電子決済等代行業者に求める基準

通番	区分	項目
（1）業務に関して取得する利用者に関する情報の適正な取扱い及び安全管理のために行うべき措置		
1	経営陣の関与	経営陣により情報セキュリティ管理態勢が整備されている
2	情報・セキュリティ管理態勢	セキュリティ管理責任の所在と対象範囲を明確にする
3		セキュリティ管理ルールを整備する
4		セキュリティ管理態勢の定着を図る
5		役職員に情報管理方法を周知し、セキュリティに対するモラルを高める
6		情報資産の取扱態勢を確認する
7		役職員との情報資産の非開示契約等の締結・就業規則等における安全管理措置を整備する
8		サービスの解約時およびシステムの廃棄にあたっては機器等から情報漏洩が生じないように防止策が講じられている
9		セキュリティ不祥事案の発生に対して、振り返りと対策を行う体制を確立する
10		セキュリティ管理態勢が整備されていることを客観的に証明する
11		不正アクセス発生を想定した対応準備ができている
12	外部委託管理	システム運用における安全性を確保する
13		外部委託事業者における委託業務の実施内容に問題がないことを確認する
14		外部委託事業者における委託業務の実施状況を確認する
15	銀行・API接続先の協力体制	セキュリティ対策の高度化を図る
16		利用者からの照会対応を的確に行う
17		利用者からの相談等対応を的確に行う
18		利用者の被害拡大を未然に防止する
19		利用者の補償対応を的確に行う
20		利用者向けの補償対応窓口を的確に運営する
21	コンピュータ設備管理	コンピュータ設備面での情報漏洩対策を行う
22		サーバルームに不正な人物の入室を防ぎ、セキュアなネットワークへの侵入や、業務情報の漏洩を防ぐ
23		政治状況、法規制の変化に対応しやすい状況下におく
24	オフィス設備管理	執務室に不正な人物の入室を防ぎ、セキュアなネットワークへの侵入や、業務情報の漏洩を防ぐ
25		重要情報にアクセスできる人間を制限する
26		内部関係者による情報漏洩の出口対策を行う
27		ウィルス感染によるシステム侵入等の攻撃を防ぐ

通番		区分	項目
	28	システム開発・運用管理	システムアクセスできる担当者の権限を適切に設定して、不正な作業を防ぐ
	29		システムアクセスに際しての特権権限の付与を可能な限り限定して、不正な作業、誤った作業の発生を防ぐ
	30		システムアクセス時の認証を適切に行い、不正なシステムアクセスを防ぐ
	31		システムアクセスとその作業についてのログを保管し、有事の際に調査が可能なようにする
	32		担当者単独のシステムアクセスの発生を抑止し、不正な作業を防ぐ
	33		システム変更の単独作業を抑止し、不正なシステム変更を防ぐ
	34		システム変更時に著しく品質が低下しないような対策を行う
	35		システム変更に伴う脆弱性の埋め込みや、利用技術に対する脆弱性発覚に対する対策を行う
	36		システムに対する外部からの不正な通信を検知する
	37		システムに対する外部からの不正な通信を防ぐ
	38		システムで利用する技術で発覚する脆弱性に対する対策を行う
	39		機密情報へのアクセスを制限して、不正な作業、誤った作業の発生を防ぐ
	40		問題発生時の原因・経緯を特定可能な状態にして、不正アクセスを抑止する
	41		持ち出された機密情報を適切に管理する
	42	サービスシステムのセキュリティ機能	データの種類・内容に応じた管理策を実施する
	43		機密性の高いデータの漏洩対策がとられている
	44		情報喪失・破損からの復旧を可能とする
	45		必要な認証機能を適切に把握できている
	46		ユーザを保護する適切な認証機能を見直す
	47		ユーザを適切に保護する認証機能を提供する
	48		スマートデバイス利用時の顧客保護として、動作するアプリケーションに対して、不正な偽アプリケーションが出回らないよう、必要な対策を実施する
	49		不正アクセス時の被害拡大を最小限に止める
	50		不正アクセス発生時に追跡調査を実施する
	51	APIセキュリティ機能	認証に関わる機密情報の漏洩対策を行う
	52		APIの想定外利用回避のための原則を把握する
	53		API利用実績の追跡調査を可能にする
	54	API利用セキュリティ	API利用に関わる利用者説明責任を果たす（利用者の誤認防止）
	55		API利用に関わる利用者説明責任を果たす（利用者への説明）
（2）業務の執行が法令に適合することを確保するために整備すべき体制			
	1	事業継続管理（BCP）	事業継続管理（BCP）態勢を確立する
	2	反社会的勢力の排除	反社会的勢力に該当しないことを確約する