別紙 「PCI DSS準拠にかかる基準及び検証方法　スキーム」

対　　象	形　　態	基　　準 加盟店は年間カード売上件数	レベル		クレジットカード情報管理の対応	PCI DSS 検証方法	対応期限（単位：年度）		
							2017	2018	2019
加盟店	非対面 ／EC・EC以外	4ブランドにより決定（※2）	A	①	クレジットカード情報非保持（※1） 又は PCI DSS準拠	オンサイトレビュー 又は 自己問診			
	対面／POS			②					
	非対面 ／EC・EC以外	100万件以上、レベルA以外（※3）	B	③		自己問診（※5）			
	対面／POS	100万件以上、レベルA以外（※3）		④					
	非対面 ／EC・EC以外	100万件未満（※4）	C	⑤					
	対面／POS	100万件未満（※4）		⑤					
	対面／スタンドアローン	全て	―	–	クレジットカード情報非保持対応済み（※1）				
クレジットカード会社	アクワイアラー	国際ブランドから直接且つ定期的にカード情報保護にかかる取組の状況について報告を求められている先	A	⑥	PCI DSS準拠	オンサイトレビュー			
		レベルA以外	B	⑥		自己問診（※5）			
	プロセシング業者	全て	A	⑥		オンサイトレビュー			
	イシュアー	全て	B	⑦		自己問診（※5）			
PSP	インターネット上の取引においてEC加盟店にクレジットカード決済スキームを自ら提供し、カード情報を処理する事業者	全て	―	⑧	PCI DSS準拠	オンサイトレビュー			

※1　クレジットカード情報非保持とは、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』しないことをいう。なお、対面POS加盟店においては非保持同等/相当の評価も同様。

※2　① VISA　：600万件以上
② Mastercard　：600万件以上
③ JCB　：100万件以上
④American Express　：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

※3　いずれかのブランドにおいて、100万件以上を指す。

※4　いずれのブランドにおいても、100万件未満を指す。

※5　オンサイトレビューによる準拠を妨げるものではない。

【対応期限等設定の理由】 ※実行計画2017の対応期限に合わせた。

① 非対面取引における情報漏えい事案が多いことから、他の形態(POS・スタンドアローン等)に比べ、早期対応が求められるが、自社でのPCI DSS準拠又はPSPなどへの業務委託等の対応期間を考慮。

② 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。

③ 非対面取引における情報漏えい事案が多いことから、他の形態(POS・スタンドアローン等)に比べ、早期対応が求められるが、自社でのPCI DSS準拠又はPSPなどへの業務委託等の対応期間を考慮。

④ 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。

⑤ PCI DSS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。

⑥ 自社クレジットカードのみならずアクワイアリングにおいて、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。プロセシング業務事業者も同様。

⑦ 自社クレジットカードの情報のみの取扱いで自己リスクの範疇であること又は国際ブランドから直接管理されない。企業規模等と期間を考慮。

⑧ ネット取引のPSP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。