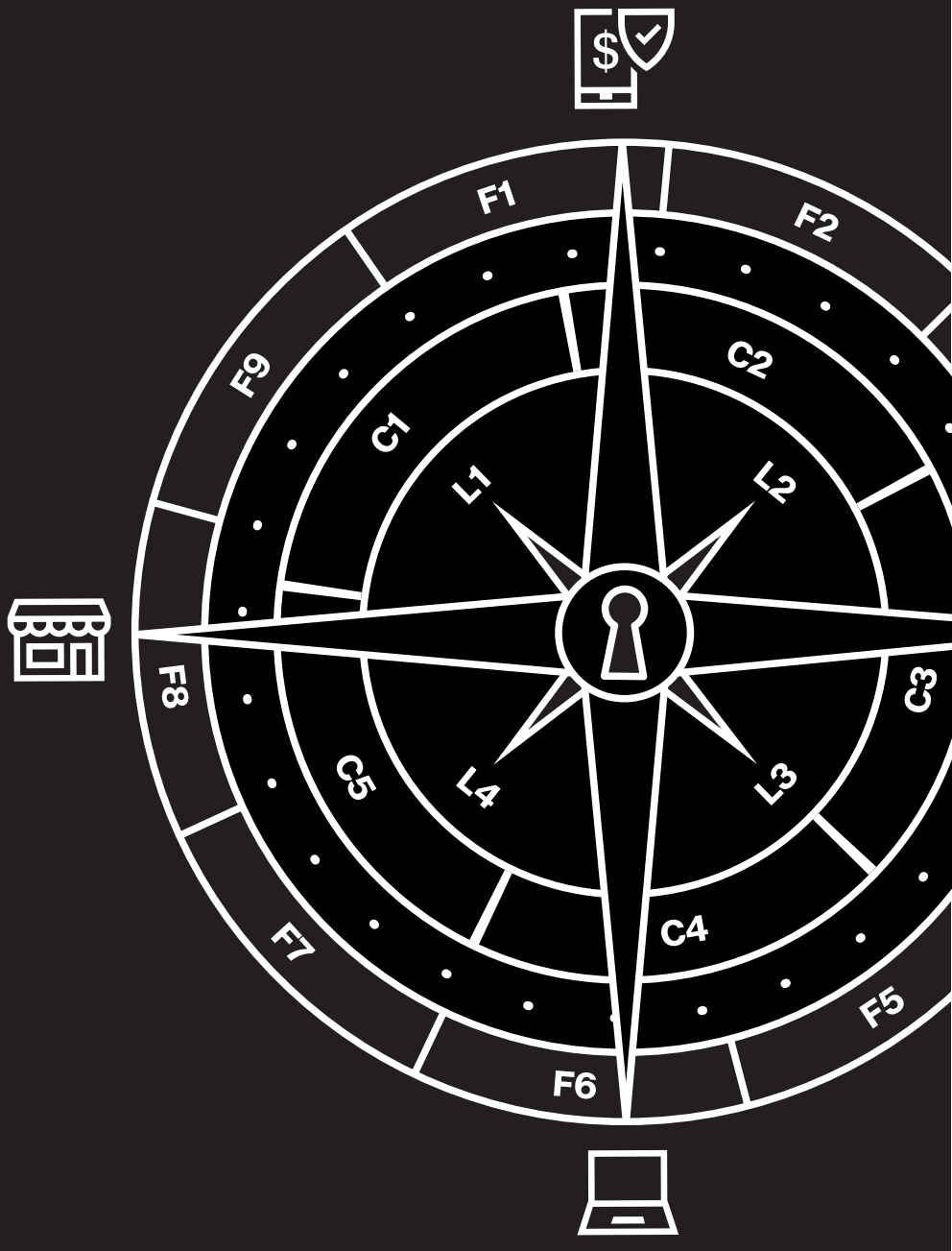
2019 ベライゾンPSR決済システムのセキュリティに関するレポート

流通・小売業界の
コンプライアンスの現状



verizon business ready

流通・小売業界の競争は、かつてないほどの激しさを見せています。このような状況で成果を上げるためには、顧客の声に十分に耳を傾けることが必要です。そして、流通・小売業界の顧客の対応では、これまで以上にデータやプライバシーの保護が重要になっています。

ある企業でデータ侵害が発生した場合、その企業の商品やサービスを利用し続けている顧客はわずか7%にとどまります。そして、競合他社よりも取引条件が良い場合でも、69%の顧客がそのような企業との取引は避けると述べています[1]。そのため、クレジットカードのセキュリティは重要な差別化要素になっています。

実効性の高いセキュリティ管理を継続的に行って、PCI DSS（Payment Card Industry Data Security Standard）の要件を満たしていれば、顧客の信頼が得られ、競争優位性を確保することができます。しかし、これを実現するためには、データ保護とコンプライアンスのプログラム（DPCP）を進化させ、成熟させねばなりません。

このような状況で役に立つのが、『2019 ベライゾンPSR決済システムのセキュリティに関するレポート』です。クレジットカードのセキュリティのトレンドに関してPSRが明らかにしている革新的なインサイトは、専門家が自身の業界の状況を理解するのに役立ちます。Verizon 9-5-4 Compliance Program Performance Evaluation Frameworkなどの新しいナビゲーションツールを使えば、データのセキュリティやコンプライアンスを向上させることができますが、2019年版のPSRでは、この点についてもご説明いたします。

ICチップやPINを導入しても流通・小売業界では依然としてデータ侵害が発生

4年前の時点では、流通・小売業界におけるデータ侵害の多くはPOSにおいて発生していました[2]。しかしそれ以降はEMV（Europay、MastercardおよびVisa）テクノロジーの登場により、クレジットカードの不正使用は激減し、主にデータ侵害はWebアプリケーションを経由して発生するようになりました[3]。ただし、それでも、クレジットカードに起因する侵害が完全になくなったわけではありません。流通・小売事業者は警戒を怠らず、クレジットカードのデータを保護しなければなりません。

2019年版のPSRでは、Verizon Threat Research Advisory Center（VTRAC）| Investigative Response Teamが2016年から2018年に行ったPCIフォレンジック調査（PFI）をもとに、データ侵害に関する調査において詳細な情報の関連付けを行っています。長期的なトレンドのデータを見ると、確認されたデータ侵害のうち、流通・小売業界で発生しているデータ侵害の割合は調査対象のほかの業界（医療、金融サービス、ITサービス）と比べて最も大きな数字になっていることがわかります。

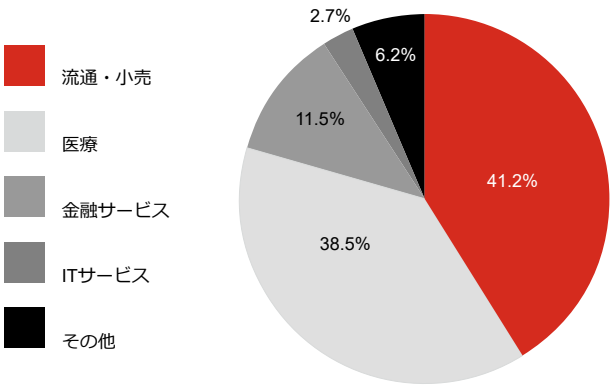


図1：業種別で見たデータ侵害の発生の割合。過去6年間のトレンド。
出典：ベライゾンPFIグローバルケースロード 2010–2016

弊社のデータによればインターネットで事業を行っている流通・小売事業者のほとんどが侵害を経験しています。『ベライゾン2019データ漏洩/侵害調査レポート』によれば、流通・小売事業者のデータを狙った侵害は金銭や脅迫が目的であるか、愉快犯によるものであると言います。侵害を受けたデータのなかには、インセンティブプログラムから盗まれた個人情報もあります。

クレジットカードのセキュリティは重要であるが、そのための基準をすべての企業が満たしているわけではない

幸いにも、クレジットカードのセキュリティを強化できる可能性はあるのです。全業界をカバーするよう、2018年版のPSRでは約55の組織を対象として調査を実施しましたが、その結果によれば、18%の組織が、データ保護とコンプライアンスのプログラム（DPCP）を定義していないと回答しています。DPCPの成熟度が最適化されていると評価している組織はありませんでした。

18%

全業界を対象とした調査で、データ保護とコンプライアンスのプログラム（DPCP）を定義していないと回答した組織の割合。DPCPの成熟度が最適化されていると評価している組織はありませんでした。

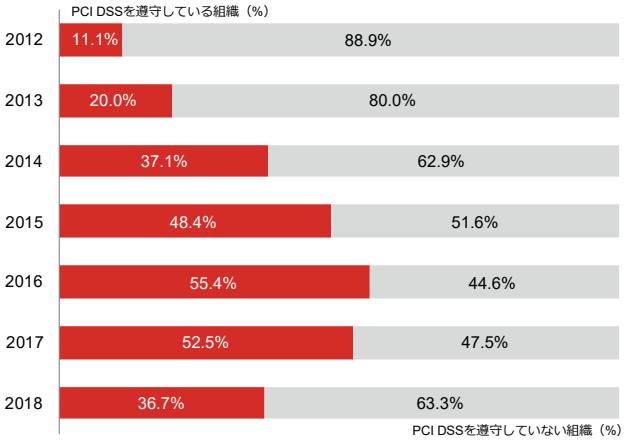


図2：コンプライアンスを完全に満たしている組織の年別の割合

ベライゾンがPSRの発行を始めてからの9年間のうち、2017年まではPCI DSSを完全に遵守している組織の割合は毎年増加していました。しかし、2017年からは2年連続でその数字は減少しています。ほかの認定セキュリティ評価機関（QSA）企業の評価でも同様に、PCI DSSの基準を完全に満たしている組織の数は減少しています。

PCI DSSとは何か

主要なカードブランドが共同で策定したPCI DSS（Payment Card Industry Data Security Standard）では、顧客との取引でカード決済を行う企業がカードの不正使用を減らすことができるようサポートします。PCI DSSはクレジットカードのデータ保護に主眼を置いていますが、そのベースとなっているセキュリティ上の強固な原則は、あらゆる種類のデータ保護に当てはまります。PCI DSSでは、データの保持に関するポリシーや暗号化、物理的なセキュリティ、認証、アクセス制御などのトピックを扱います。PCI DSSの詳細については、pcisecuritystandards.orgをご覧ください。

2019年版のPSRでは、全体としてコンプライアンスの状態が悪化していますが、一方、PCI DSSの要件を完全に満たしている状態からどの程度の乖離があるのかを示す管理のギャップは前年と同様の7.2%になっています。暫定的なコンプライアンスの評価を行っていない組織だけに目を向けた場合、管理のギャップは昨年から6.2%減少して10.2%になっており改善しています。

アジア太平洋地域（APAC）の組織は他の地域よりも、PCI DSSのコンプライアンスを完全に遵守した状態を維持する能力に長けており、そのような組織の割合は69.6%に上ります。ヨーロッパ、中東、アフリカ地域（EMEA）では、PCI DSSを完全に遵守している組織の割合は48.4%になりますが、アメリカ地域の場合そのような組織の割合は25%未満（20.4%）しかありません。

流通・小売業界ではコンプライアンスを満たす組織の割合が著しく減少

2019年版のPSRでは、PCI DSSの要件を完全に満たすことのできる組織の割合がどの業種でも減少しています。流通・小売業界全体で見ると、その割合は昨年が56.3%、2017年が50.0%であったのに対し、36.4%まで落ち込んでいます。

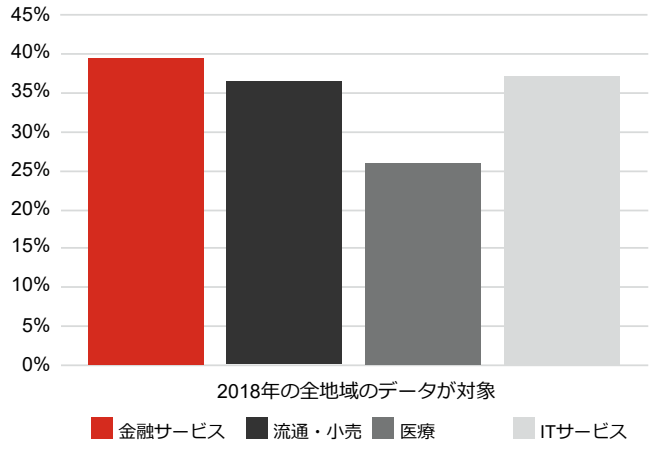


図3：コンプライアンスを完全に満たしている組織の業種別の割合

この数字はITサービスと同等であり、医療（26.3%）を上回っていますが、金融サービスを下回っています。金融サービスは、今回調査を行った4つの業種のうちで最も高く、PCI DSSを完全に遵守している組織の割合は39.0%になっています。

評価できるポイント

2019年版のPSRにある通り、流通・小売業界ではデータの移動時の暗号化（PCI DSSの要件4）と、悪意のあるソフトウェアからの保護（要件5）において、適切な対応がなされています。いずれの要件についても管理のギャップが縮小され、ほぼ完全に要件を満たす状態になっており、ほかの業界を大きく凌駕しています。

さらにこの業界では、アクセスの認証（要件8）でも極めて優秀な成果を収めており、データ漏洩が防止されています。この要件でも管理のギャップは縮小しており、70.5%の組織が要件を完全に満たしています。これは、金融サービス、ITサービスを上回る数字となっています。

また、データへのアクセスの追跡と監視（要件10）においても、著しい成果が確認できます。今回調査を行った4つの業界のうちでこの要件を最も満たしているのが、流通・小売業界でした。要件を満たしている組織の割合は81.8%に上ります。

問題となるポイント

流通・小売業界の場合、PCI DSSの要件を満たすことができていない点としては、調査対象のコンポーネントにおいて、ベンダーが提供するデフォルトの設定をあまりにも多く使っている点（要件2）が挙げられます。コンプライアンスを完全に満たしている状態からどの程度の乖離があるのかを示す管理のギャップは12.4%にもなっています。

さらに、この業界では、セキュリティを適切に管理するための要件（要件12）を満たしておらず、この点における数字が大きく落ち込んでいます。管理のギャップは昨年から18.2%減少して56.8%になりました。

興味深い事実

調査対象となったすべての業界のうちで、データ侵害のインシデントに備える準備についての数字が最も低かったのが、流通・小売業界です。以下のような多くの点でこの業界は対応に苦しんでいます。

- ユーザーを把握し、適切なレベルの権限を割り当てる（管理10.2.5）
- サービスプロバイダーと連携する場合は、プロバイダーの適正評価を実施する（管理12.8.3）
- 許可していないワイヤレスアクセスポイントを特定する（管理11.1.2）
- インシデント対応（IR）プランを最適な状態に維持する（管理12.10）

アドバイス

ベンダーの提供するデフォルトの設定を変更する

デフォルトのパスワードを別のものに置き換え、ベンダーの提供するほかのデフォルトの設定も使用しないようにすれば、攻撃に対する耐性を高めることができます。まずはこの点を最優先に考える必要があります。幸い、デフォルトの設定を置き換えるためのスキルは高い確率で組織内に存在しています。

インシデントに備える投資の実施

サイバーセキュリティインシデントはまず間違いなく発生します。その対応次第で状況は大きく変わります。セキュリティインシデントのリスクを把握し、すばやく対処を行うとともに、IRプランを最適な状態に維持していれば、問題を調査し、その影響を抑えるうえで先手を打つことができます。IRプランのメリットやその導入方法の詳細については、ベライゾンが発行している、インシデントに備える準備とインシデント対応（VIPR）についてのレポートをご覧ください。

PCI DSSの要件を満たすことが重要である理由

2008年から現在まで、ベライゾンではクレジットカードのデータ侵害を受けた組織と、それら組織のPCI DSSの遵守の状況を相互に関連付けてきました。その結果判明したのは、侵害が確認された組織の場合、データ侵害を受けた時点でPCI DSSの主要な12の要件すべてを満たしていた組織は1つも存在しなかったという事実です。

コンプライアンスプログラムの成熟度を高める

実効性のあるコンプライアンスプログラムの策定に、組織はわざと失敗しているわけではありません。プログラムの成熟度を高めるのは容易ではないのです。しかし、指針となる適切なガイドがあれば、それは不可能なことではありません。

2019年版のPSRでは、Verizon 9-5-4 Compliance Program Performance Evaluation Frameworkを提供しています。Verizon 9-5-4 Compliance Program Performance Evaluation Frameworkでは、過去のPSRの成果に新たなガイダンスを組み合わせ、統合フレームワークを構成しており、このフレームワークは、組織がコンプライアンスプログラムを強化するうえで必要とするガイドの役割を果たします。このフレームワークが実現する新たなレベルの可視性と管理性により、組織では再現性と一貫性が得られ、期待できる成果を高い精度で予測することが可能になり、この結果、データを確実に保護することやコンプライアンスを完全に満たすことができるようになります。

図4：管理の有効性と持続性に関する9つの要素の関係モデル

ブランドイメージ維持の取り組みの一環として決済のセキュリティを捉える

流通・小売業界では、ここ最近、PCI DSSを遵守している組織の割合が減少していますが、自社の決済のセキュリティ対応においてその影響を受ける必要はありません。2019年版のPSRに見られるように流通・小売業界全体のコンプライアンスのパフォーマンスは精彩を欠きますが、それでもこの業界には、PCI DSSを遵守できている組織はいくつもあります。コンプライアンスプログラムの成熟度を高められれば、顧客が求めているような信頼できるブランドを生み出して、このような業界のリーダーの一員となることができ、競争優位性を確保することができます。

詳細情報

セキュリティの取り組みで注力すべきポイントやコンプライアンスプログラムを強化する方法の詳細については、enterprise.verizon.com/resources/reports/payment-security/をご覧いただくか、ベライゾンの担当者までお問い合わせください。

verizon business ready

1 ベライゾン発行の2019年のレポート『CXの戦いに勝利するには：次世代のCXがもたらすリスクと価値』に記載の内容による。このレポートは、15か国6,000人の消費者を対象に実施したWebのアンケート調査の回答と、カスタマーエクスペリエンス（CX）の専門家に行った定性的なインタビューの結果を基にしています。Financial Timesの関連会社であるLongitudeが調査を担当。https://enterprise.verizon.com/ resources/reports/2019/winning_the_cx_war.pdf

2 ベライゾン2019 データ漏洩/侵害調査レポート https://enterprise.verizon.com/resources/reports/dbir/

3 同上