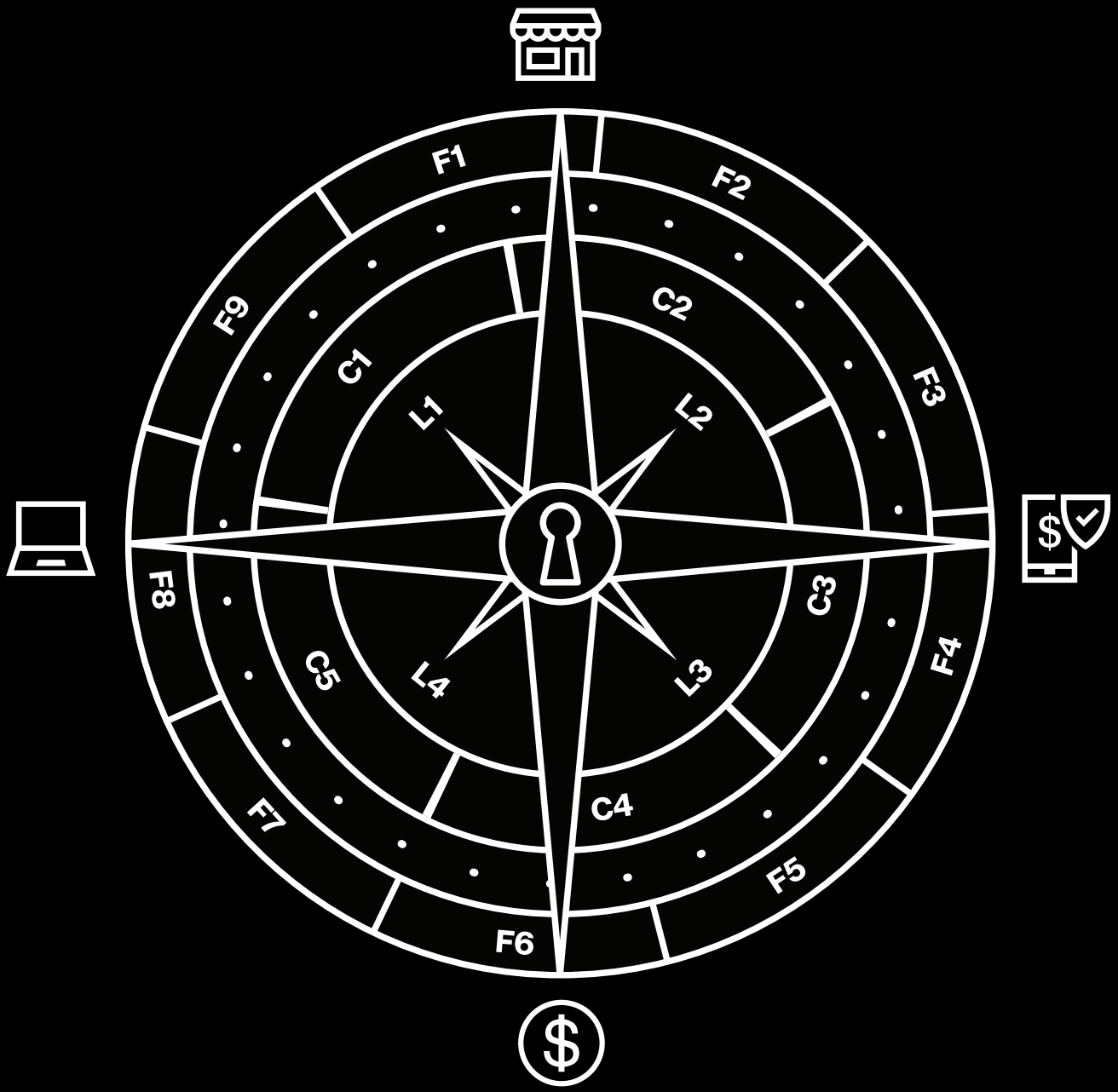
エグゼクティブインサイト

2019 決済システムのセキュリティに関するレポート



verizon

過去のレポート

ベライゾンは、Payment Security Report（PSR）を2010年から発行してきました。PSRは、PCI DSS（Payment Card Industry Data Security Standard）の価値と成果に関する初めての調査でした。過去9年を駆け足で振り返ってみると、PSRが常に独自の視点からPCI DSSのもたらす長期的な影響に視点を当てていたことがわかります。PSRは10年間にわたりグローバルレベルでPCI DSSの実態を評価してきました。

これまでにない調査・研究の成果としてPSRは、クレジットカード業界の専門家が自身の業界の状況を理解するのに役立つ革新的なインサイトを明らかにしています。決済データの保護やコンプライアンス要件の遵守に関する課題の解決を担うPCI SSC（PCI Security Standards Council）などをはじめとする業界の主要なメンバーより、依然としてPSRに大きな期待をお寄せいただいています。

2010年：複雑性と不確実性

PCIのセキュリティの複雑さ、PCIのコンプライアンスにおいて増え続けている問題点、プロセス主導型のコンプライアンスアプローチの必要性について考察する

2011年：状況の変化への対応

コンプライアンス要件の変化について考察するとともに、適切な意思決定の重要性や、成功を実現するためのポジショニングの方法についても詳しく調査

2014年：複雑さの排除

コンプライアンスの価値、PCC DSSの変更点がもたらす影響、持続性の必要性、スコープの絞り込みの方法、コンプライアンスプログラムの管理の質を向上させる方法について考察する

2015年：持続性の確保

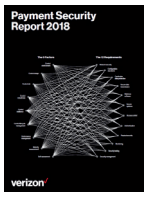
コンプライアンスの持続性の向上に焦点を当てるとともに、スコープの絞り込みと決済処理のセキュリティの現状について考察する

2016年：スキルの蓄積

データ保護のスキルや経験の蓄積と、構造型のアプローチによるコンプライアンスの管理をテーマとして取り上げる

2017年：内部管理環境の構築

内部管理環境の構築と維持の重要性、包括的なアプローチをテーマとして取り上げる。セキュリティ管理のライフサイクル管理についても扱う



2018年：持続性のある効果的な管理

持続性のある効果的な管理を実現するための実践的なモデルの5つを紹介。管理の有効性と持続性に関係する9つの要素や、組織のスキルの蓄積で制約となる5つの要素（5C）について説明する

20年間データ保護の分野をナビゲートしてきた基準

今から20年前の1999年に大手のカードブランド各社は、カード保有者のデータの保護を目的としたプログラムを個々に打ち出しました。そして2004年になるとこれらのプログラムは統合され、単一のデータセキュリティ基準になりました。PCI DSSは今年で誕生から15年目を迎えます。そのv1.0がリリースされたのは2004年のことです。実行性のある方法で持続的に環境を管理することが、現在でも多くの組織にとって今現在も重要になっています。しかし、これを実現するのも依然容易ではありません。

チェックボックスをオンオフにするような機械的な作業や、データセキュリティのソリューションに投資をするだけでは、コンプライアンスの問題を解決することはできません。このような対処の仕方をしていると、多くの場合誤った安心感を抱くことになります。あまりにも多くの組織が「同じことを何度も繰り返す」受け身のパターンに陥っており、ベースラインのコンプライアンス要件を満たすことだけに囚われています。

最新の脅威に常に対応できるようにするためには、データ保護のコンプライアンスプログラム（DPCP）を絶えず進化させて成熟したものにする必要があります。コンプライアンス活動を推進するうえで、組織には状況を深く理解する能力や、事態を掌握する能力、未来を予測する能力を鍛えることが求められるのです。受け身ではなく攻めの姿勢で事に当たらねばなりません。

DPCPの有効性や成熟度をどのようにして高め、評価するのか、そのガイダンスを業界は最も必要としているようです。このPSRのエディションでは、この点についてご説明します。

ベライゾンは25年間にわたり、コンプライアンスプログラムやセキュリティプログラムの成熟度や有効性を評価、分析し、それらの点で優れたプログラムを考案してきました。このような活動を通じて蓄積してきた経験により、2019年のPSRは、不確実性に満ち絶えず変化する状況のなかを前進するための、さらには競争優位性を確保するための理想的な指針となるガイドとして位置付けることができました。そして今年は、過去数年にわたり提供してきた情報やアドバイスをもとに、Verizon 9-5-4 Compliance Program Performance Evaluation Frameworkを構築しました。DPCPの質を向上させるためのナビゲーションツールとして、実用性の高いこの統合ソリューションをご提供いたします。

過去15年間におけるコンプライアンスのトレンドから明らかになった事実

PCI DSSコンプライアンスを達成し、必要とされる多数のセキュリティ管理項目を毎年のコンプライアンスサイクルを通じて維持できている組織の割合を、2008年よりVerizonは追跡してきました。2016年、2017年、2018年のVerizon PSRに記載したように、その割合は2012年には11.1%に過ぎなかったものの、2016年には55.4%にまで上昇しています。

2004年にPCI SSCがPCI DSSを公開しました。組織はほぼ5年以内に実効性のあるコンプライアンスを達成し、それを維持していくであろうとこのときには予想されていました。しかし約15年が経過した今、組織の半数以上が正規のコンプライアンス評価の実施からわずか数か月で、PCI DSSのセキュリティ管理を維持できなくなっているのです。図1から明らかなように、コンプライアンスを維持できている組織の割合は減少傾向にあります。

読者の声

「Verizon PSRは、必要なときに必要なテーマをピンポイントで取り上げています。そのおかげで、最も重要な事柄に優先して取り組むことができるようになっているのは間違いありません。」

—医療機関の最高情報セキュリティ責任者（CISO）

「Verizon Payment Security Reportは、マネージャーやあらゆる関係者を含む弊社プロジェクトチーム全員が対象の、会長からの課題図書になっています。」

—金融サービス機関のコンプライアンスマネージャー

「何を評価すべきか、パフォーマンスを高めねばならない点はどこなのか、レポートを通じてはっきりと理解することができます。このレポートによって意思決定者は明確かつ戦略的な指針が得られます。レポートに示されているアドバイスに従えば、効率が向上し、コンプライアンス活動全体の実効性が高まります。リソースをどこに割り当てればよいのかがわかる、実践的なガイドの役割を果たすレポートです。つまりは、ワークロードを減らし、注力すべきポイントを絞ることができるというわけです。コストも削減できます。言い換えれば、コンプライアンスプログラムのROIを高めることができるのです。」

—大手保険会社のCISO

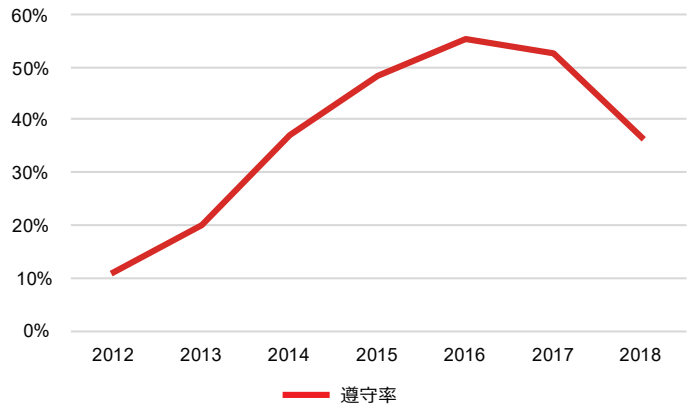


図1：2012年から2018年におけるPCI DSSの遵守率の推移
（Verizon Payment Security Reportの調査結果による）

どこに問題があるのか

データの保護やコンプライアンスの分野では、日々変化が生じています。そのような状況にあって、管理性を保ち、コンプライアンスが適切なかたちで維持されるようにするために、セキュリティスペシャリストには、常に注意を怠らないことが求められます。しかしそれを意図しているにもかかわらず、半数を超える組織が、そのような持続性のあるコンプライアンスプログラムを策定、実行、維持するのに頭を悩ませているのです。

何が問題かといえば、A、B、Cの事柄を正しい順番で行うような、特定のスクリプトに従ってさえいれば、効果的かつ持続的にデータを保護できると多くのセキュリティ専門家が信じていることなのです。

さまざまな組織がDPCPの作成に多くの時間とコストを費やしているようですが、それらの多くは実効性に乏しく、理論上のみ有効に見えるプログラムの域を脱しておらず、プロフェッショナルの行うセキュリティ評価の厳しさに耐えられるものではありません。計画、実装、レビューのプロセスや、効果的かつ持続的なプログラムを実現するための改正の要素が欠けているのです。

プログラムの成熟度

約4分の1（18%）の組織が、コンプライアンスプログラムを明確に定義していません。DPCPの成熟度が高まっていると評価している組織の割合は20%に過ぎません。一方、プログラムの成熟度が最適化されていると評価している組織は全く存在しませんでした。

メトリックの使用

PCI DSSが要求している以上に頻繁に、PCI DSSの管理を環境全体にわたって評価している組織の割合はわずか18%に過ぎません。また、管理の有効性や運用パフォーマンスに関する指標を利用している組織は約3分の1（32%）しか存在しませんでした。さらに、プログラムのパフォーマンスを評価するうえで、プログラムが受ける影響に関する指標を利用している組織はわずか7%にとどまりました。

ー 2018年にベライゾンが行った調査の結果に基づくグローバルレベルで約55の組織を対象に調査を実施

さらには、戦略が不十分であったり過度に複雑であったりする組織も見られます。DPCPの計画、実装、監視、および評価のスキルが不足していることが原因です。

データの保護には、チェスのようなアプローチを取るべきです。リスクを評価し、事前にいくつかの対策を準備しておくといったように、適切な戦略を用意します。個々の行動を評価するとともに、戦略的な行動を心掛けましょう。チェスボード上の駒を眺めるように、あらゆる要素に気を配るのです。

コンピテンシーや成熟度の観点でデータ保護の質を高めずに、ベースラインの管理活動の維持ばかりにCISOは目を奪われているようなケースがあまりにも目立ちます。結果の評価や予測ができるよう、明確でわかりやすいナビゲーションガイドがCISOには必要です。

2018年のPSRでは、管理の有効性と持続性に影響を与える重要な要素についての概要をご説明しましたが、これには大変な反響がありました。そして、管理の有効性と持続性に関係する9つの要素のフレームワークを取り入れてDPCPを強化しDPCPの質を高める方法について、実践的なアドバイスを求める問い合わせが相次ぎました。Verizon 9-5-4 Compliance Program Performance Evaluation Frameworkを導入した理由はまさにこの点にあります。

The Verizon 9-5-4 Compliance Program Performance Evaluation Framework

コンプライアンスを達成するうえで課題となる事柄は、単独で存在しているわけではありません。2018年のPSRでは、PCI DSSの管理における各種の依存関係と、管理環境によって生じる影響について説明し、管理の有効性と持続性に関係する9つの要素をご紹介しました。DPCPにおいて、これら9つの要素のいずれかが不完全であったり、欠落している場合、持続可能なレベルのプロセスの成熟度をプログラムで達成することはおそらく困難になるでしょう。パフォーマンスを制限し、管理上の目的の達成を阻害する典型的な制約事項を、我々は4つのアシュアランスラインにわたりピンポイントで特定しました。

Performance Evaluation Frameworkでは、管理の有効性と持続性に関係する9つの要素を、組織のスキルの蓄積で制約となる5つの要素および4つのアシュアランスラインと組み合わせました。

この統合フレームワークは、組織がDPCPの透明度を高めたうえで必要とするガイドの役割を果たし、新たなレベルの可視性と管理性を実現します。これにより、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ます。

9-5-4 Frameworkでは、DPCP全体で能力を開発し、プロセスの成熟度を高められるようにするための各種の要素に対応しています。Verizon 9-5-4 Compliance Program Performance Evaluation Frameworkで継続的にセキュリティフレームワークの成熟度を高めていけば、段階的かつ積極的に、コンプライアンスのキャパシティを完全な状態に維持できるようになります。このサマリーの後半では、グローバルレベルのコンプライアンス状況をまとめた本年の統計分析を概括た後このフレームワークを詳しく確認します。

グローバルレベルで見たPCI DSSの遵守状況

今年のPSRの調査結果には、いくつもの点で非常に興味深い内容を確認できます。これまでで初めて、認定セキュリティ評価機関（QSA）の企業を情報源に加え、この企業がまとめた評価データを取り込んでいます。これは、過去のPSRの視点を拡大したものです。

2019年のPSRでは、世界302のエンゲージメントからデータを集めています。PCI DSSの遵守状況を包括的に把握しようとして、QSAの企業が継続的にグローバルレベルで連携し情報を共有しているため、弊社では、エンゲージメントの数は今後増加するものと予想しています。クレジットカード業界全体が新しい基準であるPCI DSS v4.0を採用する2021年には、このデータは新たなレベルで重要な意味を持つことになります。

2018年のPSRで報告したように、PCI DSSを完全に遵守できている組織の数は減少していますが、同様の好ましくない傾向が本年もグローバルレベルで確認されました。同じ結果は、別のQSAの企業の評価にも表れています。

組織には、PCI DSSを100%遵守するだけでなく、その状態を維持することも求められます。これはつまり、あらゆる適切なセキュリティ上の管理を継続的に行い、意図したとおりに機能させることを意味します。ベライゾンでは、組織を対象とする複数の暫定的な評価を通じて、2018年にPCI DSSの個々の主要な要件を完全に満たしている組織の割合を把握しました。

この暫定評価、すなわち初期コンプライアンスレポート（iRoC）をお読みになれば、PCI DSSの管理の有効性を評価する有用な機会が得られます。この評価によれば、PCI DSSを完全に遵守している組織の割合はある期間までは増加していることがわかっています。しかし2017年にその割合は反転し、2.9%減少しました。

2017年と2018年のVerizon PSRによれば、2018年にはグローバルレベルで見た遵守率は、これまでと比較してさらに15.8%減少して36.7%となっており、2016年から2018年の過去3年間にわたり減少傾向が続いています。

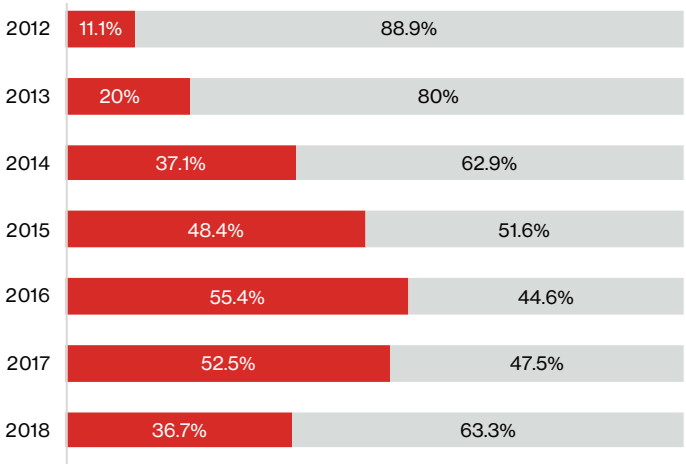


図2：PCI DSSを完全に満たしている組織の割合の推移

これは遵守率の大幅な低下を意味します。その原因としてはさまざまな要因が考えられます。たとえば、マネージャーやスタッフのメンバーが変更になった場合、DPCPの業務に混乱をきたす可能性があります。あるいは、業務環境に変化が生じると、DPCPの業務の指針が失われ、業務の方向性が定まらないまま放置されてしまう可能性もあります。

100%の準拠

暫定評価において、PCI DSSを100%遵守していることが確認できた組織の割合。これらの組織はすべて前回の評価検査に合格していることから、コンプライアンスを継続的に維持できていることになります。

管理のギャップ

PCI DSSの管理に失敗している組織の数を、管理を期待されている組織の総数で割った値。これは、評価対象の組織がどの程度PCI DSSを遵守できていないかを表す平均値になります。

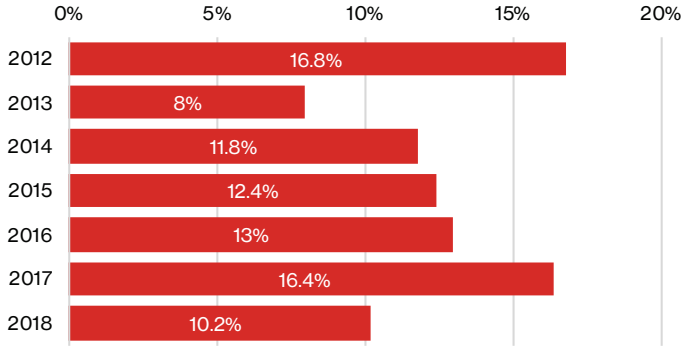


図3：管理のギャップ

コンプライアンスの実態

直近のVerizon PCI Security Practiceのデータによれば、遵守率全体が低下する一方で、完全にコンプライアンスを維持できている状態からの乖離の程度を表す管理ギャップの数字は一定水準を保っており、組織全体のデータセットで見ると前年には7.2%になっていました。

過去3年間と同様に、基準の要件5と7は最も一様に維持され続けています。

一方、脆弱性の管理、ソフトウェアの開発、プロセスの変更の領域で有効性を維持することに組織は苦戦しているため、要件6の項目では遵守率が最も大きく落ち込んでいます。また、セキュリティテストの要件を通年で満足できず、このため、コンプライアンス全体から見ても、あるいは管理のギャップの面でも、要件11の遵守率は最低を記録しています。

アジア太平洋地域（APAC）の組織は他の地域よりもコンプライアンスを完全に維持する能力に長けており、69.6%の組織がセキュリティの基準を満たしています。一方、アメリカ地域の場合、コンプライアンスを完全に維持している組織の割合は、全体の4分の1未満（20.4%）にとどまりました。

これはAPECの平均と比べ、49.1%も低い数字になります。アメリカ地域の組織の場合、セキュリティやコンプライアンスのプログラムを軌道に乗せるのに75%以上の確率でサポートが必要になります。

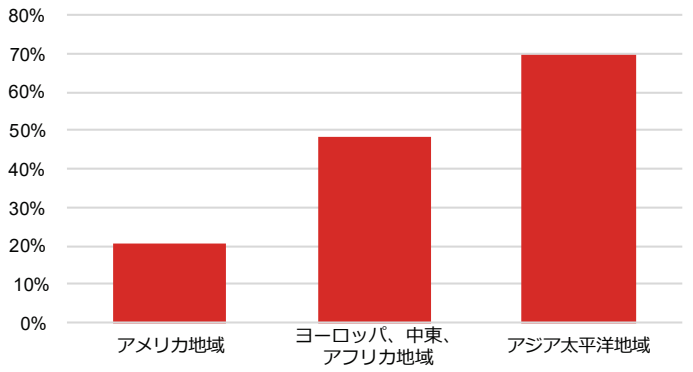


図4：PCI DSSを完全に満たしている組織の地域別の割合

金融業界の場合、コンプライアンスを完全に維持している組織の割合が他の業界と比較して大幅に上昇していますが、グローバルレベルの平均を2.4%上回っているに過ぎません。ほかの業種と同様に、コンプライアンスを完全に維持する能力には大きな落ち込みが見られます。一方、医療の分野は、Verizon PSRが提供しているアドバイスを大いに活用しており、持続性の高いセキュリティプログラムの構築に成功しています。

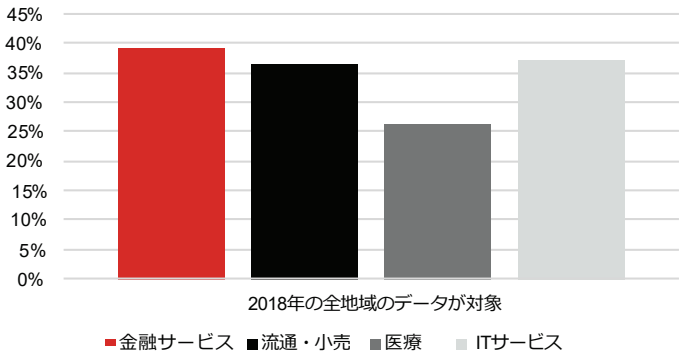


図5：PCI DSSを完全に満たしている組織の業種別の割合

管理のギャップに関する興味深い事実

多くの組織がコンプライアンスを維持できていないことがPSRの調査・研究により判明した今、機密性の高いクレジットカード情報をどのように適切に保護しているかという点が重要になってきます。PCI DSSを完全に満たしている組織の場合、管理のギャップはゼロになります。他の組織では管理のギャップは10.2%まで縮小しており、これは2018年のPSRに記載されている値と比較して6.2%の改善を意味し、ほとんどの組織において遵守率が90%をわずかに下回る数字になっていることを表します。

仮に90%を「A」ランクと位置付けた場合、平均的な管理のギャップは「B」ランクということになります。要件11は一貫して遵守率が最低であり、下位20位のリストのなかに7つの管理項目がランクインしています。

これらの管理項目は、データを保護するためのコンプライアンスプログラムを設定するうえで基本的な役割を果たします。これらの管理項目を組み込んでいない組織の場合、95%以上の確率で持続的なDPCPを実現できていない可能性があると、Verizon Threat Research Advisory Center （VTRAC）データに示されます。

管理ギャップは小さいほど望ましく、完全なコンプライアンスに対して最も大きなギャップがあるコントロールは、可能な限り低いコンプライアンスから16～33パーセントポイント離れています。これは深刻なセキュリティリスクの可能性を示唆しています。

データ侵害に関する情報の関連付け

今年のレポートでは、データ侵害に関する調査においてより詳細な情報の関連付けを行っています。この関連付けには、VTRACが2016年から2018年にかけて実施したPCIフォレンジック調査（PFI）のデータ侵害指標をベースにしています。

この場合、データ侵害につながった特定の原因やデータ侵害の拡大を助長した要因を、必ずピンポイントで特定できるとは限りません。侵害の原因となった特定の要件を調査対象の28.7%で特定することができませんでした。また、ある要件をどの程度満たしていないがために侵害が発生したのかを、調査対象の27.4%で明らかにできませんでした。これは主に、調査に使用できるエビデンスが不足していることが原因ですが、そのような状況を招いている要因としては、ログ管理の不備やインシデント対応（IR）手順の不備のほか、インシデント発生後にエビデンスを保全する組織の能力に限界があることが挙げられます。

インシデントへの備えに関係した情報のまとめ

12 の要件

2016年から2018年までのデータによれば、12の要件をすべて満たしている組織では、データ侵害を受けた組織は1つもありませんでした。

0%

侵害を受けたときに3、8、10、11、12の要件を満たしていた組織の割合は0%です。

75%

侵害を受けた組織において、PCI DSSの全要件のなかで最も遵守率が高いのが要件9ですが、75%の組織で依然として不備があります。

10.2

ほとんどの企業が要件10.2を満たすのに困難を感じています。これは、適切な監査証跡を取り込んでイベントを再現する能力に関する要件です。インシデントへの備えに関するこのPCI DSSの要件を最も満たしていないのが流通・小売業界の組織で、それに続くのが金融サービス業界です。一方、ITサービス業界はずっと優秀で、10.2の要件を満たしていない組織はわずか1%に過ぎません[1]。

以下に示すPCI DSSの管理項目は、インシデントへの準備に直接関係するものです。これらにより、組織は、サイバーセキュリティインシデントの特定とインシデント対応を効果的に実施することができます。

- **要件12.10, 12.10.1, 12.10.2**
  カード保有者データのセキュリティインシデントに素早く対応できるプランを準備する。インシデントの報告、アラート対応、効果的なプロセスの管理行うための手順を定める。
- **要件11.1.2, 12.5.3**
  無線通信の不正なモニタリング、セキュリティイベントログ、侵入検知、検知ソリューションの変更などの項目を含め、セキュリティの監視とアラート対応に関するインシデント対応（IR）の手順を確立する。
- **要件10.2, 12.10.4**
  セキュリティプランやセキュリティ対応手順を周知する。チームのメンバーにIRプランやIR手順の内容を知らせ、中身についてのトレーニングを施す。サイバーセキュリティのアラートに24時間365日の体制で対応できる能力を維持する。
- **要件12.8.3**
  適切なサードパーティーへの企業精査には、IR能力の評価及び全セキュリティインシデントの報告の義務付けが必須。具体的には、サードパーティーのIRの能力を評価する。また、すべてのセキュリティインシデントを報告するようサードパーティーに義務付ける。

1. 2017年のPCI DSSのデータセットによる。詳細は、2019 Verizon Incident Preparedness and Response Report（インシデントに備える準備とインシデント対応についてのレポート：https://enterprise.verizon.com/resources/reports/2019/vipr/2019-vipr-full-report.pdf）の13ページをご参照ください。

VTRAC調査担当者のフィールドからの報告

「PCI DSSの要件を完全に満たしている組織が侵害を受けたケースは存在しない」と業界のエキスパートが主張するのを、これまで何年にも渡り聞かされてきました。決済処理に磁気ストライプの付いたプラスチックのカードが使われるようになり、それが攻撃の対象になって以来、我々がクレジットカードの処理現場で起きた全侵害の調査データにアクセス出来たことは一度もありません。また、組織へのセキュリティ攻撃を決断した攻撃者と接触したこともありません。確認できたことついては以下の対応を行っています。

2019年のPSRでは、コンプライアンスの状態に関するセクションにおいて、侵害に関係するデータの関連付けを従来よりも詳細に行っています。また、PCIに関するデータ侵害の調査を行った担当者が現場で直接確認した情報も提示しています。

VTRACによって調査されたクレジットカードのセキュリティ侵害を再訪するとき、PCI DSSに完全準拠していながらも侵害を受けた組織を含む環境やPCIデータ侵害を一度も調査したことがないと断言できます。たとえ署名済みの準拠証明書（AOC）があったとしてもです。

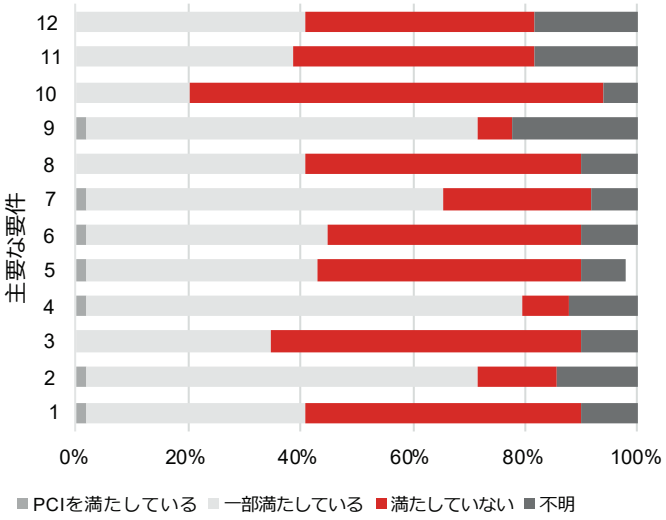


図6：侵害を受けた組織のPCI DSSの管理ステータス

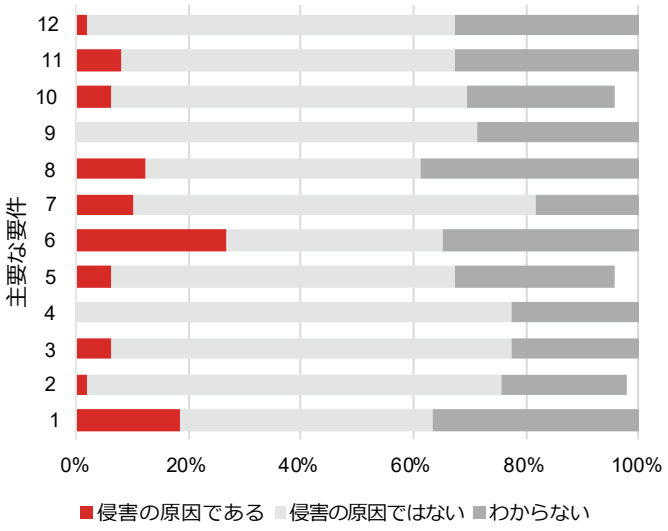


図7：不備がありデータ侵害の要因であるとPFIの調査で認定された要件

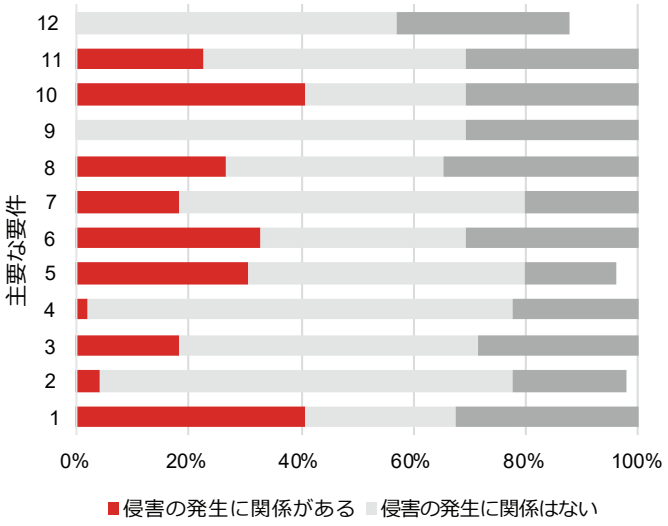


図8：不備がありデータ侵害に関係があるとPFIの調査で認定された要件

プログラムの成熟度を高める

効果的かつ持続的な管理環境の設計に、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。成熟度を高めるためには、キャパシティ（リソース）、能力、コンピテンシー、当事者意識、コミュニケーションが必須です。弊社ではこれらを、組織のスキルの蓄積で制約となる5つの要素、5Cと呼んでいます。難しい質問を自らに投げかけ、以下に示す手順を実行し、Verizon 9-5-4 Compliance Program Performance Evaluation Frameworkを利用すれば、実効性の高い成熟したDPCP環境へと組織を導くことができます。

- **優先順位を付ける**
  適切なスキルを有し経験を積んでいるセキュリティプロフェッショナルであれば、プログラムの目的に優先順位を付ける方法を理解しているはずです。どのような場合でも組織が同時に対応できる以上の問題が発生するので、注力すべき事柄を見極める方法や優先順位付け方を知っておくことが重要になります。
- **パフォーマンスの基準を詳細にドキュメント化する**
  内部データの保護基準やコンプライアンスのパフォーマンス基準に関して生じる誤差のうちで、許容できるものとできないものを定義する場合や、問題を特定する際に不可欠となるプロセスです。
- **リスク管理の手法を適用する**
  管理環境の単一の構成要素が問題の根本原因となっているケースはまれにしかありません。リスク管理の手法を適用して体系的な評価をすれば、繰り返し問題になっていて対応が不可欠な事柄と1回限りのイベントを区別することができます。

Verizon 9-5-4 Compliance Program Performance Evaluation Frameworkを使用すれば、注力すべきポイントを把握することや、必要な変更を行う方法を特定することが、ずっと容易になります。

DPCPの質を向上させるための10の難しい質問

映画監督で脚本家のWerner Herzog氏が賢しげに述べているように、「ときにははっきりとした答えを示すよりも、難しい質問を投げかけることに意味がある」のです。

1. どのようなデータを保有していますか。データはどこに保管されていますか。データの流れはどのようになっていますか。
2. 十分なセキュリティが確保されていますか。データは確実に保護されていますか。どの程度その自信がありますか。
3. 必要とする場所で確実な管理ができている自信がどの程度ありますか。
4. DPCPのパフォーマンスはどの程度予測できるようになっていますか。
5. 重要なデータの保護のプロセスやコンプライアンスのプロセスについて、それらの質や耐久性を確保するためにどのような措置を講じていますか。このようなプロセスが、どのような要素から構成されているか理解していますか。
6. ポリシーや基準や手順に誤差が生じた場合、どの程度迅速に誤差を検知して対応できますか。
7. DPCPの環境や成熟度の戦略の有効性を評価する管理手法は用意されていますか。
8. 適切なタイミングでDPCPの活動を正しく優先付けられているかを、どのようにして判断していますか。
9. 組織のスキルの蓄積で制約となる5つの要素（キャパシティ、能力、コンピテンシー、当事者意識、コミュニケーション）を十分に管理できていますか。
10. 管理の有効性と持続性に関係する9つの要素をどの程度深く理解していますか。長期的にはどのレベルの成熟度を目標に定めて達成しようとしていますか。

統合評価フレームワークを活用して有効性の高い持続的な環境を実現

弊社の調査の結果によれば、持続性のある管理環境を維持している組織の割合はわずか36.7%にとどまりました。あまりにも多くの組織が自社のDPCPの効力を効果的に評価する方法を理解していないことは明らかです。

ここに示すフレームワークでは、5つの制約事項の評価を通じ、9つの各要素に関して4つの基本的なアシュアランスラインごとに持続性と有効性の状態をマッピング、モニター、レポートすることができます。

鍵を握る質問

- 自社のコンプライアンスプログラムは適切に構成されているか。
- コンプライアンスプログラムは機能しているか。
- プログラムは効果的に管理されているか。
- 管理環境の持続性は維持されているか。
- プログラムにおいて何が制約事項になっていて、どのようなスキルが不足しているのか、ピンポイントで特定する方法を把握していますか。

9-5-4 Compliance Program Performance Evaluation Framework

4つのアシュアランスライン全てを対象として、9つの要素と5つの各制約事項の評価を行い、その内容をレポートします

アシュアランスライン：

1. **個々のアカウンタビリティ**
2. リスク管理とコンプライアンスチーム
3. 内部監査
4. 外部監査、法規制

要素	キャパシティ	能力	コンピテンシー	当事者意識	コミュニケーション
1. 管理環境	■	■	■	■	■
2. 管理の計画	■	■	?	■	■
3. 管理上のリスク	■	■	■	■	■
4. 管理の堅牢性	■	■	?	?	■
5. 管理の回復性	■	■	?	?	■
6. 管理のライフサイクル管理	■	■	■	■	■
7. パフォーマンス管理	■	■	■	■	?
8. 成熟度の評価	■	■	■	■	?
9. セルフチェック	?	■	?	?	■

図9：コンプライアンスプログラムのパフォーマンスの評価フレームワーク

図9にはサンプルのデータを記載しています。これらは、組織のスキルの蓄積で制約となる5つの要素を大まかに示すものです。これらの要素が、4つのアシュアランスラインごとに9つの要素の設計、組み込み、運用に影響を及ぼします。180の個々の制御ポイントは、DPCP内に結果として統合することができます。具体的には、まずはじめに1番目のアシュアランスラインを対象に９つの要素全てと5つの各制約事項の評価を行い、データの保護とコンプライアンスに関する有効性と持続性の有無を個人のアカウンタビリティレベルで判断します。

図9の例について以下にその内容を説明します。

- 組織内の個人のレベルでは、要素1の「管理環境」については、キャパシティ、能力、コンピテンシー、当事者意識、コミュニケーションのいずれについても大きな問題はありません（赤色の ■ でこれを表示）。
- 組織内の個人のレベルでは、要素2の「管理の計画」について必要なコンピテンシーの有無が不明確な状態です（?でこれを表示）。この場合、さらに調査が必要です。
- 要素３の「管理のリスク」については、必要なコンピテンシーが欠如しています（黒色の ■ でこれを表示）。この場合、管理のリスクを評価するうえで担当者は、知識やスキルを取得し、経験を積む必要があります。

評価は繰り返し行います。まずはアシュアランスラインごとに新たな表を用意し、組織の個々のスキルの状態（あるいは、スキルの蓄積を制限する個々の要素）を任意のアシュアランスラインの9つの要素に対応させて記入していきます。アシュアランスラインは、必要に応じ「幹部や役員による監督」を明示的に項目に追加するなどして拡張できます。

このフレームワークでは、高度に構造化された、繰り返し利用可能な一貫性のある手法により、以下のことが可能です。

- 内部と外部の管理環境を明確に定義する
- リスクを軽減するために必要な管理の内容を特定、定義する
- 管理のパフォーマンスとデータの保護に関する有効性、持続性に影響する制約事項を特定、定義する
- 管理環境の設計と運用に関するパフォーマンス要件、パフォーマンス基準を規定し、周知する

この統合評価アプローチには、以下の点でメリットがあります。

- **透明性**
  このアプローチでは、プロセス、制約事項、結果を結び付けることによって、コンプライアンス投資の価値を詳しく把握することができます。
- **正確性**
  このフレームワークでは、特定の制約事項を解消するためのコアコンポーネントに詳細かつ正確に焦点を合わせることができます。これにより、個々のニーズにあわせて管理の内容を的確にカスタマイズすることができます。また、管理の有効性をあらかじめ評価することも可能になります。
- **拡張性**
  このアプローチでは段階的に成熟度を高めることが可能です。キャパシティなどのリソースが利用できるようになれば、能力やプロセスの成熟度は高められます。
- **柔軟性**
  Verizon 9-5-4 Compliance Program Performance Evaluation Frameworkは、National Institute of Standards and Technology Cybersecurity Framework（NIST CSF）やControl Objectives for Information and Related Technology（COBIT）、Committee of Sponsoring Organizations of the Treadway Commission（COSO）などの既存の基準を補完します。
- **評価**
  管理の有効性を評価し、その評価データを活用して、管理の内容を環境全体にわたり正確にカスタマイズできます。

2019 決済システムのセキュリティに関するレポートの概要

コンプライアンスプログラムと組織のさまざまな能力が進化するときが訪れています。受け身でなく攻めの姿勢でデータを保護できるようコンプライアンス活動を推進するには、状況を詳しく理解する能力や、事態を掌握する能力、先を予測する能力を鍛えることが求められます。

『2019年版 - Payment Security Report（フルレポート）』では、そのような能力を高めるための指針を提供し、Verizon 9-5-4 Compliance Program Performance Evaluation Frameworkなどの新規ツールを使用して、新たなレベルのコンプライアンス管理を実現する方法をご説明いたします。新しい手法を使えば、個々のデータ保護のコンプライアンスプログラム（DPCP）においてアシュアランスと予測能力を高めることや、環境の効果的な管理が可能になります。その方法をこのレポートでご確認ください。

2018年のPSRをベースとするこのレポートでは、データセキュリティやコンプライアンスの能力を段階的に高めるための統合フレームワークを、ガイダンスに成熟度モデルを使用して示します。具体的には以下のような内容を扱います。

- グローバルレベルで見たコンプライアンスの状況：PCI DSSを遵守できている組織とできていない組織
- コンプライアンスプログラムを作成するうえで考慮すべき重要事項
- データ侵害に関する情報の関連付けとインシデントへの備え
- モバイル決済システムにおけるセキュリティのトレンド
- PCI DSSコンプライアンスのリファレンスカレンダー

表紙のデザインについて

表紙には、方位を示すために使用する、18のポイントから成る羅針盤の絵が描かれています。この表紙では、羅針盤は、2019年のPayment Security Reportから導入された9-5-4 Compliance Program Performance Evaluation Frameworkを表しており、レポートが包括的な可視性と管理性を備えた成熟度の高いデータ保護管理に役立つことを示しています。また、通常は東西南北を意味する4つの方位は、主要な4つの業種（医療、流通・小売、金融サービス、ITサービス）を表しています。通常の羅針盤には主な8つの風の方位が記されていますが、この表紙の羅針盤ではその代わりに、管理の有効性と持続性を表す9つの要素が示されています。羅針盤の中心近くには4つのアシュアランスラインが配置され、組織のスキルの蓄積で制約となる5つの要素がハーフウインドの代わりにそれらのアシュアランスラインを取り囲んでいます。そして羅針盤の中央には、効果的で持続的なデータコンプライアンスプログラム管理の扉を開くための鍵が置かれています。

verizon

Verizon 2019 Payment Security Report（PSR：2019年版 - 決済システムのセキュリティに関するレポート） - エグゼクティブインサイト

発行日：2019年9月17日

編集チーム

筆頭著者：
Ciske van Oosten

共著者および監修者：
Anne Turner、Clarence Hill、Cynthia B. Hanson、Dyana Pearson、John Grim、Neal Maguire

データアナリスト：
Anne Turner, Noel Richards、Saravanan Thangam、Sundeep Paderu、Ron Tosto

セキュリティアシュアランスプラクティス

マネージングディレクター：
Rodolphe Simonetti

PCIおよび決済システムのセキュリティに関するコンサルティングプラクティス

グローバルリード：
Ron Tosto

アメリカ地域：
Franklin Tallah

アジア太平洋地域：
Sebastien Mazas

ヨーロッパ、中東、アフリカ地域：
Gabriel Leperlier

ビジネスインテリジェンス：
Ciske van Oosten

チームのメールアドレス：paymentsecurity@verizon.com

Payment Security Reportは以下のURLからダウンロードいただけます。

https://enterprise.verizon.com/resources/reports/payment-security/

本レポートの作成にご協力をいただいた組織

ControlScan　FOREGENIX

MEGAPLANIT　schellman