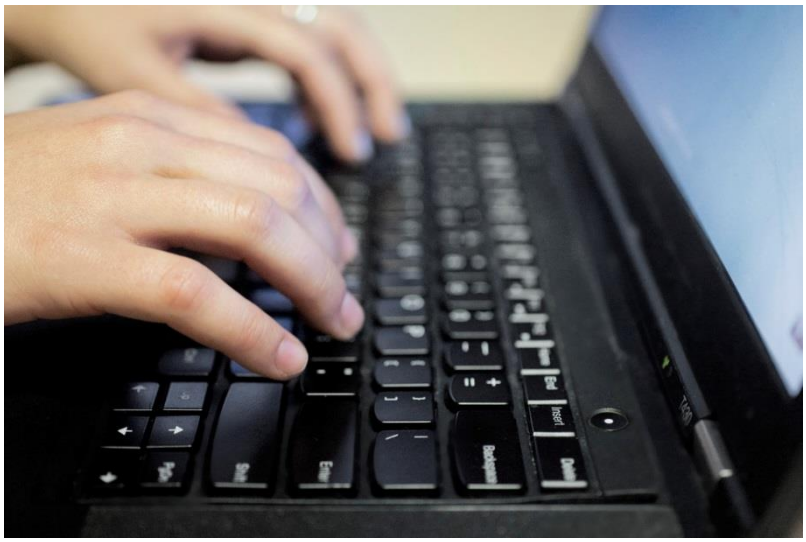
Secure SketCH

改正割賦販売法に向けた「実行計画2018」の対策ポイント徹底解説

改正割販法施行間近の2018年3月1日に公開された、カード情報取り扱い事業者のとるべきセキュリティ対策を具体的に記述した文書「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」（実行計画2018）、本書では、その全体概要とポイントについて紹介する。

目次



※ １.～ ３.まではSecure SketCHブログにて公開中

1.

はじめに

2015年に120億円、2016年は142億円、2017年は236億円超。

この年々増加している金額は、日本におけるクレジットカード不正利用被害額である。昨今、世界的にクレジットカードの不正利用対策が進む中、対策の遅れている日本が格好のターゲットと言われている。

待ったなしの状況にメスを入れるべく、改正割賦販売法（以下、改正割販法）が2018年6月1日に施行される。これにより、クレジットカード会社、決済代行事業者、EC・通販事業者、対面決済加盟店等のカード情報を取り扱うあらゆる事業体はセキュリティ対策の強化が義務付けられる。

そして、この改正割販法の成立、施行に備えるため、経済産業省が支援し、一般社団法人日本クレジット協会（以下、JCA）が事務局を務めるクレジット取引セキュリティ対策協議会は2016年から、カード情報取り扱い事業者のとるべきセキュリティ対策をより具体的に記述した文書「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」（以下、実行計画）を毎年公開、改訂してきた。

改正割販法施行間近の2018年3月1日に2018年版の実行計画(以下、実行計画2018)が公開されたため、その全体概要とポイントについて紹介する。

2.

『改正割販法』『実行計画』『PCI DSS』の関係とは？

クレジットカードのセキュリティといえば、グローバルなクレジットカード情報セキュリティ基準であるPCI DSSを聞いたことがある方も多いだろう。
PCI DSS（Payment Card Industry Data Security Standard）とは、クレジットカード国際ブランド５社(VISA, Master, JCB, AMEX, Discover)が共同で策定した情報セキュリティ基準であり、クレジットカード情報を保護するためのシステム、運用、ポリシー、物理セキュリティに至るまで非常に網羅的かつ具体的に整理されたセキュリティ基準となっている。

そして、PCI DSSのセキュリティ要件を満たすことにより、クレジットカード情報保護のための一定のセキュリティレベルが確保できていることを社内および対外的に示すことができるのである。

では、法律である改正割販法、そして、実行計画、PCI DSSの関係はどのようになっているのだろうか。

改正割販法自体に「実行計画」や「PCI DSS」という固有の文書やセキュリティ基準名称は書かれていない。これは日々、攻撃手法とその対策が進化するセキュリティ分野において、時代の流れによって変わる可能性のある固有の名称を、法律の条文に取り入れてしまうことで、その都度、名称変更等による法改正を避けるためである。

よって、改正割販法の中では、クレジットカード情報取り扱い事業者に対し、セキュリティ対策を義務付けることの記述に留め、具体的な対策や取り組みを示した規則については認定割賦販売協会であるJCAが制定することとしている。（[割賦販売法（後払分野)に基づく監督の基本方針]より）

それを受ける形でJCAが事務局を務めるクレジット取引セキュリティ対策協議会が、具体的に取るべきセキュリティ対策の水準等を載せた文書「実行計画」を策定・提示している。そして、「実行計画」において、求めているセキュリティ対策水準が「PCI DSS準拠」であり、加盟店に限っては「PCI DSS準拠」の他にも、クレジットカード情報を原則持たない「非保持化（同等/相当含む)」を選択肢のひとつとしている。

「非保持化(同等/相当含む)」については後述するが、このような流れで改正割販法によって、「実行計画」に従うこと、そして、「PCI DSS準拠」、または「非保持化(同等/相当含む)」のセキュリティ対策をとることが加盟店を含むクレジットカード情報取り扱い事業者に対し、法的に義務付けられたのである。

なお、「PCI DSS準拠」には、処理件数等の基準により外部審査を必要とする場合と、自己問診にて準拠証明を行う場合がある。前者の場合は認定審査機関(QSA)による訪問審査が必要となり、当社は、その認定審査機関(QSA)として、改正割販法対応にあたりカード会社（イシュア）、加盟店管理会社（アクワイアラ）からサービスプロバイダ、加盟店まで業界の多くのお客様に対し、PCI DSS準拠支援、準拠審査・認定、および実行計画に記載の非保持化の両面のサポートを行っている。

3.

「実行計画」の三本柱

最初の「実行計画」は2016年2月に公開された。その中では、特に日本におけるカード情報漏えい事故の多くが非対面加盟店で起きている状況から、非対面加盟店の対策期限は2018年3月末とされ、対面加盟店の対応期限は2020年3月末までと定められた。これにより、多くのクレジットカード情報取り扱い事業者は情報収集や対策に乗りだすことになったのである。
そして、2017年3月に「実行計画2017」、2018年3月に「実行計画2018」と、毎年の改訂を経て、各クレジットカード情報取り扱い事業者が対応を進める中で「実行計画」上、曖昧となっていた部分や課題に対し、JCAや経済産業省、業界団体による議論が重ねられ、その解決案が提示された形となっている。

「実行計画2018」の構成として、以下のセキュリティ対策の３本柱を掲げている。

(1)クレジットカード情報保護対策
◇カード情報を盗らせない
・ 加盟店におけるクレジットカード情報の「非保持化」
・ クレジットカード情報を保持する事業者のPCI DSS準拠

(2)クレジットカード偽造防止による不正利用対策
◇偽造カードを使わせない
・ クレジットカードの「100%IC化」の実現
・ 決済端末の「100%IC対応」の実現

(3)非対面取引におけるクレジットカードの不正利用対策
◇なりすましをさせない
・ リスクに応じた多面的・重層的な不正利用対策の導入

引用： クレジット取引セキュリティ対策協議会 実行計画 -2018- の概要について P7

これらの内容を実行計画2018において多くの加筆・修正がされた(1)を中心として、順に見ていきたい。

4.

クレジットカード情報保護対策

クレジットカード情報保護対策の章は、ECや通販の非対面取引や、店舗等による対面取引に関わらず、クレジットカード情報が『保存』『処理』『通過』されるシステムやネットワーク、媒体に対し、カード情報を保護するための対策が記述されている。そして、「非保持化」や「PCI DSS準拠」はまさにこの保護対策である。

＜非保持化とは＞
加盟店においてカード情報を保存する場合に、それらの情報が紙のレポートやクレジット取引にかかる紙伝票、紙媒体をスキャンした画像データ、電話での通話データのみであり、電磁的に送受信しないこと、すなわち「自社で保有する機器・ネットワークにおいて「カード情報」を『保存』『処理』『通過』しないこと」。
また、決済専用端末（CCT）及びそれと同等以上のセキュリティレベルのものから直接外部の情報処理センター等に伝送している場合も同様に非保持とする。と実行計画2018では述べられている。

ここで注意が必要なのは、非保持化の適用対象は加盟店であり、イシュア、アクワイアラはもちろん、決済代行事業者やコールセンター、パンチ業者等のサービスプロバイダ(PSP)に対する考え方ではないということである。

例外として、委託元の加盟店が1社のみである場合に限り、サービスプロバイダであっても非保持化適用可能とクレジット取引セキュリティ対策協議会は認めているものの、あくまで例外としている。これはサービスプロバイダが情報漏えいを起こした場合の被害が複数加盟店に及ぶ可能性が高いため、十分なセキュリティ対策が必要という意図と考えられる。

前述の非保持化の定義を前提とし、「実行計画2018」によって、以下の表のとおり、非対面加盟店（EC・通販事業者）、対面加盟店における非保持化策がすべて出揃った形となった。
今後も非保持化策が追加になる可能性はあるものの2018年3月時点では追加検討されている非保持化策はない。

No.	加盟店業態	内回り/外回り	非保持化策(非保持と同等/相当含む)
1	非対面加盟店（EC）	-	非通過型の決済システムの導入 「リダイレクト（リンク）型」又は、「Java Scriptを使用した非通過型(トークン型)」
2	非対面加盟店（MO・TO）	外回り	決済専用端末を利用した方式の採用
3			タブレット端末を利用した方式の採用
4		内回り	PCI P2PE認定ソリューションの採用(認定端末の利用)
5	対面加盟店	外回り	IC対応の決済専用端末連動型・ASP/クラウド接続型
6		内回り	PCI P2PE認定ソリューションの採用(認定端末の利用)
7			非保持相当の策（セキュリティ基準11項目）の採用

ここからは、非対面加盟店（EC）、非対面加盟店（MO・TO）、対面加盟店それぞれの非保持化策を整理していきたい。

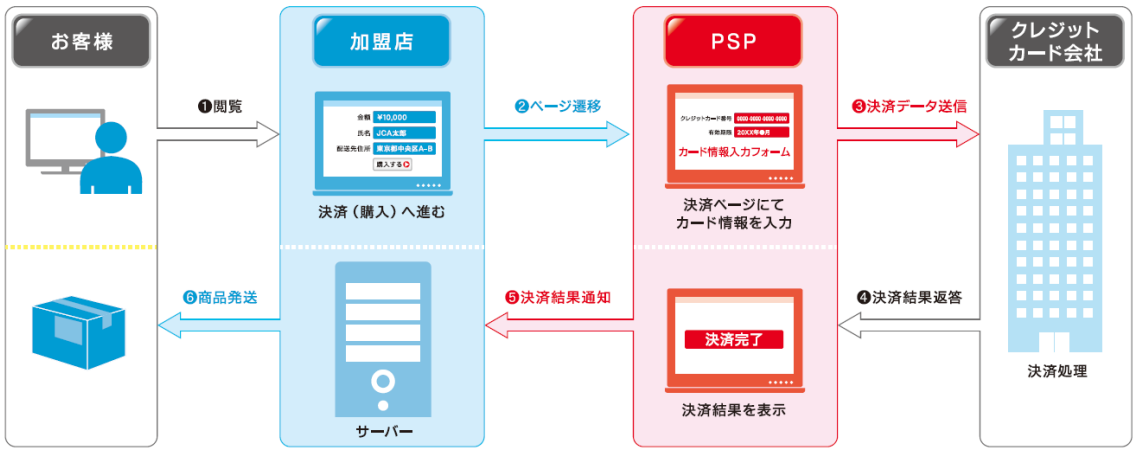
4−1.

非対面加盟店(EC)による非保持化策

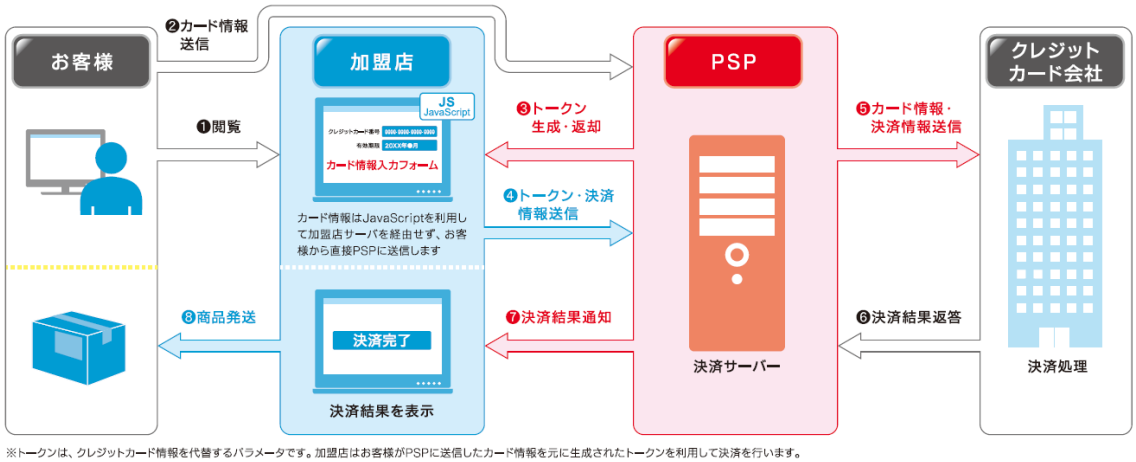
ECにおける非保持化策は、2016年から変わっておらず以下１つのみである。

＜非通過型の決済システムの導入＞
決済代行事業者の決済ページに利用者を誘導する「リダイレクト型（リンク型）」や、「Java Scriptを使用した非通過型(トークン型)」によりカード情報をトークン化して決済代行事業者へ連携し、自社のシステムにカード情報を一切通過させないことによって非保持化となる。　なお、いずれの方式においても利用する決済代行事業者はPCI DSSに準拠している必要がある。

＜リンク型＞



＜JavaScript型（トークン型）＞



※トークンは、クレジットカード情報を代替するパラメータです。加盟店はお客様がPSPに送信したカード情報を元に生成されたトークンを利用して決済を行います。

引用： クレジット取引セキュリティ対策協議会 実行計画 -2018- の概要について P13

4−2.

非対面加盟店(MO･TO加盟店)による非保持化策

MO・TOとはメールオーダー、テレホンオーダーの単語の頭文字を取ったもので、郵便や電話、またはFAXでのカード情報の受け取りを行う加盟店、例えば通信販売事業者やコールセンター業等がこれにあたる。

MO・TO加盟店に対する非保持化策は、３つ提示されている。

＜外回り＞

① 決済専用端末を利用した方式の採用

② タブレット端末を利用した方式の採用

＜内回り＞

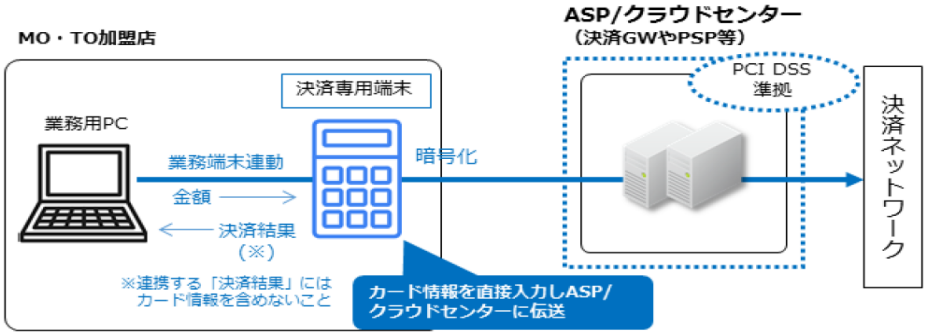
③PCI P2PE認定ソリューションの採用(認定端末の利用)

「外回り」、「内回り」とは、外回りがカード情報を自社のシステムやネットワークを通過させることなく、決済ネットワークや決済代行事業者に直接送信する方式のことであり、内回りはその逆、つまりカード情報を自社のシステムやネットワークを通過させる方式である。

①決済専用端末を利用した方式

外回り方式の1つとして提示されている「決済専用端末を利用した方式」では、CCTと同等/相当のセキュリティの決済専用端末を用いて、コールセンターのオペレータ等がカード情報を端末へ直接入力し、決済ネットワークや決済代行事業者へ直接伝送するという、カード情報を社内システムへ連動しない方式である。

カード情報以外である金額や決済結果等は内部連携可能なため、業務用PCでのカード情報入力が決済専用端末への入力に変更になるものの、業務フローの変更は比較的少ない方式であると言えるだろう。



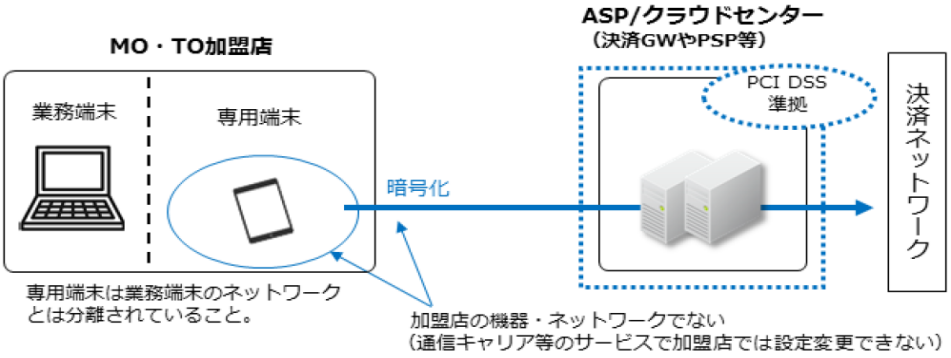
※ASP は Application Service Provider の略

引用： クレジット取引セキュリティ対策協議会 実行計画 -2018- の概要について P14

② タブレット端末を利用した方式

２つ目の方式も外回り方式となっているが、これはサービスプロバイダである決済代行事業者や通信事業者から専用のセキュリティ対策が施されたタブレット端末の貸与をうけることが前提である。その端末を利用することで社内にカード情報を連携することなく、携帯回線を通して決済代行事業者にカード情報を直接連携する方式である。

業務端末とは基本的にカード情報以外であっても内部連携ができなくなるため、業務としては、タブレットと業務端末への金額の２度打ちによる誤入力リスクへの対策や、タブレットの操作や管理運用等、これまでの業務フローからの変更が少なくないだろう。また、タブレットの貸与を受けるためのランニングコストも考慮の上、方式選定することをおすすめする。

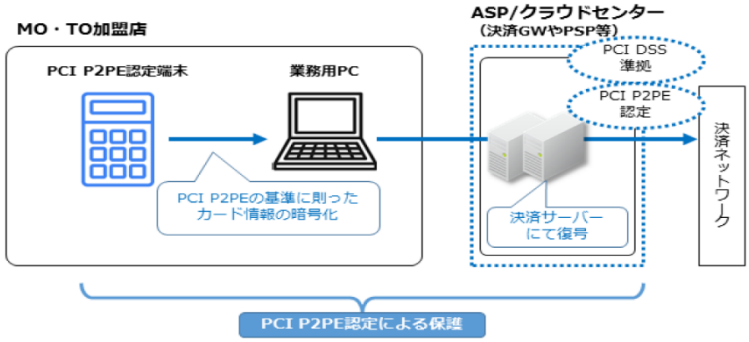


引用： クレジット取引セキュリティ対策協議会 実行計画 -2018- の概要について P14

③ PCI P2PE認定ソリューションを利用した方式

3つ目の方式は、MO・TO唯一の内回り方式となっており、PCI P2PEソリューションを採用することで非保持となる。加盟店はPCI P2PEソリューション認定を受けた決済端末を使用することで、1回の決済ごとに暗号鍵が異なる方式(DUKPT方式)によってカード情報が暗号化され、決済代行事業者等に連携することとなる。それにより、高い安全性を保つことができるため自社システムを通過する内回りが認められている。

一方で、このPCI P2PEソリューションを提供する国内の事業者は非常に限られており、加盟店が容易に採用できる選択肢が揃っていないことが課題となっている。PCI P2PE認定ソリューションは順次開発されてきており、この状態も2018年～2019年にかけて解消されていくことが期待されている。



引用： クレジット取引セキュリティ対策協議会 実行計画 -2018- の概要について P15

4−3.

対面加盟店による非保持化策

対面加盟店における非保持化策についても、３つ提示されている。

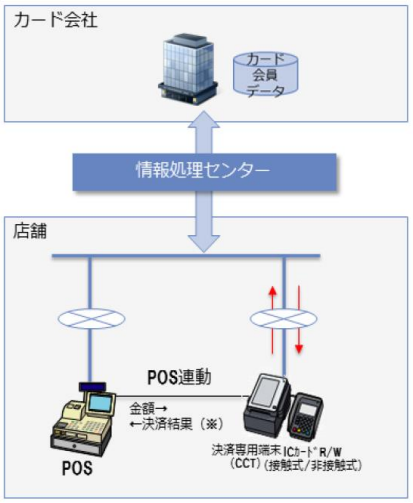
＜外回り＞
① IC対応の決済専用端末連動型・ASP/クラウド接続型
＜内回り＞
② PCI P2PE認定ソリューションの採用(認定端末の利用)
③ 協議会にて取りまとめた技術要件に適合するセキュリティ基準(11項目)を満たした上で、決済代行事業者等に接続する方式

① IC対応の決済専用端末連動型・ASP/クラウド接続型

基本的にMO・TO加盟店の非保持化策①と同様の外回りの考え方である。
CCTと同等/相当のセキュリティの決済専用端末を用いて、カード情報を決済専用端末から直接外部の情報処理センターまたは、決済ネットワークに伝送する方式、つまり、カード情報はPOS等の社内システムへ連動しない方式である。もちろん、カード情報以外の金額や決済結果等は社内システムへ連動してもよい。

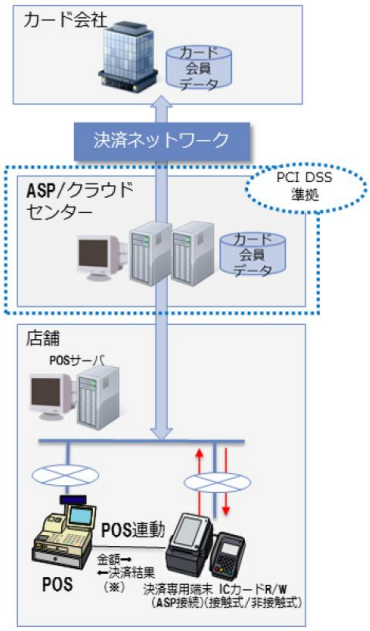
また、POSがない加盟店の場合、IC対応した決済専用端末のみを使用し、直接外部の情報処理センター等に伝送することで非保持化となる。

【決済専用端末（CCT）連動型（外回り）】



※POS連動する「決済結果」にはカード情報を含めないこと

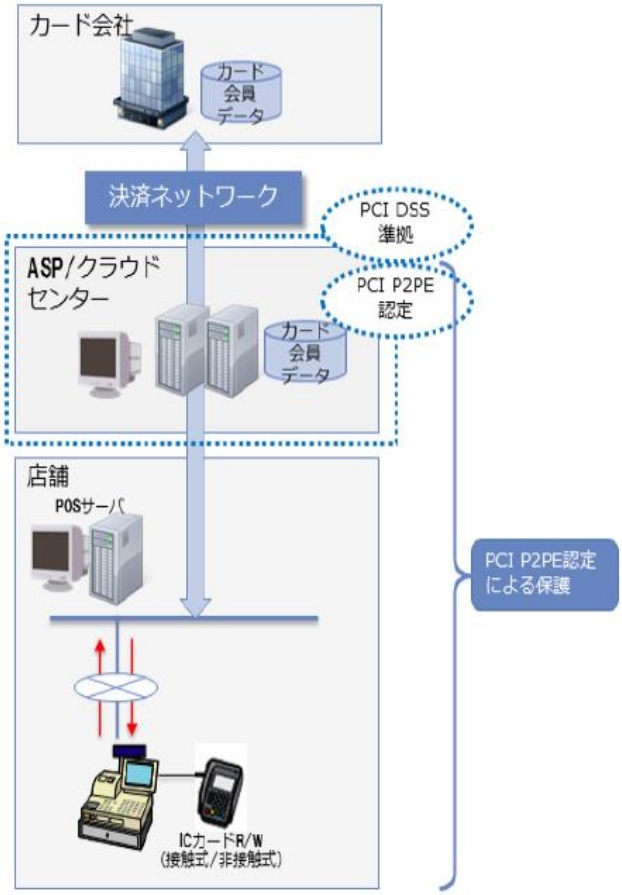
【ASP/クラウド接続型（外回り）】



引用： クレジット取引セキュリティ対策協議会 実行計画 -2018- の概要について P16

② PCI P2PE認定ソリューションの採用(認定端末の利用)

こちらもMO・TO加盟店の非保持化策③と同様の考え方である。内回りだが、PCI P2PEソリューションを採用することで非保持とすることができる。



引用： クレジット取引セキュリティ対策協議会 実行計画 -2018- の概要について P17

③ 協議会にて取りまとめた技術要件に適合するセキュリティ基準(11項目)を満たした上で、決済代行事業者等に接続する方式

こちらも内回りとなるが、PCI P2PEとは異なるセキュリティ基準PA-DSSに準拠したアプリケーション搭載のPOSやPCI PTSに準拠した決済専用端末を用い、かつ、ネットワークの分離やウイルス対策等のPCI DSSの要件を抜粋したようなセキュリティ基準11項目を満たし、PCI DSS準拠した決済代行事業者等に連携するという方式である。

②のPCI P2PEソリューションとは異なり、PA-DSSやPCI PTSに準拠した端末の利用だけでは非保持化とならないことに注意が必要である。

4−4.

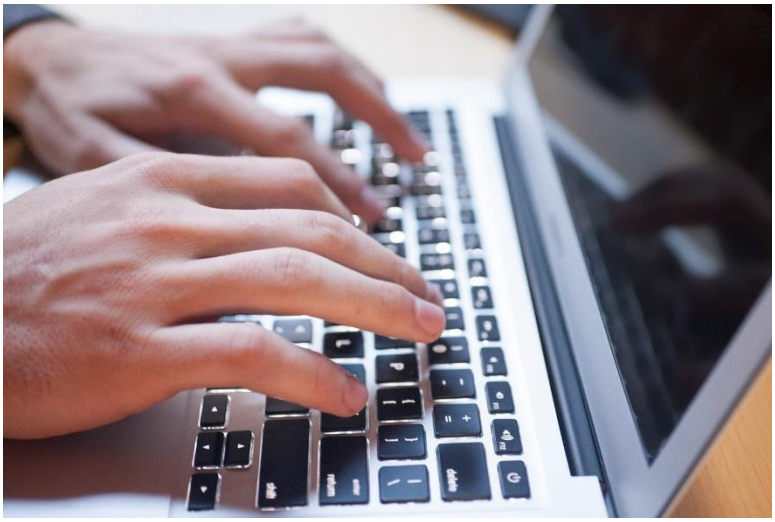
非保持化が維持される例外事項

これまで挙げてきた非保持化策を既に講じた環境において、例外的に非保持化が認められるケースが２つ存在する。それが以下である。

① 非保持化における顧客問合せ対応
② 電子帳簿保存法による過去データ（テキスト形式）の保存

①は、非保持化された環境において、返品問合せ等により、一時的にPCI DSSに準拠した決済代行事業者等の提供する取引データを照会する必要がある場合に、カード情報が自社内を『通過』することになるが、これは非保持を妨げるものではないとされた。

また、②は電子帳簿保存法に基づく管理が求められる場合、つまり、一部の国税関係書類に限り、画像データではない形式（テキスト形式等）でクレジットカード情報の過去データを保存することも可能とされた。その理由は、電子帳簿保存法で管理対象としたカード情報を含むデータを遡り修正することは帳簿の改ざんにあたるためであり、やむを得ない例外措置といえる。ただし、この場合にはスタンドアローン環境で保管することや、その環境へのアクセスを厳格に管理する対策が追加で必要となる。



4−5.

対応の期限と間に合わない場合の措置

加盟店、カード会社、PSPがいつまでに非保持化およびPCI DSS準拠の対応を実施する必要があるのかについて、実行計画2017,2018を基に整理するとそれぞれ以下の期限となる。

対象	形態	対応期限
加盟店	非対面加盟店(EC加盟店)	2018年3月末
	非対面加盟店(MO・TO加盟店)	
	対面加盟店	2020年3月末
カード会社	アクワイアラー	2018年3月末
	イシュアー	
PSP	形態問わずすべて	

なお、実行計画2018で2017年まで書かれていたEC加盟店の対応期限が書かれなくなった理由は、すでに対応が完了しており、継続的な対応のフェーズにあることを前提としているためである。

では、期限に間に合っていない場合は、どのように理解すればよいのだろうか。

ご存知かもしれないが、この対応期限や改正割販法が施行される2018年6月1日に間に合わないことに対する罰則規定は現状、存在しない。一方で、実行計画2018には以下のように書かれている。

> カード会社（イシュア）に加え、カード会社（アクワイアラ）等について「登録制」が導入され、カード会社（アクワイアラ）等は契約先加盟店の調査等を実施することが求められることとなる。調査の結果、セキュリティ対策が不十分な加盟店については、契約先のカード会社（アクワイアラ）等からの指導により合理的な期間内に法令上の基準に適合することが求められる。
>
> ***引用： クレジット取引セキュリティ対策協議会 実行計画 -2018- の概要について P5***

つまりは、加盟店において対応が間に合っていない場合は「合理的な期間」をアクワイアラと調整の上で、対応を速やかに進めることが必要なのである。

5.

クレジットカード偽造防止による不正利用対策

3本柱の2つ目。2020年3月末までに、イシュアによるIC対応のクレジットカード発行を進めるとともに、対面加盟店において、IC決済への対応が必要となっている。

なお、技術的また法的課題により、期限までにICカード対応ができない業界である鉄道事業者やガソリンスタンドについては、別途、それぞれに向けた指針に従った対応をとることになる。

6.

非対面取引におけるクレジットカードの不正利用対策

非対面取引における不正利用防止のため、すべての非対面加盟店にカード取引時の善管注意義務とオーソリゼーション処理（以下、オーソリ）を必須とした。
また、これまでの不正利用の被害状況からリスクの高い商材を扱う加盟店を「高リスク加盟店」と定義し、高リスク加盟店に対しては、オーソリ以外に下記の4つの方策の１つ以上を求めることとしたのである。
ただし、＜方策＞③④は取引履歴の無い状態では効果がないため、外部サービスの利用を強く推奨している。

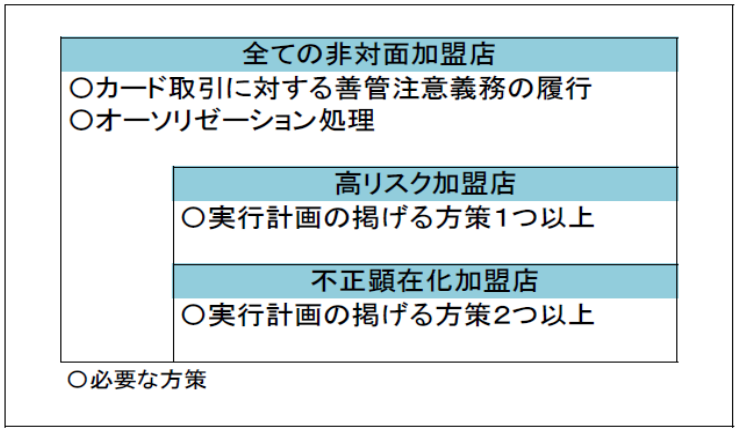
＜方策＞
①本人認証（３Dセキュア、認証アシスト）
②セキュリティコード
③属性・行動分析
④配送先情報

また、高リスク加盟店とは、以下の商材を扱う加盟店と定義された。

＜商材＞
①デジタルコンテンツ（オンラインゲーム含む）
②家電
③電子マネー
④チケット

そして、継続的に一定金額を超えた不正利用があった加盟店に対しては、2つ以上の対策を求めるとしている。なお、一定金額の基準は、現時点では3ヶ月にわたり、50万円の被害を超える場合となる見込みである。

加盟店分類表



引用： クレジット取引セキュリティ対策協議会 実行計画 -2018- の概要について P40

7.

3Dセキュアの進化と利用拡大

非対面取引(EC決済)における本人認証の仕組みとして、これまでも3Dセキュアの仕組みが選択肢としてあった。しかしながら、必ずパスワード入力を求められ、しかも、そのパスワードを利用者が覚えていないことが多く、そこで買い物をやめてしまうことが少なくない。そのため、EC事業者は3Dセキュアを極力利用しないという実態がある。

昨今、3Dセキュアの規格のバージョンアップに伴い、パスワード入力の前段階でリスクベース認証が行われ、リスクが高いと判定された場合のみパスワード入力を求める方式が導入されつつある。また、ブラウザによるパスワード入力ではなく、スマホアプリを用いた認証方法も実現可能となっており、それらのサービスが開発、浸透することによって、今後の3Dセキュアの利用拡大が期待される。

8.

おわりに

今回は、いよいよ2018年6月1日に施行される「改正割賦販売法」とその「実行計画」のポイントについておさらいしてきた。

2020年の東京オリンピックに向け、訪日外国人の数は増加の一途をたどっている。 2017年には2800万人を超す外国人が日本を訪れており、オリンピック開催となる２年後には更なる人数が予想される。また、世界がキャッシュレスの時代に向かう中、世界の都市部ではクレジットカード、デビットカード、QRコード決済等が主流となり、現金払いはもはや時代遅れになってきている。そのため、多くの訪日外国人は店舗でクレジットカード支払いを求めることだろう。

このような状況の中、安心・安全なクレジットカード決済を提供できるインフラが整備されていることは、世界に誇れる安心・安全な国、日本を実感してもらう上で、重要な要素の一つではないだろうか。

右肩上がりのクレジットカード不正利用を防止するには、カード情報の漏洩を防ぐこと、不正利用の防止対策を講じることの両面から対策を進めなければならない。そして、すべてのクレジットカード情報取り扱い事業者がそれらを意識し、実行計画に基づく対策と継続的な運用を実践していくことが肝要である。

非保持化、PCI DSS準拠について、また、その他にもサービス提供に向けたPCI P2PEソリューションや3Dセキュア、その他キャッシュレス時代に向けた決済セキュリティに関して、専門化の知見が必要な場合には、いつでもご相談いただければ幸いである。

＜引用文献＞
クレジット取引セキュリティ対策協議会 実行計画 -2018- の概要について
https://www.j-credit.or.jp/security/pdf/overview_2018.pdf
割賦販売法（後払分野)に基づく監督の基本方針
http://www.meti.go.jp/policy/economy/consumer/credit/pdf/170530_kihonhoushin.pdf

筆者略歴

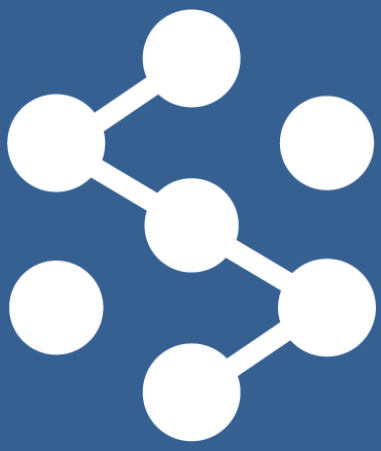
村松　直紀（むらまつ なおき）

大手SIerにてクレジットカード基幹、周辺システムを中心とした長年のアプリ開発・ＰＭを経て、2016年に野村総合研究所に入社。NRIセキュア出向後、セキュリティコンサルティングに従事。現在は、QSAとしてPCI DSS準拠支援コンサルティング、準拠審査を軸とした決済セキュリティ支援を担当。

連絡先：muramatsu@nri-secure.co.jp

本記事に関連したサービス：

PCI DSS 準拠支援コンサルティング/審査
https://www.nri-secure.co.jp/service/consulting/qsa.html



Secure SketCH

セキュリティ経営をシンプルに

https://www.secure-sketch.com