クレジットカード情報を守る PCI DSS 最新動向

キャッシュレス決済普及の一方で増大する脅威から顧客を守るには

進行するキャッシュレス化で求められるセキュリティ対策

日本においても、キャッシュレス化は着実に進行している。経済産業省によると、2021 年のキャッシュレス決済比率は 32.5%。政府は 2025 年までにこれを 4 割程度、将来的には 8 割に高めようとしている。こうした動きに対して、多くの企業が、デジタルマーケティングの強化などを目指して積極的に対応しているのが現状だ。

キャッシュレス決済において多用されているのが、クレジットカードである。EC はもちろんだが、Suica などの交通系電子マネーもクレジットカードとの連携により利便性を高めている。QR コード決済でも、実際の支払いのところではクレジットカードが利用されている場合が多い。

ただ、キャッシュレス化を進める事業者にとっては課題もある。それが、クレジットカードに関係する情報をいかに守るかである。個人情報、お金に関する情報を扱うだけに、強固なセキュリティ対策が求められる。

店頭にせよ EC サイトにせよ、クレジットカード情報の入り口はそれぞれの事業者が運営している。また、自社内でクレジットカード情報とひも付けて、個人情報を管理している企業も多い。その管理責任は重い。

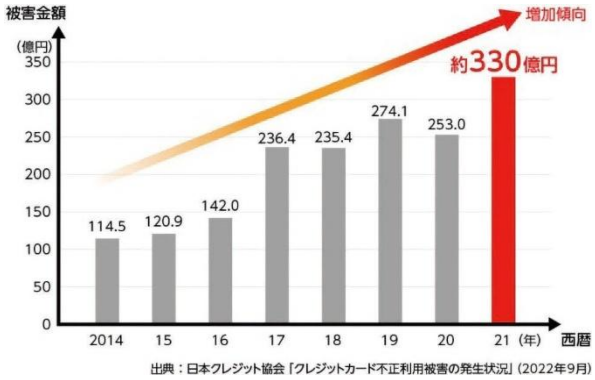
クレジットカード情報に関するグローバルセキュリティ基準としては、PCI DSS(Payment Card Industry Data Security Standard)がよく知られている。その新たなバージョンである PCI DSS v4.0 への対応が進みつつある中で、クレジットカード情報のセキュアな管理をどう進めればよいだろうか。

年々増加しているクレジットカードの不正利用

サイバー攻撃の巧妙化はよく指摘されるが、一方で、高度とはいえない攻撃の裾野も広がっている。

「攻撃を行うためのツールは豊富で、初心者でも攻撃しやすい環境が生まれています。ほとんどの場合、その目的は金銭です」と語るのは、富士通の小寺 夕理氏である。同社は PCI DSS の準拠認定に関するコンサルティングサービスを提供し、多くの実績を積み重ねてきた。

攻撃者は個人情報を不正に持ち出して換金することもあるがクレジットカードの不正利用による被害も絶えない。日本における不正利用の被害は年々増加している(図 1)。



出典：日本クレジット協会「クレジットカード不正利用被害の発生状況」(2022年9月)

図 1：急増するクレジットカード不正利用の被害
不正利用による被害金額は、7 年間で 3 倍近くに増えた。Web サイトへの容易な攻撃により「小銭稼ぎ」の感覚でクレジットカード情報を窃取しようとする攻撃者が増えている

「大きな被害が生じるケースの 1 つは、Web サイトの改ざんです。改ざんされたホームページを訪れたユーザーが、偽の決済ページに誘導されます。ユーザーは普通に買物をしているつもりで、クレジットカード番号やパスワードを打ち込んでしまう。こうしてクレジットカード情報が盗まれてしまうのです」と小寺氏は解説する。ホームページを改ざんされた企業は、責任を問われることになる。

これは一例であり、攻撃のバリエーションは増え続けている。こうした被害を防ぐための国際的なセキュリティ基準が PCI DSS だ。

日本では割賦販売法でクレジットカード情報の適切な管理が義務付けられており、クレジット取引セキュリティ対策協議会が具体的なガイドラインを策定している。ガイドラインによると、加盟店はカード番号や名義、有効期限などのクレジットカード情報を保持する場合、PCI DSS への準拠が求められる。2021 年 4 月から施行された改正割賦販売法では、準拠すべき事業者として大量のクレジットカード番号などを取り扱う決済代行業者やコード決済事業者へ対象が広がっている。

富士通株式会社
グローバルマーケティング本部
インフラ＆ソリューションフォーカル統括部
デジタルインフラフォーカル部
小寺 夕理氏

増大する脅威に対応した PCI DSS v4.0 への移行が必要

「PCI DSS には企業のシステム全体の『あるべき姿』が整理され、まとめられています。基本的にはクレジットカード情報が対象ですが、企業内にはそれ以外にも重要な情報は多くあります。そうした重要情報に対して、PCI DSS の手法を適用することもできます。PCI DSS によるセキュリティ対策は、様々な場面で有効です」と、富士通の小川 魁氏は語る。

企業を取り巻く脅威は増大する一方であり、顧客のクレジット情報を扱うことのリスクも高まっている。こうした環境変化に対応して、PCI DSS はこれまでバージョンアップを繰り返してきた。そして、2022 年 3 月には PCI DSS v4.0 がリリースされた。約 8 年ぶりのメジャーバージョンアップである。

現行バージョンから v4.0 への移行期間は 2024 年 3 月末まで。同年 4 月からは、v4.0 の評価だけが有効になる。そのスケジュールを踏まえて、既に v4.0 準拠に向けて動き出した企業は少なくない。v4.0 のポイントは 3 点である(図 2)。

第 1 に、PCI DSS 前段部分の詳細化。前段というのは PCI DSS 要件の適用性情報や適用範囲、PCI DSS が求めるタイムフレームなど。タイムフレームを例にとると、これまでは曖昧だった時間的な概念が明確に定義された。v4.0 の要件における「毎日」は、「営業日に限らず、1 年を通じて毎日」という具合だ。

第 2 に、PCI DSS 要件の追加／変更である。クレジットカード情報を扱う際のセキュリティ対策ニーズに対応して、v4.0 ではその要件が大幅に見直された。 150 以上の要件が追加または変更され、一部要件については新たな機能の導入が必要になる。

第 3 に、カスタマイズアプローチの登場。PCI DSS で定義されたアプローチではなく、カスタマイズされたアプローチが認められる。独自のやり方でセキュリティ対策の目的を達成しなければならないので、高度なリスク管理能力を持つ企業が対象とされる。

PCI DSS v4.0 に盛り込まれた新要件は多い。その一例として、マルウェアによる通信の検知がある。富士通の高橋 弘志氏はこう説明する。

富士通株式会社
ネットワーク&セキュリティサービス事業本部
セキュリティコンサルティングセンター
小川 魁氏

「最も怖いのは、情報の外部への持ち出しリスクでしょう。v4.0 では外部 C&C サーバーとの秘密の通信の検知、対策の実行、必要に応じて追跡を行うことが求められます。怪しい相手と通信をしていないか、その通信の挙動などについてもチェックする必要があります」

こうした対策を含めて、v4.0 に対応するためには専門的な知見が求められる。

「新しい要件を満たそうとするとき、『どこまでやれば十分か』という判断は難しいかもしれません」と小川氏。さらに、高橋氏はこう続ける。

「v4.0 では、ターゲットリスク分析という考え方が様々な場面で導入されています。自社でリスクを分析した上で、適切な対策を実行できるので、自由度や柔軟性が高まりました。一方で、自分たちで判断するにはそれなりの専門的な知見が求められます」

企業が自社だけで最適なセキュリティ対策を描くのは容易ではない。こうした課題の解決に向けて、富士通はコンサルティングサービスを提供している。

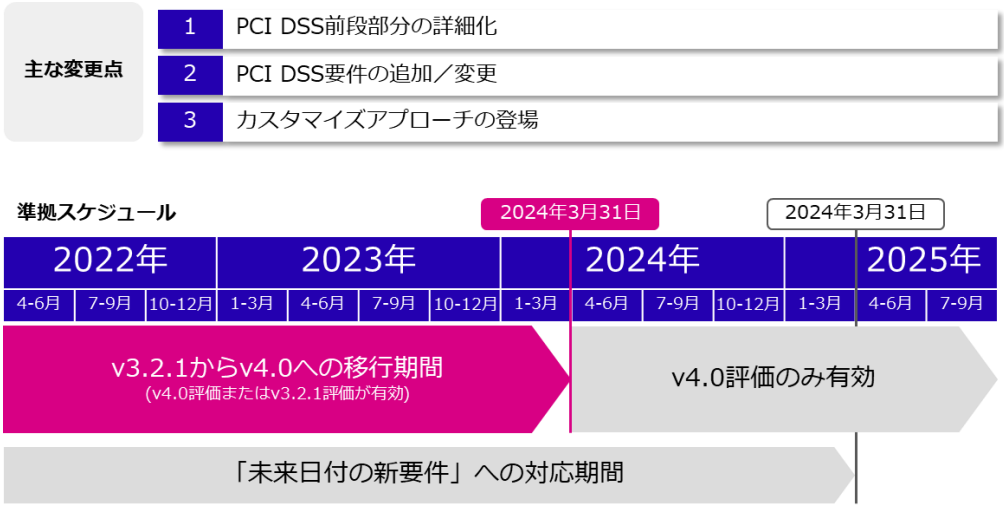


図 1：PCI DSS v4.0 の変更点と移行スケジュール

PCI DSS v4.0 における追加、変更点は多い。要件を満たすためのアプローチの自由度が高まるなど、準拠のための考え方にも変化が見られる。こうした要件を適切に解釈した上で、自社特有のビジネス特性を踏まえて具体的な計画に落とし込む必要がある。その際、高度な専門性が欠かせない

富士通の強みとしては、まず、あらゆる産業分野における豊富な SI 実績が挙げられるだろう。セキュリティ対策ソリューションに限っても、多くのメニューを揃えている。加えて、PCI DSS 領域における深い専門性がある。

「当社は PCI DSS 準拠を認定する審査機関としての QSA(Qualified Security Assessors：認定セキュリティ評価機関)資格と、PCI DSS で必要とされる脆弱性スキャンを実施する ASV(Approved Scanning Vendors：認定スキャンベンダー)資格の両方を持っています。日本で両方の資格を持っているサービス提供社は限られています」(小川氏)

富士通は PCI DSS 準拠認定に向けたプロセスを、トータルにサポートしている(図 3)。また、数多くの SI 経験などを踏まえて、ビジネス特性に応じた最適な提案ができるのも強みだ。

「例えば、100 台の端末を運用している企業と 1 万台の端末を運用している企業では、PCI DSS v4.0 の要件を満たすための対策は変わります。クレジットカード取引の額や頻度によっても、最適な対策は異なるでしょう。私たちはお客様の状況に応じた最適な対策案を考え、提案しています」と高橋氏はいう。

富士通は近年、ゼロトラストの考え方に基づくセキュリティソリューションに注力している。セキュリティ対策の最前線で培ったノウハウは、PCI DSS v4.0 における支援サービスでも生かされている。

富士通株式会社
ネットワーク＆セキュリティサービス事業本部
セキュリティコンサルティングセンター
マネージャー
高橋 弘志氏

図 2：PCI DSS 準拠認定のプロセスと富士通の実績

富士通は PCI DSS 準拠認定のプロセスをトータルサポートしている。また、支援実績も豊富だ。準拠のためのコンサルティング提供では 100 社超、脆弱性スキャンのサービス提供先は 2500 社超に上る。高度な専門性を持つセキュリティコンサルタントの厚みも大きな強みだ

関連リンク

セキュリティ診断による脆弱性の発見・攻撃の未然防止
脆弱性マネジメントを効率化し IT 資産の堅牢化を実現

[2023 年掲載]

本記事中に記載の肩書きや数値、固有名詞等は掲載日現在のものであり、このページの閲覧時には変更されている可能性があることをご了承ください。

お問い合わせ先

製品・サービスについてのお問い合わせはコチラ
富士通株式会社　〒211-8588　神奈川県川崎市中原区上小田中 4-1-1

