポリシーまたは一連の手順の順守が徹底していない状況を指します。この意味で、「怠慢」は組織が適切なセキュリティ対策を講じていないこと（本調査の方針ではこれを過失と見なさない）と同義ではなく、システムの配備と日常的な管理の過程に見られる、より積極的な形態の過失である「不適切な設定・構成」とも異なります。怠慢は 2004 年から 2007 年にかけては結果のかなりの割合を占めていましたが、2008 年にはその割合は低下しました。このことが、昨年 1 年間で保証のメカニズムが劇的に改善されたことに起因するものであれば良かったのですが、残念ながらそうではなく、統計の方針を変更したことが実際の理由です。怠慢に分類される過失の割合があまりに高かったため、定義をより厳密にして「プログラミングエラー」の分類を追加しました。

ここで過失とは、不適切な意思決定、コンプライアンス非準拠、システムの不適切な設定・構成、不適切な手順などを指し、このような過失が重なってインシデントにつながります。

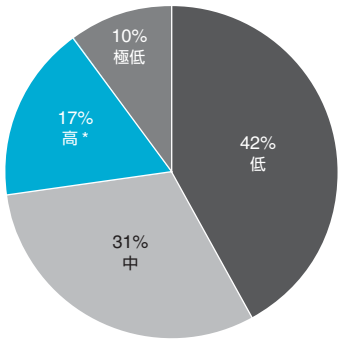
図 21 に示すように、データ漏洩 / 侵害に寄与した過失の分類の中では、不適切な設定・構成が怠慢と並んで首位でした。2008 年は、周辺デバイスの ACL の設定または制約が不適切だった事例がかなりの件数確認されました。怠慢の一般的な例には、ポリシーで禁止されているにもかかわらず既定のパスワードを使用していた、というものがあります。このような一般的なミスを識別して是正するための手順を設計することは、ほとんどの組織でセキュリティ対策の強化に非常に有効であることは明らかです。記録された過失の 21%は、不適切なコーディング慣習に起因していました。当然のことながら、この種の過失は SQL インジェクションやそれに類する攻撃の発生と密接に関係します。安全なコードを書くことは容易ではありませんが、そのためのトレーニングとツールは存在します。以上の調査結果を踏まえれば、開発者はその両方を利用するのが賢明であるといえます。

攻撃の難しさ

データ漏洩 / 侵害に結びつく攻撃の相対的な難しさは、現在の脅威環境だけでなく、現代のセキュリティ態勢の状況を示す優れた指標であります。各事例の調査中、調査担当者は攻撃の詳細を評価し、以下の難易度に各攻撃を分類しました。

- **極低：**特別な技術やリソースを必要としない攻撃です。このような攻撃は、普通のユーザーでも可能です。
- **低：**基本的な方法である、カスタマイズを加えない、必要なリソースが少ない、のいずれかまたは全部の性質を持った攻撃です。自動ツールによる攻撃で、実行者はスクリプトキディー（幼稚なクラッカー）です。

図 22. 攻撃の難しさと漏洩 / 侵害に占める割合



* 難易度の高い攻撃は、漏洩 / 侵害の被害を受けた全レコードの 95%に関係していました。

このページ内容に関するコメントまたは質問をお寄せください（英語のみ）

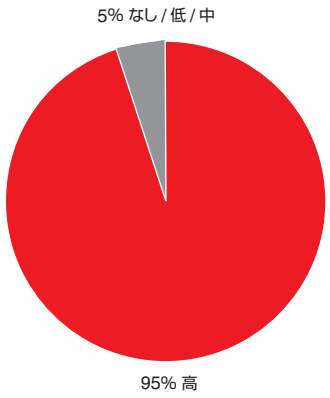
http://securityblog.verizonbusiness.com/category/2009dbir/ にアクセスし、「Attack Difficulty」のページから英語でコメントを投稿できます。

- **中：**スキルとテクニックが必要、多少のカスタマイズを加える、ある程度のリソースが必要、のいずれかまたは全部の性質を備えた攻撃です。
- **高：**高度なスキル、大幅なカスタマイズ、質量ともに豊富なリソース、のいずれかまたは全部が必要な攻撃です。

多少の主観を含んでいますが、これは有益な測定基準であると考えられます。

前回の DBIR で示された重要な調査結果の 1 つは、半数以上の漏洩 / 侵害が、むしろ初歩的な攻撃によって引き起こされているというものでした。2008 年の事例も、多少の誤差はあるもののきわめて似通った統計を示しています。特別なスキルやリソースを必要としない漏洩 / 侵害（極低）の割合が増加した一方で、「低」難易度の攻撃は減少してその伸びを相殺しました。「中」難易度の攻撃は数ポイント上昇し、「高」難易度の攻撃は同じ割合のままでした。これらの微妙な差は取るに足りないもので、2008 年に攻撃のパラダイムが変化したことの根拠としては不十分です。全体としては、企業の情報システムを侵害するために犯罪者が莫大な苦労を強いられるという段階にはまだ至っておらず、そのような傾向は 2008 年になっても前年までとあまり変わらなかったように見受けられます。ただ、この統計の見かけに騙されてはいけません。

図 23. 攻撃の難しさと全レコードに占める割合



過半数の漏洩 / 侵害が高スキルの攻撃の結果ではないというのは事実ですが、データを別の角度から見ると、本当に価値の高い標的の攻略には途方もない努力が要求されることが読み取れます。図 23 に分かりやすく示されているように、調査対象事例全体で漏洩 / 侵害の被害を受けた 2 億 8500 万レコードのうち実に 95%の被害が、件数ではそれほど多くない高難易度の攻撃によってもたらされています。実に驚くべき統計であり、これはより大きなストーリーの一部です。

ハッキング行為の詳細についての節で述べるように、企業システムに侵入するために犯罪者が用いるテクニックは、それほど高度なものはまだ多くありません。デフォルトの認証情報や ACL の不適切な設定の悪用にはそれほど高いスキルは必要ありませんが、攻撃の端緒としては、より精巧な攻撃と同じくらい有効な場合があります。データを収集および侵害したり、システムにアクセス可能な状態を永続的なものにしたりすることを試みる攻撃はますます複雑化しています。これらを遂行するための手段は通常はマルウェアであるため、マルウェアは現代の攻撃の難易度を決定づける要素になりました。そのようなことから、難易度の高い攻撃を防ぐことは必ずしも難しいとは限りません。いささか平凡かもしれませんが、ここでは「後手に回るよりも早めに手を打ったほうが、攻撃を最も効率的かつ効果的に防止できる」というメッセージを強調しておきます。

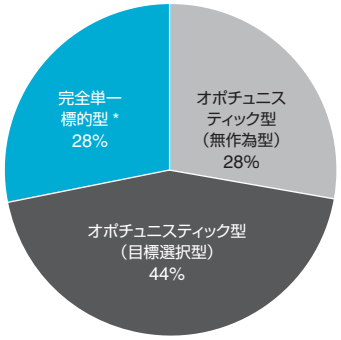
2008 年の DBIR では、十分な時間、リソース、そして意欲さえあれば、犯罪者は事実上、どのような単一組織であっても侵害を加えることが可能だが、すべての組織を侵害するのに必要なリソースは持ちあわせていない、ということを述べました。逆に言えば、アタッカーにとって情報の価値が非常に高くても、その企業の防御が固く侵害が不可能であれば、限られたリソースをつぎ込むのは最良の策ではありません。防御の弱い企業を狙ったほうが楽なのです。これらの統計から明確になるのは、高度なスキルを持ったサイバー犯罪者は、容易に実行できるピッキングを差し控え、きわめて価値の高い標的を優先しているという事実です。2008 年は残念ながら、犯罪者がその労苦に見合った成果を手に入れた年でした。

攻撃の標的選定

セキュリティ業界では一般に、アタッカーによる攻撃を大きくオポチュニスティック型攻撃と単一標的型攻撃に分けています。この分類にはグレーゾーンが多いため本報告書では、オポチュニスティック型攻撃を 2 つに分けることにしました。アタッカーによる攻撃としては、次のように定義するとします。

- **オポチュニスティック型攻撃（無作為型）:** 無作為かつ広範囲にわたって弱点のあるシステムを探しながら目標を定め（多数のアドレスをスキャン）、その弱点を利用して攻撃。
- **オポチュニスティック型攻撃（目標選択型）:** システムのうち何らかの弱点があると分かっているシステムを選び、その弱点を利用して攻撃。
- **完全単一標的型攻撃:** まず特定の目標を決め、使用することに決めた何らかの方法を使ってデータ漏洩 / 侵害を実行。

図 24. 単一標的型攻撃とオポチュニスティック型攻撃が漏洩 / 侵害に占める割合



* 単一標的型攻撃は、漏洩 / 侵害の被害を受けた全レコードの 90%に関係していました。

犯罪者は高価値の標的に狙いを絞り、その標的の防御をかいくぐるために設計された精巧な攻撃を構築しているようだという前節のメッセージを前提にして、2008 年は単一標的型の攻撃が増加した、という推論が成り立つかもしれません。今回の調査で扱った事例の証拠を踏まえれば、それは正しい推論であるといえるでしょう。実際、単一標的型攻撃はここ 5 年間で最高を記録しており、漏洩 / 侵害の被害を受けた全レコードの 90%に関係しています。この観点から 2008 年の特異性を裏付ける比較を挙げると、2004 年から 2007 年の調査で漏洩 / 侵害の被害を受けた約 2 億 3000 万レコードのうち、完全単一標的型攻撃の結果であったのは 14%にすぎませんでした。金融サービス企業は、大量の消費者データを処理、送受信、保存するという理由で、たびたび犯罪者の標的に選ばれます。

昨年の報告書で述べたように、とくに小売業界と飲食料品業界で、完全に無作為でもなければ完全に単一標的型でもないように思われる漏洩 / 侵害が数多く確認されています。代表例として、まず、アタッカーは A 小売店チェーンの X ソフトウェアにアタッカーが不正にアクセスし、その後、B 小売店チェーンでも X ソフトウェアを使用していることを知ります。その後の攻撃では、利用できる弱点があるというだけの理由で、B 小売店チェーンが標的とされます。

2008 年に、利用できる弱点の完全無作為な探索またはスキャンによって引き起こされた漏洩 / 侵害は、以前の年に比べると減少しています。すべての組織で実施することが望ましい基本的な自己診断の 1 つは、自分たちの組織が、単一標的型攻撃とオポチュニスティック型攻撃のどちらの対象になる可能性が高いかを見極めることです。前者の場合、確信的かつ高度な攻撃を予測して、それに備えます。後者の場合、攻撃の標的とされる確率を下げるために、アタッカーにつけ込まれる機会を最小化するような対策を講じます。少なくとも、自分たちの組織が他の組織よりもアタッカーに目を付けられにくいことを確認します。

すべての組織で実施することが望ましい基本的な自己診断の 1 つは、自分たちの組織が、単一標的型攻撃とオポチュニスティック型攻撃のどちらの対象になる可能性が高いかを見極めることです。

このページ内容に関するコメントまたは質問をお寄せください（英語のみ）

http://securityblog.verizonbusiness.com/category/2009dbir/ にアクセスし、「Attack Targeting」のページから英語でコメントを投稿できます。

漏洩 / 侵害の対象となる資産

ここで、各種の攻撃により漏洩 / 侵害の被害を受ける情報資産の種類に話題を移します。ここでは、攻撃の侵入経路ではなく終点に焦点を当てます。前回の報告書と比較できるよう、図 25 では前回と同じ資産グループを使用します。これらの資産の詳細に興味がある読者のために、表 7 ではより具体的な分類を示しています。

オンラインデータ（各種のサーバーおよびアプリケーション）は 5 年連続で、漏洩 / 侵害の被害を受けることが最も多かった資産であり、2 位以下を大きく引き離しています。また、2008 年の調査対象事例全体で漏洩 / 侵害の被害を受けた 2 億 8500 万レコードのほとんどすべて（99.9%）がこのグループに属します。図 25 に示すように、5 年間の調査期間中、オンラインデータがレコードに占める割合は一貫して高い割合を保っています。リモートからアクセス可能な大規模データストアが、サイバー犯罪活動の標的であり続けていることは明らかです。

図 25. 資産の種類と漏洩 / 侵害件数の割合（黒）およびレコード数の割合（赤）

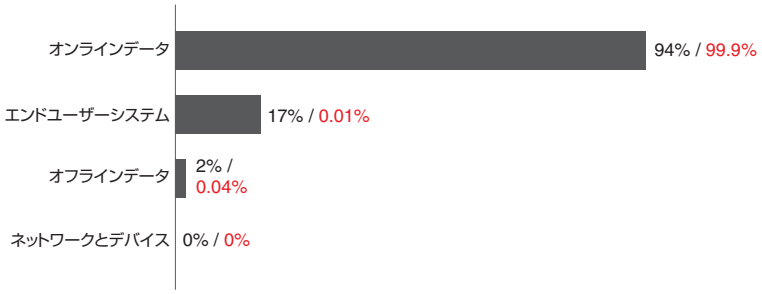


表 9 のオンラインデータをもう少し詳しく見ると、POS システムは漏洩 / 侵害にさらされる機会が最も多かったものの、レコード数の割合はわずかにとどまりました。POS システムの漏洩 / 侵害で主に被害に遭ったのは小売業界および飲食料品業界であると推測されます。データベースは、事例数に占める割合では 2 位ですが、被害を受けたレコードの数では非常に大きな割合を占めました。表 9 のその他のオンラインデータについては、合計すると漏洩 / 侵害の件数では約 3 分の 1 を占めましたが、データの被害はアプリケーションサーバーに集中していました。

オンラインデータに関連した最後の要点の 1 つは、仮想化です。昨年の報告書の発表後、仮想化に関して調査結果がどのような意味を持っていたかについて議論が起こりました。そのため今回は、事例に関係する資産が仮想化されていたかどうかにあえて注目しました。2008 年の事例中、資産が仮想化されていた事例は 5 件ありましたが、何らかの形で漏洩 / 侵害に関係していたものは 1 件もありませんでした。

オフラインデータ、モバイルデバイス、エンドユーザーシステムに関しては、不安の声が大きく、かなりのセキュリティ予算も投じられていますが、今回検証できた調査データに限った範囲では、これらの資産は漏洩 / 侵害とほとんど関わりがありませんでした。従業員によるポータブルメディアの不正使用やノートパソコンの紛失が実際に起こっていることは間違いなく、DatalossDB.org* や ID Theft Center** のような公開型の漏洩 / 侵害開示リストの情報に基づけば、これらの資産に関連したインシデントで多数のレコードの漏洩が報告されていることも明らかです。そのような傾向が今回の報告書の結果に反映されていないことは、今回の調査対象事例、調査データ、そしてデータ漏洩 / 侵害の一般的性質の副産物です。Verizon Business では、デバイスの紛失に関連した調査に従事する機会はそれほど多くなく、今回の調査データは漏洩 / 侵害が確認された事例のみに限定されています。さらに、紛失または盗難に遭ったノートパソコンやメディアに入っていた情報は、犯罪者によってアクセスされたり悪用されたりすることはめったにありません。データがリスクに瀕している状況は、多くの場合報告が必要ですが、実際のデータ漏洩 / 侵害と同じではありません。

*http//datalossdb.org
**http://www.idtheftcenter.org

このページ内容に関するコメントまたは質問をお寄せください（英語のみ）

http://securityblog.verizonbusiness.com/category/2009dbir/ にアクセスし、
「Compromised Assets」のページから英語でコメントを投稿できます。

図 26. オンラインデータ資産から漏洩 / 侵害の被害を受けたレコードの割合

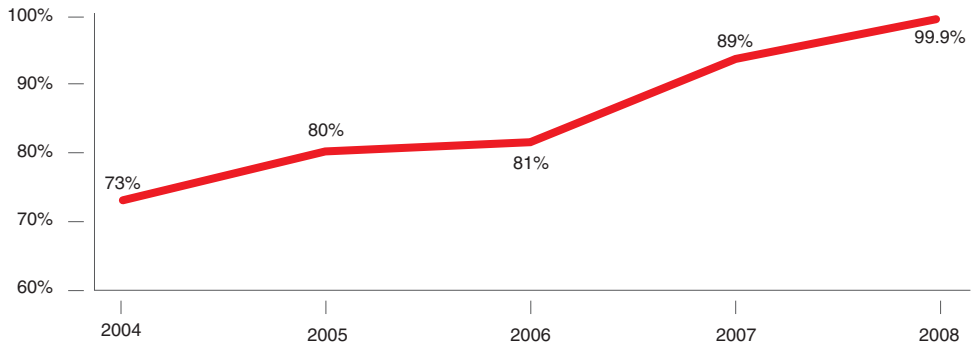


表 9. 漏洩 / 侵害の被害を受けた資産の詳細リストと漏洩 / 侵害件数およびレコード数に占める割合

資産	資産グループ	漏洩 / 侵害に占める割合（%）	レコードに占める割合（%）
POS システム	オンラインデータ	32%	6%
データベースサーバー	オンラインデータ	30%	75%
アプリケーションサーバー	オンラインデータ	12%	19%
Web サーバー	オンラインデータ	10%	0.004%
ファイルサーバー	オンラインデータ	8%	0.1%
公共キオスク端末	オンラインデータ	2%	0.4%
認証 / ディレクトリサーバー	オンラインデータ	2%	0.1%
バックアップテープ	オフラインデータ	1%	0.04%
文書	オフラインデータ	1%	0.000%
ワークステーション	エンドユーザーシステム	8%	0.01%
ノートパソコン	エンドユーザーシステム	4%	0.000%
PIN 入力デバイス	エンドユーザーシステム	2%	0.004%

漏洩 / 侵害の対象となるデータ

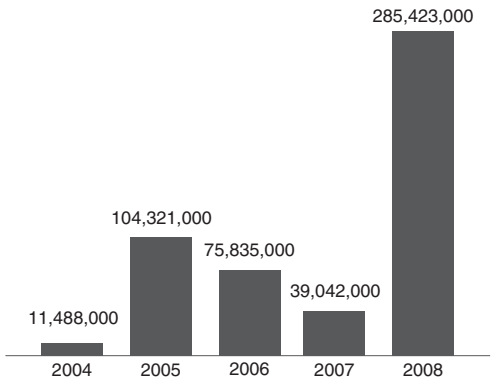
Verizon Business が調査した漏洩 / 侵害の事例で被害に遭ったレコードの数だけに限れば、2008 年は記録的な年でした。2008 年に被害に遭ったレコードの数は、1 年間の数字としては過去最高であるばかりか、その前の 4 年間を合わせた数字をも上回りました。IR チームが過去 5 年間に調査した事例で被害に遭ったレコードの数は 5 億を超えます。

そのような異常ともいえるレコード数が 2008 年に記録されたことは、数件のきわめて大規模な漏洩 / 侵害の結果です。上位 5 件の漏洩 / 侵害で、被害を受けたレコード全体の 93%を占めています。漏洩 / 侵害 1 件あたりのレコード数の平均が約 450 万であった一方で、中央値は 37,847 でした。これらの統計から、調査データは明らかに偏っており、図 28 の分布でもその偏りを確認できます。

昨年の報告書で指摘したとおり、データ漏洩 / 侵害の調査で重要な要素の 1 つに、その漏洩 / 侵害の結果として被害を受けたデータの種類を特定することがあります。ここで特定された種類により、組織の対応戦略は大きく左右されます。たとえば、被害を受けたデータの種類によっては、その事実の公表や通知が必要になります。また、規制に厳格にしたがって扱うことを求められたり、不正アクセスを厳重に監視しなければならない種類のデータもあります。これは、データ漏洩 / 侵害が発生した場合、被害を受けた組織だけでなく何百万人という個人がデータ漏洩 / 侵害の影響を受ける可能性があり、そうした個人への通知も必要になるためです。

全体としては、2008 年の結果はその前の 4 年間の結果とある程度一貫しています。調査対象事例に占める割合では、クレジットカード情報の漏洩 / 侵害が依然として 80%近くを占め、数字上は他の種類のデータを大きく引き離しています。1 年間で漏洩 / 侵害の被害に遭った全レコードのうち、クレジットカード情報の漏洩 / 侵害が関係していたものは 98%に上ります。IP アドレスなどの他の種類のデータを狙う特殊なグループもありますが、大多数のサイバー犯罪者の望みは、手っ取り早く容易に成果を手に入れることです。クレジットカード情報はその条件を満たします。このことの証拠として、調査した事例の 83%で、盗まれたカードデータの詐欺的使用が確認されました。

図 27. Verizon Business が調査した各年の漏洩 / 侵害で被害を受けたレコード数

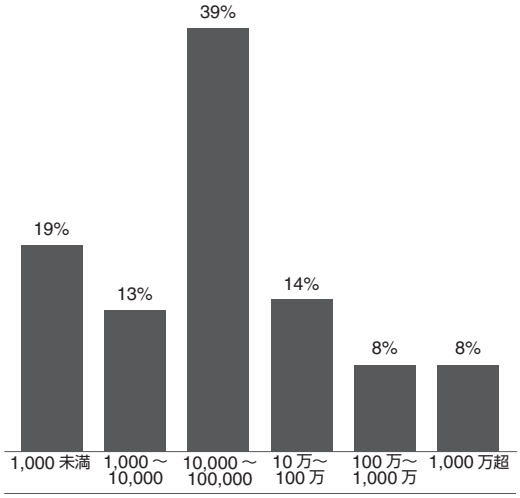


先に示したクレジットカードデータの漏洩 / 侵害の割合には、カード介在詐欺およびカード不介在詐欺を働くのに十分な通常のデータシーケンスだけでなく、消費者のクレジットカード口座に関連付けられた個人識別番号（PIN）情報も含まれています。後者が標的とされる割合は 2008 年にますます増加しました。これらの攻撃では、磁気ストライプデータの保存場所が識別され、その場所から PIN とともにデータが盗み出され、より有害な形態のアイデンティティ詐欺のお膳立てをしています。これにはたとえば、偽造カードによる ATM からの現金引き出しやその他の PIN ベースの取引が含まれ、実際の現金や関連資産が直接、消費者から盗み取られる事件にしばしば結びついています。PIN 情報に対する攻撃は、統計的に 2008 年の調査対象事例全体の中でもそれほど大きな割合を占めているわけではありませんが、被

このページ内容に関するコメントまたは質問をお寄せください（英語のみ）

http://securityblog.verizonbusiness.com/category/2009dbir/ にアクセスし、
「Compromised Data」のページから英語でコメントを投稿できます。

図 28. 漏洩 / 侵害の規模と被害に遭ったレコード数の分布

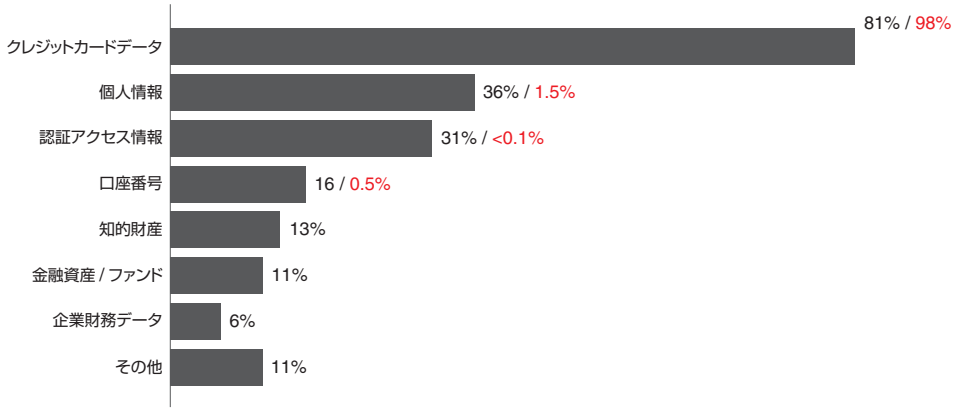


害に遭った一意のレコード数という点では最も深刻な事例である個人データ窃盗事例の代表的な例です。言い換えれば、PIN ベースの攻撃と、漏洩 / 侵害の被害に遭ったレコード数が前年から大きく増加したことの間には密接な関係があります。

個人識別情報（PII）は漏洩 / 侵害の被害を 2 番目に多く受けたデータの種類ですが、その情報が詐欺行為にも役立つことを考えればこの結果は理にかなっています。その名が示すとおり、PII には名前、ID 番号など、人の一意なアイデンティティの要素が含まれています。認証アクセス情報の盗難は、2008 年に発生した漏洩 / 侵害事例の約 30%を占めましたが、これは 2004 年から 2007 年にかけての数字の 2 倍に上っています。このことが犯罪戦略の何らかの変化を示唆するかどうかは不明なままです（この数字は 2007 年までは毎年減少していました）。アクセス情報は確かに、不法行為を目的としたアクセスがやりやすくなるという見込みをアタッカーに与えます。また、この報告書のハッキングに関する節で既に示した結果を見る限り、アタッカーはそうした 利点を活用しているように見受けられます。

まだ漏洩 / 侵害全体に占める割合は低いものの、調査対象事例で確認された知的財産の窃盗は 2008 年、過去 5 年間で最高を記録しました。そのようなインシデントは数こそ少ないものの、業務を揺るがすような出来事になる可能性があります。口座番号と金融資産は、2008 年にデータの種類のリストに追加されました。どちらもまだ数は少ないものの、それぞれ複数の事例が確認されました。口座番号は多くの場合銀行口座のもので、クレジットカード番号とは別物です。理由は明白ですが、これら 2 種類のデータは多くの場合、同時に被害に遭います。2008 年には、被害に遭った口座から数百万ドルが直接盗み出される事件が発生しました。

図 29. 漏洩 / 侵害の被害を受けたデータの種類と漏洩 / 侵害件数（黒）およびレコード数（赤）*



* 一部のデータの性質により、図 29 に示されたすべての種類がレコード統計の割合に含まれているとは限りません。

多くの知られていない要素

数年前の調査事例の中で、調査が不明なシステム、見落とされた資産、または忘れられた資産に結びつくことを避けられないという、ある強力なパターンが出現しました。頻繁に確認されるようになったそのようなシナリオはいつしか「多くの知られていない要素」と呼ばれるようになりました。そのようなシナリオには、以下のいずれかが含まれます。

- **システム**のうち、企業または企業の業務部門が、その存在を知らなかったシステム（サーバーやデスクトップなど）に対するデータ漏洩 / 侵害（知られていないシステム）
- システムに保存されている**データ**のうち、企業が、その存在を知らなかったデータに対する侵害（知られていないデータ）
- 企業が気がつかないうちにネットワークに**接続**またはアクセスされ、その結果、発生したデータ漏洩 / 侵害（知られていない接続）
- システムに知られていないアカウントまたは**権限**が存在したことにより発生したデータ漏洩 / 侵害（知られていない権限）

図 30. 多くの知られていない要素と漏洩 / 侵害に占める割合

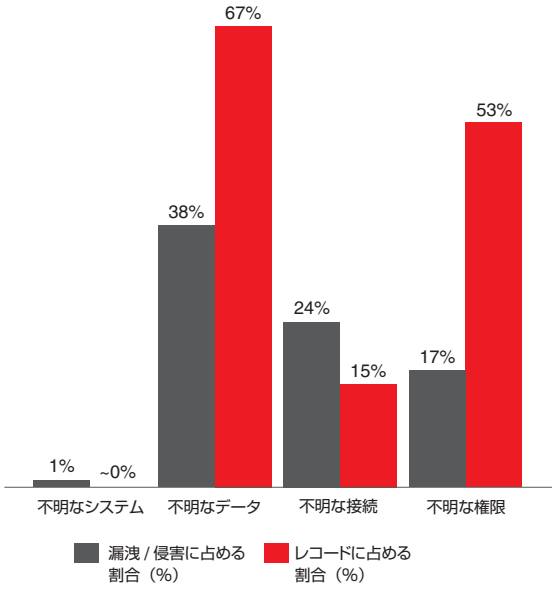


図 30 は、2008 年の事例のうち、これらの各要素がデータ漏洩 / 侵害に寄与したもの割合を示します。

2008 年に調査されたすべての漏洩 / 侵害の約半分で、少なくとも 1 つの不明なタイプが確認されました。これは大きな割合ですが、その前の 4 年間の 90%という数値からは大きく低下しています。不明な接続は 25%弱にとどまり、不明な権限は 7%上昇した一方で、完全に不明の資産は 1 つの事例で確認されたのみでした。システムに存在することを被害者が知らなかったデータの割合は大幅に低下し、この差によって、2008 年の調査データとそれ以前の調査データの間にある大きな差はほとんど説明がつきます。このような変化が生じた正当な理由は、何らかの種類のサンプリング効果のほかにもいくつか存在します。

2008 年のデータ漏洩 / 侵害調査補足報告書に、金融サービス業界の組織では他の業界に比べて不明なシステムが確認されることは少ない、という記述があったことを覚えている読者もいるかもしれません。金融サービス業界の組織は、2008 年の調査対象事例の中でも大きな割合を占めていることから、金融サービス業界で不明なシステムの確認例が少なかったことが、不明なシステムの統計値を引き下げるのに寄与したと考えるのは合理的です。また、不明な権限の増加と不明な接続の減少もこれによって説明がつくかもしれません。第 2 に、この報告書の他の節で述べられている調査結果に基づけば、単一標的型攻撃とカスタマイズされた攻撃が今年、通常よりも数多く確認されたことは明らかです。犯罪者は「最も貴重なお宝」を狙っているように見受けられ、被害者は通常、それらのお宝のありかを知っています。これらの漏洩 / 侵害は、意図しないデータ移行の結果として生じることも確かにありますが、それよりもむしろ、犯罪者の強い意志と、機密データが含まれているシステムを被害者が適切に防御できないことの組合せによって生じます。さらに、多くの漏洩 / 侵害である種の不明データが確認されましたが、それはマルウェアによって収集され、組織がその存在を知らないシステムに保存されたデータでした。

このページ内容に関するコメントまたは質問をお寄せください（英語のみ）

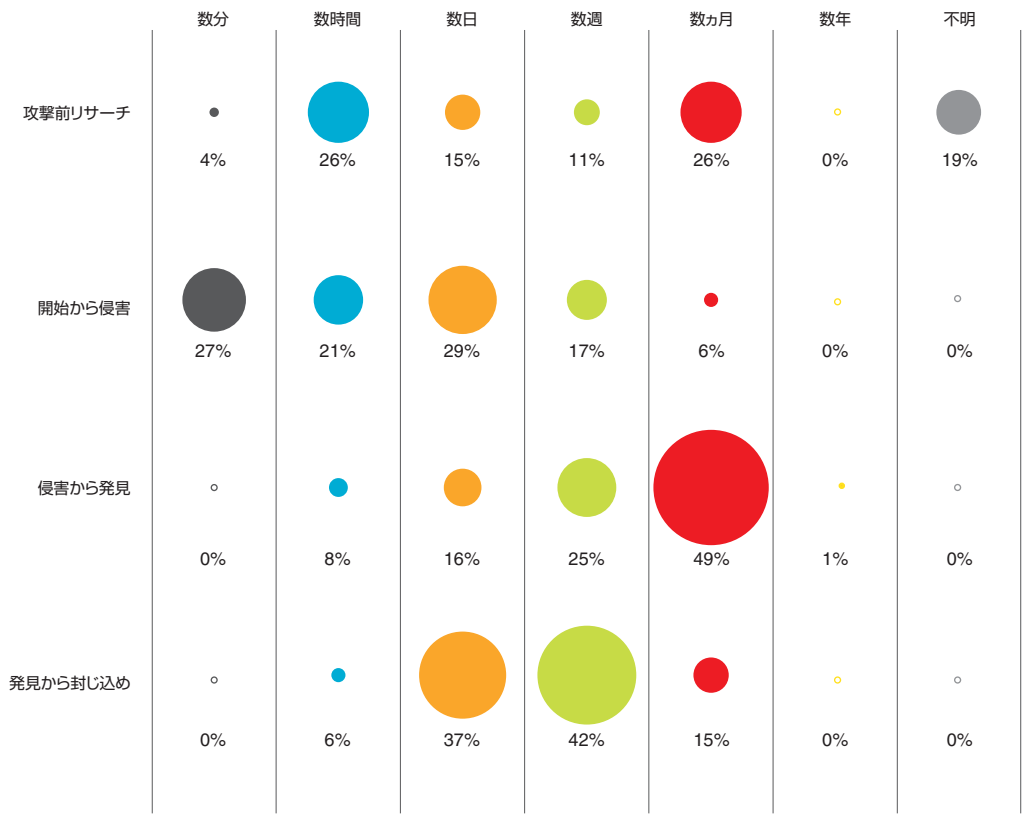
http://securityblog.verizonbusiness.com/category/2009dbir/ にアクセスし、
「Unknown Unknowns」のページから英語でコメントを投稿できます。

不明なデータが関係する漏洩 / 侵害は減少しましたが、アカウントと権限の不適切な管理は、漏洩 / 侵害の事例に占める割合と被害を受けたレコード数の両面で、近年ますます問題の度を強めています。図 30 を見る限り、「多くの知られていない要素」が確認される事例はまだ相当数に上ります。これは、IT 運用環境の可視性を高めて変動性を下げることが、リスク管理対策の最優先事項であることを示唆しています。

漏洩 / 侵害の段階

何らかのイベントが始まってから実際のデータ漏洩 / 侵害が発生し、その後の対応に至るまでの流れは、各種の要素によって大きく異なります。急速に展開する攻撃もあれば、長期にわたる計画と実行を必要とする攻撃もあります。分析の目的のために、開始から侵害、侵害から発見、発見から封じ込めの 3 つの段階にインシデントを大きく分けることにします。攻撃前リサーチに費やされた時間の長さについての情報も興味深いものであるため、入手可能であれば記録されます。次の図は、各段階の間に経過した時間の長さを示したものです。

図 31. 漏洩 / 侵害の各段階と各段階終了までの所要時間（期間）分布



このページ内容に関するコメントまたは質問をお寄せください（英語のみ）

http://securityblog.verizonbusiness.com/category/2009dbir/ にアクセスし、「Time Span of Breach Events」のページから英語でコメントを投稿できます。

攻撃前リサーチ

攻撃前活動の確固たる証拠は把握するのが難しいことが多いのですが、調査担当者は、攻撃開始よりも前の時点にさかのぼって、攻撃についての情報をできるだけ多く識別しようと努めます。そのような試みを繰り返すことで、標的がどのようにして捕捉されたか、どのような偵察方法が使用されたか、そして最も重要な点として、差し迫った攻撃のどのような兆候が被害者に前もって警告されたか、に関してのヒントが解明されます。

2008 年の事例のうち、調査担当者が攻撃前リサーチの何らかの兆候を発見できたのは半数未満でした。最も多く用いられた手法は、基本的なシステムフットプリンティング、スキャニング、対象システムに関わる一覧情報の取得でしたが、アタッカーが被害者の拠点内を偵察した事例も確認されています。最後に挙げた行動の目的は、POS システムの製造元やモデルを調べたり、PIN 入力デバイス（PED）の不正操作に適した時間帯を特定するために人の出入りのパターンを調べたりすることです。いくつかの事例では、入手に成功したプライベート情報（ベンダーの顧客リストなど）を利用して、アタッカーが攻撃をさらにカスタマイズしたり、攻撃の標的をさらに広げたりした例も確認されています。図 31 に示すように、これらの活動を実施するために必要だった時間（期間）は数分から数ヵ月までさまざまでした。

開始から侵害

周辺部の侵害を終えた後で、アタッカーは被害者のネットワークとシステムを調べ、目的の情報を見つけます。この段階に必要な時間（期間）の長さは、アタッカーの事前知識、スキルセット、環境の熟知度、攻撃の方法、被害者の防御の強固さなどの要因に大きく左右されます。全体として、2008 年の事例は、2004 年から 2007 年にかけての調査データと非常に似通った分布を示しています。ただし、数分以内に発生する漏洩 / 侵害が増加し、所要時間は短縮されました。以前の調査と同様、半数近くの事例で、犯罪者は数分または数時間以内にデータにアクセスできるようになります。数日、数週間、数ヶ月、数年の各所要期間の割合はほとんど変わりませんでした。

侵害から発見

2008 年の調査では、組織が漏洩 / 侵害を発見するまでの時間（期間）は、全体的にわずかですが速まりました。ただし、「速まった」を「速くなった」と混同しないように、この結果には多少の補足が必要です。漏洩 / 侵害の 75%の事例では、数週間または数ヵ月経っても、封じ込めはおろか発見すらされていません。どのような組織のどのような最高セキュリティ責任者であれ、これをもって「速くなった」と呼べるかどうかは疑わしいものです。とはいえ、2008 年の調査では、発見までに数ヵ月から数年を要した漏洩 / 侵害はちょうど半分程度で、これは過半数を大きく上回っていた前年までの状況よりは大きく改善されました。明るいほうの話題では、数週間以内の発見は数ヵ月以内の発見よりも高い伸びを示し、数時間以内の発見は 5%増加しました。そうした傾向が今後も続くことを願うばかりです。

2008 年の調査では、組織が漏洩 / 侵害を発見するまでの時間（期間）は、全体的にわずかですが速まりました。ただし、「速まった」を「速くなった」と混同しないように、この結果には多少の補足が必要です。漏洩 / 侵害の 75%の事例では、数週間または数ヵ月経っても、封じ込めはおろか、発見すらされていません。どのような組織のどのような最高セキュリティ責任者であれ、これをもって「速くなった」と呼べるかどうかは疑わしいものです。

発見から封じ込め

前回の報告書では、この段階の名称は「発見から軽減（解決）」でした。その後、「封じ込め」という表現のほうがより分かりやすく意味を提示するという判断に至りました。ここでいう封じ込めとは本質的には「止血」を意味し、根本問題の対応戦略が完了したことを指すわけではありません。漏洩 / 侵害が封じ込められた時点で、不正アクセスは遮断され、情報の流出が止まります。

ご想像のように、データ漏洩 / 侵害の状況をできるだけ早急に封じ込めることは対応プロセスよりも優先されます。ただ残念なことに、この目標はめったに達成されません。過半数の漏洩 / 侵害が封じ込めまでに数週間以上の期間を要し、2 ～ 3 日以内に封じ込められたものは少数にとどまりました。問題の核心は準備が不十分であることだと考えられます。多くの組織は、危機が発生したときに対応する準備ができていません。このことの証拠として、インシデント発生時の適切な対応慣習に関連した調査結果では、大多数の組織が、インシデントに対処するための適切な準備をしていなかったことが示されています。次の「発見と対応」の節で、インシデント対応慣習の成熟度に関連する調査結果を提示します。

発見と対応

発見および封じ込めまでの時間（期間）の統計に加えて、発見方法、検出能力、インシデント対応慣習に関連した情報を活用することで、漏洩 / 侵害の頻度と重大度に寄与する要素についてより明確な理解を得ることができます。このトピックは非常に重要であるものの、前回の報告書の調査結果は物足りないものであったため、より精密な調査を可能にするための新しい評価指標が 2008 年の調査で追加されました。まず、発見の方法から検討します。

発見方法

昨年の調査では、漏洩 / 侵害の発生を組織が認識する方法に関して見直しを行いました。2008 年の調査でも、発見方法にそれほど大きな変化はなく、前年までと同様に過半数の漏洩 / 侵害が第三者によって発見されています。図 32 の「第三者からの連絡」の項目について、前回の報告書と分類が変わっていることに気づいた読者もいるでしょう。この発見方法は（今回の調査でもそうですが）割合が大きすぎたため、詐欺行為に関する連絡とそれ以外の連絡にこの項目を分けることにしました。この見方から明らかなのは、十分な数の詐欺的取引が発生し、第三者が漏洩 / 侵害のポイントを切り分けられるようになるまで、漏洩 / 侵害が気づかれないままである、ということです。

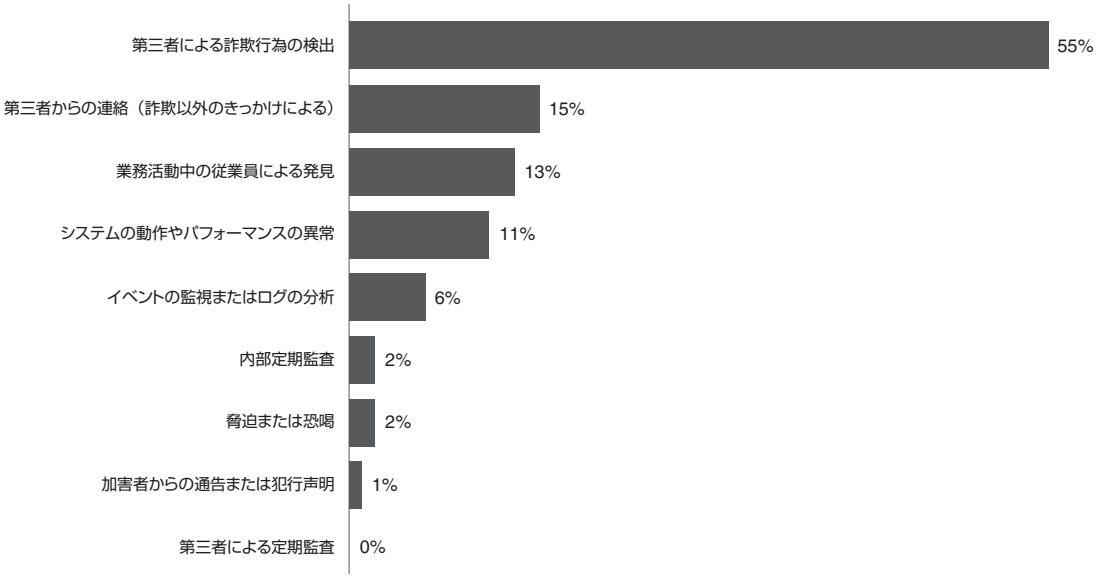
通常の業務活動中に漏洩 / 侵害をたまたま発見する従業員は 13%で、1 位の項目（第三者による検出または連絡の分類を合算したもの）から大きく離れた 2 位を維持し、システムの異常な動作が 11%と僅差でそれに続きます。これらの 2 つの方法は、計画的ではないものの、組織が自力で漏洩 / 侵害を発見する最大のチャンスとなっているように見受けられます。それは信じがたい話ですが、すべて同じような結果を示している 5 年間のデータから導かれた結論を否定するのも困難です。

図 33 は、漏洩 / 侵害の発見方法を簡略化して示したもので、第三者による発見と内部での発見の規則性を簡潔に対比します。以前の数年間に関しては、組織が講じた「積極的な」対策（明確に検出を目的として設計された対策を指す）によって検出された漏洩 / 侵害の割合はわずかにとどまりました。2008 年になっても、漏洩 / 侵害の発見の多くは相変わらず受動的な方法によるものだったことが読み取れます。

このページ内容に関するコメントまたは質問をお寄せください（英語のみ）

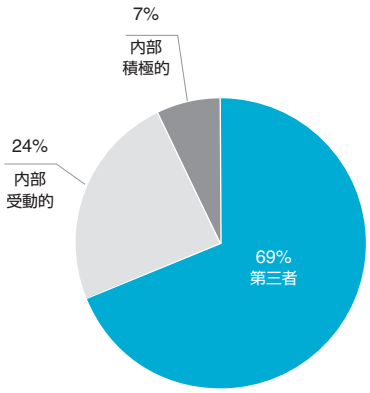
http://securityblog.verizonbusiness.com/category/2009dbir/ にアクセスし、
「Discovery and Response」のページから英語でコメントを投稿できます。

図 32. 漏洩 / 侵害の発見方法と漏洩 / 侵害に占める割合



以前からと同様、イベントの監視とログの分析の効果が明らかに低いことは理解に苦しみます。検出の機会は間違いなくそこにあります。調査担当者の指摘によれば、被害者の 66%については、漏洩 / 侵害を発見するための十分な証拠がログに残っていたにもかかわらず、イベントやログの分析への取り組みが熱心でなかったためにそのような証拠を見逃していました。その前の数年間よりは数字は下がっている（2004 年から 2007 年にかけての数字は 82%）ものの、この調査結果は、実現された有効性が潜在的な有効性をはるかに下回ったままであることを示唆しています。もちろん、有効性が期待値を下回るこのような状況の程度は、これらのテクノロジーの配備状況に大きく依存します。次の節でこれを検証します。

図 33. 漏洩 / 侵害の発見方法（簡易版）



検出型統制の利用

上記で提示された情報は、検出指向の統制の普及と運用面の成熟度についての明白な疑問を提起します。正解を見つけるために、調査担当者は 2008 年の調査対象事例から、各組織でのこれらの統制の利用状況についての情報を収集しました。調査結果を示したものが図 34 です。

このデータは、基本的なシステムログやデバイスログの域を越えた検出型統制が、漏洩 / 侵害の被害者の間でそれほど利用されていないことを示唆します。我々に近い思考プロセスを持った読者であれば、侵入検出システムの 30%という数字にすぐに目を留め、その低さに驚嘆したことでしょう。小規模であったり、セキュリティ

態勢が未成熟であったりする組織が多数を占めるサンプルから得られた結果だという理由により、これらの結果が無意味なように思えてしまうかもしれません。これは事実と異なり、大企業の状況を反映していないものとしてこれらの結果を無視するのは誤った判断です。予想に反して普及が進んでいないことは事実ですが、この結果を裏付ける正当な理由はいくつかあります。

まず、侵入検出システム（IDS）が導入済みであることはほぼ確実と思われた多くの大規模組織で、IDS が導入されていませんでした。IDS が配備済みであったにもかかわらず、有効化されていなかった組織もありました。さらに多く（約 12%）の組織では IDS によってネットワーク活動を監視していましたが、漏洩 / 侵害に関係した場所または資産で監視が行われていませんでした。その他の事例では、IDS やその他の検出機構の存在を（さまざまな理由により）確認できませんでした。最後に、調査対象に含まれていた一部の組織には、イベント検出に関する規範的なコンプライアンス要件が存在していなかったことは注目に値します。

IR チームが注目したのは、イベントの監視とログの分析によって検出された 5 件の漏洩 / 侵害のうち、3 件については syslog が収集され IDS が実行されていた、1 件については syslog の収集と定期的な確認が行われていた、1 件については図 34 に示したすべての検出型統制が採用されていた、という点です。

図 34. 漏洩 / 侵害の被害者への検出型統制の普及状況

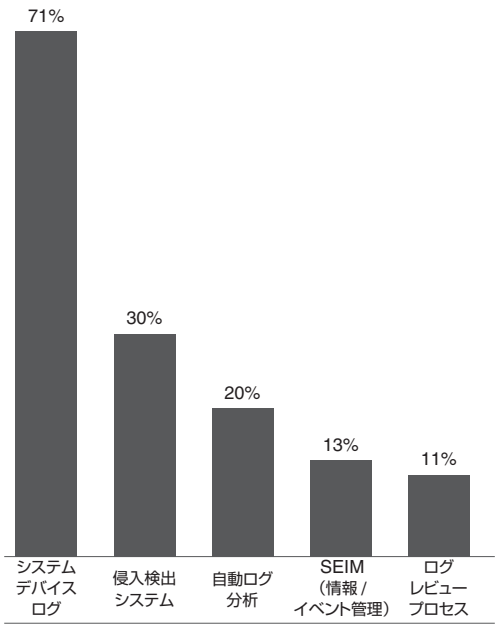


図 35. 漏洩 / 侵害の被害者へのインシデント対応慣習の普及状況

インシデント対応慣習

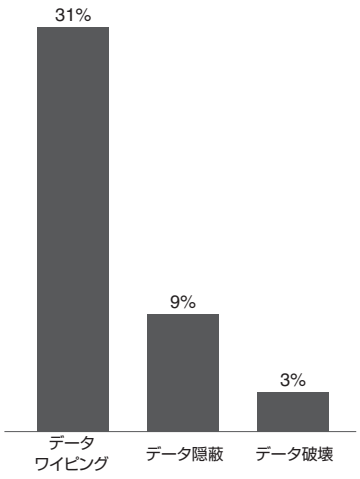
2008 年の事例の調査中、調査担当者は、図 35 に示したインシデント対応慣習の普及状況にも注目しました。全体として、結果が示唆するのは、検出能力の低さに加えて、漏洩 / 侵害が発見されたときにそれに適切に対応するための準備がほとんどの組織で整っていなかったという点です。とくに驚くべきことと思われたのは、適切なインシデント対応計画を整備していたのが被害者の 28%にすぎなかった点です。

アンチフォレンジックス

企業のネットワークに侵入してデータを盗み出すことを決意したときに、捕まることを想定して計画に盛り込む犯罪者はまずいません。多くの犯罪者は、犯行現場を汚して犯罪行為の証拠を隠滅し、インシデント後の調査を妨害しようとするでしょう。そのような活動はアンチフォレンジックスと呼ばれ、以前の節で述べた、漏洩 / 侵害の発見と対応に向けた取り組みの一部に対抗するためのものです。

調査担当者は、2008 年の事例のうち 3 分の 1 以上でアンチフォレンジックスの痕跡を発見しました。現場で確認されたアンチフォレンジックス対策の中で最も一般的な形態は、データワイピング、データ隠蔽、およびデータ破壊です。図 36 は、昨年実施した調査におけるこれらの対策の普及状況を示したものです。（データの消去と削除を含む）データワイピングの広範な普及は驚くに値しません。フリーウェアのユーティリティに加えて、この機能を実行する多くの既製商用製品が利用可能です（データのワイピングには多くの合法的な用途が存在します）。データ隠蔽に関して、電子透かしの使用はあまり一般的ではなく、前年とほとんど変わりませんでした。一方で、データ隠蔽を目的とした暗号化の使用は約 10%増加しました。データ破壊が確認された事例では、ほとんどがログの不正操作によるものでした。

図 36. 確認されたアンチフォレンジックスの種類と漏洩 / 侵害に占める割合



直感的な見解では、アンチフォレンジックスが利用された漏洩 / 侵害は、規模に関してはより大規模、持続期間に関してはより長期に及ぶ傾向がありました。小規模な「ウィンドウ破り」型攻撃の多くについては、証拠の隠滅は割に合わない努力です（加えて、そのような攻撃を実行するのは大概、アンチフォレンジックス対策を知らない低スキルのアタッカーです）。この意味で、アンチフォレンジックスの使用は、訴追を回避するために用いられる防衛戦術としてそのルーツを越えた進歩を遂げており、データの漏洩 / 侵害を図る攻撃者の能力を拡張および強化することを目的とした、攻撃的な性質での利用が増加しています。

このページ内容に関するコメントまたは質問をお寄せください（英語のみ）

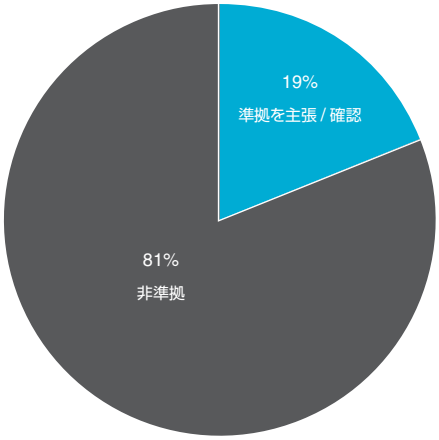
http://securityblog.verizonbusiness.com/category/2009dbir/ にアクセスし、
「Anti-Forensics」のページから英語でコメントを投稿できます。

クレジットカード業界情報セキュリティ基準

漏洩 / 侵害を防ぐための規制および統制ガイドラインの有効性に関しては、公開議論が活発に行われましたが、このトピックの実証研究は乏しいままです。ニーズの高いこのような分析を提供することはこの報告書の目的ではありませんが、2008 年の調査データは、組織がクレジットカード業界情報セキュリティ基準（PCI DSS）の順守を要求されるインシデントに関して、ある程度の情報を提供します。

PCI DSS は、組織によるカード所有者情報の保護を支援する目的で制定された一連の統制要件です。金融機関および小売業者が調査データに占める割合を踏まえれば、調査対象事例中の大多数の組織が、PCI DSS に規定された要件に従属するのも当然のように思われます。これらはデータ漏洩 / 侵害の事例であったことから、漏洩 / 侵害の被害者のコンプライアンスステータスに関して明白な疑問が生じます。この疑問に対する答えは図 37 に示されますが、適切な解釈を保証するためにさらなる明確化が必要です。

図 37. 最終査定に基づいた PCI コンプライアンスステータスと漏洩 / 侵害の被害者に対する割合



調査対象事例のうち、クレジットカード情報の漏洩 / 侵害の被害を蒙っている組織の 4 分の 3 超が PCI DSS に準拠していなかったか、または一度も監査を受けたことがなかったことが判明しました。このステータスは調査対応チームの判定によるものではなく、被害者の証言または認定セキュリティ審査機関（QSA）によって判定されました。しかしながら、非準拠のこれらの組織よりも興味深いのは、最終査定中に準拠と認定された 19%の組織です。QSA によって準拠と認定されたにもかかわらず、これらの組織がインシデントに巻き込まれた事実は、PCI DSS が漏洩 / 侵害の防止に効果がなかったことを意味するのでしょうか。今回の調査結果はそのような結論を支持しません。

PCI 査定の時点的な性質により、最終監査で準拠と認定された組織が、漏洩 / 侵害の時点では準拠状態ではなくなっている可能性があります。その上、PCI コンプライアンスは漏洩 / 侵害に対する絶対的な保証ではなく、査定プロセスも一貫していません。理由が何であれ、IR チームによって実施された漏洩 / 侵害後レビューはいくつかの非常に興味深い調査結果を明らかにします。

フォレンジックス調査の間、事例を扱う調査担当者は、PCI DSS 要件が漏洩 / 侵害の時点で満たされていたか（および、適切であったか）どうかのレビューを実施します。この査定の結果は PCI 要件マトリックスに記録され、事例報告書に追加されて、関連するクレジットカード会社に通知されます。この行使は正式な PCI 認定監査ではなく、被害者のコンプライアンスステータスを是認も却下もしま

このページ内容に関するコメントまたは質問をお寄せください（英語のみ）

http://securityblog.verizonbusiness.com/category/2009dbir/ にアクセスし、「PCI DSS」のページから英語でコメントを投稿できます。

せん。ただし、データ漏洩 / 侵害の被害を受ける組織に関して、どの要件が満たされていない傾向があるかについての有益な洞察を提供します。表 10 は、2008 年の間に実施された漏洩 / 侵害後 PCI レビューの全結果を集計したものです。

表 10。Verizon Business IR チームによって実施された漏洩 / 侵害後 PCI DSS レビューの結果。値は各要件が満たされていると認定された組織の割合を表す。

安全なネットワークの構築と維持	準拠状況
要件 1：データを保護するためのファイアウォール構成をインストールして維持する。	30%
要件 2：ベンダーが定める既定値をシステムパスワードやその他のセキュリティパラメータに使用しない。	49%
カード所有者データの保護	
要件 3：保存されたデータを保護する。	11%
要件 4：パブリックネットワークを介したカード所有者データおよび機密情報の伝送を暗号化する。	68%
脆弱性管理プログラムの維持	
要件 5：ウイルス対策ソフトウェアを使用し、定期的に更新する。	62%
要件 6：安全なシステムとアプリケーションを開発および維持する。	5%
厳格なアクセス制御対策の実装	
要件 7：業務上知る必要のあるデータのみにアクセスを制限する。	24%
要件 8：コンピュータにアクセスする各人物に一意な ID を割り当てる。	19%
要件 9：カード所有者データへの物理的接触を制限する。	43%
ネットワークの定期的な監視とテスト	
要件 10：ネットワークリソースとカード所有者データへのすべてのアクセスを追跡および監視する。	5%
要件 11：セキュリティシステムとセキュリティプロセスを定期的にテストする。	14%
情報セキュリティポリシーの維持	
要件 12：情報セキュリティを扱うポリシーを維持する。	14%

上記の各要件の準拠率を見直していくと、いくつかの非常に興味深い統計が浮かび上がります。多くの組織が不満を訴える要件 3、6、10 は最も面倒なもので、調査対象事例全体で見ても、実際に最も準拠率が低くなっています。今回（および前回）の報告書で広く議論された、不必要または不明なデータストアの蔓延、SQL インジェクション攻撃の頻度、侵害から発見までの期間の長さを考慮すれば、この調査結果はほとんど驚くに値しません。この 3 つの不備は、過去 5 年間に IR チームが調査した最大規模の漏洩 / 侵害の多くで、高い確率で要因となっていました。残念なことに、これらの統計（および、発見と検出のための統制が普及していないことに関連して以前に挙げた統計）は、これらの弱点を利用した攻撃が当面の間、課題であり続けるだろうということを示唆します。

言い換えれば、典型的な組織において、PCI DSS 要件の順守率が 3 分の 1 を下回っていたことになります。これよりもずっと高い（またはずっと低い）数字を示した組織もありますが、これらのデータが物語る結論は次のとおりです。これらの漏洩 / 侵害は一般的に、PCI DSS の順守率が高かった組織では発生しませんでした。

準拠率の高いほうの要件に話を移すと、パブリックネットワークを介して伝送されるデータの暗号化は 68%、ウイルス対策ソフトウェアの使用は 62%と、高水準の準拠を達成しています。ただ残念なことに、それらの要件は一般的な攻撃の形態にはほとんど関係がありません。この報告書で以前に述べたように、情報はプライベートネットワーク経由で、またはシステムの内部で収集されます。また、ウイルス対策ソフトウェアは、リモートアタッカーの制御のもとでシステムにインストールされた、カスタマイズされたマルウェアに対してはほとんど効果がありません。ただそれでも、ウイルス対策ソフトウェアは企業の防御に確かに大きな役割を果たします。また、被害者の 40%がそれを使用（または更新）していなかったというのはかなり驚くべき結果です。

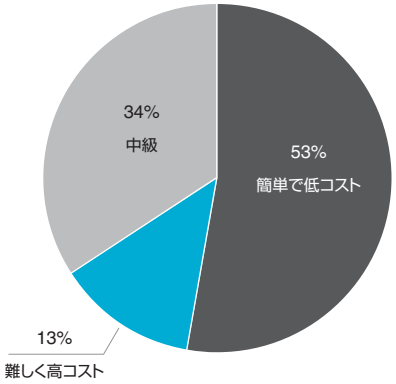
信じがたいことに、被害者の 51%が、機密データを扱うシステムでベンダーの既定のパスワードを使用していました。事例の 80%以上で、被害者の組織は共有アカウントをシステムアクセスに使用し、ユーザーに一意な ID を割り当てていませんでした。これらの要件の順守率の低さが、サードパーティに委託したリモート管理サービスで既定および共有のアクセス情報が使用されたことに起因する多数の漏洩 / 侵害に一定の役割を果たしたことは明白です。

この情報の要件中心の見方が興味深いこともさることながら、組織中心の見方も無視できない論点を生み出します。IR チームが実施した非公式の侵害後 PCI レビューによると、調査対象事例の被害者全体を通じた、全 12 要件の平均順守率は 29%でした。言い換えれば、典型的な組織において、PCI DSS 要件の順守率が 3 分の 1 を下回っていたことになります。これよりもずっと高い（またはずっと低い）数字を示した組織もありますが、目の前にあるデータが物語る結論は次のとおりです。これらの漏洩 / 侵害は一般的に、PCI DSS の順守率が高かった組織では発生しませんでした。

結論と推奨事項

前回の報告書の結論部分は、「妥当なセキュリティ態勢を整えておけばデータ漏洩 / 侵害を回避できたかもしれない事例が全データ漏洩 / 侵害事例の 87%にも上る」という統計に関する記述で始まりました。「妥当な」という表現を使用したことが、一部の読者から分かりにくいというご意見があった（こちら * で説明を参照できます）ことから、今回はあえて異なる表現を選びました。ただし、あくまで表現が違うだけで、最終的に行き着いた結論はまったく同じものでした。

図 38. 漏洩 / 侵害を防ぐために必要な予防対策の難易度と費用ごとの割合



2008 年の調査では、初歩または中級レベルの管理を実施していれば侵害の 87%は回避できたと結論づけています。これらはすべて、セキュリティ業界の人間にとっては、毎日のように目にして使用する、標準的でありふれた慣習でした。（労力と費用の点で）コストの高い統制が、侵害を回避するための最も効率的で効果的な手段として推奨されていたのは事例の 13%にすぎませんでした。さらに、これらの大半は、高コストではあるものの標準的なセキュリティ統制でした。図 39 は、これらの同じ統制の異なる分類を示したものです。

オリジナルの DBIR の結論部では、2004 年から 2007 年にかけての漏洩 / 侵害調査の結果を直接のベースにした多数の推奨事項を提示しました。また、データ保護とインシデント対応に対する意識について、セキュリティ業界では常識である意識への転換を読者に呼びかけていました。今年は、その同じ呼びかけを繰り返し、前回提示した推奨事項の要点をおさらいすることに加えて、2008 年の調査対象事例に基づいた追加のガイダンスを提供したいと思います。

以下に示すのは、2008 年版の DBIR で述べられた推奨事項を簡略化した内容です。これらの推奨事項は、昨年までと同様に現在でも通用します。

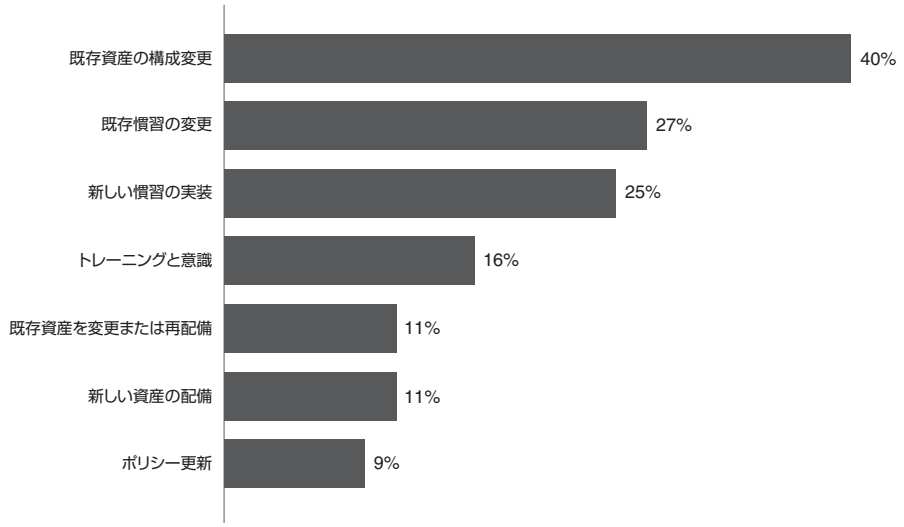
ポリシーにしたがってプロセスを実施する：多くの組織はセキュリティに関するポリシーと手順を策定しましたが、いまだにそれらを一貫した形で実装できていません。責任を持ってセキュリティの管理を行うとともにポリシーを実際に実施することで、データ漏洩 / 侵害のリスクを大幅にまた確実に軽減できます。

まず、基本的なセキュリティを確保し、その後、高度なセキュリティを構築する：大半のシステムには高度なセキュリティを確保している一方で、セキュリティ管理がまったく無視されている部分もあるという現象が、多くの組織に見られました。より安全な経路を好むのは犯罪者の常です。まず、基本的なセキュリティ方針を決定し、その方針に基づいて企業全体にわたって隅々までセキュリティを確保し、その後、必要に応じて高度なセキュリティを構築します。これが、実際の攻撃に対抗する上で優れた戦略です。

ビジネスパートナーの接続のセキュリティを確保する：セキュリティ評価、契約に基づく合意、共有資産管理の改善と同様に、パートナーに対する基本的なセキュリティ対策はすべて、パートナーに関連するリスクを管理する上で有益と考えられます。

*http://securityblog.verizonbusiness.com/2008/06/19/reasonable-controls/

図 39. 推奨される予防対策の単純分類と漏洩 / 侵害に占める割合



データ保持プランを作成する：これを考慮すると、企業内部にどんな情報があるか、その情報のビジネス上の用途、その情報が流れる経路、また情報がどこに保存されているかを企業自身が理解しておくことは、明らかに情報の保護にとって不可欠です。業務で特に保持する必要がないデータは、保持する期間をできるだけ短くするとともに、データの複製もできるだけ避けます。

トランザクションゾーンを作成してデータを保護する：組織では、データの発見と分類のプロセスに基づいて、異なるリスク領域をトランザクションゾーンに分離するようにします。これらのゾーンを利用することで、より厳格なアクセス制御、ログ、監視、アラートを含む（ただし、これらに限られない）、より包括的な統制を実装できるようになります。

イベントログを監視する：漏洩 / 侵害につながるイベントの証拠を被害者が入手できたにもかかわらず、その情報が認識されることも、その情報に基づいて何らかの対処がなされることもなかった、というケースが多すぎました。実用的で、効率的で、効果的な監視および対応を提供するプロセスはデータの保護に不可欠です。

インシデント対応プランを作成する：データ漏洩 / 侵害が発生したと思われる場合、企業では必ず、何らかの対応策をとらなければなりません。効果的なインシデント対応プランは、漏洩 / 侵害の規模の最小化に役立ち、証拠が適切な方法で収集されることを保証します。

意識を高める：データ漏洩 / 侵害のリスク、予防のために各自が果たすべき役割、インシデント発生時の対応方法について従業員に教育するトレーニングは、効果的に行えば、漏洩 / 侵害の防御および発見に大きな効果を発揮することができます。

疑似インシデントテストを実施する：効率的な運用のために、インシデント対応戦略、脅威の見つけ方、脅威の種類、対応の実行プロセス、証拠の扱い方、疑似インシデントテストの内容やスケジュールを網羅した定期的なインシデント対応トレーニングを組織で実施するようにします。

これらの「古き良きもの」に加えて、2008 年のデータの分析に基づいた、以下の新規または改訂版の推奨事項を提示します。従来どおり、データ漏洩 / 侵害に関する推奨事項や対策を記載しましたが、いずれも企業のデータ保護の包括的戦略ではなく、またこれらの方法で必ずしもデータ漏洩 / 侵害を防止できるとは限りません。むしろ、本研究の元データである数百件のデータ漏洩 / 侵害事例の分析から得た推奨事項であり、記載の意図は、データ漏洩 / 侵害を受けた企業が共通して経験した問題を明らかにすることにあります。

デフォルトの認証情報の変更は重要：犯罪者が企業の資産を侵害する方法として 2008 年に最も多く用いられたのは、デフォルトの認証情報を利用する方法でした。これは確かに、先の「まず基本的なセキュリティを確保し、その後高度なセキュリティを構築する」の推奨事項に分類されますが、このような不注意があまりに多いことから、特別に注意を促すことが必要と判断しました。ユーザー名とパスワードの変更が重要だという認識が被害者になかったわけではありません。被害者はごく一部の資産に対して変更を怠った（そして、当然のように侵入者に発見された）にすぎないか、または資産の管理を委託した第三者が当然そのような変更を行うものと想定していました。教訓は次のとおりです。同僚またはパートナーが、すべてのポリシーと手順を常に完全に順守するという想定は捨ててください。

アクセス情報を共有しない：当たり前だがしばしば守られず、しばしば悪用されるもう 1 つの問題です。デフォルトの認証情報を変更することに加えて、すべてのパスワードを一意にする、パスワードをユーザー間で共有しない、異なるシステムでパスワードを使用しない、の各原則を組織内で厳守する必要があります。共有されたアクセス情報を使用していたために、単一点の漏洩 / 侵害が複数のインシデントにまで発展した事例が、2008 年に相当の件数確認されています。このことは、第三者に管理を委託していた資産でとくに問題となりました。

ユーザーアカウントのレビュー:これは先の 2 つの推奨事項に関連しますが、個別に注意を促す必要があると判断しました。ユーザーアカウントの定期的なレビューの必要性が認識されるようになった要因は、デフォルトの認証情報や共有されたアクセス情報が悪用された漏洩 / 侵害の多発、不明な権限が関係した侵害の増加（および、それに伴う多数のレコードの流出）、そして長年の経験です。レビューには、アクティブなアカウントの有効性、必要性、構成の適切さ、付与された（できれば最低限の）権限の適切さの各項目を確認する正式なプロセスを含めるようにします。

アプリケーションのテストとコードのレビュー：ハッキングまたはネットワーク侵入が原因の漏洩 / 侵害の半数近くで、SQL インジェクション攻撃、クロスサイトスクリプティング、認証バイパス、セッション変数の悪用がその発生に寄与していました。アタッカーがより上位のスタックであるアプリケーション層を標的にしつつあるのは周知の事実です。先例にならった防御策を講じる必要があります。他の対策と同様に、まずは火を消します。去年に大規模な漏洩 / 侵害につながった問題のほとんどは、Web アプリケーションの簡易スキャンやテストでさえ発見されていたでしょう。次に、アーキテクチャ、権限、ソースコードの定期的なレビューを取り入れます。アプリケーション開発のためのセキュリティ開発ライフサイクル（SDLC）アプローチを取り入れることも推奨されます。最後に、開発者が安全なコードの価値を理解し、そのようなコードを書けるようになるための学習を支援します。

よりスマートなパッチ管理戦略：2008 年にハッキングおよびマルウェアの攻撃によって利用されたすべての脆弱性について、漏洩 / 侵害を防ぐために必要なパッチは、少なくともインシデントが発生する半年以上前から入手可能な状態でした。実際、1 件を除いて、パッチは 1 年以上前から入手可能な状態でした。組織のパッチ適用が遅かったことが原因だと結論付けるのが合理的なように思われるかもしれませんが、これは正しい解釈ではありません。これらすべての組織で、6 ヵ月よりもずっと短いパッチサイクルが導入

済みでした。この 5 年間の調査期間を通じて、問題になることが多かったのはパッチ適用の早さではなく範囲のほうです。公開されたパッチをとにかく早急に適用することより、一貫したペースで、すべての資産に漏れなくパッチを適用できる態勢を整えることにリソースを割いたほうが、組織として得られるメリットは大きくなります。

従業員の解雇手順の整備：昨年に起きた数件の漏洩 / 侵害は、直近に解雇された（またはその通知を受けた）一部の従業員が関与した悪意のある活動の結果でした。各組織は包括的な従業員解雇ポリシーを整備する必要があります。そのポリシーの役割は、解雇プロセスに責任を負う当事者を識別し、解雇のための手順とチェックリストを定義し、組織の全財産の回収を保証し、そして最も重要な点として、ユーザーアカウントの迅速な無効化とすべてのアクセス権限の削除のためのプロセスを確立することです。

アプリケーションログを有効にして監視する：「イベントログを監視する」は昨年の報告書で提示した、またこの報告書でも既におさらいした推奨事項です。ただし、多くの組織におけるログ監視の取り組みは、ネットワーク、オペレーティングシステム、IDS、ファイアウォールのログに集中していて、リモートアクセスサービス、Web アプリケーション、データベース、その他のクリティカルアプリケーションは軽視されていることが判明しました。これらのログも、漏洩 / 侵害の検出、被害の最小化、そして調査に役立つデータを豊富に提供する可能性があります。

「疑わしい」と「異常」を定義する（その後、該当するすべてのものを捜す）：これは確かに曖昧ですが、実際、すべての人に理解されるように言葉の定義が必要とされているのに、言葉自体を一般化する、というのは要点に反します。この報告書の作成中、規模こそ小さいが破壊力の強い一部の攻撃の性質が、ますます標的を絞り込んだ、ますます高度なものになってきたことを幅広く議論してきました。これらは通常、犯罪コミュニティが貴重と評価するデータを大量に処理または格納する組織の内部で行われます。そのような組織は最も典型的な「うってつけの標的」です。この分類に該当する組織は、非常に意志が固く、豊富な資金に支えられ、高いスキルを持ち、特定の組織を標的とした攻撃に対して防御を固め、またとくに、そのような攻撃を検出するための準備を整える必要があります。この報告書で強調した「大規模な漏洩 / 侵害」のシナリオを考えます。アタッカーは、企業ネットワークにアクセスし（潜在的警告サイン 1）、ネットワーク内をうろつき（サイン 2）、機密情報が含まれるシステムを発見して侵害し（サイン 3）、マルウェアをインストールし（サイン 4）、システムの状態や処理を変更します（サイン 5）。マルウェアはデータをローカルに、多くの場合は一切のデータが保存されるべきでないシステムに保存し（サイン 6）、犯罪者は定期的に戻って来て（サイン 7）データを収集し、通常と異なるポート経由で（サイン 8）、または既知の悪意のある IP アドレスから（サイン 9）たびたびデータを収集します。これらが疑わしい、また異常であると思われるでしょうか。IR チームの考えも同じです。重要な資産を特定し、通常の動作を識別し、通常と異なる状態を検出して警告するための焦点を絞ったメカニズムを整備します。

1 年間で 2 億 8500 万ものレコードが漏洩 / 侵害の被害に遭ったという事実は、情報の保護を専門とする業界に向けて鳴らされた、少し大きめの目覚ましベルです。アラームを止めてまた眠りに落ちる余裕はありません。我々の仕事は少しも楽になっていません。世界の情報の総量は絶えず増え続け、人間のすべての行為と人間が行くすべての場所に浸透しています。攻撃の大半はむしろ平凡なもの（それでも、まずはそのような攻撃に対処しましょう）であり続ける一方で、犯罪者たちは、最新のデータ保護戦略への適応を図り、自分たちが価値を見出すデータを獲得するための新しい方法の開発に取り組んでいます。

好材料は、ますます多くの情報が自由に手に入るようになってきていることです。発展を続ける調査チームは、現実をより正確に認識し、本当に正しいことに確実に集中していられるように、現実のデータと現実の結果を活用することを目指しています。まだノイズが多いことも確かですが、シグナルはその強さを日々増しているようにも思われます。この報告書の提言が、読者にとってノイズでなく有益なシグナルであると感じてもらえればこれに勝る喜びはありません。

Verizon Business調査対応チームについて

セキュリティ侵害と機密情報への不正アクセス、その結果としての機密情報の漏洩 / 侵害は、世界中の企業にとって非常に深刻な問題です。このようなインシデントが発見された場合、適切な対応が不可欠です。被害が広がらないように直ちに対応するとともに、顧客データを保護し、原因を突き止めなければなりません。また、法執行機関用の資料として、インシデントの状況を正確に記録することが必要です。さらに、インシデントの証拠を収集しなければならず、その場合、証拠の収集は、被害を受けた情報資産の完全性、信頼性が損なわれないように注意して行うことが必要です。

IR チームは豊富な経験と専門知識を有し、過去 5 年間に約 600 件のセキュリティ侵害とデータ漏洩 / 侵害の事例を扱ってきました。これには、公表されたすべての漏洩 / 侵害のかなりの割合に加えて、未公表の事例も数多く含まれています。この調査対象事例は、この期間中に漏洩 / 侵害の被害を受けた既知のレコード全体のかなりの割合と、これまでに報告された最大規模の侵害の多くをカバーします。

そうした調査の間、調査チームは、世界各国の政府機関や捜査当局のスタッフと定期的に連絡をとり、証拠の提出や起訴の準備などの作業にあたりました。調査チームはまた、セキュリティ侵害やデータ不正アクセスの調査のほか、訴訟支援、電子情報開示（eDiscovery）、専門家による証言、書類受け渡し記録の管理、インシデント模擬訓練、インシデント対応プログラムの開発といった作業も行いました。

上記の調査により大量のデータが取得され、このデータにより、コンピュータ犯罪やデータ不正アクセス、データ漏洩の傾向を見ることができます。その分析結果が、この報告書に記載されています。

yr puvsser vaqrpuvssenoyr

www.verizonbusiness.com

verizonbusiness