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3回 カード情報を非保持化したことを確認する方法

非保持化以前のカード情報の有無を確認することも必要

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

前号まで、非対面加盟店がカード番号とのカード情報を非保持化する、あるいは暗号化により非保持と同等／相当の措置を講ずるためのソリューションを紹介してきた。ただし、ソリューション導入前に取り扱ったカード情報が消去できるわけではない。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）も、「既に通過型を導入しているEC加盟店は、自社サイトにカード情報を含む決済情報等のログが蓄積される等のシステム的課題を認知できていないケースもあることから、カード会社（アクワイアラー）及びPSPは、引き続き加盟店に対する注意喚起を行い、システムログ等の消去を求める」と注意喚起している。今回は、情報セキュリティに関する第三者認証及び審査／監査サービスを提供しており、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、非保持化できたことを確認するための方法を紹介する。

（編集部）

非保持化が完了したと本当に言い切れるのか

実行計画2018では、非対面加盟店におけるカード情報の非保持化について、非通過型としてリダイレクト（リンク）型とJava Script（トークン）型が示されている。既存のシステムや運用を見直しながら、非保持化ソリューションをあれこれ選定し、コストをかけて導入にいたり、「ようやく非保持化達成！」と肩の荷を下ろしたEC サイト事業者も多いことだろう。

しかし、水を差すつもりではないが、非保持化達成と宣言するには、注意が必要である。これらセキュリティ措置の導入は、今後の運用において非保持化されたことを意味するにすぎない。

以前のシステムや、国内外にある拠点のサーバー、クライアントPCにカード情報は残っていないだろうか。とくにモジュール型などの通過型は、実行計画で危惧されているとおり、カード情報等のログが蓄積される等のシステム的課題を認知できていないケースが多発している。それら残存するリスクを把握しないまま、非保持化を達成したという認識でいると、最悪の場合、カード情報漏洩事故を発生させ、非保持化の意義をすべて失うことになる。

[図表1] 想定外のところでカード情報が発見される例

それでは、実際非保持化できたことをどのように確認できるのだろうか。本稿では非保持化のレベル、確認の方法などを紹介したい。

非保持化達成の証明はカード会社と協議を

まず、実行計画2018でいう「非保持」とは、「カード情報を保存、処理、通過しない」ことである。非保持化とは、(いままでカード情報を保持していた、またはその可能性も含めて)「カード情報を保存、処理、通過しない」事業体になることである。つまり、非保持化対策のセキュリティ措置の導入を完了した、ということではない。導入前後を含め、事業体内においていま現在、また今後においても「カード情報を保存、処理、通過しない」事業体になることが「非保持達成」といえる認識でいたほうがよいと筆者は考える。

非保持化(非保持と同等/相当を含む)の達成について、PCIDSSのように専門のQSA(PCIDSS認定監査員)が監査を行い、PCIDSS準拠証明書を発行するといった、第三機関による非保持化のセキュリティ措置を検証する機関はとくに設立されていない。

クレジット協会が提供する実効計画FAQでは、その点について、カード会社(アクワイアラー)・ベンダー等と協議のうえ対応してくださいとの回答が記載されている。カード会社(アクワイアラー)にて、加盟店の対応状況を確認するのが改正割賦販売法の考え方と追記されている。また、非保持化達成の報告についても特段義務づけられていないようである。

それであれば、実行計画で記載がない非保持の実証や非保持達成のレベルを気にする必要はない、と考えるかもしれない。

しかし、改正割賦販売法を受けカード会社（アクワイアラー）やＰＳＰは経済産業省にクレジットカード番号等取扱契約締結事業者の登録手続を行っている。登録申請にあたっては、加盟店調査に関する社内規程や手順を求められており、今後は加盟店調査や指導が厳しくなることが予想される。いままではアンケートレベルの調査であったが、より厳格な調査を行うことが求められるであろう。

思わぬところにカード情報は残っている

先述したとおり、事業体が把握していない場所から発見されるカード情報は、筆者の監査会社における監査において、実際にさまざまな箇所から発見されている。

実例をあげると、カード番号を含むエラーログがリダイレクトされ受信していたケース、あってはならないがイシュアーからのエラー応答にカード番号が含まれていたケース、消費者が入力フォームの備考欄にカード情報を入力していたログやメール本文内に含まれるケース、待機系サーバーでの設定変更の漏れからトランザクションログに含まれていた等々、実に多様なシーンにわたる（図表1）。

そこからひとたび漏洩事故が起きれば、非保持化した事業体からの流出事故として、カード会社や消費者にはなおさらインパクトを与えてしまうのではないだろうか。想定外の箇所からカード情報が発見されている実例を見てきた筆者としては、せっかく非保持化対策を講じたのだから、ここはもう一歩進み、過去分を含みカード情報が想定外のところに隠れていないか、検証していただきたいと考える。そこまで徹底して非保持を確認すれば、非保持化達成と宣言できるレベルといえるのではないだろうか。

認識している過去のカード情報への対応

それでは非保持化・非保持と同等／相当を検証するには、どのような方法があるのだろうか。

まず、非保持化の実現前における、「認識している過去のカード情報」については、どのような対処が適切なのだろうか。これについて実行計画２０１８では、電子帳簿保存法に基づく管理が求められた場合のみと限定したうえで、非保持化対応完了以前に取り扱った過去のカード情報を画像データ以外のテキスト形式等で電子帳票として保存する場合、ネットワークを利用しないスタンドアローン環境での保管・利用することが必須、とされている。

実行計画２０１８の主旨からすれば、実現前後にかかわらずテキストデータで保存していれば、非保持といえないことになるのだが、そこは電子帳簿保存法を考慮したやむを得ない例外的措置として、最低限スタンドアローンでの保存を認めているといったところだろう。それでもカード情報をより安全な方法で保持したい場合は、ＰＣＩＤＳＳのカード情報を保存する手法の要件を参考にするとよい。

カード情報検出ツールで非保持を確認する方法

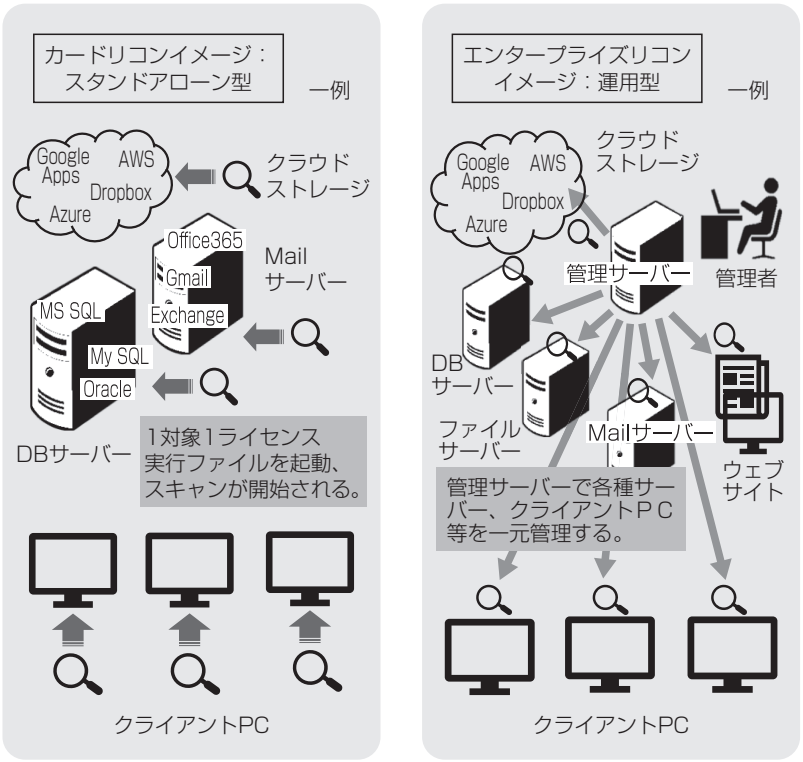
次に事業体が上記の方法で管理されている特定の場所以外で、カード情報が保存されていない「非保持である」ことを確認する方法としては、カード情報検出ツールの類を利用するのが一番確実といえる。調査結果でカード情報「０」を確認できれば、非保持あるいは非保持と同等／相当のセキュリティ措置が適切に行われているといえよう。

また、これらツールによる調査結果のレポートは、カード会

社等から実行計画に準じたセキュリティ措置の対応報告を求められた際に、非保持化の証跡にそのまま使えるのではないだろうか。

非保持化達成後の検証については、担当者やシステムが変わっても非保持化セキュリティ措置が適切に運用されるように、徹底した教育に加え、ツールの力を借りて定期的に事業体内のチェックを行い、非保持が継続されていることを確認する運用を推奨したい。

［図表２］「カードリコン」を用いたカード情報検出のイメージ



ここで筆者が知り得る非保持化の検証と運用で活用できそうなツールをいくつか紹介する。一つは、クレジットカード番号を含む個人情報を検出するツールである。代表的なものに「P-Pointer」（提供事業者：アララ）があげられる。検出後の対処は自動で移動、削除、また保管ルールに合わせて自動対処が可能であり、ＰＣとファイルサーバーにおいて個人情報全体の検出、管理の運用ができる。

パソコン利用者やウェブアクセス・作業履歴、削除ファイルの復元などＰＣの証跡調査に重きをおいたフォレンジックツールを使い、クレジットカード番号含む個人情報の含まれた重要なファイルを検出することもできる。「ARGOS DFAS」（アンペール販売）のポータブル版は、ＵＳＢ接続により一台で複数の対象ＰＣをスキャンできる、利便性が高い簡易フォレンジックツールだ。エンタープライズ版では国内、海外拠点の各ＰＣの詳細な調査が可能となるので、挙動監視、流出の抑止力としても活用できるだろう。

ＩＣＭＳが扱う「カードリコン」は、もともとＰＣＩＤＳＳ監査目的に開発されたもので、カードデータ検出に特化したデータ検出ツールである。スタンドアローン型で対象先はクライアントＰＣからＤＢサーバー、クラウド等広くカバーしている。エンタープライズ版は、カード情報を含む機密データ全体を管理、検出、自動対応する運用ツールだ（図表２）。

スタンドアローン型は監査やクライアントやサーバーなどのスポットのデータ検出チェック用に、ＰＣＩＤＳＳに準じた運用を目的としたエンタープライズ版は大・中企業向けに、世界中で利用されている。先述したカード情報が発見された実例は、監査の過程でこのツールを活用して遭遇したケースであ

る。

なお、ＩＣＭＳのスタッフがオンサイトで本製品を使ってスキャンを行い、スキャン結果を提出するスポットサービスも提供しているので、第三機関による「非保持化達成」の実証や、単発で調査を望む企業でも利用することができる。

繰返しになるが、非保持化ソリューションの導入がゴールではなく、少なくともいま現在、事業所内にカードデータがないことを確認する検証は、いままでのカード情報が発見された現場を見てきた監査会社としては、大いに推奨したいところである。とくに冒頭で触れたモジュール型の通過型からの漏洩事故は、いまも後を絶たない。現在も含め、以前通過型で非保持化にしたＥＣサイトは、カード情報がどこにも隠れていないかチェックすることを強くお薦めする。このようなツールがない場合のチェック方法は、おそらくシステム担当者がひたすら目視で確認するという原始的な手法になるだろうが、膨大なシステムログを一般人の目でカード情報の有無を確認していくのは、見落としの可能性も大きく、現実的でないといえよう。いずれの製品も無料体験やトライアルが用意されているようなので、まずは非保持化した事業所内にカード情報があるかどうかの検証をしてみてはどうだろうか。

労して「非保持」にするセキュリティ措置を講じたのだから、非保持を「達成」したといえるレベルに、非対面加盟店はもう一歩進んで肩の荷を軽くしていただくことを監査会社として願っている。

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。 ◈