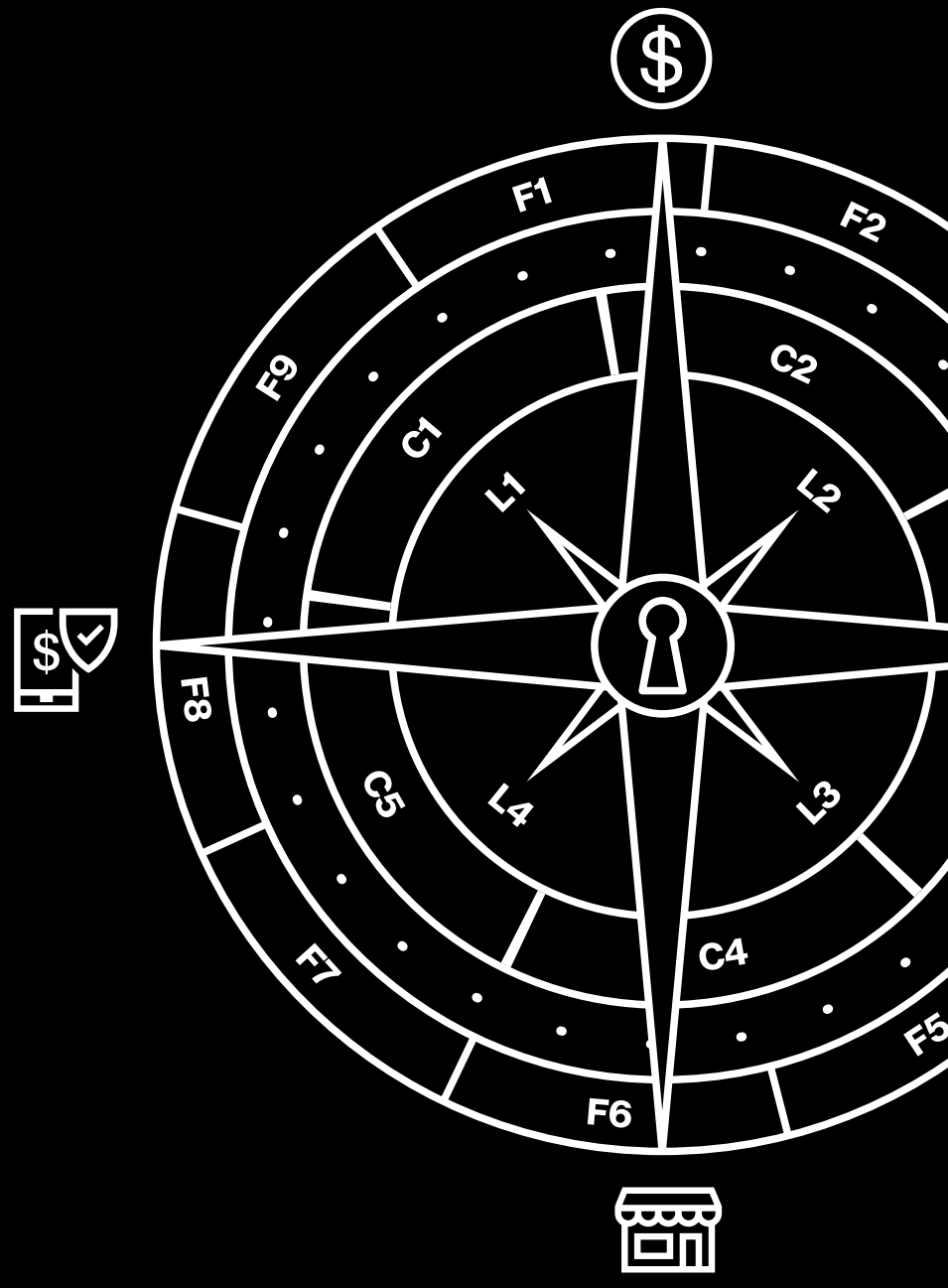
2019 ベライゾンPSR決済システムのセキュリティに関するレポート

金融サービス業界の
コンプライアンスの現状



verizon business ready

金融サービス業界を取り巻く環境は急速に変化しています。顧客は、組織とのやり取りやパーソナライズされた取引が新たな方法で実現されることを望んでおり、特にモバイルデバイスでこれらのことができる環境を求めています。一方、この業界では、金融商品の販売を手掛ける他業種の組織の参入も続いています。

このような競争の激しい、そして規制の厳しい環境においては、クレジットカードのデータを保護できる能力は、重要な差別化要素になります。金融サービスプロバイダーには、ほかのどの業種の企業よりも決済のセキュリティの必要性を十分に認識して欲しいと顧客は強く望んでいます。

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。

PCI DSSを完全に遵守している組織の割合は減少傾向にある

実効性の高いセキュリティ管理を継続的に行って、クレジットカードのデータを保護し、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、2019年版のPSRのデータを見ると、クレジットカードのセキュリティを維持するうえで金融サービスプロバイダーが支援を必要としていることがわかります。

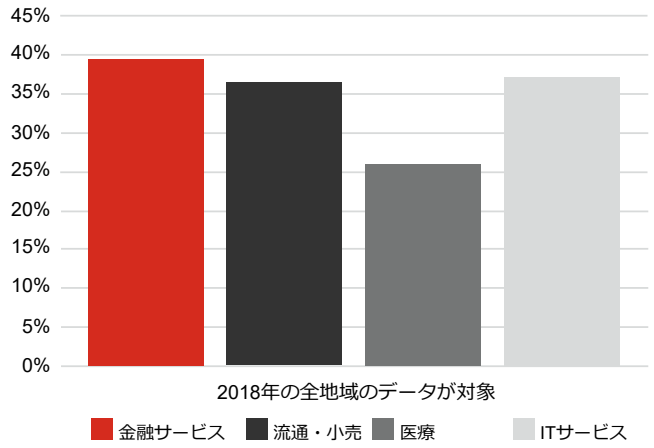


図1：コンプライアンスを完全に満たしている組織の業種別の割合

金融サービス業界は、レポートの調査対象となった全業界（流通・小売、医療、ITサービス、金融サービス）のなかで、PCI DSSを完全に遵守している組織の割合が最も高く、その数字は39.0%に上ります。しかし、業界全体では、そのような組織の割合は2年連続で低下しており、金融サービス業界の場合は、2017年版のPSRでは59.1%が2018年版のPSRでは47.9%に低下し、今年のPSRでは、39.0%にまで落ち込んでいるのです。

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。

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

金融サービス業界の数字が落ち込んでいるのはおかしなことではありません。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、調査対象の全業界で見たときに、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。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。

2019年版のPSRのデータでは、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、数字が改善しています。

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、残念なことに、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。

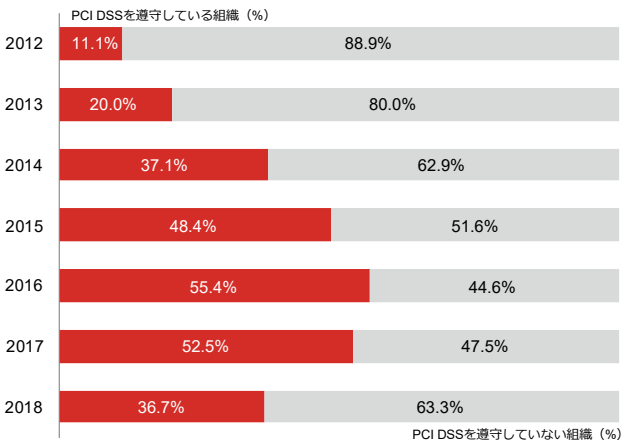


図2：コンプライアンスを完全に満たしている組織の年別の割合

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。

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。これは、成熟したPCI DSSコンプライアンスプログラムを今よりも優れたかたちで策定、維持できることを意味します。そしてそれが可能になれば、今度は決済のセキュリティが向上するのです。

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。

金融サービス業界では、クレジットカードのセキュリティを維持する場合、既存のDPCPに頼ることはできない

評価できるポイント

2019年版のPSRによれば、金融サービス業界は、PCI DSSの以下の要件に関するパフォーマンスがほかの業界よりも優れています。

- ファイアウォールの構成の維持（要件1）
- ベンダーの提供するデフォルトの設定の変更（要件2）
- 物理的なアクセスの制御（要件9）
- セキュリティの管理（要件12）

金融サービス業界では、ファイアウォールの構成を維持できている組織の割合は2018年より2.2%増加しており、これは、業界全体でコンプライアンスの遵守が低下傾向にある状況において明るい材料となっています。さらにこの業界ではこの要件をほぼ完全に満足しつつあり、管理のギャップも7.3%と業界全体で最も優秀な数字になっています。

また、金融サービス業界は保管しているカード所有者のデータを保護する要件（要件3）に関して、コンプライアンスの遵守が2018年よりも向上している唯一の業界となっており、その管理ギャップも14.1%から5.9%へと全業界で最大の改善を示しています。

問題となるポイント

一部の金融サービスプロバイダーでは、金融関連データの移動が業務の大部分を占めますが、データ移動時のデータ暗号化の要件（要件4）の遵守に改善の余地があるように見受けられます。この要件の遵守に関して全業界で最もパフォーマンスが悪化しているのが、金融サービス業界であり、前回より17.1%低下しています。

また、金融サービス業界は、悪意のあるソフトウェアからの攻撃の防御（要件5）の対応に苦しんでおり、この要件を満たす組織の割合が全業界で最低（82.9%）であり、管理ギャップもどの業界よりも大きく（8.5%）なっています。

さらに、金融サービス業界は、PCI DSSにおけるインシデントに備える準備の要件を遵守する組織が2番目に少ない業界となっています。特に金融サービス業界の組織は、アクセスを常時追跡、監視（要件10）することができておらず、適切な監査証跡を使ってセキュリティ侵害のイベントを再現する能力に困難を抱えています。

興味深い事実

2019年版のPSRでは、Verizon Threat Research Advisory Center（VTRAC）| Investigative Response Teamが行った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。長期的なトレンドを見ると、確認されたデータ侵害の11.5%が金融サービス業界で起きていることがわかります。一方、ITサービス業界で発生している侵害の割合は全体の2.7%になりますが、これは確かに目標とするのにふさわしい数字であると言えます。それどころか、十分に価値のある目標となり得ます。

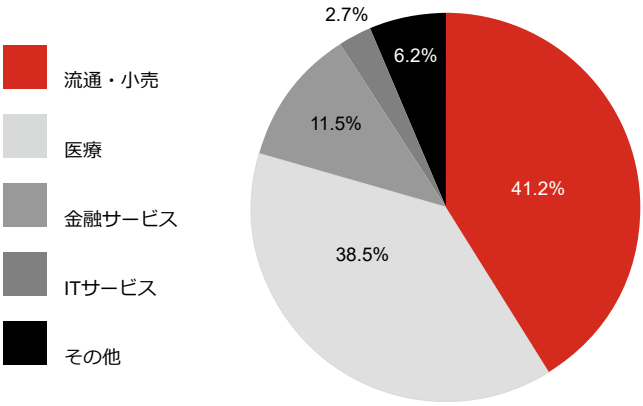


図3：業種別で見たデータ侵害の発生の割合。過去6年間のトレンド。
出典：ベライゾンPFIグローバルケースロード 2010–2016

アドバイス

インシデントに備える準備を強化

インシデントは必ず発生します。その対応次第で状況は大きく変わります。強力なインシデント対応（IR）プランを策定するために時間を割くことは、十分に価値があります。一方で、適切な監査証跡を提供できるようにすることも不可欠です。サイバーセキュリティやコンプライアンスのエキスパートからサポートが得られるのは、発生した事象をこれらのエキスパートが把握できた場合に限られるからです。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。

モバイルのセキュリティに気を配る

モバイルバンキングをはじめとして、モバイルの利用とモバイルデータがグローバルレベルで増加している状況にあっては、個人所有のものも含めた職場で使用するデバイスのセキュリティの課題をいち早く解決することが、大いに価値のある取り組みであると言えます。ベライゾンの2019年版のモバイルセキュリティインデックス（MSI）によれば、金融サービス業界では、モバイルデバイスを導入している企業での問題が増加しており、侵害を受けたと報告している企業の割合が増えています。2018年の報告では25%であった割合が、2019年には、42%に増加しています[1]。2019年版のPSRとMSIでは、最新の脅威に関する情報を提供するとともに、モビリティを実現しながらデータを保護する方法をご説明しています。

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をご提供しています。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、PCI DSSの要件を確実に満たすことができるようになります。

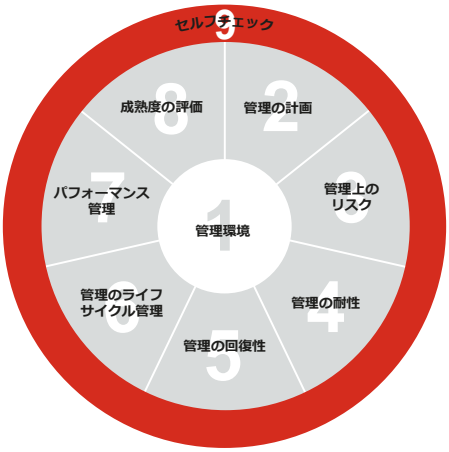


図4：管理の有効性と持続性に関する9つの要素の関係モデル

今こそ主導権を握る

金融サービス業界は、金融規制の遵守と技術イノベーションの導入において優位性を確保しようと努めています。たとえば、人工知能をベースにした不正検知の仕組みなどはまさに、多くの金融サービス企業が取り組み始めている分野です。今こそ、この種のイノベーションを強力かつ持続性のあるPCI DSSコンプライアンスプログラムと連携させるべきときです。決済のセキュリティとPCI DSSのコンプライアンスを向上させることができれば、競合他社との完全な差別化を実現でき顧客からの信頼を高められるようになります。

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 「サイバー犯罪者はセキュリティに問題のあるモバイルデバイスを悪用しています。対応はできていますか」 - Verizon モバイルセキュリティインデックス2019 - 金融サービス業界に関する報告より抜粋（https://enterprise.verizon.com