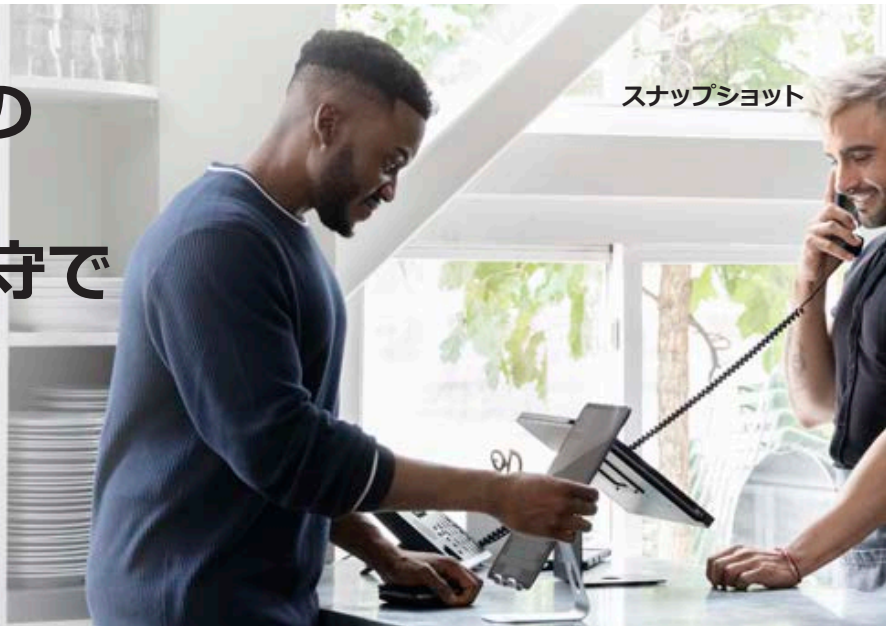
進化する小売業の決済システムをPCI DSS v4.0遵守で保護

アップデートで複雑化した準拠要件への対処方法



認証情報の盗難、ランサムウェア、フィッシングの被害は、小売業にとって依然として課題であり、明確な救済措置は見当たりません。業界のセキュリティ基準に従いデータのセキュリティコントロールを行う企業は、データ漏洩/侵害を防げる可能性が高くなりますが、それでも、攻撃者の悪用に対して常に先回りしておくことは、最高情報セキュリティ責任者（CISO）やセキュリティ管理者が日々頭を抱える終わりのない課題です。小売業のセキュリティプロフェッショナルはまた、ペイメントテクノロジーの進化、クラウドコンピューティング、増加するオムニチャネルの採用、ペイメントカードによる取引の増加、攻撃対象の拡大ーこのような様々な要素からなる複雑な状況に、うまく対処しなければなりません。データ漏洩/侵害は、小売業にとって特に大きなダメージとなりやすく、結果的に顧客の信頼を失い、評判を下げ、利益の減少を引き起こします。

小売業界のセキュリティ動向

ベライゾンの『2022年度データ漏洩/侵害調査報告書（DBIR）』によると[1]、小売業におけるソーシャルエンジニアリング攻撃は、2016年から2021年にかけて、7%から29%に増加しました。認証情報はサーバーへの侵入やランサムウェアのロードに悪用されやすく、小売業の中で漏洩したデータタイプの1位であることがDBIRで明らかにされています。窃盗犯は、様々な新しいフィッシングの手口や、Webフォームから処理されるクレジットカード情報を取り込む「アプリデータ」マルウェアを使っています。中でも「アプリデータを取得する」マルウェアについては、他の業界と比べて7倍という高い比率になっており、2022年度のDBIRでは、小売業における上位3つのパターンのうち、「システム侵入」が1位となっています。

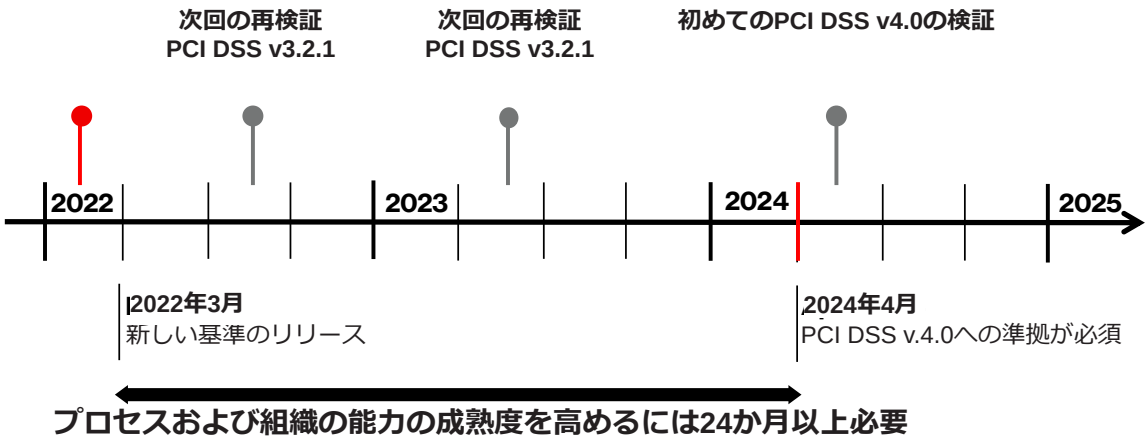
このような決済システムのセキュリティの変化や課題に対応するため、Payment Card Industry Security Standards Council（PCI SSC）は、PCI Data Security Standard（DSS）を大幅にアップデートしました。PCI DSS v3.2.1からPCI DSS v4.0へのシフトは、組織が持続的かつ効果的なコントロールとコンプライアンス環境を構築するための新たな道標を提供しています。これは、2004年の最初のリリース以来、最大のアップデートとなります。

PCI DSSは、すべての組織に適用されます。小売業においても、他の業種と同様に、PCI DSS v4.0の新しい要件に迅速に対応する必要があります。小売業者は、データ漏洩/侵害の被害を防ぐために厳格なセキュリティ対策を講じるべきでしょう。さらに、データのセキュリティとコンプライアンスを管理するための戦略を持つべきです。PCI DSS v4.0を遵守するための明確な指示書を備えた、実用的な「ツールボックス」です。

PCI DSS v4.0には、2006年に導入されたお馴染みのコントロール目標（Control Objectives）と、12の主要要件（Key Requirements）はそのまま残されています。最も大きなアップデートは、継続的なコンプライアンスに重点が置かれた点、コンプライアンスコントロールの設計と検証のために、カスタマイズされたアプローチが新たに追加されたことの2点です。検証手法と検証手続きの強化については、これまでの事前定義済みのアプローチと、目的に応じてカスタマイズされたアプローチの2択へと変更されました。

verizon business

PCI DSS v4.0



ペイメントカードのデータは収益化が非常に容易なデータの1つであるため、社内外の攻撃者から最も狙われやすいデータの1つです。

事前定義済みのアプローチとは、PCI DSSに記載されているお馴染みの（従来の）要件とテスト手順に従うことを意味します。カスタマイズされたアプローチを採用すれば、組織は、それぞれにカスタムしたプロセスを通じてセキュリティコントロールを個別に設計したり、事前定義済みのコントロールとは異なるコントロールを導入することができます。つまり、実装要求ベースのアプローチではなく、成果ベースのアプローチです。カスタマイズされたコントロールはすべて、要件に定められたセキュリティ上の目的も満たす必要があります。

PCI DSS v4.0への準拠は、2024年3月までは必須ではありません。PCI DSS v3.2.1は、PCI DSS v4.0のすべての資料がリリースされた後、18か月間は有効です。この移行期間が終了するとPCI DSS v3.2.1は廃止され、PCI DSS v4.0が準拠すべき唯一のバージョンとなります。PCI DSS v3.2.1とPCI DSS v4.0の両方が有効な18カ月の期間に加えて、PCI DSS v4.0には「未来日付」とされる新しい要件を段階的に満たしていくための延長期間が設けられています。コンプライアンス環境のアップグレードに取り組んでいる組織は、コントロールを再構成するための時間が十分にあると考えるかもしれません。しかし、カスタマイズされたアプローチのような大幅な変更に取り組むことを考えれば、今すぐ準備を始めても早すぎるということはありません[2]。

PCI DSS v4.0 に移行する小売業のためのツールボックス

コンプライアンスプログラムの管理を設計するためのアプローチは数多くあります。アプローチの採用にあたり、「どれが最も効果的かつ効率的か?」という問いを立てることが重要です。ベライゾンは、そのための方法を『2021決済システムのセキュリティに関するレポートにおけるインサイト：PCI DSS v4.0』ホワイトペーパーで説明しています[3]。

ベライゾンは、決済システムの持続的なセキュリティフレームワークの導入において、優れた支援実績を持っています。先日公開した『2022決済システムのセキュリティに関するレポート（PCR）』(英語）では、PCI DSS v4.0への準拠を成功させるための準備についてまとめています。このレポートでは、潜在的な課題を解決するために必要なツールを見つける方法、そして、目標を設定し、達成するために最善なルートを選択する方法を紹介しています。また、新しい要件に適応しながら複雑な決済システムのセキュリティを簡素化する手段として、管理手法、モデル、フレームワークなどのツールについても解説しています。

ベライゾンのサービス

ベライゾンは、PCI DSS v4.0への移行をナビゲートするために設計された複数のサービスを提供しています。一連のサービスは、準拠を達成するために体系化されたロードマップを提供しています。これは、移行に伴う不確実性を減らし、特に、セキュリティおよびコンプライアンス管理プロセスが十分に成熟していない組織にとって有益です。各サービスでは、組織が新しい要件に対して先回りした対応ができるようになるための支援をしています。

PCI DSS v4.0要件の重要な変更点

新しい要件の数：74

サービスプロバイダーに対する新しい要件：12

加盟店に対する新しい要件：62

要件の変更：1、3、5、8、9、12

重要な変更点：

- **ディスクレベルまたはパーティションレベルの暗号化では不十分**
- **フィッシング対策ソリューションが必要**
- **Webアプリケーションファイアウォール（WAF）の導入が必要**
- **多要素認証（MFA）が必要**
- **保存されたハッシュ値に暗号鍵が必要**
- **カード会員データ（CHD）を保護する証明書には、有効な認証局（CA）による署名が必要**
- **決済ページスクリプトの整合性コントロールの実施が必要**
- **アプリケーションにハードコードされたパスワードを使用しない**
- **認証された脆弱性スキャンが必要**
- **アプリケーション/システムアカウントのパスワードには有効期限の設定が必要**

サービス1：PCI DSS v4.0 の理解

このサービスは、お客様がPCI DSSを理解するための体系的なアプローチを開発する目的で設計されています。次のようなチームで構成される組織に対して、PCI DSSの基準を伝え、正しい理解を促すために役立つフレームワークが含まれています。

- 現場の従業員
- リスクおよびコンプライアンスチーム
- 内部監査チームおよび上級管理職
- •社外関係者およびベンダー

次のプレゼンテーションとガイダンスが含まれています。

Why：PCI DSS v4.0の目標、目的、成果、期待

How：ガイダンス（ワークブックのハードコピーまたはeラーニングの開発サポート）

Who：社内外のステークホルダーグループそれぞれに合わせたメッセージング

When：各コミュニケーションを開始する順序とステップ、およ、その期間に関する推奨事項

サービス2：PCI DSS v4.0 リソース要件のアセスメント

PCI DSSの新基準によってお客様に課される範囲、要件、制約に関する統合分析を提供します。分析では、PCI DSS要件が組織に及ぼす影響の特定と分類、新規に追加された、あるいは、更新された各要件に対する改善策に焦点を当てます。（1）形式化/文書化、（2）プロセスの変更、（3）構成の変更、（4）アーキテクチャの変更、（5）文化の変更、（6）ビジネスモデルの変更が含まれます。本サービスは、セキュリティおよびコンプライアンスチームとの一連のインタビューを含め約2週間で提供されます。分析により、PCI DSS v4.0の目標に準拠するために必要な作業時間を算出することが可能になります。

サービス3：PCI DSS v4.0 ギャップアセスメント

現在運用されている決済システムのセキュリティ対策と、PCI DSS v4.0の要件とのギャップを特定します。本審査時に提出が求められる証拠の種類と品質に焦点を当て、改善が必要なPCI DSSの要件とコントロールを詳述したレポートを提供します。なお、ベライゾンは、PCI DSS v3.2.1とPCI DSS v4.0とのギャップのみを特定するギャップアセスメントも提供しています。

サービス4：PCI DSS v4.0 プレアセスメント

証拠のサンプルと、準備の進捗度をレビューします。セキュリティおよびコンプライアンスチームが、本審査を受ける準備をどの程度整えられているかを把握することを目的としています。証拠の妥当性を確認するための直前のチェックを含め、必要な調整や修正をピンポイントでお知らせします。

サービス5：PCI DSS v4.0 準拠検証アセスメント（本審査）

PCI DSS v4.0の全適用要件に対する年次検証の本審査です。準拠報告書（ROC）と準拠証明書（AOC）が作成されます。

ベライゾンが選ばれる理由

ベライゾンは、業界をけん引するソートリーダーとして、PCI（Payment Card Industry）のセキュリティにおけるコンプライアンスについてのレポートを執筆しています。2010年より定期発行している『決済システムのセキュリティに関するレポート（PSR）』は、高い評価をいただいております。同レポートは、決済システムのセキュリティに関する課題を改善するために、PCI DSS遵守の現状について調査し、独自のインサイトを提供している業界唯一のレポートです。

Qualified Security Assessor（QSA）のなかでも世界有数の規模を誇るベライゾンは、これまで、多数のフォーチュン500企業やグローバル企業を含むあらゆる規模の企業のために、20,000件以上のセキュリティアセスメントを行ってきました。また、グローバルに展開しているネットワークオペレーションセンターとセキュリティオペレーションセンターで、毎日100万件以上のセキュリティイベントを分析することで、急速に変化するサイバー脅威に日々対応しています。さらに、過去10年以上にわたり、『データ漏洩/侵害調査報告書（DBIR）』などのレポートを通じて、私たちの知識を社会へ提供し続けています。

詳細情報：

ベライゾンのPCI DSSアセスメントの詳細については、Verizon Businessのアカウント担当者にお問い合わせいただくか、以下のページ（英語）をご覧ください。
verizon.com/business/products/security/cber-risk-management/goverance-risk-compliance/payment-card-Industry-data-security-standard-assessment/

最新の『2022決済システムのセキュリティに関するレポート』(英語）をご覧ください。
verizon.com/paymentsecurityreport

『2021決済システムのセキュリティに関するレポートにおけるインサイト：PCI DSS v4.0』ホワイトペーパーをご覧ください。
verizon.com/business/verizonpartnersolutions/business/resources/ whitepapers/payment-security-report-insights.pdf

ベライゾンが提供するその他のセキュリティソリューションやサービスの詳細については、以下のページをご覧ください。
verizon.com/business/products/security/

verizon business

1 『2022年度データ漏洩/侵害調査報告書』：https://www.verizon.com/business/solutions/secure-your-business/business-security-tips/
2 『2022決済システムのセキュリティに関するレポート』(英語）：https://www.verizon.com/business/reports/payment-security-report/
3 『2021決済システムのセキュリティに関するレポートにおけるインサイト: PCI DSS v4.0 』
https://www.verizon.com/business/verizonpartnersolutions/business/resources/whitepapers/payment-security-report-insights.pdf