平成 23 年 3 月

【日本におけるクレジットカード情報管理強化に向けた実行計画】

１．背景

クレジットカード取引は、世界的に昨今ネット取引の拡大に伴いクレジットカード決済の機会も増加するなど、その規模はますます拡大傾向にある。我が国でもクレジットカードの 1 年間の新規信用供与額は約 44 兆円規模となり、ネット取引の増加等により、その規模は拡大傾向を維持している。その一方で、昨今クレジットカード決済に携わる事業者のコンピュータなどからクレジットカード番号等のクレジットカード取引情報の漏えいも多発している。特にインターネット回線から侵入し、クレジットカード情報等経済価値の高い情報を窃取する SQL インジェクション等によるクレジットカード情報流出、およびそれに伴う不正使用被害が増加傾向にあるなど、特にネット加盟店や決済代行業者におけるクレジットカード情報管理体制の強化は、喫緊の課題となっている。また、海外に目を転ずれば、対面取引の加盟店や決済代行業者でもクレジットカード情報流出事故が発生しているうえ、1 回の事故が甚大な規模の流出と不正使用被害をもたらす事例も多く確認されている。我が国でも、依然としてクレジットカード決済の大半は対面取引が占めており、潜在的なリスクが高いことから、ネットならびに対面環境における包括的なクレジットカード情報管理体制の構築が求められている。

我が国では、平成 22 年 12 月に改正割賦販売法が施行され、クレジットカード会社は、クレジットカード番号等の適切な管理が図られるよう、加盟店やその委託先に対する指導その他の措置を講ずることが義務づけられた。更に、国際ブランド会社においては、5 ブランドが加盟店および業務委託先のクレジットカード情報が安全・確実に管理できるためのクレジットカードセキュリティの国際統一基準「ペイメントカード産業データセキュリティ基準」(PCI DSS)を策定し、クレジットカードデータを取扱う加盟店や情報処理会社などにクレジットカード契約会社を通じて PCI DSS の対応を求めている。

そのような状況を踏まえ、(社)日本クレジット協会　インフラ整備部会では、経済産業省とも連携し、「日本におけるクレジットカード情報管理強化に向けた実行計画」を策定し、クレジットカード情報の管理強化に取り組むものとする。

２．目的

国際クレジットカードネットワークにつながる日本のクレジットカード決済に関わる全ての事業者が、安全なクレジットカード取引を確保するために、クレジットカード決済に携わる全ての関係者が統一的な考え方を構築し、それぞれの立場でクレジットカード情報の管理において責任ある対応を行うための実効性を確保することを目的に、クレジットカードネットワーク全体におけるクレジットカード情報管理強化を目指し、相互に同等な高度のセキュリティレベルを確保する。

また、現在一部の国際ブランドが欧米諸国の実情に合わせて設定した要請レベルや対応期間は、必ずしも日本の実情に合っていないことから、日本の実情に即した内容とスケジュールによる強化策を構築し、実効性を確保する。

３．「実行計画」の前提

国際的なネット取引の拡大に伴い、国際的にクレジットカード情報を取扱う企業は、高度なセキュリティレベルを構築することで、当該企業における情報管理上のリスク回避を行うことが社会の趨勢となっており、PCI DSS 準拠が国際的な基準とされている。この「実行計画」では、我が国においても、国際的なクレジットカードネットワークに参加する一員として、クレジットカード情報管理強化の基準を、この国際基準である PCI DSS を前提に策定している。

４．具体的内容

（１）適用対象（各対象とも、自社でクレジットカード情報を保持していることが前提）

この「実行計画」の適用対象は、以下の通りとする。

①クレジットカード会社

クレジットカード情報を保有している全てのクレジットカード会社を対象とする。ただし、他社情報も扱うアクワイアラーや、他社の情報処理を受託しているプロセッシング業務を行っている企業は、情報漏えい等が発生した場合、被害の規模も相当程度が予想されることから、高度なセキュリティ対策が求められ、客観的な証明が求められると考えられる。一方で、イシュイングのみであっても発行枚数が多い企業は、アクワイアラーと同等の考え方であるが、その被害が及ぶ範囲は、自社の取扱に限定されることから、準拠方法を自己問診としている。さらに、規模の小さいイシュアーについては、自社リスクの範囲で対応可能と判断し、他社のクレジットカード情報を一切保有しない前提で、PCI DSS 準拠の対象外という考え方を整理した。

②加盟店(およびその委託先)

ここでいう加盟店には、加盟店がクレジットカード決済に係る業務を受託する場合や、加盟店が独自にクレジットカード決済に係る業務を委託する先も含め、総称して加盟店という。非対面/ネットの場合、現状でも、外部からのクレジットカード情報窃取による被害が発生するなど、最優先対象と考えられる。また、対面/POS については、一般に大量のクレジットカード情報を取扱っており、情報漏えい等が発生した場合、被害の規模も相当程度が予想されることから、高度なセキュリティ対策が求められる。一方で、対面/スタンドアローンの場合、ほとんどのケースは、専門店等の形式で信用照会端末のみでカード決済しており、クレジットカード情報の「処理」と「送信」は行っているものの、一般的にはクレジットカード情報を保持していないことなどを考慮し、「クレジットカード情報の非保持」を確立することに主眼を置いて整理した。

③決済代行事業者

主たる業務が、他の加盟店に代わって、クレジットカード決済業務を行うものであることから、相当程度のクレジットカード情報を処理し、保持している。特にネットの場合は、情報漏えい等が発生した場合、被害の規模も相当程度が予想されることから、高度なセキュリティ対策が求められるが、対面であったとしても、様々なクレジットカード会社の情報を処理する立場から、クレジットカード会社のアクワイアラー等と同等の対応が必要不可欠であるとの認識から、その対象を区別することなく、全ての決済代行業者は PCI DSS 準拠を求めることで整理した。

（２）取引形態等

この「実行計画」の適用対象のうち、複数の取引形態が想定される「加盟店」と「クレジットカード会社」の対象とする取引形態を以下の通りとする。

[加盟店]

①非対面/ネット取引	ネット環境のみで商品取引を行う形態。
②対面/POS 取引	実際に店舗等で顧客に対し対面で、商品取引を行う形態。
③対面/スタンドアローン	インプリンタのみでカード会員データを処理する対面取引とスタンドアローンのダイヤルアップ端末を用いてクレジットカード会員データを処理している対面取引。

［クレジットカード会社］

①アクワイアラー（ACQ）	加盟店契約会社
②プロセッシング(企業)	決済業務や事務処理等(を行う会社)
③イシュイング（ISS）	クレジットカード発行会社

（３）適用レベルと基準（レベルの単位:レベルＢ・Ｃの決済代行業者/加盟店は、年間クレジットカード売上件数。クレジットカード会社はクレジットカード発行枚数。）

［加盟店］

①レベル A　：基準	4 ブランドの基準により選定　※1
②レベル B　：基準	レベル A 以外(非対面／ネット)、100 万件以上、レベル A 以外（対面/POS）　※2
③レベル C　：基準	トランザクション件数が年間 100 万件未満
④レベルなし：基準	対面/スタンドアローンの形式については全て対象とする。

※1)　アメリカン・エキスプレス 250 万件以上、JCB100 万件以上、マスター、ビザ 600 万件以上の対象企業のうち、2 ブランド以上の基準に該当した企業を 4 ブランドにより選別する。なお、これらの基準は、既に各国際ブランド会社が設定したレベルを参照し、国際ブランド会社の定めたルールとの整合性を考慮した。

※2)　いずれかの国際ブランド会社において、トランザクション件数が年間 100 万件以上を指す。

［クレジットカード会社］

①レベル A：基準	ACQ またはプロセッシング業務を行っている事業者は全て対象とする。
②レベル B：基準	イシュイングのみで、かつクレジットカード発行枚数が 100 万枚以上の事業者を対象とする。
③レベル C：基準	イシュイングのみで、かつクレジットカード発行枚数が 100 万枚未満の事業者を対象とする。

（４）クレジットカード情報管理の対応（PCI DSS 準拠対応）

「実行計画」では、クレジットカード情報管理のための基準を PCI DSS とし、レベルに応じた PCI DSS 準拠対応を整理した。

①PCI DSS 準拠

「PCI セキュリティ基準審議会」（PCI SSC）が定めた PCI DSS の要件に完全準拠すること。

②センシティブ認証情報非保持

センシティブ認証情報である完全な磁気ストライプデータやチップ上の同等データ、CAV2／CVC2／CVV2／CID、PIN／PIN ブロックの情報をオーソリゼーション後、保持しないこと。

③クレジットカード情報非保持

クレジットカード情報非保持とは、クレジットカード情報の「保存」全てを PCI DSS に準拠したサービスプロバイダー等に委託していて、自社では業務を行っていないことを指す。ただし、単純に情報を「処理」したり、「送信」する場合で、保存しない場合は「保持」に該当しない。「クレジットカード情報非保持」のみでは PCI DSS 準拠にはならないが、PCI DSS 準拠のサービスプロバイダーに「保存」を委託すれば、残存リスクを相当程度縮小することが可能であり、また、一般に PCI DSS 準拠よりも低コストで実現できる。従って、クレジットカード取引件数が少ない形態に限り、本方式を「実行計画」に組み込むことにより、実効性の確保を図る。

（５）PCI DSS 準拠等に関する検証方法

①オンサイトレビュー（レベルＡに適用）

認証セキュリティ評価機関（QSA）による訪問審査。加盟店やサービスプロバイダーへのインタビューやドキュメント確認、サーバーの実機確認など、オンサイトにて監査を実施。

②自己問診（レベルＢに適用）

WEB サーバのセキュリティ診断、アプリケーション、ネットワークのペネトレーションテストなど、国際ブランド会社等がＨＰ上で公開している問診票の質問項目についてチェックし、全ての項目を対応済とするまで繰り返し実施。

③ネットワークスキャン（レベルＡ・Ｂに適用）

脆弱性スキャニングベンダー（ASV）による PCI DSS の脆弱性スキャニングテストの実施。

（６）適用対象毎の対応期限

・各適用対象、取引形態ごとの対応期限と期限設定の考え方については、以下の通りとする。

対象	形態	レベル	PCI DSS 準拠対応	対応期限	期限設定理由
決済代行業者	形態問わず全て	－	PCI DSS 準拠	2013 年 3 月迄	ネット取引の決済代行業者は、責任も重大で且つリスクが高いことから早期に対応が必要であること。また大手同業者の大半準拠済みであることから、準拠が比較的容易で早期対応が可能と判断。
加盟店	非対面/ネット	Ａ	センシティブ認証情報非保持	2012 年 9 月迄	国際ブランド会社では、PCIDSS 準拠以前に、センシティブ認証情報を保持することが禁止されている。また、セキュリティーコードが漏洩した場合の影響の大きさを考慮。
加盟店	非対面/ネット	Ａ	PCI DSS 準拠	2013 年 3 月迄	ネット分野における情報漏洩事案が多いことから、他の形態(POS・ｽﾀﾝﾄﾞｱﾛｰﾝ等)に比べ、早期対応が求められるが、自社での PCI DSS 準拠または決済代行業者などへの業務委託等の対応期間を考慮。
加盟店	対面/ＰＯＳ	Ａ	センシティブ認証情報非保持	2013 年 3 月迄	国際ブランド会社では、PCI DSS 準拠以前に、センシティブ認証情報を保持することが禁止されており、特にフルトラックデータが漏洩した場合の被害の大きさを考慮。但し、委託先（決済代行業者・ＡＳＰ等）が対応する期間を考慮。
加盟店	対面/ＰＯＳ	Ａ	PCI DSS 準拠	2018 年 3 月迄	加盟店自らが PCI DSS に準拠すること、POS システム改修（例えば、センターサーバ化・クラウド化　等)、POS 入替え期間等を考慮。
加盟店	非対面/ネット	Ｂ	センシティブ認証情報非保持	2012 年 9 月迄	国際ブランド会社では、PCIDSS 準拠以前に、センシティブ認証情報を保持することが禁止されている。また、セキュリティーコードが漏洩した場合の影響の大きさを考慮。
加盟店	非対面/ネット	Ｂ	PCI DSS 準拠またはクレジットカード情報非保持	2013 年 3 月迄	ネット分野における情報漏洩事案が多いことから、他の形態(POS・ｽﾀﾝﾄﾞｱﾛｰﾝ等)に比べ、早期対応が求められるが、自社での PCIDSS 準拠または決済代行業者などへの業務委託等の対応期間を考慮。

加盟店	対面/ＰＯＳ	Ｂ	センシティブ認証情報非保持	2013 年 3 月迄	国際ブランド会社では、PCI DSS 準拠以前に、センシティブ認証情報を保持することが禁止されており、特にフルトラックデータが保持されていることによる情報漏洩時の影響が大きいことを考慮。但し、POS システムの対応等を行う期間を考慮。
加盟店	対面/ＰＯＳ	Ｂ	PCI DSS 準拠またはクレジットカード情報非保持	2018 年 3 月迄	加盟店自らが PCI DSS に準拠すること、POS システム改修（例えば、センターサーバ化・クラウド化等）、POS 入替え期間等を考慮。
加盟店	対面/ＰＯＳ	Ｃ	PCI DSS 準拠またはクレジットカード情報非保持	2018 年 3 月迄	PCI DSS未準拠の委託先による準拠対応､PCI DSS準拠先への委託先変更のための期間を考慮。
加盟店	対面/スタンドアローン	－	クレジットカード情報非保持	2013 年 3 月迄	PCI DSS未準拠の委託先による準拠対応､PCI DSS準拠先への委託先変更のための期間を考慮。
クレジットカード会社	ＡＣＱ/プロセッサー	Ａ	PCI DSS 準拠	2018 年 3 月迄	自社クレジットカードのみならずアクアリング業者において、広く他社のクレジットカード情報も保持しており、責任も重大で且つリスクも高いことを考慮。対象となる全てのクレジットカード会社において PCI DSS 準拠の為の期間を考慮。
クレジットカード会社	イシュイングのみ	Ｂ	PCI DSS 準拠	2018 年 3 月迄	自社クレジットカードの情報のみの取扱いであることから、自己リスクの範疇であること、並びに自ら PCI DSS 準拠の為、企業規模等と期間を考慮。
クレジットカード会社	イシュイングのみ	Ｃ	他社クレジットカード情報非保持	2018 年 3 月迄	自社クレジットカードのみの取扱いであることから、自己リスクの範疇であること。また保有情報が少ないこと及びシステム改修等も期間を考慮。

（７）日本におけるクレジットカード情報管理スキーム※〔別添〕参照

以上

日本におけるクレジットカード情報管理　スキーム

対　　象	形　態	基　準 決済代行業者／加盟店の場合⇒年間カード売上件数 カード会社の場合　⇒　発行枚数	レベル	PCIDSS準拠対応	PCIDSS 検証方法
決済代行業者	形態問わず全て	全て	―	① PCIDSS準拠	オンサイトレビュー ネットワークスキャン
加盟店	非対面／ネット	4ブランドにより決定（※3）	A	② センシティブ認証情報（※2）非保持	
				③ PCIDSS準拠	
	対面／POS			④ センシティブ認証情報（※2）非保持	
				⑤ PCIDSS準拠	
	非対面／ネット	レベルA以外	B	⑥ センシティブ認証情報（※2）非保持	自己問診 ネットワークスキャン
				⑦ PCIDSS準拠またはクレジットカード情報非保持	
	対面／POS	100万件以上、レベルA以外（※4）		⑧ センシティブ認証情報（※2）非保持	
				⑨ PCIDSS準拠またはクレジットカード情報非保持	
	対面／POS	100万件未満（※5）	C	⑩ PCIDSS準拠またはクレジットカード情報非保持（※1）	
	対面／スタンドアローン	全て	―	⑪ クレジットカード情報非保持（※1）	
クレジットカード会社	ACQまたはプロセッシング	全て	A	⑫ PCIDSS準拠	オンサイトレビュー ネットワークスキャン
	イシュイングのみ	100万件以上	B	⑬ PCIDSS準拠	自己問診 ネットワークスキャン
		100万件未満	C	⑭ 他社クレジットカード情報非保持（※1）	

対応期限　（年度単位⇒2017年＝2018年3月まで）

2010		2011				2012				2013	2014	2015	2016	2017
Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4					

インフラ整備部会における検討期間

※1　クレジットカード情報非保持とは、クレジットカード情報の「保存」全てをPCIDSSに準拠したサービスプロバイダー等に委託していて、自社では業務を行っていないことを指す（「処理」・「送信」は含まな
※2　センシティブ認証情報とは、完全な磁気ストライプデータ、CAV2／CVC2／CVV2／CID、PIN／PINブロックを指す。
※3　①　VISA　：　600万件以上
②　Master　：　600万件以上
③　JCB　：　100万件以上
④American Exp　：　250万件以上
　　このリストを基に4ブランドにより対象企業を選別する
※4　いずれかのブランドにおいて、100万件以上を指す。
※5　100万件未満の場合については、クレジットカード情報は自社保有せず、他社で保有することを推奨する。

【スケジュール等設定の理由】

① ネット取引の決済代行業者は、責任も重大で且つリスクが高いことから早期に対応が必要であること。また大手同業者の大半準拠済みであることから、準拠が比較的容易で早期対応が可能と判断。
② 国際ブランド会社では、PCIDSS準拠以前に、センシティブ認証情報を保持することが禁止されており、特にフルトラックデータが保持されていることによる情報漏洩時の影響が大きいことを考慮。但し、POSシステムの対応等を行う期間を考慮。
③ ネット分野における情報漏洩事案が多いことから、他の形態(POS・ｽﾀﾝﾄﾞｱﾛｰﾝ等)に比べ、早期対応が求められるが、自社でのPCIDSS準拠または決済代行業者などへの業務委託等の対応期間を考慮.
④ 国際ブランド会社では、PCIDSS準拠以前に、センシティブ認証情報を保持することが禁止されており、特にフルトラックデータが漏洩した場合の被害の大きさを考慮。但し、委託先（決済代行業者・ASP等）が対応する期間を考慮。
⑤ 加盟店自らがPCIDSSに準拠すること、POSシステム改修（例えば、センターサーバ化・クラウド化　等）、POS入替え期間等を考慮。
⑥ 国際ブランド会社では、PCIDSS準拠以前に、センシティブ認証情報を保持することが禁止されている。また、セキュリティコードが漏洩した場合の影響の大きさを考慮。
⑦ ネット分野における情報漏洩事案が多いことから、他の形態(POS・ｽﾀﾝﾄﾞｱﾛｰﾝ等)に比べ、早期対応が求められるが、自社でのPCIDSS準拠または決済代行業者などへの業務委託等の対応期間を考慮。
⑧ 国際ブランド会社では、PCIDSS準拠以前に、センシティブ認証情報を保持することが禁止されており、特にフルトラックデータが保持されていることによる情報漏洩時の影響が大きいことを考慮。但し、POSシステムの対応等を行う期間を考慮。
⑨ 加盟店自らがPCIDSSに準拠すること、POSシステム改修（例えば、センターサーバ化・クラウド化　等）、POS入替え期間等を考慮。
⑩ PCIDSS未準拠の委託先による準拠対応、PCIDSS準拠先への委託先変更のための期間を考慮。
⑪ PCIDSS未準拠の委託先による準拠対応、PCIDSS準拠先への委託先変更のための期間を考慮。
⑫ 自社クレジットカードのみならずアクアリング業者において、広く他社のクレジットカード情報も保持しており、責任も重大で且つリスクも高いことを考慮。対象となる全てのクレジットカード会社においてPCIDSS準拠の為の期間を考慮。
⑬ 自社クレジットカードの情報のみの取扱いであることから、自己リスクの範疇であること、並びに自らPCIDSS準拠の為、企業規模等と期間を考慮。
⑭ 自社クレジットカードのみの取扱いであることから、自己リスクの範疇であること。また保有情報が少ないこと及びシステム改修等も期間を考慮。