短期集中連載

非対面加盟店のためのセキュリティ対策入門

第4回 非保持化を断念してPCI DSS準拠を目指す

日本基準ではなく国際標準で より高度なセキュリティレベル確保を

国際マネジメントシステム認証機構
取締役 営業部 部長 PCI QSA 監査員
荒井 亮介

本連載ではこれまで、非対面加盟店が非保持化するための方策と非保持化を達成したことを確認する方法について紹介してきたが、クレジットカード番号等を顧客管理に利用しているとか、顧客により簡便で一貫したユーザーインターフェースを提供したいといった理由で、あえてカード情報を保持し、PCI DSSに準拠する非対面加盟店も存在する。また、非保持化はあくまでも日本だけで認められている緩やかな基準にすぎないことから、さらに高度なセキュリティレベルを確保するために、世界標準のPCI DSS準拠を目指す非対面加盟店もあると思われる。今回はPCI DSS準拠を達成するためのポイントを、PCI DSSやPCI P2PEのQSA（認定セキュリティ評価機関）である国際マネジメントシステム認証機構（ICMS）が解説する。

（編集部）

非保持化は本当にPCI DSS準拠と同等か？

「クレジットカード取引におけるセキュリティ対策の強化に向けた実行計画－2018－」（以下実行計画2018）を受け、多くの加盟店が非保持化を目指す流れになっている。非保持化を実現することが困難な加盟店は、しかたなくPCI DSS準拠のような捉え方をされているのは、PCI DSS監査会社（QSAカンパニー）としては多少複雑な気持でいる。

おそらく難解な表現の要件やその項目数、業務への負荷、準拠と運用の費用対効果などの理由から、PCI DSSには難易度及び費用が〝お高い〟セキュリティ規格のイメージがあるのだろう。そこは世界基準でカード情報を守る重要性と、その備えによるビジネス効果について、われわれPCI DSS監査会社が理解を広める努力不足と責を認識している。

そのうえであえていえば、実行計画2018が「EC加盟店における非保持化とされるセキュリティ措置は、PCI DSS準拠とイコールではないものの、カード情報保護という観点では同等の効果がある」と記述している点については、セキュリティ対策を進めていくという意味においては前向きに捉えること

【図表１】 非保持化とPCIDSSの相違

	非保持化（同等／相当含む）	PCIDSS
基準	国内のみ有効	グローバルで有効
セキュリティ措置／SAQタイプと項目数	リンク型	SAQ A：24項目
	JavaScript型（トークン型）	SAQ A-EP：193項目
セキュリティ措置の対象外となるカード情報	あり ※紙、紙媒体をスキャンした画像データ、電話での通話（通話データ含む）は、保存をしていても非保持扱いとなる。	なし ※データである限り通話データも含まれる。媒体（紙、リムーバブルディスク、ファクス等）には、おもに物理的なセキュリティ要件が適用される。

ができるが、ＰＣＩＤＳＳ準拠と同等の効果があると位置づけた点については、うなずきかねる部分がある。

ＰＣＩＤＳＳでは非保持という概念はなく、ペイメントカードを扱うすべての事業体は、ＰＣＩＤＳＳの準拠対象である。本稿では、非保持化とＰＣＩＤＳＳの違いを掲示し、セキュリティレベルの違いを認識したうえで、非保持化に該当する、あるいは非保持化を検討中、導入済みの加盟店を含め、すべてのＥＣ加盟店に向けてＰＣＩＤＳＳ準拠に取り組む意義と、具体的なＰＣＩＤＳＳ準拠の進め方を述べていく。

非保持化とＰＣＩ－ＤＳＳの比較

非保持化とＰＣＩＤＳＳの相違を図表１にまとめてみた。

○基準

非保持化は、各業界の関係者、経済産業省から構成されるクレジット取引セキュリティ対策協議会が提示した、日本独自のセキュリティ措置である。措置を導入した際の適正を判断する第三機関はいまのところ設立されておらず、報告方法や検証などはカード会社と加盟店との間での協議に任せられている。

対しＰＣＩＤＳＳは国際基準であり、ＱＳＡ（ＰＣＩＤＳＳの監査を行うＰＣＩＳＳＣ認定監査員）が準拠性を確認するオンサイト監査により、あるいは事業者みずから行う自己問診（ＳＡＱ）で該当タイプの項目を適切に満たすことにより、ＰＣＩＤＳＳに準拠できる。

○セキュリティレベル

非保持化のセキュリティ措置である非通過リンク型は、ＰＣＩＤＳＳの自己問診（ＳＡＱ）の「Ａ」に該当し、セキュリティチェックの項目数は24ある。非通過型JavaScript型（トークン型）はＳＡＱの「Ａ－ＥＰ」に該当し、項目数は１９３に及ぶ。また、非保持化ではカード情報が紙媒体、紙媒体をスキャンした画像データ、通話データについては対象にならないが、ＰＣＩＤＳＳでは対象となる。

○リスク

実行計画２０１８では、非保持化すればＰＣＩＤＳＳ準拠までは求めないとされている。これは業界の実態を考慮し、取り組みやすいセキュリティ措置にすることで、ＥＣ界全体のセキュリティレベルの底上げをする狙いがあると考えられる。しかし、ＰＣＩＤＳＳの要件によりリンク型やJavaScript型（トークン型）でカバーしている脅威を、非保持化においてはどう対処するのだろうか。ＰＣＩＤＳＳは、漏洩事故の教訓を生かした要件である。ＳＡＱの項目数は、これらセキュリティ要件を満たしていない非保持化のＥＣ事業者が負うリスクの数といえる。とくに項目数が１９３ある

「A－EP」に該当するJava Script型（トークン型）については、PCIDSSと同等のセキュリティ措置というには、どうにも無理があるといわざるを得ない。

大方のQSAが懸念していたように、非保持化に取り組んだECサイトからの漏洩事故は、18年も相次いで発生した。JavaScript型（トークン型）において、カード情報を入力する際に起動するJavaScriptの脆弱性をつかれたパターンが多いようだ。ECサイト事業者は非保持化したことにより安心し、ECサイト自体のセキュリティ対策を実施しておらず、脆弱性を抱えたまま運営をしている可能性が高いのではないか。対してPCIDSS（SAQ）の要件は、このあたりのリスクも認識してあり、しっかりと防止策が講じられている。

漏洩事故を起こした場合、事業への影響は深刻だ。フォレンジック調査が入り、調査が完了するまでクレジットカード決済はやめなければならない。加えて顧客の問合せ対応、警察への被害届、広報、カード取扱い再開のための対応に追われ、事業主と従業員は心身ともに疲労困憊する。漏洩規模によっては事業の存続を揺るがしかねない。

日本クレジット協会によるとクレジットカードの不正利用額は、15年120・9億円、16年142億円、17年236・4億円と急激に増加した。その6割前後が番号盗用被害額である。これら事象を鑑みると実行計画2018は、実効性の効果についての検証によっては、見直しや変更が発生する可能性もあるのではないかと考えられる。これらセキュリティ措置がPCIDSSに近づくことはあっても、乖離していくことはないだろう。事業者はこれらリスクを考慮した長期的な視野で、事業利益を安定確保するビジネス効果として、何より重要なカード情報を守る確かな基準として、すべての非対面加盟店に国際基準であるPCIDSS準拠を薦める。

PCIDSS準拠を目指すための第1歩

PCIDSS準拠するには、その道のプロ、監査会社やコンサルタントに相談するのが一番近道だ。会社によってサービスに差があるので、自社の規模や予算にあった準拠支援を比較検討するとよい。クレジットカードの年間トランザクション数が600万件（Visa、マスターカードの場合、JCBは100万件）以上の場合は、QSAによるオンサイト監査が必須とされる。それ以下のトランザクション数の場合は、自己問診（SAQ）の策定でPCIDSS準拠と見なされる。

SAQは、PCISSCのサイトからダウンロードして入手できる。タイプ別になっているので、該当するタイプがわからない場合は、監査会社やコンサルタントに相談してみるとよい。筆者の監査会社でもQSAによるSAQの策定支援をメールベースで相談できる手軽なものから、打合せをしながら準拠を進めていくフルサポートまで、事業規模や予算に応じた準拠支援サービスを提供しているので利用いただきたい。

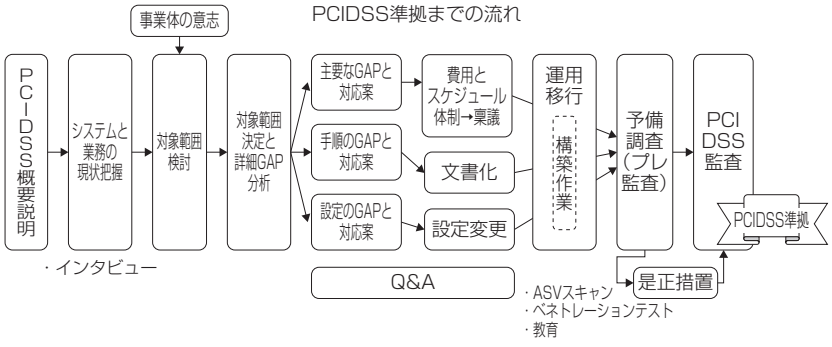
各社が提供しているセミナーやワークショップでSAQのイメージをつかむのも、準拠を進めていくうえで参考になるだろう。非保持化とされるリンク型（SAQのA）とトークン型（同A－EP）に該当する加盟店は、自社、または先述の支援サービスを利用してSAQの該当項目を満たせば、国際水準でカード情報を守る装備をしていることになる。カード情報を保持する（通過、処理を含む）加盟店はSAQのDに該当し、オンサイト監査相応の準拠項目数が331と多いので、まずは監査会社やコンサルタントに相談することをお薦めする。自社でSAQ策定する場合は、要件について理解が不十分であったり、事業体の意思を反映した独自解釈であったり、不適切な準

拠になる可能性があるので、少しでも疑問を抱いた場合は、プロに問合せしていただきたい。

準拠支援サービスの流れと留意点

ここでＩＣＭＳが提供する準拠支援サービスの流れを一例としてあげる（図表2）。自社で行う場合や他の準拠支援のサービスを利用した場合でも、大筋な流れは同様と思われるので参考にしていただきたい。

【図表２】 PCIDSS準拠の流れ



まずはカード情報の流れとしてシステムや業務の現状把握から始まり、ＰＣＩＤＳＳの対象範囲を確定していく。このプロセスが最も重要である。対象範囲を誤ってしまうと、結果的にリスクとコストの増大につながるからだ。また、業務にも影響を及ぼす可能性もあるので、その点も考慮し範囲を決めることが要になる。次にＰＣＩＤＳＳ準拠する場合の状況と、現状の差異（ＧＡＰ）を分析する。ＰＣＩＤＳＳの要件事項は、大きく分けるとシステム化と文書化に分類される。それぞれの対応策を策定していく。システム化要求については、事業体の環境により、サーバーやネットワーク機器の導入、ツール、ソリューション、アプリケーションの改修等が発生する。文書化については、ポリシー文書、各種手順書、帳票（記録）関連の文書が必要になる。その後、必要なセキュリティ診断、運用移行を行い、ＰＣＩＤＳＳ準拠となる。

すぐ準拠に進められない事業体には、段階的なアプローチとしてＰＣＩＳＳＣ公式ホームページのドキュメントライブラリにある「Prioritized Approach for PCI DSS」を参照に、セキュリティで優先されるものから取りかかり、部分準拠をしながら中期、長期的にＰＣＩＤＳＳの完全準拠を目指す道もある。

◇　◇　◇

非保持化が困難でＰＣＩＤＳＳにするしかないといった加盟店は、むしろ世界基準のセキュリティ措置でお客様のカード情報と自社のビジネスを守る好機と捉え、前向きに取り組んでいっていただきたい。同様に非保持化している加盟店も、よりセキュアな業務運用を確保するためにＰＣＩＤＳＳを参考にしてほしい。

キャッシュレス社会が進むにつれ、お客様の大切な情報を守ること、セキュリティ対策を施すことは、事業者にとっては責務と考える。クレジットカードでのネット決済においては、まだまだ不安に思う消費者は多くいる。お客様が安心して利用出来るようなキャッシュレス社会を実現できるように、今日からでも、できることからでもセキュリティ対策を進めていただきたい。微力ながら、本記事から業界の発展と、事業者のセキュリティ対策に役立つことになればと願っている。連載３回、４回とわたって、ＱＳＡカンパニーとして会社役員として、すべての非対面加盟店に送る言葉で締めくくる。

本稿に関するお問合せは、国際マネジメントシステム認証機構（ＩＣＭＳ）事業推進室（電話０３―５７１９―７５３３またはＥメールsuishin@icms.co.jpまでお願いします。