エグゼクティブサマリー

verizon

2013年度
データ漏洩/侵害調査報告書

ベライゾンRISKチームによる世界のデータ漏洩/侵害調査。
下記の各機関・組織から協力をいただきました。

AFP AUSTRALIAN FEDERAL POLICE
CERT
Software Engineering Institute Carnegie Mellon
Consortium for Cybersecurity Action
CyberSecurity MALAYSIA An agency under MOSTI
Deloitte.
EC3 EUROPOL
ES ISAC Electricity Sector Information Sharing Analysis Center
DANISH DEFENCE INTELLIGENCE SERVICE
FE
G-C PARTNERS
GUARDIA CIVIL
Homeland Security
IRISS Irish Reporting and Information Security Service
POLITI
POLITIE
ThreatSim™

47,000件以上のセキュリティインシデントを分析。

621件の実際にデータ漏洩/侵害がおきた事例を分析。

世界の19の機関・組織から提供された事例データを使用。

本調査報告書は6年連続して発行。

このデータ漏洩/侵害事例数と提携機関・組織数の規模で分析した報告書は世界で本書だけ。

ベライゾンの「2013 年度データ漏洩/侵害調査報告書（DBIR）」には、世界で発生したデータ漏洩/侵害の分析結果が掲載されています。本報告書は、最近の脅威を理解し防御対策を講じる上で、どの企業・組織にとっても、有用な報告書です。本年の報告書で使用した事例データは実に豊富で、その量は過去最高でした。具体的には、法執行機関や国家インシデント報告機関、研究所、民間セキュリティ会社など、データ漏洩/侵害の捜査や研究に尽力している世界の 19 の機関・組織から事例データの提供を受け、そのデータをもとに分析を行いました。

協力機関・組織の数は、年々増えています。データ漏洩/侵害調査報告書の発行は 2008 年に始まりましたが、それ以降、協力機関・組織から提供された事例データの累計は 2,500 件余り（確認済みの事例）、侵害されたレコードの数の累計は 10 億余りにのぼります。

協力機関・組織から提供された事例データは「生データ」であり、そのままでは分析には適しません。分析には分類が必要です。DBIR の作成にあたり、VERIS（Vocabulary for Event Recording and Incident Sharing）を用いて分類を行いました。VERIS では、あらかじめ決められた用語を使って「*誰が誰に何をして、どのような結果が生じたか*」を定形化さたたデータで記録できます。協力機関・組織から提供された事例データは、その状態では膨大な数のデータの塊に過ぎず、VERIS を使って標準化を行うことで初めて、分析が可能になります。VERIS の詳細については veriscommunity.net を参照してください。

エグゼクティブサマリー

2013 年度データ漏洩/侵害調査報告書

貴社、またはお勤めの企業・組織で、今年、セキュリティ侵害の被害はございませんでしたか。企業・組織の規模に関係なく被害に遭う可能性は等しくあります。ハッカーがデータにアクセスするときに使う手法は多数あり、また世界中のどこでも攻撃でき、種類も増え機能も向上しています。これは見過ごせない脅威です。

昨年は、政府機関から消費者用品ブランドまで、あらゆる業種・業態の企業・組織からデータ漏洩/侵害発生の報告がありました。見出しを賑わすようなデータ漏洩/侵害の多くは米国で発生しましたが、本年のデータ漏洩/侵害調査報告書（DBIR）によると、世界の 27 カ国で発生しています。もはや、一国の問題ではなく、また無視できるような問題でもありません。米国の 46 州にはすでに情報公開法がありますが、欧州連合を含め世界各国でも、この種の法律の制定を真剣に検討しています。

情報公開法によると、データ侵害を受けた場合、被害の対応を行うとともに、その事実を報告しなければなりません。また、企業・組織は、そもそもデータ侵害に遭わないように努力しなければならず、さらに侵害を迅速に検出し、データの漏洩を最小限に抑える能力を備えている必要があります。

最新の脅威状況を常時、把握しておくことは簡単ではありません。もっとも効果的な方法は、確実なデータと専門家による分析結果を知識として身につけておくことです。本年の DBIR では、19 の協力機関・組織から提供された 2012 年の事例データを使用して分析を行っており、事例データの事例の合計は 47,000 件超（そのうち確認済みの事例は 621 件）でした。本報告書を読むことで、攻撃者とその手口について今までにないほどの知識を得ることができ、その知識は、読者の企業・組織を保護する上で非常に有効です。

ベライゾンでは、2008 年からデータ漏洩/侵害調査報告書の発行を続けています。本年は、47,000 件を超えるセキュリティインシデントを事例データとして使用しました。これほどの数は、今まで初めてです。

このエグゼクティブサマリーでは、データセキュリティについてよくある 3 つの「思い込み」をチェックし、また、ベライゾンが収集したデータを使って実在のリスクにスポットを当てます。企業・組織にとって、その規模を問わず、大きな脅威である国家スパイ活動関連のデータ漏洩/侵害を見ていきます。また、どのようにして攻撃が実行され、どのようして防御すればいいかを検討します。この検討は、データセキュリティに関して確かなデータに基づいて意思決定を行う場合に有効であるとともに、金銭的損失と社会的評判の低下を軽減する上でも役に立ちます。

69%のデータ漏洩/侵害は外部の第三者が発見、9%は顧客が発見。

ソーシャルエンジニアリング（電子メールや電話、ソーシャルネットワークを利用して個人から情報を窃取）は、従来はあまり問題にされませんでしたが、この手口によるデータ漏洩/侵害が29%を占めています。

76%のネットワーク侵入が、脆弱性、または盗んだ認証情報の悪用を通じて実行されています。このリスクは、厳格なセキュリティポリシーを策定・実施することで容易に軽減できます。

国家スパイ活動関連の攻撃など、自分には関係ない。

スパイは、うちのような会社には興味はないはずだ。

2013 年の報告書の分析結果を見ると、国家スパイ活動関連の攻撃に対して悠長に構えている企業・組織がほとんどです。原因は、企業・組織では一般に、この種の攻撃の標的は政府や軍隊、大手有名企業に限られる、と考えていることにありますが、分析結果ではそれは間違いであることが示されています。自分の企業・組織が標的になる可能性は十分にあり、甘く見ることはできません。

75%がオポチュニスティック型の攻撃（特定の個人や企業ではなく不特定多数を標的として攻撃）で、そのほとんどが金銭目的。

攻撃者は誰か?

サイバー攻撃の実行者は、主に下記の 3 種類に分類できます。それぞれ動機と手法が異なり、また目的（破壊、金銭窃取、評判や信用の低下など）も異なります。この 3 種類の実行者の特徴を把握しておくことは、準備態勢の構築やリスクの軽減に有効です。

活動家グループ

活動家グループは、いまだにごく基本的な攻撃方法を使っていますが、それでもここ数年、大きな成功をいくつか収め、話題になっています。考え方は楽観的ですが、支持者は少なくありません。目標は、攻撃対象の人間を混乱と困惑の極地に追い込むことです。

犯罪者

犯罪者の動機は金銭の入手で、入念かつ慎重に標的を選びます。活動家グループより複雑なハッキング手法を用います。いったん侵入に成功すると、金銭的価値のあるデータを物色し、盗みます。

スパイ

通常、国家に支援され、非常に洗練されたツールを使用し、特定の標的に対して攻撃を行います。狙いは、知的財産や財務データ、組織の内部情報で、執拗に攻撃しようとします。

本年の分析対象のデータ漏洩/侵害事例のうち 19%が国家関連の実行者による事例、言い換えると国家スパイ活動に関連した事例。

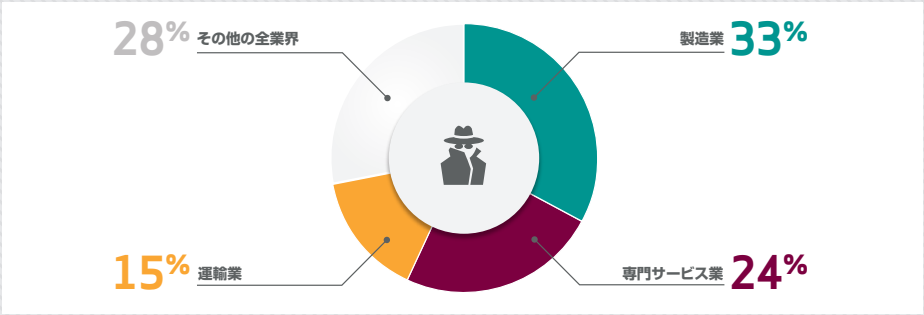
攻撃はどこから実行されるか?

金銭目的の事例の場合、米国または東欧（特にルーマニア、ブルガリア、ロシア）から実行されるケースが大半を占めます。一方、国家スパイ活動関連の事例は、東アジアから実行される場合がほとんどです。ただし、世界中の企業･組織が標的となっています。国境はもはや、サイバー攻撃に対する防衛線ではありません。

動機は何か?

国家スパイ活動より、金銭目的や社会･政治運動（活動家グループ）を動機とする事例が多く、これは、ほとんどの業界に当てはまります。図 1 は、国家スパイ活動関連の事例が多い業界と、各業界の当該事例の割合を示した図です。いずれの割合も、金銭目的または社会・政治運動（活動家グループ）を動機とする事例の割合に比べると低めです。

図 1：国家スパイ活動関連の事例が多い業界と当該事例の割合



国家スパイ活動関連の攻撃（事例）のうち、製造業、専門サービス業、運輸業を標的とした事例がほぼ 4 分の 3 を占めます。

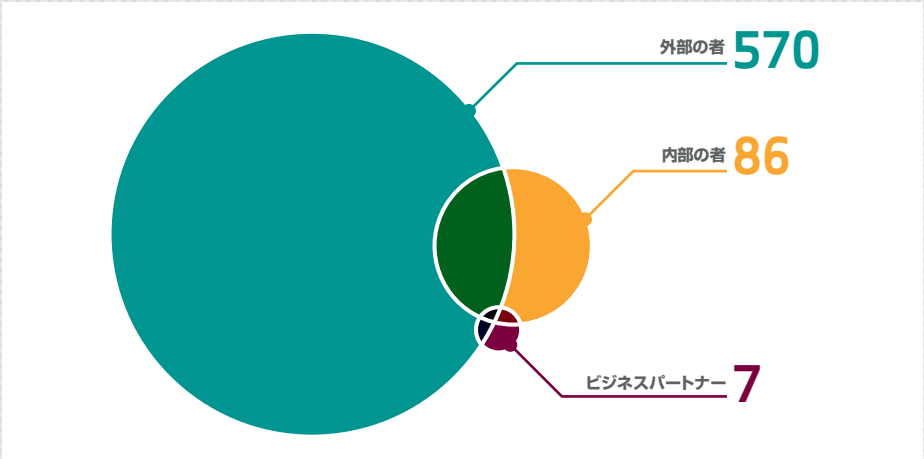
妨害工作を行った部内者のうち半分以上が元従業員で、その手口は、無効化されていない自分のアカウントまたはバックドアを悪用するというものでした *。

上記はいずれも、企業・組織が国家スパイ活動関連の攻撃を直接受けた場合ですが、懸念はこればかりではありません。例えば、ビジネスパートナーやサプライヤーが国家スパイ活動関連の攻撃に遭う可能性もあります。また、自社のサプライチェーンが攻撃を受けた場合、被害は、自社への直接攻撃と同様に甚大です。さらに悪いことに、自社を通じて顧客に攻撃が及ぶこともあります。そうなれば、深刻な状況に陥ります。

実行者は、部内者または部外者?

一般に従業員などの部内者によるデータ侵害が多いと考えられていますが、それとは裏腹に、86%の事例が部内者（内部の者）ではなく部外者（外部の者）によるものでした（図 2）。従業員などの部内者による事例は 14%で、そのうち、内部のセキュリティが緩く、部内者が侵入するのが意外と簡単だったという事例が多く見られました。

図 2：データ漏洩/侵害の実行者



分析対象のデータ漏洩/侵害事例のうち 534 件（86%）が部内者以外の者による事例

部内者による IP（知的財産）窃盗事例のうち 70%以上の事例が、部内者が会社を辞めると言ってから 30 日以内に発生しています *。

* カーネギーメロン大学（http://www.sei.cmu.edu/library/abstracts/reports/12tr012.cfm）

今の対策のままで十分だ。

ネットワークを切り離している限り、安全だ。

紙媒体またはオンラインの別を問わず、多くの新聞や雑誌で、最新技術のリスクに関する記事が大々的に掲載されています。このような状況の中、当然のことながら、クラウドコンピューティングのセキュリティに大きな関心を寄せる経営幹部は少なくありません。しかしながら、6 年間にわたるデータ漏洩/侵害調査報告書の分析結果から言うと、攻撃者は、従来と同様のテクニックを用い、同じ種類の情報資産を攻撃しているという傾向が見て取れます。この傾向は、本年も変わりません。

攻撃を受けやすい資産

1.	ATM	30%
2.	デスクトップ	25%
3.	ファイルサーバー	22%
4.	ノートブック	22%
…		
12.	ウェブアプリケーション	10%

上記の数字を合計すると100%を超えますが、これは複数の資産がデータ漏洩/侵害に遭うことがあるためです。

主な脅威は?

毎年、多数のデータ漏洩/侵害事例を扱いますが、その中で驚くような事例はほとんどありません。言い換えると、まったく目新しい事例は稀で、変化があったとしても、昔から使われている攻撃のバリエーションにすぎないというのが普通です。とは言っても、「古い攻撃手法」の脅威を無視することはできません。このような脅威は次第に勢力を伸ばしており、また今まで通り危険です。

リスクが最も高いのは、従来からの資産（ノートブック、デスクトップ、サーバー）です。比較的新しい資産であるウェブアプリケーションが危ないと思われがちですが、そうではありません。また、不正使用によるデータ 事例のうち、41%が「許可されていないハードウェアの使用」（携帯型カードスキマー、個人所有のストレージ機器など）によるものでした。

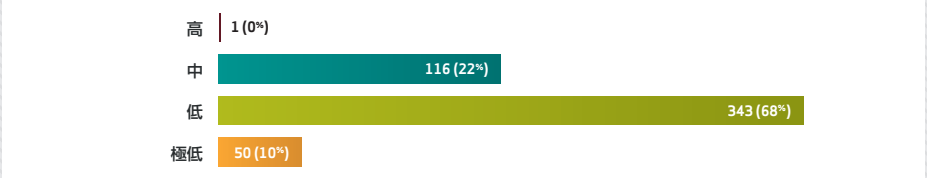
攻撃の難しさ

- **極低レベル**：一般的な個人が実行できるようなレベルの攻撃。
- **低レベル**：基本的な攻撃。カスタマイズや資源は不要またはほとんど不要。
- **中レベル**：ある程度の技術とカスタマイズが必要。
- **高レベル**：高度な技術を用いた攻撃。相当なカスタマイズまたは豊富な資源、もしくは両方が必要。

攻撃の技術的レベルは年々向上していますが、それでも、ほとんどのデータ漏洩/侵害は容易に防止できます。

攻撃者は最近、新しい攻撃テクニックを試したり、攻撃に必要な人的・物的資源を増やしたりしています。しかしながら、最初の侵害の技術的レベルが VERIS の「難しさ」スケールで「高」だった事例は 1%未満にすぎませんでした。また、「低」または「極低」である事例が合計で78%を占めました（図 3）。ハッカーになりたい人にとって、「敷居」は非常に低いのです。

図 3：最初の侵害における攻撃の難しさ

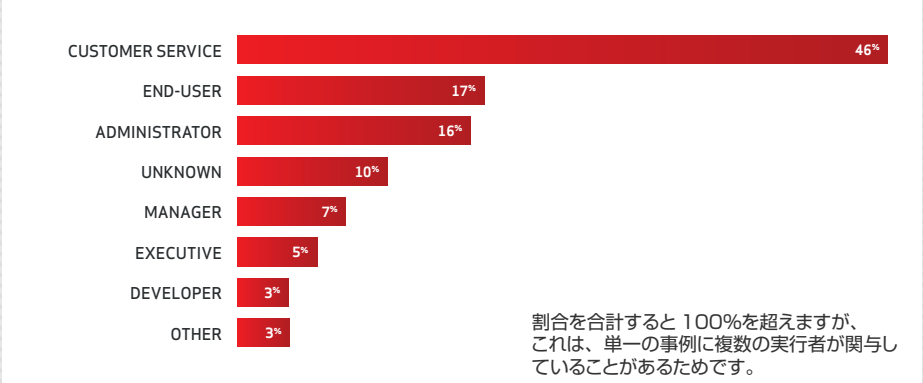


簡単な攻撃だからといって、侵害には至らない、または被害が少ないということはありません。従来からよく知られている攻撃によって、甚大な被害をこうむることもあります。

何に注意すればいいか?

複雑な行為が深刻な結果を生むとは限りません。ほとんどのデータ漏洩/侵害は意図的に実行されますが、意図的でないデータ漏洩/侵害も少なくありません。例えば、仕事のデータを自宅に持ち帰ったり、極秘データを USB メモリーにコピーしたり、機密情報ファイルを電子メールに添付したり、さらには、その電子メールを誤って第三者に送信したりするとデータ漏洩/侵害につながります。ノートブック PC をタクシーの中に置き忘れるのも同様です。

図 4：部内者によるデータ漏洩/侵害事例を実行者別で分類したときの割合



部内者によるデータ漏洩/侵害事例のうち、割合が大きいのはソフトウェア開発者や管理職ではなく、カスタマーサービス担当者（レジ係やコールセンターの従業員など）とユーザー（コンピューターを使用している従業員）による事例です。システム管理者は 3 番目ですが、システム管理者による事例の 60%は過失によるものです。

分析結果から、ユーザーを標的とした攻撃手法としては、マルウェアやフィッシング、認証情報の不正使用が多く使われていることが分かりました。特に、フィッシングのテクニックはますます洗練され、また特定の個人を狙ったフィッシング（スピアフィッシング）が増えるとともに、IT スタッフによる対応が難しい手法が使用される傾向があります。例えば、最近では電子メールを利用したフィッシングに注意を払う人が増えたため、代わりに電話やソーシャルネットワークを利用したフィッシングが多く見られるようになりました。

この節の結びとしてもう一つ。データは、ある場所から別の場所に転送されているときに侵害（犯人により抽出）されることが一番多いと考えられがちですが、実際はどうでしょうか。ベライゾンの調査対応チームでは、企業・組織から依頼を受けてデータ漏洩/侵害の調査を行う場合、一般的な調査のほか、データが侵害されたときの状態もチェックします。その結果、「転送中」に侵害された事例は一件もありませんでした。一方、「保管中」（データベースまたはファイルサーバーに置かれている状態）にデータが侵害された事例が 3 分の 2 を占めました。残りは、何らかの処理と同時に侵害されていました。この結果から、どこに重点を置いてセキュリティ対策を講じればいいかが分かります。

ハッキングツールは、どこにいても簡単に入手できます。試しに「password cracker」（パスワードクラッカー）を検索ワードとしてインターネットで検索すると分かります。また、現在の世界はあらゆる情報がネットワークで接続されている世界であり、そのため洗練度の高いツールやテクニック（国家スパイ活動関連の攻撃で使用されるようなもの）も、すぐに普及します。

国家スパイ活動関連の攻撃の 95%が、何らかの形のフィッシング手法を使って実行されています。フィッシングのテクニックは比較的単純で、これは、特定の標的を執拗に攻撃する場合も同じです。

本年は、不正使用によるデータ漏洩/侵害事例のうち、「許可されていないハードウェアの使用」による事例が 41%を占めました。

ベライゾンの調査対応チームが調査の依頼を受けた場合、データがいつ実際に侵害（犯人により抽出）されたかも調べますが、データが「転送中」に侵害された事例は一つもありませんでした。

ハッキングされれば、すぐ分かる。

システムが侵害されても、それを見つけるのは簡単だ。

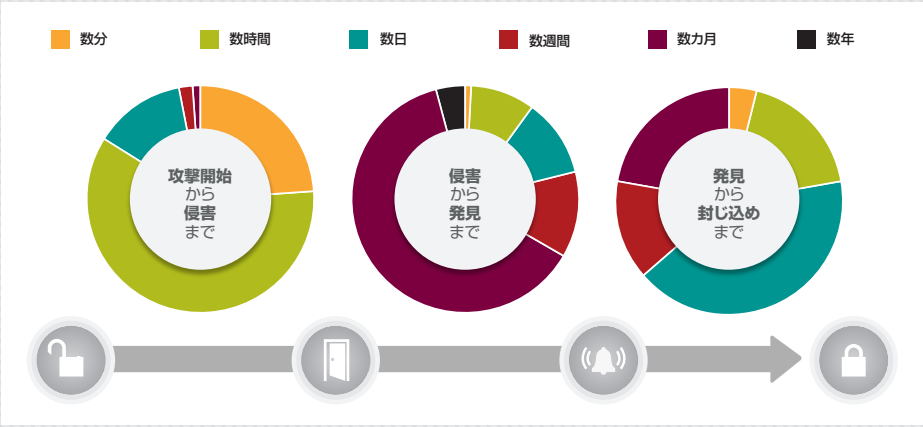
ある企業で、すでに詳細なセキュリティポリシーを作成・実施しており、セキュリティ監査やハードウェア、専門家によるアドバイスにも多額の費用を注いでいらっしゃる、とします。そのような場合、データ漏洩/侵害が発生したときには、「警報が鳴るはず」と考えているのが普通です。あいにく、そうは行きません。

データ漏洩/侵害の発見までどのくらいの時間がかかるか?

防御がどんなに堅固でも、攻撃者による侵入を検知できなければ何の意味もありません。企業・組織には、データ漏洩/侵害を発見し、できるだけ迅速に阻止（被害の拡大を防止）する能力が必要ですが、分析結果を見る限り、そうではないケースがほとんどです。

2013 年度データ漏洩/侵害調査報告書では、分析対象のデータ漏洩/侵害のうち、発見までに数カ月もしくは数年かかった事例が 66%を占めました（数カ月は 62%、数年は 4%）。

図 5：データ漏洩/侵害が発見されるまでの時間（期間）



- 攻撃の開始から最初の侵害まで数時間以下の事例が 84%
- 侵害の発見まで数カ月または数年かかった事例が 66%
- 侵害の封じ込めまで数カ月かかった事例が 22%

この 66%という数値は問題です。というのは、昨年の 2012 年度データ漏洩 / 侵害調査報告書の場合、発見までに数カ月もしくは数年かかった事例は 56%だったからです。つまり、増えたのです。

攻撃開始から侵害まで数時間で完了する事例が非常に多いのですが、それほど驚くべきことではありません。金銭目当ての攻撃者は、攻撃がうまく行かなければ次の標的に移ることが多く、これが理由の一つです。

ここで注目しなければならないのは、データ漏洩/侵害の発見まで非常に時間がかかり、封じ込めまでの時間も長いことです。機密データが窃取可能な状態になっていれば、その間にデータの漏洩は進み、評判や信用はさらに低下します。

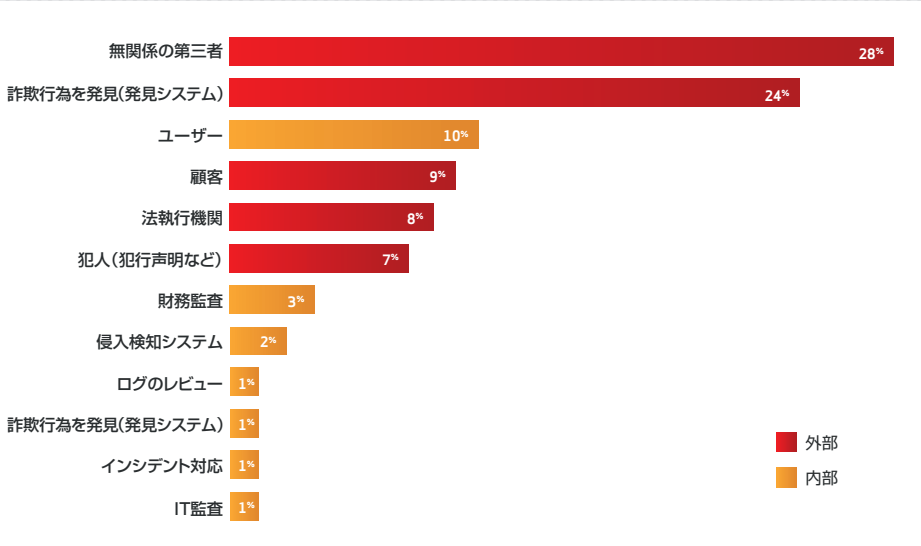
残念ながら、上記の傾向は驚きではありません。この傾向は、過去のデータ漏洩/侵害調査報告書でも同様でした。

誰がデータ漏洩/侵害を発見したか?

データ漏洩/侵害の発見者は多種多様です。顧客が発見した事例は意外と多く、9%でした（図 9）。内部の者が発見した事例のうち、半分以上はユーザー（コンピューターの使用者）が発見しています。一般に IT スタッフによる発見が多いと思われていますが、そうではありません。

効果的な発見手順を定め実施するとともに、従業員を教育してセキュリティ意識を高めることがデータ漏洩/侵害の発見に非常に有効です。この方法により、発見までの時間が短縮され、また攻撃の多くを水際で食い止めることができます。

図 6：データ漏洩/侵害の発見者



発見の割合が 1%に満たない発見方法に過剰な時間と費用を投じている企業・組織も多く見られます。

データ漏洩/侵害の 69%は、外部の第三者が発見。

攻撃は避けられません。企業では、今まで以上に時間と労力を費やし、攻撃の検出と検出方法の改善に努める必要があります。攻撃を阻止することでデータ漏洩/侵害を防止し、データ漏洩/侵害を阻止することで財務上の被害と信用の失墜を防止することが必要です。

データ漏洩/侵害の 9%は、顧客が発見。

弱点または大事な資産?

上で見てきたように、攻撃の標的は多くの場合、人間です。従業員は、確かに攻撃に対しては脆弱ですが、大切な「資産」でもあります。つまり、データ漏洩/侵害を発見する方法や、ソーシャルエンジニアリングを回避する方法を教えることで、従業員は、防御の最前線に立つ力強い存在となります。また、IT スタッフにも、セキュリティ意識のトレーニングを行う必要があります。例えば、ユーザーから、コンピューターの調子がおかしいという連絡が入れば、データ漏洩/侵害の発生を疑うように指導します。

推奨事項

このエクゼクティブサマリーは、ベライゾンの「2013 年度データ漏洩/侵害調査報告書」の要約です。報告書では、企業・組織に対する脅威に関して、業界や場所、企業・機関の規模を基準に詳しく分析しており、脅威に対してどのような対策を講じればいいかについても書かれています。

万能な解決策があり、これを使えば自社の資産と評判を守れるという考えは捨てなければなりません。

データ漏洩/侵害を防ぐための万能薬はなく、そのような方法はデータ漏洩/侵害調査報告書にも書かれていません。データセキュリティインシデントの発見と防止は終わりのない仕事であり、また、IT 部門や最高情報セキュリティ責任者（CISO）に任せきりにすることはできません。データの保護は、会社全体の業務であって、当然ながら取締役会の仕事でもあります。セキュリティ対策を講じる場合、データ漏洩/侵害調査報告書は、その一助となるはずです。

以下、セキュリティ対策に関する推奨事項として基本的なものを 8 項目記載します。

- 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。
- 定期的にチェックを行い、基本的なセキュリティ対策が機能していることを確認する。
- インシデントに関する情報を収集分析し、共有する。収集した情報をもとにデータソース（参照データ）を作成し、そのデータソースを利用してセキュリティプログラムを策定・実施する。
- 脅威インテリジェンス（脅威に関する情報）、特にデータ侵害インジケーター（IOC）を収集・分析し、共有する。IOC は、データ漏洩/侵害の防御と検出に非常に有効。
- 防御を維持したまま、人員、手順、技術を組み合わせてデータ漏洩/侵害を正確かつ迅速に検出できる体制を整える。
- 「侵害されたシステムの数」や「発見までの平均時間」といった情報を定期的に計算し、その結果をもとにセキュリティ対策を改善し、実施する。
- 治療戦略の優先順位付けを行うべく、脅威の状況を評価する。「フリーサイズ（万能）」のセキュリティ戦略は避ける。
- 攻撃者（特に国家スパイ活動関連の攻撃者）は執拗であり、その点を過小評価してはならない。また、自由に使えるインテリジェンスとツールが手元にあれば、それを過小評価せず、十分に活用する。

ベライゾン「2013年度データ漏洩/侵害調査報告書」

「2013 年度データ漏洩/侵害調査報告書」には分析結果がすべて掲載されておりますので、是非、ダウンロードしてお読みください。データセキュリティに関する傾向や解釈、事実が豊富に盛り込まれており、この種の出版物としては最多の読者を誇ります。企業・組織がデータセキュリティ対策を講じる場合、どのような対策を推進し、どのように管理すれば効果的かを理解する上で役に立つはずです。

verizonenterprise.com/jp/DBIR/2013

質問や意見、また提案したいことがありますか?

あれば是非、お知らせください。電子メールの場合、dbir@verizon.com までお送りください。LinkedIn やFacebookもありますし、Twitter(hashtag #dbir)も利用できます(英語での会話となります)。

ベライゾンは、急速に変化し続ける今日の環境において、ネットワーク、情報システム、モバイルテクノロジーの設計、構築、運用に関するサービスを提供しています。世界各国の企業や政府機関では、このようなサービスを利用することで、業務範囲の拡張、生産性の向上、アジリティーの改善、組織存続性の確保が可能になります。

M2M、ダイナミッククラウド、高機能なネットワーキング、モバイルワークはいずれも、新たな可能性の追求や、新たな収入の道の開拓を望んでいる企業にとって効果的なソリューションであり、しかも、このような作業を今までにないほど効率的に推進できます。

ベライゾンでは、セキュリティ、データセンター、4G/LTE、クラウドコンピューティング、大規模グローバル IP ネットワークに多大な投資を行っています。ベライゾンの多様なソリューションは、その成果であり、したがって現在のテクノロジーとビジネスのニーズを満たし、また課題を解決するのに十分な機能を備えています。

ベライゾンは、テクノロジーを自身の力とする企業や個人は世界を変えると考えています。ベライゾンは、その信念を胸に新たなソリューションを生み出しています。さまざまな産業にまたがって新たな可能性につながる道を切り開き、前進し、整備することができるよう、たえず挑戦しています。

ES15581 (A4) 4/13