2011年度 データ漏洩/侵害 調査報告書

本調査は、アメリカ合衆国シークレットサービスおよびオランダハイテク犯罪ユニットの協力の下でベライゾンのRISKチームが実施しました。

エグゼクティブサマリー

3億6100万から1億4400万、さらに400万に。過去3年間の侵害レコード数（侵害により漏洩したレコードの数）の推移です。ベライゾンとアメリカ合衆国シークレットサービス（USSS）の過去3年間のデータ漏洩/侵害事例を総合し、集計した結果です。侵害レコード数は2004年から2007年まで増加を続け、2008年に3億6100万に達しました。翌年の2009年には一転して1億4400万に減少。この減少は偶さかの出来事か、それとも今後の変化の予兆なのか、内部で審念熟慮。結局、2010年には400万未満に減り、やはり兆しだったようです。では、どちらでしょうか。減少の一途を辿るのか、それとも一時の回り道に過ぎないのか。

『2011年度データ漏洩/侵害報告書』の作成にあたっても、アメリカ合衆国シークレットサービス（USSS）の協力を得ることができ、この協力は、上記の質問に回答する上で不可欠のものと考えます。また、本年は、オランダハイテク犯罪ユニット（NHTCU）からも協力をいただくことができ、ここに感謝とともに報告します。このような協力により、本年は幸運にも（といっても分析は簡単ではありませんでしたが）、新たに約800件（2010年の事例は正確には761件）のデータ漏洩/侵害事例の分析が可能でした。過去を振り返ってみると、2004年から2009年までのベライゾンとUSSSのデータの事例数（合計）は900件強です。したがって、本年の場合、2004年から2009年までの事例にほぼ匹敵する数の事例が追加されたことになります。

2010年の場合、上述のように侵害レコード数は過去最低で、その一方、データ漏洩/侵害事例数は過去最高であり、これは分析という点から見ると興味深い事実です。2010年は、事例数が大幅に増加しましたが、それに呼応するように脅威因子や脅威アクション、被害を受けた資産、セキュリティ属性が大幅に多様化しています。例えば、外部因子（第三者）が高度に自動化された手法を使って大規模な攻撃を仕掛けるといった事例があった反面、技術レベルが低く速度にも劣る攻撃もありました。また、内部の詐欺集団によるデータ漏洩/侵害のほか、広範囲での多数の機器の改ざん（タンパリング）、巧妙なソーシャルエンジニアリングによる攻撃など、種々の事例が見られました。本報告書に記載されている統計データによっては、多様化と矛盾するデータ、言い換えると著しく変化したデータがあるかもしれませんが（例えば、外部因子を原因とする事例の割合は過去最高に増加）、その場合、「縮尺」を勘案する必要があります。つまり、従来の年間の事例数は100～150で、この場合、10%の増加は事例数で言うと10～15件の増加に相当します。一方、2010年の場合（事例数は761件）、10%の増加は約75件に当たります。この「縮尺」を念頭に置いて、以下の分析結果を読んでいただくと読者の正確な理解に資するものと思われます。

本年は、ベライゾンが2010年に調査したデータ漏洩/侵害事例に加え、USSSとNHTCUから提供された2010年のデータ漏洩/侵害事例が追加されました。『データ漏洩/侵害調査報告書』は7年間にわたってデータが蓄積され、結局、扱ったデータ漏洩/侵害事例は合計で1700件以上に上り、侵害されたレコード数の合計は9億を超えます。今後も、この報告書を通じて分析を続ける予定であり、本年も読者の皆さんに分析結果を見ていただけることを喜ばしく思っています。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していただくことにあります。本報告書でも、従来と同じく概要から紹介することにします。

データ漏洩/侵害の背後にいるのはだれか？

92% が外部因子によるもの（+22%）

17% がインサイダーによるもの（-31%）

<1% にビジネスパートナーが関与（-10%）

9% が複数の実行者が関与（-18%）

左記の結果は、過去の結果と比較すると随分と変化しています。実際、RISKチームのメンバーの中には、その意味の解釈を巡って頭を捻る者も少なくありませんでした。まず、2009年にはインサイダー（部内者）による事例が増加しましたが（USSSのデータを採用したことが起因）、2010年では、インサイダーによるデータ漏洩/侵害はUSSSのデータを採用する前のレベルに低下しています（本年も引き続きUSSSのデータを使用しました）。このインサイダーによる事例の減少に留意しながら、本書をお読みください。一方、外部からの攻撃（外部因子）が前年と比べて大幅に増加しており、インサイダーによる事例の減少に劣らず、この点にも注意が必要です。一方、ビジネスパートナーを原因とするデータ漏洩/侵害は、これまでと同じく減少を続けています。

データ漏洩/侵害はどんな方法で実行されたか？

今回は内部因子によるデータ漏洩/侵害の割合が減り、その結果、不正使用が減少しました。昨年は、不正使用が脅威アクションの中ではトップでした。代わりに、ハッキングとマルウェアが上位に返り咲き、かつてないほどの暗躍ぶりを見せています。これは、認証情報が設定されていなかったり、脆弱だったり、もしくは盗まれたりといったケースが多かったことを示しています。一方、物理的脅威が第3位に上がりました。物理的脅威（物理的攻撃）は、以前から徐々に増加を続け、2010年には2009年の約2倍に増加しました。これは、サイバー犯罪が徐々に「サイバー」ではなくなって来ていることを示しているのかもしれません。権限の不正使用とソーシャルエンジニアリングは、全体に占める割合こそ減っていますが、発生件数は依然として多く、不正行為や詐欺、騙りなど、その手口も多岐にわたっていました。

50% が何らかのハッキングによるもの（+10%）

49% がマルウェアによるもの（+11%）

29% が物理的攻撃により発生（+14%）

17% が権限の不正使用によるもの（-31%）

11% がソーシャルエンジニアリング（-17%）

データ漏洩/侵害に見られる共通点は？

83% がオポチュニスティック型の攻撃（前年と同じ）

92% の攻撃は、技術的にそれほど高度とは思われない（+7%）

76% がサーバーに置かれていたデータ（-22%）

86% が第三者による発見（+25%）

96% 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（前年と同じ）

89% 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未準拠（+10%）

左記の結果を見て分かるように、残念ながら企業・機関は未だに、技術的にそれほど高度とは思われない攻撃の犠牲になっており、攻撃は、標的選択型ではなくオポチュニスティック（不特定）型が大半でした。また、ほとんどのデータがサーバーから盗まれ、第三者から連絡を受けて初めてデータ漏洩/侵害の発生を知ったという事例が一般的でした。さらに、データ漏洩/侵害はいずれも、技術的に高度で高コストの対策を講じなくても回避できることも示されています（ただし、少なくても経験則を活用する必要があります）。本年も、大きな変化（減少）を期待していたのですが、その期待は叶えられなかったようです。調査した企業・機関の中には、PCI DSSが適用される企業・機関もありましたが、PCI DSSへの準拠義務を果たしていた例はわずかでした。

調査チームでは全員が鳩首し、新たな対策を提案できないかどうか真摯に検討しましたが、見つかりませんでした。「見つからない」というのは正確な表現ではありません。それは、ATM、カード対応給油機、POS端末など、ペイメントカード（クレジットカードやデビットカードなど、現金以外で決済が可能なカード）の読み取りが可能な機器を各所に設置している場合、タンパリング（装置の改ざんや細工）やスキミング（情報の抜き出し）の形跡がないか、組織が定期的にチェックする必要があるということを思い出していただきたいからです。ここ数年、この手口による犯罪が増えています。

もちろん必要とあれば、データ漏洩/侵害に有効な対策や推奨措置を紹介する予定です。現在のところ、右に示した推奨事項（「結論と推奨事項」の節にも記載してあります）が「バランスのとれた措置」と言えます。2010年の事例を分析した結果、この「バランスのとれた措置」をまだ施していらっしゃらない方が大勢おられることが分かりました。しかし、これらの「バランスのとれた措置」を施さなければ、提案する人に非礼になりかねません。もっとも、バランスの取れていない措置がお好みであれば、そういう措置を推奨し、提供するベンダーには、事欠きません。

データ漏洩/侵害に有効な対策や措置は充分に！

どのような軽減措置を講じればよいか？

- 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。
- 必要な管理基準が満たされているかどうか確認する。
- 上記を再度、チェックする。
- リモートアクセスサービスをチェックする。
- ウェブアプリケーションのテストとレビューを行う。
- ユーザーアカウントを監査し、特権ユーザーの行動を監視する。
- イベントログを監視し、内容をチェックする。
- ATMなどのペイメントカード入力装置が改ざん（タンパリング）されていないかどうかをチェックする。

2010年のデータ漏洩/侵害の概要

クラウド、オーロラ、ゼウス、APT、ウイキリーク、スタックスネット、アノニマス。2010年の情報セキュリティ関連の紙誌を賑わせた語を挙げよと言われれば、恐らく、こうなります。実際、興味深い組み合わせです。というのも、この組み合わせから、クラウドとモバイル機器の普及によりユーザーは場所や時間を問わず、任意の相手と通信できるようになったものの、その一方、オーロラやゼウス、APT（高度で継続的な脅威）、ウイキリーク、スタックスネットの登場によって情報資産の保護が難しくなっていることを改めて認識できるからです。本報告書で扱ったデータ漏洩/侵害事例（ベライゾンの事例のほか、USSSとNHTCUの事例も含む）は、上記の状況を映す鏡であり、この鏡を通して2010年のデータ漏洩/侵害の傾向を窺うことができると期待している読者も多いはずです。もちろん、本報告書は、その期待に応えています。

2010年RSAカンファレンスでは、プレゼンテーションのタイトルは「セキュリティ」を使ったものが一番多く、その次に多かったのが「クラウド」でした。また、この「クラウド」が調査チームのメンバー全員の意中にある概念でした。つまり、クラウドがどの程度、データ漏洩/侵害の発生に関係しているかがメンバーの関心事であり、実際、この件に関して幾度となく検討しました。この問題に答えるのは、簡単でもあり難しくもあります。簡単に答えれば、「それほどは関係していない」です。これは、ハイパーバイザーを悪用して複数の仮想マシン（VM）を渡り歩き、データ侵害を行ったというアタッカーは今までいないことから、ほぼ明らかです。一方、ホステッドシステムやアウトソース管理、不法・悪徳ベンダーのほか、VM（VMが攻撃の経路であるか、または実際の標的であるかを問わず）に関連するデータ漏洩/侵害は、頻繁に発生しています。したがって、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。

クラウドがどの程度、データ漏洩/侵害の発生に関係しているかがメンバーの関心事であり、この件に関して幾度となく検討しました。簡単に答えれば、「それほどは関係していない」です。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。

上記のように資産やデータの管理も問題ですが、モバイル機器についても考慮する必要があります。モバイル機器のデータ漏洩/侵害については、最近、情報セキュリティ関連のプレゼンテーションや議論でよく取り上げられています。ただし、ベライゾンの事例データには、モバイルコンピューティング機器（タブレット、スマートフォン、携帯電話など）をたまたま紛失し、その結果としてデータが漏洩したという事例はほとんどありませんでした。これは、主にベライゾンの事例の性質に関係しています（ベライゾンの事例データの場合、モバイル機器の紛失ではなく故意を原因とするデータ侵害の事例が大半です）。また、本報告書では確定されたデータ侵害事例のみを扱っていることも、上記の理由の一つです。

ゼウスは、2009年のデータ漏洩/侵害事例（2010年の報告書）では「蕾」でしたが、2010年は百花繚乱の体をなしています。ベライゾンの事例でもUSSSの事例でも、ゼウスによる口座乗っ取り（アカウントテイクオーバー）や振込詐欺が多数見られ、個人と企業の両方が被害を受けました。以下、ゼウスとAPTなどについて少し触れます。詳細は本文に掲載してあり、ここでは簡単な説明に留めてあります。

ゼウスの場合、犯人の目的は金銭の詐取ですが、オーロラ、APT、スタックスネット、アノニマスの場合、金銭以上のもの、例えば企業の機密情報などを目当てとしているアタッカーもいるようです。このことを念頭に2010年のデータ漏洩/侵害を見てみると、自分が標的になっているという不気味な感覚が以前に増して強くなったような気がします（絶望的と感じる人もいるかもしれません）。ただし、実際に情報リスクが増し、その結果、そのような気分になったのかを判断するのは簡単ではありません。情報リスクが実際に増したかもしれません。もしくは、そうでないかもしれません。または、情報リスクに変化はなく、リスクに対する自分の感覚が変わっただけなのかもしれません。そのほか、恐れや不安、疑念に何重にも包まれ、真実が見えなくなったというのが本当のところかもしれません。どちらにしても、今回、2010年のデータ漏洩/侵害を分析することで、ゼウスやAPTなどに関連すると思われる事実をいくつか明らかにできました。例えば、公的機関でのデータ漏洩/侵害発生数が過去最高を記録しています。また、知的財産を含め、企業・機関の機密情報の盗難が、これまでにないほど増加しました。この結果は、今回、扱ったデータ漏洩/侵害事例数が大幅に増えたことによるものであり、したがって実際の変化によるものではないと考える読者もおられるかもしれません。そうかもしれませんし、そうでないかもしれません。

APTについて、ここで少し触れます。記憶している読者もおられると思いますが、昨年の2010年度データ漏洩/侵害報告書で、セキュリティコミュニティでAPTヒステリーが蔓延しているという話を披露しました。いわば「スコープクリープ（肥大化）」現象で、この現象は依然として続いています。APTという用語の考案者は、何らかの国からの攻撃という意味で、この用語を使っているようです。一方、技術レベルとパワーが平均以上の脅威をすべてAPTと呼ぶ人もいます。前者の場合、政府機関や国防産業界はセキュリティ態勢を綿密にチェックし、また堅固なセキュリティ態勢を構築しなければならないというのが論理的な結論です（この結論は正解です）。後者の場合、「誰もがAPTの標的になる」というのが論理的な結論です（これは矛盾です。泥棒は留守の家に入るのが普通なのに、自宅にいる人に泥棒が来ると言って脅かすのと同じです）。ただし、誰もがAPTの標的になることなどありません。もちろん、調査の結果によれば、国家から攻撃を受けることはあり、これは確かです（例えばアジアの国家など）。同じく調査の結果によると、APTによって侵害を受けたと思っていても、実際には犯罪組織やハッカー、スクリプトキディー（技術レベルの低いハッカー）による侵害、または自分の過失によって侵害が発生したということもあり、これも事実です（経験則から、そう言えます）。どちらにしても、良い意味でも悪い意味でも「APT」は無視できない存在であり、その意味を正確に定義するとともに防御を固める必要があります（でなければ、いつまでも迷妄に振り回されることになります）。

2010年のデータ漏洩/侵害事例では、上記のほかにも、昨年と異なる現象がいくつか判明しました。例えば、ベライゾンとUSSSの総合データによると、侵害レコード数は大幅に減少し、過去最低を記録しました。DataLossDBやアイデンティティ窃盗リソースセンターなどの資料でも、侵害レコード数は顕著に減っています。何が起きているのでしょうか。一方、報道記事では、侵害レコード数はそれほど減ってはいません（中には大幅に減ったという報道もあります）。この相違の原因は何でしょう。どちらが「本当」の2010年の事例でしょうか。どちらにも真実はあるというのが、その答えと思われます。つまり、侵害レコード数はそれほど減っていないという報道も一部、真実です。また、ベライゾンとUSSSの事例で示されるように侵害レコード数が大幅に減ったというのも部分的に真実であり、このことは、情報を窃取する際のアタッカーの動機や戦術が変わった可能性があること、または実際に変わったことを表しています。本報告書では、このような傾向、また傾向に関連する統計データを示しながら、そこに込められているメッセージや意味を読み解いて行くことにします。本書の説明が、読者の皆さんが今後、ハッピーエンドへの道を歩む上で些かなりとも寄与することになれば、それは喜ばしいことです。

ゼウスの場合、犯人の目的は金銭の詐取ですが、オーロラ、APT、スタックスネット、アノニマスの場合、金銭以上のもの、例えば企業の機密情報などを目当てとしているアタッカーもいるようです。このことを念頭に2010年のデータ漏洩/侵害を見てみると、自分が標的になっているという不気味な感覚が以前に増して強くなったような気がします。

結論と推奨事項

昨年の報告書では、次のように書きました。

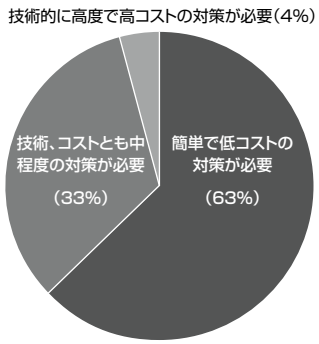
> 本調査報告書（DBIR）には推奨項目を記載してありますが、実効性の高いものを考案するのは年々難しくなってきています。考えてみればレポートの分析結果は、年ごとに徐々に変化し進化しますが、まったく新しくなったり一変したりすることは稀と言えるでしょう。推奨は、分析結果に基づいているのですから、分析結果が変わらなければ推奨措置も変わらないのは当然です。必要であれば、多数の推奨事項を盛り込んだリストを作り、提供することもできますが、このようなリストは他からも入手できるでしょう。弊社の関心は、数ではなくメリットにあります。

ところが、2010年の事例（約800件）は昨年とは数も内容もかなり異なっているのだから、本年は、データ漏洩/侵害回避の推奨事項として新たなものが提唱されるはず、と期待していた読者も多いかもしれません。その意に反し、全く違いました。最終的な結論は、以前と同じです。つまり、データ漏洩/侵害の対策は、基本的には変える必要はありません（図43にあるように、本年の推奨事項の種類は今までとほぼ同じです）。ただし言うまでもなく、実際に実施しているかどうか、また実施方法が順当かどうかによって効果の有無が決まります。

アタッカーは老獪で、適応能力にも長けているから「陳腐化」した防御態勢を突破するのは造作もないことだ、と言う読者もいるかもしれません。これは真実でしょう（適応の例は実際にありましたし、本報告書でも述べました）が、現実を振り返ってみなければなりません。つまり、企業・機関では、今の防御態勢が、アタッカーが適応に苦労しなければならないほど堅固かどうかを考えてみる必要があります。残念ながら、今までの事例データでは堅固ではないようで、したがって是正が必要です。是正してもアタッカーは適応するでしょうが、それはそれで構いません。しかしながら、こちらの手薄な防御態勢に乗じて利を得るという行為は、アタッカーに許してはいけません。

新たな手口の攻撃もいくつかありましたが、いずれも基本的には従来の対策で対応できます。したがって本年は、2010年の主な攻撃手法を分析し、その種の攻撃手法に有効と思われる対策を過去の報告書から拾い出し、掲載することにしました。それぞれ種類に応じて分類し、下記に記載してあります（変更や追加も多少あります）。データ漏洩/侵害防止対策のプランニングと予算の予測の一助となれば幸いです。

図43. 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*



* ベライゾンのデータのみ

概要

初めに基本を固め、次に細部を仕上げます。部門や部署によって高度のセキュリティが確保されているが、別の部門や部署ではそうではないという企業・機関が多数あります。簡単な道を選ぶというのがアタッカーの定法です。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。

アタッカーは老獪で、適応能力にも長けているから「陳腐化」した防御態勢を突破するのは造作もないことだ、と言う読者もいるかもしれません。これは真実でしょうが（適応の例は実際にありましたし、本報告書でも述べました）、現実を振り返ってみなければなりません。つまり、企業・機関では、今の防御態勢が、アタッカーが新入に苦労しなければならないほど堅固かどうかを考えてみる必要があります。

アクセス制御

デフォルトの認証情報を変更します。簡単かつ実用的な方法です。システム管理者やネットワーク管理者は、新規のシステムを立ち上げたら必ずデフォルト（初期設定）のパスワードを変更しなければなりません。ベンダーに新規のシステムの構築をアウトソースした場合、デフォルトのパスワードが変更されていることを確認します。また、従業員やパートナーが企業・機関のセキュリティ関連のポリシーや規則を遵守しているかどうかをチェックします。デフォルトの認証情報の変更のほか、企業・機関では、同じパスワードが複数存在していないこと、同じパスワードが複数のユーザーの間、または複数のシステム（PCなど）で使用されていないことを確認しなければなりません。特に資産の管理をベンダーにアウトソースしている場合、パスワードの扱いに注意が必要です。

データ漏洩/侵害の原因となる脅威アクションについては毎年、分析を行っていますが、結論は同じです。つまり、正体不明で阻止できない攻撃に企業・機関が圧倒されているというわけではありません。というより、ほとんどの場合、脅威アクションの種類や内容は十分に分かっており、また防止する方法も分かっています。

ユーザーアカウントのチェック： 昨年のDBIRの分析結果、また過去の経験から、ユーザーアカウントの定期チェックが重要です。具体的には、現在使用されているユーザーアカウントの中に不正なユーザーアカウントがないか、不要なものがないか、さらにユーザーアカウントの設定が適切かどうか、付与されている権限が適切かどうか（権限はできるだけ小さいのが理想的）をチェックします。

権限を持つユーザーの数を減らし、監視する： 信用していても確認を行います。試用期間中の社員をしっかりスクリーニングし、問題が発生する前に対処します。ユーザーに必要以上の権限を与えないようにし（これは特に重要）、職務の分担を行います。適切な指示（会社のポリシーと規定の周知）と監督（ポリシーなどを遵守しているかどうかの確認）がおこなわれるよう体制を整えます。特権ユーザーの作業はすべてログを取り、管理・経営部門に報告されるように設定します。特権ユーザーが予定に無い行動を行った場合、アラームが発動し、調査を実施します。

ネットワーク管理

リモートアクセスサービス： リモートアクセスサービスが常時有効になっており、またインターネットに直結されているケースが少なくありません。特定のIPアドレスやネットワークからだけ、リモートアクセスサービスにアクセスできるようにします。また、ネットワーク内部の機密システム（機密情報が置かれているPCなど）に対するアクセスを制限することも重要です。企業・機関では、ネットワーク上の任意の機器から別の任意の機器に接続し、アクセスできるケースが多いようですが、このような状態は避けなければなりません。特定の管理ネットワークからアクセスコントロールリストを介してのみ、リモートアクセスサービスにアクセスできるようにします。

アウトバウンドネットワークトラフィックの監視とフィルタリングを行う： データ漏洩/侵害では多くの場合、一連のイベントが発生している間、データが外部に流れたり、外部に対して通信や接続が実行されたりします。このような状態を防止することで、連鎖を断ち切り、結果的にデータ漏洩/侵害を終わらせることができます。アウトバウンド・トラフィックの監視、状態の把握、管理を行うことで、侵害行為が軽減される可能性が大きく向上します。

セキュア開発

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によるデータ漏洩/侵害事例のうち、ほぼ半数が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（迂回）、セッション変数の悪用によるものでした。今、アタッカーが「梯子」を登り、アプリケーション層に攻撃の的を絞っていることは明白です。こちらも相応の対応が必要です。何事もそうですが、まず火を消さなければなりません。今では軽量のウェブアプリケーションを使ってスキャニングやテストを実行でき、昨年も、このようなスキャニングやテストで問題を発見していれば、防止できたデータ漏洩/侵害も多かったかもしれません。次に、アーキテクチャーや権限、ソースコードを定期的にレビューします。また、セキュリティ開発ライフサイクル（SDLC）手法を使ってアプリケーション開発を進めることも有効です。さらに、脆弱性のないコードを書くことが重要で、その重要性を開発チームのメンバーに周知します。

ログの管理と分析

アプリケーションとネットワークのログを記録し監視する： 一般にデータ漏洩/侵害の発生に先立ち、その予兆となるイベントが発生しますが、そのイベントに全く気がつかず、もしくは対応が一切行われないという状況が実に頻繁に見られます。この種のイベントを正確に、また効果的、効率的に監視できる手法や手順（ロギング機能）を用意することがデータを保護する上で不可欠です。

なお、ネットワークやオペレーティングシステム、IDS、ファイアウォールのログだけでなく、リモートサービス、ウェブアプリケーション、データベース、その他の重要なアプリケーションのログにも注目する必要があります。このようなログは、データ漏洩/侵害の検出、防止、調査にとって貴重で有用なデータです。

「不審」と「異常」を定義します（その後、その不審または異常を探します）： 表現は曖昧ですが、その意味は、「処方箋」を作り、その処方箋にしたがって全員が必要な時点で対応できるようにすることです。具体的には、まず、「不審な状態」と「異常な状態」を定義し、それを基準に「正常な状態」を定義し、続いて、対応に必要なメカニズム（機能やシステム）を用意します。その後、正常な状態からの差（不審な状態または異常な状態）を探し、その差が見つかれば対応します。

イベント監視とログ分析の方法を見直し改善する： 漏洩/侵害の段階に関する分析結果によれば、企業・機関では、データ漏洩/侵害の発生を「すぐに検出する」というより、「今週中に検出する」という姿勢で望んだほうが得策のようです。「すぐに検出する」のはほぼ不可能であり、「数日」が妥当だからです。「侵害から発見まで」の期間を「数週間」または「数カ月」から「数日」に短縮できれば、被害は大幅に軽減されます。「数日」で検出する場合、木より森に目を向けます。この作業は、それほど難しくはありません。たとえば、ログの行数や長さをカウントし、値が許容値を超えたらアラートが出力されるような簡単なスクリプトを作成します。この方法はメリットが大きく、時間や労力、費用もそれほどかかりません。

教育と意識の喚起

ソーシャルエンジニアリングに対する意識の喚起： ソーシャルエンジニアリングの手口や経路について、従業員に詳しく説明します。事例データでは、電子メールの不審なリンクをクリックしたり、知らない相手からの電子メールの添付ファイルを開いたため感染したという事例が多く見られました。疑わしい電子メールやウェブサイトを発見したら報告するように指導し、また報奨制度を作るのも一策です。

タンパリングや詐欺行為に注意するように従業員を指導、また顧客に注意を喚起： タンパリング（機器の改変や細工）や詐欺行為については、地域によっては防止のための活動やキャンペーンが行われていますが、それでもATMやカード対応給油機のタンパリングと詐欺は数が増加しており、発生している地域も広がっているようです。ATMなどを設置・運用している企業・機関では、定期的に機器をチェックする必要があります。また、この種の詐欺の犠牲にならないように顧客に注意を促すとともに、タンパリングなどを見つけたら企業・機関に通知するように依頼します。

インシデント管理

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・機関では、迅速に対応しなければなりません。その観点から、事前にインシデント対応プランを作成しておくとが重要であり、このプランにはデータ漏洩/侵害による被害を抑制する方法のほか、証拠を確実に収集する方法を記載しておきます。

擬似インシデントテストを実行する： よく聞いてください。練習です。インシデントではなく練習の話です。何より練習が大事です。しつこいようですが、練習が必要です。練習を繰り返してこそ、完璧に近づくからです。データ漏洩/侵害が発生した場合、迅速かつ効率的に対応しなければなりませんが、そのためにはインシデント対応訓練を定期的に実施する必要があります。訓練は、擬似場面を設定し、戦略に沿って脅威の特定と分類を行い、手順にしたがって行動し、証拠を保全するという順序で進めます。

データ共有のお願い

情報リスクを管理するための取り組みにおいてはさまざまな課題が支障となっていますが、なかでも最も重要かつ持続的な課題の 1 つはデータ不足です。セキュリティ業界の関係者として一言吐露させていただくと、現在データが不足している理由としては、まずデータが共有されていないことが挙げられます。次に、もう一つの理由として（ほかにも多数あります）、仮に共有されていたとしても有用なデータが少なく、プライバシーが守られず、また相互の利益に結びついていない場合が多いということが挙げられます。その点、本報告書は、有用なデータを提供し、プライバシーも保護され、しかも多数の方々の利益に寄与している共有方法の一例であると自負しています。過去2年の間に数社の調査会社が分析結果の共有に踏み切り、これには敬意を表します。どんな些細なことであっても、共有すれば有益です。共有に参加する調査会社が増えれば、その効果は増します。また、VERISを使用して分析結果を記録していただければ、「同じ土俵」で結果を比較できます。VERISを使用される方には、協力を惜しみません。

また、調査会社以外の企業・機関の方々には、 VERISコミュニティウェブサイト の利用をお勧めします[12]。このサイトでは、匿名でセキュリティインシデントに関する情報を入力できます（データ漏洩/侵害以外の情報も入力できます）。記録された情報はすべて（集計後の情報、すべて匿名）、VERISコミュニティで利用可能です。つまりインシデント情報を記録することでVERISコミュニティの情報が増加し、その情報（VERISデータセット）に自分もアクセスできます。VERISコミュニティの目的は、インシデント情報の「土台」を提供することです。この土台の上で相互に協力しながら建設的にインシデントに関する状況を把握し、その知識をリスク管理の向上に活用できます。

貴方の貴重な時間をこの報告書に割いていただき、ありがとうございました。ここで改めて、本報告書を読んでいただいた方に感謝します。

12 https://www2.icsalabs.com/veris/（内容英語）

verizonbusiness.com/jp

verizonbusiness.com/jp/socialmedia　verizonbusiness.com/thinkforward（内容英語）