2012 年度データ漏洩 / 侵害調査報告書

オーストラリア連邦警察、オランダハイテク犯罪ユニット、アイルランドレポートおよびインフォメーションセキュリティーサービス（IRISSCERT）、ロンドン警視庁サイバー犯罪合同捜査本部、アメリカ合衆国シークレットサービスの各機関による協力のもと、ベライゾン RISK チームによる調査が実施されました。

2012 年度データ漏洩 / 侵害調査報告書：エグゼクティブサマリー

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

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

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

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

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

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

上記の機関からいただいた資料により、今回の DBIR で扱うことができた
データ漏洩 / 侵害事例は、これまでと比較して大幅に増加しました。
各機関の協力に心より感謝申し上げるとともに、
本報告書がサイバー犯罪に対する警鐘として、
また犯罪防止の有効な道具として寄与することを願うものであります。

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

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

データ収集

ベライゾンのデータ収集メソドロジーは、基本的には今までの方法と同じです。つまり、2004 年から 2011 年の間にベライゾンが実施したフォレンジック調査で得られた直接証拠を事例データとし、分析を行いました。USSS、NHTCU、AFP、IRISSCERT、PCeU でのデータの記録方法は、厳密に言えば異なりますが、基本的には同じです。つまり、各機関のデータはすべて VERIS を活用していますが、機関によってデータ入力の具体的な方法は多少異なりました。事例については、2011 年に各機関が扱ったもののうち、企業･組織に関連するデータ漏洩 / 侵害の事例であり、かつデータ漏洩 / 侵害が実際に確認されたものだけを抽出しました。

VERIS について

VERIS は、共通の言語でセキュリティインシデントに関する情報を記録できるフレームワークです。反復可能な構造化形式で情報を入力でき、「誰が、何にまたは誰かに、どの様なことをして、結果はどうなったか」という物語風に情報を入力すると一定形式のデータ（本報告書に記載されているようなデータ）に変換されます。ベライゾンでは、DBIR のデータ収集方法について質問を受けることが多く、また今以上にセキュリティインシデントに関する情報をより多くの企業・方々と共有したいと考えていることから VERIS は公開されており、誰でも無料で使用できます。VERIS の概要については弊社 ウェブサイト[1] に掲載されていますが、詳しい説明は VERIS コミュニティ wiki[2] で閲覧できます。弊社のウェブサイトと VERIS コミュニティはどちらも、本報告書の内容や用語を理解する上で有用です。

1 http://www.verizonbusiness.com/resources/whitepapers/wp_verizon-incident-sharing-metrics-framework_ja_xg.pdf
2 https://verisframework.wiki.zoho.com/

統計情報のあらまし

データ漏洩 / 侵害の背後にいるのは誰か?

98% が外部因子によるもの（+6%）

4% が内部の従業員（内部因子）によるもの（-13%）

<1% がビジネスパートナーによるデータ漏洩 / 侵害（同）

データ窃盗の **58%** が活動家グループの関与によるもの

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

データ漏洩 / 侵害はどのようにして発生するか?

81% が何らかのハッキングによるもの（+31%）

69% がマルウェアによるもの（+20%）

10% が物理的攻撃により発生（-19%）

7% がソーシャルエンジニアリング（-4%）

5% が権限の不正使用によるもの（-12%）

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

どのような共通点があるか?

79% がオポチュニスティック（無作為）型の攻撃（-4%）

96% の攻撃は、技術的にそれほど高度とは思われない（+4%）

全データ漏洩 / 侵害の **94%** がサーバー上のデータの侵害（+18%）

データ漏洩 / 侵害の **85%** が数週間以上経過した後に発見（+6%）

データ漏洩 / 侵害の **92%** が第三者によって発見（+6%）

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

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

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

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

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

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

2011 年はどこがどう「悪化」したのでしょうか。

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

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

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

被害軽減策で重点を置くべき領域は?

小中規模の企業・組織

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

大規模企業・組織

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

脅威イベントの概要

昨年のデータ漏洩 / 侵害調査報告書で初めて、脅威イベント（VERIS で定義されている脅威イベント）の表を掲載しました。この脅威イベントの表は、各協力組織から提供される新たな事例データと同じく、本報告書の特徴の中でも高く評価されている特徴の一つです。本報告書では、データ漏洩 / 侵害事例を脅威因子、脅威アクション、資産、属性（A4 脅威モデルの 4 つの要素）を基準にして個別に分析していますが、この脅威イベントの表では 4 つの要素の相互関係を見ることができます。言い換えると、2011 年のデータ漏洩 / 侵害に関連している脅威イベント（データ漏洩 / 侵害の原因であるイベント）を確認できます。図 1（全企業・組織の事例）と図 2（大規模企業・組織の事例のみ）は、本報告書完全版のメソドロジーの節の図 1 を基にして作成したものです。そこではマス目の値は脅威イベント番号（TE#）ですが、図 1 と図 2 では、マス目の値は、その脅威イベント（他の脅威イベントも関係していることもあります）によって引き起こされたデータ漏洩 / 侵害の数です。[3] 図 1 と図 2 は今回の 855 件のデータ漏洩 / 侵害事例を集計した表であり、注目すべき点がいくつかあります。

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

全企業・組織の事例の脅威イベントの表（図 1）の内容は、昨年の報告書の結果とほぼ同じです。大きな違いは、本年は、脅威アクションが不正使用と物理の脅威イベントの値が昨年より多少減少している一方、脅威アクションがマルウェアとハッキングの脅威イベントの値が増えていることです。

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

図 1. VERIS の脅威イベントの表（マス目の値はデータ漏洩 / 侵害事例の数）

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

脅威イベントの表の話に戻ります。全企業・組織の事例の脅威イベントの表（図 1）の内容は、昨年の報告書の結果とほぼ同じです。大きな違いは、本年は、脅威アクションが不正使用と物理の脅威イベントの値（データ漏洩 / 侵害の数）が昨年より多少減少している一方、脅威アクションがマルウェアとハッキングの脅威イベントの値が増えていることです。同様に上位 10 位までの脅威イベントも、本年は昨年とよく似ています。

図 2 は大規模企業・組織の事例のみの場合の脅威イベントの表ですが、ここで注意点をいくつか簡単に紹介します。まず、お気づきかもしれませんが、図 2 は図 1（全企業・組織の事例）に比べて、値が 0 を超える脅威イベントの種類が少ないのです（315 種類の脅威イベントのうち 22 種類しかなく、割合にすると 7%です）。少ないのは、大規模企業・組織の場合、セキュリティが固く防御態勢も堅固であるからと考える読者もいるでしょう。この理由はおそらく正しく、本報告書の分析結果と矛盾するものではありません。私どもの見解では、図 2 が図 1 に比べて脅威イベントの種類が少なく疎らなのは、大規模企業・組織のデータ漏洩 / 侵害事例が少ないこと（大規模企業・組織の事例は、全 855 件中の 60 件）が主な理由と思われます。また、脅威イベントの値の分布に注目すると、大規模企業・組織の事例の場合、侵入型の脅威イベントの値の分布が図 1 に比べてはるかに均等です（図 1 では脅威アクションがマルウェアまたはハッキングの脅威イベントの値は大きな開きがありますが、図 2 ではそれほど開きはありません）。最近、ソーシャルエンジニアリングによる攻撃が目立っていると報じられていることを考慮すると、これは不思議ではありません。

図 2. VERIS の脅威イベントの表（マス目の値はデータ漏洩 / 侵害事例の数）（大規模企業・組織の事例のみ）

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

本報告書の完全版では昨年 2011 年の漏洩 / 侵害でもみられた脅威因子、脅威アクション、侵害された資産についてさらに詳しく検証していきます。またベライゾンや協力機関によるデータ収集の手法についてもさらなる情報を基に詳しくご紹介します。

2012 年度データ漏洩 / 侵害調査報告書：結論と推奨事項

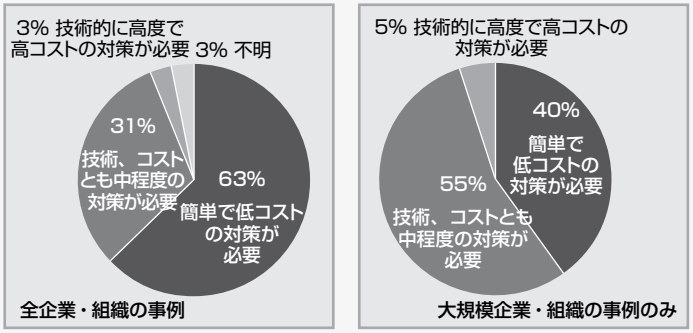
本年は、新たな推奨事項をご紹介します。なお、環境保護グループとしては、資源を大切にする義務があります。そのため、新たな推奨事項を紹介する前に昨年の「序文」を再利用し、下に掲載します。

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

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

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

図 3. 推奨される予防対策の種類で分類した場合のデータ漏洩 / 侵害の割合 *



* ベライゾンの事例データのみ

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

POS のセキュリティと対策

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

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

- ✓ **すべての POS システムの管理者パスワードを変更しましょう。**
  - ハッカーはインターネット上で常時、簡単に解読できるパスワードを探しています。
- ✓ **ファイアウォールをインストール、またはリモートアクセスサービスにアクセスコントロールリストを設置しましょう。**
  - 上記の対策によりハッカーはお店のシステムに侵入できなくなり、その結果、簡単に情報が盗まれることはなくなります。

以上に加えて、次の対策も実施するとさらに効果的です。

- POS システムを使ってウェブを閲覧することはやめてください。（インターネット上で閲覧と同様の操作をすることも控えます）。
- POS 環境が PCI DSS に準拠しているかどうか確認してください。（POS のベンダーにお聞きください）。

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

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

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

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

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

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

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

マルウェア：バックドア、コマンド&コントロール ハッキング：バックドアまたはコマンド&コントロールチャンネルの不正使用	
概要	コンピュータウィルスに感染したコンピュータに外部からアクセス、またはコンピュータを制御することを目的とした攻撃手法。バックドアプログラムとコマンド／コントロールプログラムはどちらも、コンピュータ上の通常の認証メカニズムやセキュリティコントロールを迂回する機能があり、また秘密裏に動作するように設計されています。
徴候	コンピュータの動作やパフォーマンスが異常になり（マウスを触っていないのに勝手にカーソルが動いてファイルを操作しているように見える）、またネットワークの動作も異常になります。徴候のチェック方法としては、IDS/IPS（非カスタマイズバージョン）の使用、レジストリの監視、プロセスの監視、定期的ログ監視、コンピュータ上にマルウェアが存在しないかどうかの確認、アンチウィルスが無効になっていないかのチェックなどがあります。 調査対応チームがマルウェアの調査を行う場合、通常、アクティブのプロセスをチェックします。また、コンピュータの全内容を作成日または修正日を基準にしてソートした後、リストを出力します。この作業により、Windows¥system32 ディレクトリやユーザーの暫定ディレクトリに悪意のファイルが見つかることがよくあります。

マルウェア：バックドア、コマンド&コントロール ハッキング：バックドアまたはコマンド&コントロールチャンネルの不正使用	
対策	出口フィルタリング（この攻撃手法の場合、通常とは異なるポートやプロトコル、サービスを介してデータが送信されるのが一般的です）、アウトバウンドトラフィックに対するプロキシの使用、IP ブラックリスティング（業務に直接関係のないアドレスが多い場合、IP ブラックリスティングで一括してアドレスをブロックします）、ホスト IDS（HIDS）、整合性監視、管理者権限を持つユーザーの数の制限、パーソナルファイアウォール、データ漏洩防止ツール（DLP）、アンチウィルスとアンチスパイウェア（アンチウィルスは、カスタマイズすると効果が弱くなります。アンチウィルスベンダー 40 社の製品を試してみましたが、バックドアの検出に成功したのは、その中の 1 つだけでした）、ウェブ閲覧ポリシーの強化。

物理：タンパリング	
概要	タンパリングとは、資産の通常の状態または機能を無許可で改ざんまたは阻害することをいいます。ソフトウェアやシステム設定の改ざんではなく、機器などを物理的に改ざんすることです。
徴候	予定がないのに機器の保守点検が行われている。傷がある、接着剤を使った跡がある、カメラに穴があいている、キーパッドの上に何かのせられているなど。タンパリングは発見が困難です（オーバーレイスキーマーは機器の上に乗せられているため注意すれば発見できますが、内部タンパリングは一般に外部からは見えません）。タンパリング防止シールが破れている。心当たりのないブルートゥース信号が長い間、続くのも徴候の一つです。ATM やガソリンスタンドに取り付けられたスキマーは、通常は数時間後に取り外されます。数日や数週間、設置されたままになっていることはありません。
対策	タンパリングを発見するように従業員を指導し、顧客にも注意を呼びかけます。定期的に（勤務交代の際など）、タンパリングの対象となる機器を点検します。カードと PIN（暗唱番号）が必要な機器の場合、通常は両方が標的になります（「徴候」を参照）。チェックを行うときは、その点（スキマーが 2 つないかどうかなど）に注意します。 スタッフ全員に研修を行い、保守点検作業について詳しく説明します。保守点検作業のスケジュールのほか、保守員や保守ベンダーの入館許可についても説明します。 機器を購入する際、機器にタンパリング防止技術・機能を搭載するようにベンダーに依頼するか、タンパリング防止装置（例えばタンパースイッチ。プラスチックで覆われた電子機器で、メモリーの初期化が可能）付きの POS 装置や PIN 入力装置だけを購入します。

キーロガー / フォームグラバー / スパイウェア	
概要	いずれもマルウェアで、ユーザーが行う操作の監視やログ、また入力したデータの収集を目的として設計されています。大規模な攻撃に先立ち、ユーザー名やパスワードの収集に使用されるのが普通です。また、侵害した POS 機器からペイメントカード情報を盗むのにも使われます。ほとんどの場合、秘密裏に実行されるため、ユーザーは気がつきません。
徴候	通常、コンピュータの動作やパフォーマンス、ネットワーク動作が異常になります。徴候のチェック方法としては、IDS/IPS（非カスタマイズバージョン用）の使用、レジストリの監視、プロセスの監視、定期的ログ監視、コンピュータ上にマルウェアが存在しないかどうかのチェック、物理的改ざんがないか（見慣れない機器が取り付けられていないか）の確認などがあります。認証（ログイン）情報の不正使用のチェックについては、「ハッキング：盗んだログイン情報の使用」の説明（前頁）を参照してください。 調査対応チームがマルウェアの調査を行う場合、通常、アクティブのプロセスをチェックします。また、コンピュータの全内容を作成日または修正日を基準にしてソートした後、リストを出力します。この作業により、Windows¥system32 ディレクトリやユーザーの暫定ディレクトリに悪意のファイルが見つかることがよくあります。

キーロガー / フォームグラバー / スパイウェア	
対策	管理者権限を持つユーザーの数を最小限にします。防御対策としては、コードサイニング、ライブブート CD、ワンタイムパスワード、アンチウィルスとアンチスパイウェア、パーソナルファイアウォール、ウェブコンテンツフィルタリング、ブラックリスティング、出口フィルタリング（この攻撃手法の場合、通常とは異なるポートやプロトコル、サービスを介してデータが送信されるのが一般的です）、ホスト IDS（HIDS）の使用・適用のほか、整合性監視、ウェブ閲覧ポリシーの強化、セキュリティ意識強化トレーニングの実施、ネットワークのセグメント化などがあります。

プリテキスティング（ソーシャルエンジニアリング）	
概要	ソーシャルエンジニアリングとは、アタッカーが何らかの状況を用意し、目標（人間）を説得したり巧みに操ったり、もしくは策謀し何らかの行為を行わせたり、情報を漏洩させる行為です。「ヒューマンハードウェアのバグ」を悪用した脅威アクションで、残念ながらパッチは存在しません。
徴候	この攻撃手法は、人間の弱さを悪用し、技術的な警戒メカニズムを迂回するという発想を基礎としているため、発見は非常に難しいというのが現状です。おかしな話を持ちかけられたり、一般的な作業から逸脱した作業を要求されたり、情報の提供や何らかの行為の実行を求められ、それが会社のポリシーに違反するような場合が、この攻撃手法の徴候です。電話や訪問者、電子メールの記録のチェックも徴候を発見するのに有効です。
対策	セキュリティ意識強化トレーニングを実施し、また明瞭なポリシーと規則を策定します。ポリシーに違反する行為があった場合、すぐに指摘し、ポリシーを厳格に遵守するように指導します。ソーシャルエンジニアリングに注意し、その疑いがあったには、必ず報告するように指導します。普通でない依頼や要請を受けた場合、信頼できる社員や部署に相談するように指示しておきます。社員名簿（その他、類似の情報の記録）を公開しないようにします。

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

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

2012 年度データ漏洩 / 侵害調査報告書

オーストラリア連邦警察、オランダハイテク犯罪ユニット、アイルランドレポートおよび
インフォメーションセキュリティーサービス（IRISSCERT）、ロンドン警視庁サイバー犯罪合同捜査本部、
アメリカ合衆国シークレットサービスの各機関による協力のもと、ベライゾン RISK チームによる調査が実施されました。

verizon.com/enterprise/jp