クレジット加盟店向け
“情報セキュリティのためのガイド”
（PCI DSS／ISMS 準拠のためのガイド）

2009 年 10 月

2011 年 1 月改訂

クレジット産業向け ISMS ガイド検討作業部会

1）加盟店様へのメッセージ －何故、情報セキュリティが必要なのかー

クレジットカードを取り扱う加盟店の皆様は、毎日大量の情報を取得・保有・利用されています。その中には特に取扱いに配慮が必要である情報（顧客情報、クレジットカード情報、購買情報等）も含まれるため、情報の保護について日常的に気をつける必要があります。

情報の保護に関しては、情報システム担当者による技術的な側面に加え、経営者主導により組織全体で対策を施す必要があります。

お客様が安心してクレジット取引を行えるように、クレジットカード会社、ネットワーク情報処理会社等だけでなく、加盟店様も含めたクレジット産業に携わる皆様で取組むことが重要となります。

加盟店様が取り扱う支払いカードは、日本だけでなく国際ブランドで発行されたカードも対象となりますので、国際的な基準に従うことになります。国際的な基準には、PCI DSS と ISO/IEC 27001※があります。

※ISO/IEC 27001 については、以下 ISMS 認証基準と記述する。

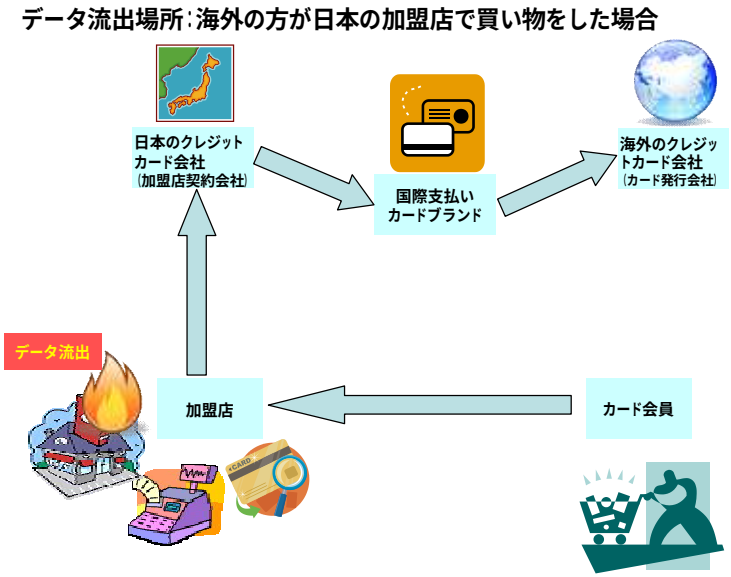

図 1．加盟店様、カード会員、カード発行会社、加盟店契約会社の関係

2）両規格の概要、及び両規格を満たすことのメリット

①両規格の概要

[PCI DSS とは]

支払いカード産業において個人情報を含むアカウント情報（カード会員情報）を保護するために PCI SSC※が定めた国際的な基準です。

安全なネットワークの構築、カード会員データの保護やアクセス制御手法の導入などの技術的な要件が規定されており、例えば、「重要なセキュリティパッチは、リリース後 1 カ月以内にインストールする。」や「パスワードに 7 文字以上が含まれることを要求する。」など具体的な設定まで明記されています。

PCI SSC※（Payment Card Industry Security Standards Council）とは、PCI DSS の策定・維持管理・普及、及び認定スキャニングベンダー（ASV：Approved Scanning Vendor）・セキュリティ評価機関（QSA：Qualified Security Assessor）の認定等を行う組織です。

2010 年 10 月 28 日に PCI DSS が Version 1.2.1 から Version 2.0 へと改訂されました。PCIDSS Version 2.0 は 2011 年 1 月より有効となりました。また、PCI DSS Version 1.2.1 の有効期限は、2011 年 12 月末までです。PCI DSS の次の改訂は、2013 年を予定しています。

[ISMS 認証基準とは]

情報全般を保護するためのマネジメントシステムを確立、導入、運用、監視、レビュー、維持及び、改善するための ISO/IEC が定めた国際的な基準です。

情報全般とは、個人情報はもちろんのこと、営業機密情報、パートナーとの共有情報、企業戦略情報などを含みます。このような情報全般に対し、情報セキュリティに対する方針を確立し、情報セキュリティ対策を実施し、日々の継続的な改善によって管理していく仕組みに関する要求事項が明記されています。この仕組みを運用していく上では、経営陣の関与が重要となり、必要に応じて適切な資源（人、資金など）を確保することが求められます。

また、本認証基準の要求事項を満たすために、実施することが望ましい管理策を体系化した「情報セキュリティマネジメントの実践のための規範」として、ISO/IEC 27002 も ISO/IEC が定めた国際的なガイドラインです。

②両規格を満たすことのメリット

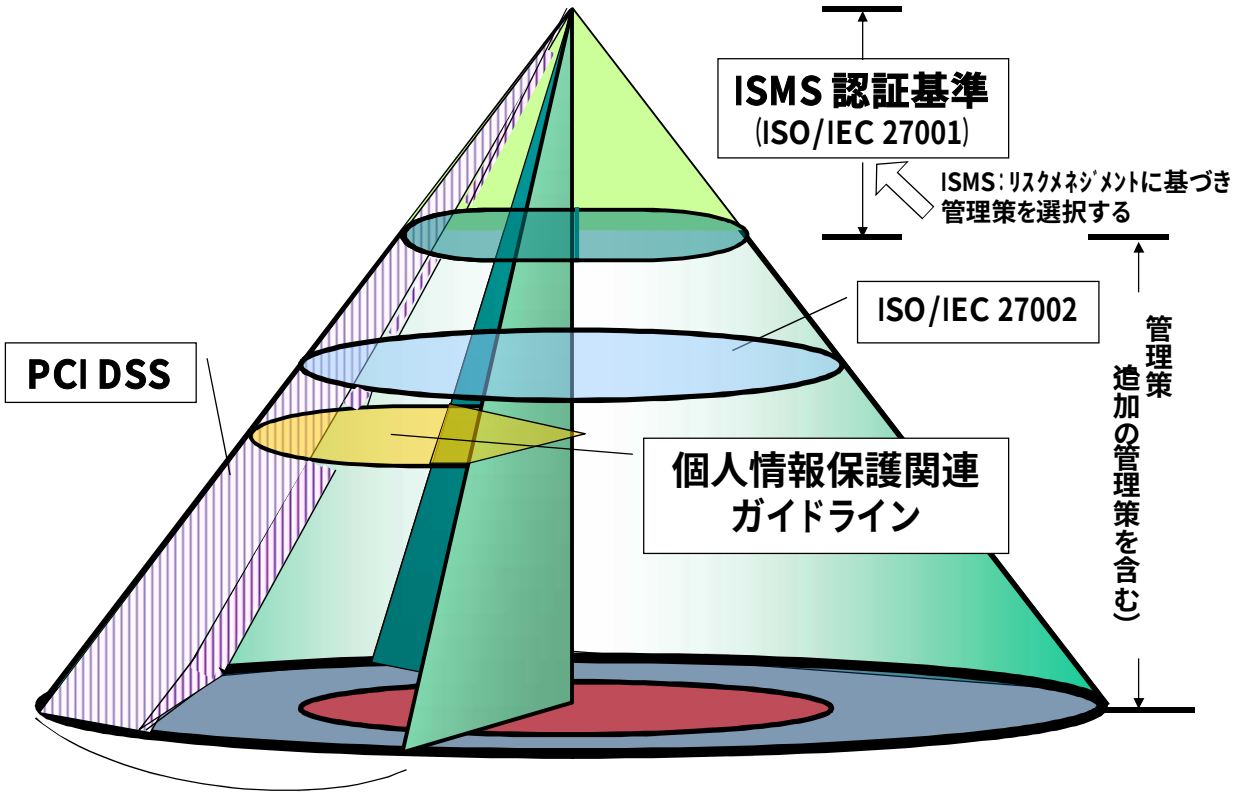

図 2.　PCI DSS と ISMS との関係イメージ図

ISMS 認証基準と PCI DSS は共に情報セキュリティに関する基準です。ISMS 認証基準は経営的観点で企業・組織内の情報全般に対する情報セキュリティを、PDCA サイクルを通じ最適化することを目的としています。但し、リスクマネジメントに基づく対策を要求していることから、必ずしも具体的な対策を規定したものではありません。一方、PCI DSS はカード会員情報を保護するためのより具体的な対策を規定していますが、マネジメントシステムの仕組みについては詳細までは規定していません。従って、両者を順守／取得することにより、クレジットカード会員情報を継続的に保護することが可能となります。

また、P(ISMS の確立)、D(ISMS の導入・運用)、C(ISMS の監視・レビュー)、A(ISMS の維持・改善)のプロセスから構成される ISMS のフレームワークがあることによって、PCI DSS の Version が変更された場合を含む、管理策等の変更への対応も容易になるといえます。

なお、ISMS・PCI DSS 共通の審査機関（認証機関）を利用すれば、並行して効率よく審査を受けることができます。

3）PCI DSS に準拠するために何からはじめたらよいか？

まず、PCI SSC 作成の自己問診票を使って特に下記の点に注意してチェックを行い、当てはまるものがあれば必要な措置を行ってください。自己問診票の URL は、https://www.pcisecuritystandards.org/merchants/self_assessment_form.php です。日本語は、http://ja.pcisecuritystandards.org/minisite/en/pci-dss-supporting-docs.php を参照してください。

１．センシティブ認証データを保管していますか？

センシティブ認証データの保管は、禁じられています。もし保管しているようだったら、直ちに保管しないような措置を取ってください。次表内の”２．センシティブ認証データ”を参照してください。

２．クレジットカード信用照会端末のソフトウェアはカード会員データを自動的に保管するような機能を持っていますか？

もしその機能があるならば直ちに保管機能を削除してください。ご不明な場合は、端末設置会社か端末メーカーに連絡してカード会員データを保管する機能があるのか否か検査してもらってください。

３．カード会員データを保管していますか？

保管しているか否か不明な場合は、保管の有無を検証してください。
もし保管しているとしたら、本当に保管する必要があるのか再度検証してください。保管する必要のないものは直ちに保管しないような措置を取ってください。
カード会員番号を保管している場合、暗号化されていますか？
暗号化されていない場合、暗号化するか又は暗号化に代替する措置をとってください。
次表内の”１．カード会員データ”を参照してください。

なお、印刷されたもの、データとして処理・保管されているものなど情報の形態を問わず、保護されるべき対象となります。（PCI DSS 要件３）

		データ要素	保管可否	データ保護	暗号化
アカウントデータ	１．カード会員データ	カード会員番号	可	必須	必須（注２）
		カード会員名	可	必須（注１）	任意
		有効期限	可	必須（注１）	任意
		サービスコード	可	必須（注１）	任意
	２．センシティブ認証データ（Sensitive Authentication Data）	磁気ストライプ全情報	不可	－	－
		セキュリティコード（CAV2/CVC2/CVV2/CID）	不可	－	－
		暗証番号（PIN）	不可	－	－

（注１）このデータ要素はカード会員番号と関連付けて保管する場合には保護が必要です。
（注２）暗号化するか又は暗号化に代替する措置が必要です。

具体的な要件については、「４．PCI DSS の１２要件の内容について」を参照してください。
上記で不明な点があれば、専門家である以下の認定審査機関に相談してください。

■認定スキャニングベンダー（ASV）及びセキュリティ評価機関（QSA）の一覧表

ASV　https://www.pcisecuritystandards.org/approved_companies_providers/approved_scanning_vendors.php
補足：上記ページのプルダウンメニューから「Locations Served」及び「Japan」を選択し「Search」ボタンをクリックすると、日本でサービスを提供している ASV を検索することができます。

QSA　https://www.pcisecuritystandards.org/approved_companies_providers/qsa_companies.php
補足：上記ページのプルダウンメニューから「Servicing Market」及び「Japan」を選択し「Search」ボタンをクリックすると、日本でサービスを提供している QSA を検索することができます。

4）PCI DSS の１２要件の内容について

PCI DSS は、国際支払いカードブランドのカード会員データを保護するための１２の要件で構成されており、加盟店、プロセシング会社、インターネット決済サービス事業者など、カード会員データの処理、保管、伝送を行っている全ての企業に適用されます。

	PCI DSS V2.0 の１２要件
安全なネットワークの構築と維持	１．カード会員データを保護するために、ファイアウォールをインストールして構成を維持する ２．システムパスワードおよび他のセキュリティパラメータにベンダ提供のデフォルト値を使用しない
カード会員データの保護	３．保存されるカード会員データを保護する ４．オープンな公共ネットワーク経由でカード会員データを伝送する場合、暗号化する
脆弱点管理プログラムの整備	５．アンチウィルスソフトウェアまたはプログラムを使用し、定期的に更新する ６．安全性の高いシステムとアプリケーションを開発し、保守する
強固なアクセス制御手法の導入	７．カード会員データへのアクセスを、業務上必要な範囲内に制限する ８．コンピュータにアクセスできる各ユーザに一意の ID を割り当てる ９．カード会員データへの物理アクセスを制限する
ネットワークの定期的な監視およびテスト	１０．ネットワークリソースおよびカード会員データへのすべてのアクセスを追跡および監視する １１．セキュリティシステムおよびプロセスを定期的にテストする
情報セキュリティポリシーの整備	１２．すべての担当者の情報セキュリティポリシーを整備する

PCI DSS Verion 1.2.1 と Version 2.0 との変更点について：
- 全体的には、要求事項を明確化したことが主な変更点として挙げられます。
- その他、変更の詳細については、PCI SSC の WEB サイトを参照ください。
  URL https://www.pcisecuritystandards.org/security_standards/documents.php
  文書名：PCI DSS Summary of Changes Version 1.2.1 to 2.0

PCI DSS の URL
https://www.pcisecuritystandards.org/security_standards/documents.php
上記 WEB ページから PCI DSS Version 2.0(日本語の対訳版)等が、ダウンロードできます。

5）PCI DSS の訪問調査でよく発見される技術的な問題点と一般的な対処方法について

１．データベース内のカード会員データが安全な形で保管されていない

（対処方法）
業務上、「不必要なカード会員データは持たないこと」あるいは「必要なカード会員データの場合は、最小限の期間のみ保持し、期限終了時には確実に削除すること」であるが、即座に削除できない時は適切な鍵管理プロセスを用いた「暗号化」などを施して判読不能な状態にする

２．センシティブ認証データが保管されている

（対処方法）
センシティブ認証データ（磁気ストライプ全情報／セキュリティコード／暗証番号）はオーソリゼーション処理が完了した時点で確実に破棄する

３．カード会員データを伝送、処理、保管するサーバや機器のログが管理されていない

（対処方法）
カード会員データを伝送、処理、保管するサーバや機器のログを取得するよう設定し、取得したログはログ収集サーバに伝送、保管する。ログ収集時に、カード会員番号が平文で記録されないよう、記録するカード会員情報の取捨選択、暗号化やトランケーションの使用もあわせて検討、実装する必要がある。ログ収集サーバでは、問題発生時に迅速に確認できるようにするため、可能な限り3ヶ月程度保持し、それ以前の古いログはメディアなどに記録して1年以上保管する。このメディアは、アクセスする必要のある限られたユーザのみアクセス可能となる、施錠された場所に保管する

４．外部から直接アクセスできる Web サーバにアプリケーション・サーバが共存している

（対処方法）
Webサーバとアプリケーション・サーバを分離しDMZにWebサーバを配置し、アプリケーション・サーバ（データベース等）は外部（インターネット）から直接アクセスすることのできない内部のセグメントに配置すること。その場合、インターネットとDMZおよびDMZと内部における境界にファイアウォール等を設置し、必要最低限の通信のみ許可するようにアクセス制御を施す

５．ファイアウォールの定期的なチェックが実施されていない

（対処方法）
ファイアウォールのアクセス制御のルールを定期的に見直すためにポリシー・手順を策定・実施する

6）参考情報

1．両制度のしくみ

（1）PCI DSS の制度（プログラム）

PCI DSS の制度（プログラム）は、各国際支払いカードブランドが推進しています。各推進プログラムは次の通りですが、支払カードデータセキュリティ基準は PCI DSS で共通です。

ｱﾒﾘｶﾝ･ｴｷｽﾌﾟﾚｽ	データセキュリティ運営方針（Data Security Operating Policy）
JCB	JCB Data Security Program
MasterCard	SDP（Site Data Protection）プログラム
Visa	AIS（Account Information Security）プログラム

なお、各プログラムの詳細は、”6)参考情報　2．PCI　DSS 関連情報”をご参照ください。

加盟店様は、PCI SSC 認定セキュリティ評価機関やスキャニングベンダーとサービス提供についての契約を結び、検証を受けることによって自らのセキュリティレベルの現状が把握できます。もし PCI DSS 基準を満たさない項目がある場合には、加盟店様は改善プランを作成し、必要な資源を使って改善プランを実施する必要があります。

各国際支払いカードブランドは、加盟店様が契約するカード会社を通して検証結果の報告と証明書の提出を受け、加盟店様のセキュリティレベルを確認します。詳細は図３の PCI DSS 実施の流れをご参照ください。

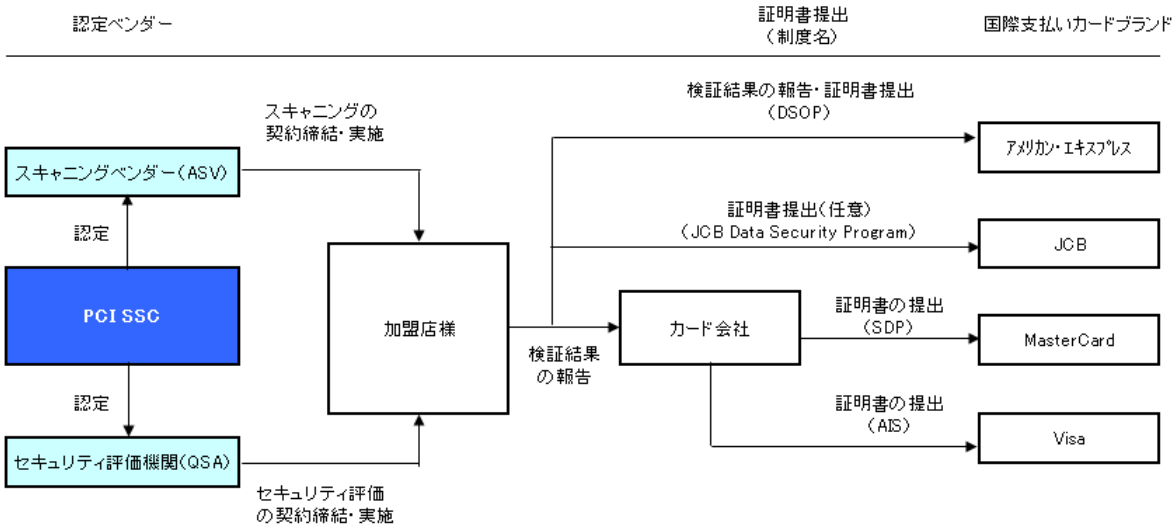

図３　PCI DSS 実施の流れ（QSA/ASV 認定と証明書提出）

（2）ISMS の制度

ISMS 制度の認証基準は、国際規格である ISO/IEC 27001（JIS Q 27001）です。ISO 規格の第三者認証制度については国際的な認定・認証の仕組みがあり、（財）日本情報処理開発協会（JIPDEC）では、この仕組みに基づいて ISMS 適合性評価制度（ISMS 制度）を運営しています。この仕組みに従い、ISMS 制度の組織構成は、認証希望組織が認証基準に適合しているかを審査し認証登録する「認証機関」、審査員の資格を評価登録する「要員認証機関」、及びこれらの各機関がその業務を行う能力を備えているかを審査する「認定機関」から成っています。詳細は、図４をご参照ください。

ISMS 制度では、認証取得を希望する組織は、JIPDEC によって認定を受けた認証機関に申請し、審査・認証を受けます。組織は、ISMS 認証を取得することによって、情報セキュリティ管理体制の整備や社内組織の体質強化だけでなく、対外的な情報セキュリティの信頼性の向上にもつながります。

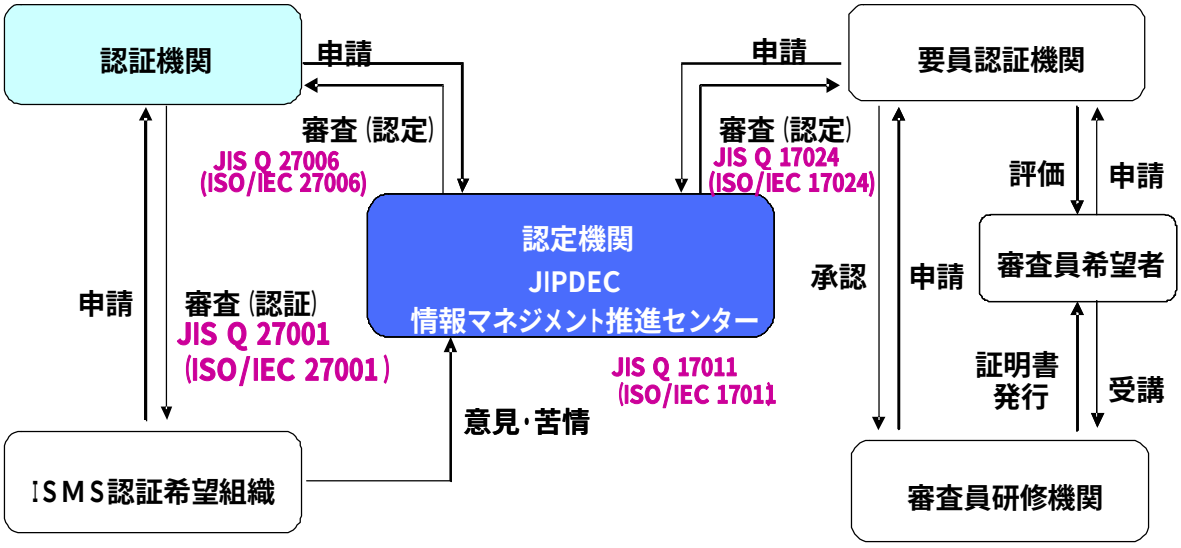

図４　ISMS 適合性評価制度の仕組み

2．PCI DSS 関連情報

■PCI SSC の URL
https://www.pcisecuritystandards.org/
■認定された ISMS 認証機関一覧表
http://www.isms.jipdec.or.jp/lst/isr/index.html
■PCI DSS と各国際支払カードブランドのプログラムの詳細

アメリカン・エキスプレス
http://www.americanexpress.com/datasecurity

JCB
http://www.jcb-global.com/pci/index.html

MasterCard
http://www.mastercard.com/jp/merchant/jp/security/what_can_do/SDP/merchant/index.html

Visa
http://www.visa-asia.com/ap/jp/merchants/riskmgmt/ais.shtml

■PCI DSS と各国際支払カードブランドのプログラムの遵守企業一覧

MasterCard
http://www.mastercard.com/us/sdp/serviceproviders/compliant_serviceprovider.html

Visa
http://www.visa-asia.com/ap/jp/merchants/riskmgmt/ais_companylist.shtml
http://www.visa-asia.com/ap/jp/merchants/riskmgmt/vrsp_index.shtml
※ここに記載されている情報は、掲載を希望された加盟店、サービスプロバイダに限定されています。

3．ISMS の詳細

■ISMS 適合性評価制度全般の URL
http://www.isms.jipdec.or.jp/isms.html
■情報セキュリティマネジメントシステム(ISMS)適合性評価制度の概要
http://www.isms.jipdec.or.jp/about/index.html
■ISMS 認証取得に関する文書
http://www.isms.jipdec.or.jp/std/index.html
■クレジット産業向け　“PCI DSS“ / ISMS ユーザーズガイド
http://www.isms.jipdec.or.jp/doc/JIP-ISMS116-30.pdf
■法規適合性に関する ISMS ユーザーズガイド
http://www.isms.jipdec.or.jp/doc/JIP-ISMS115-20.pdf

4．個人情報保護法関連

■個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン

「個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン」の別添でも、クレジットカード情報等の取扱いについては、以下の事項を実施することが望ましいとしています。

①クレジットカード情報等について特に講じることが望ましい安全管理措置の実施

- クレジットカード情報等について、利用目的の達成に必要最小限の範囲の保存期間を設定し、保存場所を限定し、保存期間経過後適切かつ速やかに破棄
- クレジット売上伝票に記載されるクレジットカード番号を一部非表示化
- クレジットカード読取端末からのクレジットカード情報等の漏えい防止措置を実施（例えば、クレジットカード読取端末にはスキミング防止のためのセキュリティ機能（漏えい防止措置等）を搭載する等）
- クレジットカード情報等を移送・送信する際に最良の技術的方法を採用
- 他のクレジットカード販売関係事業者等に対してクレジットカード情報等が含まれる個人情報データベース等へのアクセスを許容している場合においてアクセス監視等のモニタリングを実施

②クレジットカード情報等の保護に関する規定を含む契約の締結

- クレジットカード情報等を取り扱う業務に係る契約の締結の際に、クレジットカード情報等の保護に関する規定を設定（例えば、クレジットカード情報等の保護の観点から情報提供を求める旨の規定や、クレジットカード情報等の取扱いが不適切なことが明らかな場合において当該情報を取り扱う業務の是正を求めることや当該業務に係る契約を解除する旨の規定を設定）

③クレジットカード情報等を直接取得する場合のクレジットカード情報等の提供先名等の通知又は公表

- インターネット取引においてクレジットカード情報等を本人から直接取得するなど、クレジットカード情報等を本人から直接取得する場合、法第１８条各項の規定に基づき、本人に利用目的を明示又は通知若しくは公表するほか、クレジットカード情報等の取得者名、提供先名、保存期間等を通知又は公表

「個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン」については、以下の URL をご参照ください。

http://www.meti.go.jp/policy/it_policy/privacy/kaisei-guideline.pdf

■経済産業分野のうち信用分野における個人情報保護ガイドライン

「経済産業分野のうち信用分野における個人情報保護ガイドライン」では、「与信事業者」を、割賦販売、ローン提携販売、割賦購入あっせんその他の物品又は役務の取引に係る信用供与を業として行う者と定義づけ、それらを対象に個人データの安全管理措置等を規定しています。

与信事業者

「与信事業者」とは、個人情報取扱事業者のうち、個人の支払能力に関する情報を用いて割賦販売法（昭和３６年法律第１５９号）第２条第１項に規定する割賦販売、同条第２項に規定するローン提携販売、同条第３項に規定する包括信用購入あっせん、同条第４項に規定する個別信用購入あっせんその他の物品又は役務の取引に係る信用供与を業として行う者をいう。

安全管理措置（法第２０条関連）

与信事業者等は、その取り扱う個人データの漏えい、滅失又はき損の防止その他の個人データの安全管理のため、組織的、人的、物理的及び技術的な安全管理措置を講じなければならない（2-1-4.※電話帳、カーナビゲーションシステム等の取扱いについての場合を除く。）。その際、本人の個人データが漏えい、滅失又はき損等をした場合に本人が被る権利利益の侵害の大きさを考慮し、事業の性質及び個人データの取扱状況等に起因するリスクに応じ、必要かつ適切な措置を講じるものとする。なお、その際には、個人データを記録した媒体の性質に応じた安全管理措置を講じることとする。
また、個人情報の記載されたクレジットカードの申込用紙その他の個人情報データベース等を構成する前の入力帳票についても、個人データに相当する扱いとすることとする。（以下3)〔従業者の監督〕、4)〔委託先の監督〕において同じ。）

「経済産業分野のうち信用分野における個人情報保護ガイドライン」については、以下のURLをご参照ください。

http://www.meti.go.jp/policy/economy/consumer/credit/pdf/091020shinyougl.pdf

５．割賦販売法関連

■　特定商取引に関する法律及び割賦販売法の一部を改正する法律について

個別の契約ごとに与信を行う個別クレジットを利用した訪問販売などによる被害が深刻化し、中でも、悪質な勧誘販売行為を助長するクレジット会社の不適正与信あるいは過剰与信の事例が目立っています。また、インターネット通信販売などの新しい分野においては、クレジットカード情報の漏えいなど、多くの消費者被害が発生しています。こうした状況に対処するため、規制の抜け穴の解消、訪問販売規制、クレジット規制、インターネット取引等の規制の強化などを内容とする「特定商取引に関する法律及び割賦販売法の一部を改正する法律」が策定されました。

クレジットカード番号等の適切な管理等

六　クレジットカード番号等の適切な管理等
包括信用購入あっせん業者等は、その取り扱うクレジットカード番号等の漏えい、滅失又はき損の防止その他のクレジットカード番号等の適切な管理のために必要な措置を講じなければならないものとすること。（第三十五条の十六及び第三十五条の十七関係）

「特定商取引に関する法律及び割賦販売法の一部を改正する法律」については、以下の URL をご参照ください。

http://www.no-trouble.jp/page?type=gallery&id=1238061611899

「特定商取引に関する法律及び割賦販売法の一部を改正する法律 新旧対照条文」については、以下の URL をご参照ください。

http://www.no-trouble.jp/page?type=gallery&id=1238123546891

「改訂のポイント」については、以下の URL をご参照ください。

http://www.no-trouble.jp/page?id=1238059308632

「特定商取引に関する法律及び割賦販売法の一部を改正する法律の施行期日を定める政令」については、以下の URL をご参照ください。

http://www.meti.go.jp/press/20090616001/20090616001.html

「割賦販売法施行規則の一部を改正する省令」については、以下の URL をご参照ください。

http://www.meti.go.jp/press/20090626001/20090626001.html

本ガイドに関するお問合せ先

（財）日本情報処理開発協会　情報マネジメント推進センター

http://www.jipdec.or.jp/ask/toiawase8/

お問合せ内容 の記入欄の冒頭に、「加盟店向け“PCI DSS／ISMS 準拠のためのガイド”について」と明記したうえで、お問合わせ内容を記載してください。

免責事項

本ガイドの内容や情報は、明示または黙示を問わず何らかの保証を伴うことなく現存するままの状態で提供されるものです。　（財）日本情報処理開発協会　情報マネジメント推進センターでは、今後も本ガイドに掲載する情報（URL 等の情報を含む）について、充分注意・確認をした上で掲載することに努めますが、閲覧時点で内容が変更（リンク先サイトのリンク切れを含む）されている場合もありますので予めご了承ください。

また、適時情報を最新にする目的等で、本ガイドの内容や URL 等は予告なく変更・改訂される場合がありますので予めご了承ください。

クレジット産業向け ISMS ガイド検討作業部会メンバー

本ガイドは、以下のメンバーによって作成されました。

氏名	所属
荒川　明良	マスターカード・ジャパン㈱
五十嵐　浩志	ビザ・ワールドワイド・ジャパン㈱
石渡　洋平	マスターカード・ジャパン㈱
井上　憲司	㈱ジェーシービー
井原　亮二	ビザ・ワールドワイド・ジャパン㈱
大沼　靖秀	有限責任あずさ監査法人
駒瀬　彰彦	㈱アズジェント
坂崎　守寿	アメリカン・エキスプレス・インターナショナル，Inc.
日辻　治彦	㈱ジェーシービー
松尾　正浩	㈱三菱総合研究所
丸山　満彦	デロイトトーマツリスクサービス㈱

（敬称略･五十音順）

オブザーバー
経済産業省 商務情報政策局 取引信用課
経済産業省 商務情報政策局 情報セキュリティ政策室

財団法人 日本情報処理開発協会
情報マネジメント推進センター
〒105-0011 東京都港区芝公園3丁目5番8号 機械振興会館内
TEL 03-3432-9386　FAX 03-3432-6200
URL http://www.jipdec.or.jp/
http://www.isms.jipdec.or.jp/