クレジット産業向け
“ＰＣＩ ＤＳＳ”／ＩＳＭＳユーザーズガイド

ISMS：Information Security Management System
情報セキュリティマネジメントシステム

PCI DSS：Payment Card Industry Data Security Standard
PCI データセキュリティ基準

平成２１年3月３１日

財団法人　日本情報処理開発協会

はじめに

「情報」は、個人や組織が活動するために貴重な資産であることから、情報を安全に管理する事の重要性は、情報技術の進展に伴って益々高まっています。情報をコンピュータで取り扱うか否かにかかわらず、自らが保有する情報を安全に管理する事は、当然の責務である事は論を待ちません。また、特に企業などにおいては、多数の関係者がそうした情報に関与するため、安全管理は、組織として行わなければ効果的ではありません。情報セキュリティマネジメントを怠ると、その被害は自らに及ぶのみならず、他者にも及ぶことが考えられます。

最近では個人情報やクレジットカード情報の漏洩・流出事件が相次いで発生しており、その価値の高さゆえ､漏洩事件は経営的な問題として大きな影響を与えています｡2005 年 4 月の個人情報保護法の完全施行に伴い、情報とりわけ個人情報が重要な経営資源となっている組織においては、これを適切に保護しなければならなくなりました。また、個人情報保護法だけ順守していればよいという姿勢ではなく、企業にとって重要な情報は、すべて適切に管理しなくてはならないのです。さらには、個人情報保護法の全面施行により、個人情報漏洩を起こした企業・組織には罰則を適用されることもあり得ます。

このようなことから、個人情報を保有している企業にとっては、個人情報保護に対応する社内体制を整備し、個人情報保護ガイドラインに従って個人情報を適正に取扱うためのシステムを構築維持することが重要な経営課題となっています。

わが国においては、クレジット分野における個人情報保護に関するガイドラインとして「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」が策定され、改正されています（策定：平成 16 年 12 月 17 日経済産業省告示第 436 号。見直し：平成 1 8 年 10 月 16 日経済産業省告示第 321 号)。これは、個人情報の保護に関する法律（平成 15 年法律第 57 号。以下「法」という。）第 7 条第 1 項に基づき平成 16 年 4 月 2 日に閣議決定された「個人情報の保護に関する基本方針」を踏まえ、「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」（平成 16 年厚生労働省・経済産業省告示第 4 号。見直し：平成 20 年 2 月 29 日厚生労働省・経済産業省告示第 1 号。以下「経済産業分野ガイドライン」という。）を基礎として、また、法第 6 条及び第 8 条に基づき、経済産業省が所管する分野のうち信用分野（物品又は役務の取引に係る信用供与に関する分野）における個人情報について、保護のための格別の措置が講じられるよう必要な措置を講じ、及び当該分野における事業者等が行う個人情報の適正な取扱いの確保に関する活動を支援する具体的な指針として定められたものです。

また、「クレジット産業における個人信用情報保護・利用に関する自主ルール運営協議会」では、個人信用情報を保護するために、「クレジット産業における個人信用情報保護・利用に関する自主ルール」を平成 13 年 3 月 28 日に制定しており、現在「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」との整合を図ったルールに改訂しています。自主ルールの運営は、現在は認定個人情報保護団体クレジット個人情報保護推進協議会が行っております。

一方、情報セキュリティマネジメントの国際的なガイドラインとして、ISO/IEC 27002:2005（旧番号：ISO/IEC 17799:2005。2007 年 7 月に規格番号が変更された。）が定められており、医療、金融サービス、製造業を始めとする各業種で普及が進んでいます。他にも、クレジット分野においては、クレジットカードのアカウント侵害の影響として、

－不正・カード犯罪
－正常取引の混乱・中断
－ブランドイメージの損傷

などが挙げられ、これに伴いクレジットカードなどのアカウント情報や取引情報を保護するための国際的な情報セキュリティ基準である PCI データセキュリティ基準（Payment Card Industry Data Security Standard：以下、PCI DSS とよぶ）が策定されました。この基準は、国際カードブランドが共同で 2005 年 10 月に制定し、2008 年 10 月に Version1.2 に改訂され、本基準を用いた監査が日本国内のみならず全世界で実施されています。

このように、クレジット産業においても、個人情報を含むアカウント情報や取引情報に対する保護、すなわち情報セキュリティへの対応が重要な課題となっています。そこで、本ガイドでは、クレジット産業における ISMS 構築を主眼として、併せて上記で紹介した「PCI DSS」や「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」と ISMS との関連を説明し、これらの規範を順守する上で非常に有効な手段であることを解説しております。また、本ガイドはクレジットカードを用いる事業者を前提として解説しておりますが、クレジットカードを用いない与信業者においても有効なガイドです。

本ガイドは JIS Q 27001:2006、JIS Q 27002:2006 をベースに作成し JIS Q 27001:2006、JIS Q 27001:2006 附属書 A 管理目的と管理策と JIS Q 27002:2006 との比較表を掲載しました。

本ガイドの作成にあたり、クレジット産業向け ISMS ユーザーズガイド検討作業部会の皆様、ISMS 適合性評価制度運営委員会の皆様をはじめご協力頂いた関係各位に対し厚く御礼申し上げます。

2009 年 3 月

ISMS 適合性評価制度技術専門部会
財団法人日本情報処理開発協会

目　次

１．クレジット産業における情報セキュリティの重要性

１．１　クレジット産業について

クレジット産業と一言で言っても、対象とする企業の範囲は、言葉を使う人の立場や考え方によってさまざまなのが現状です。個人信用情報並びにクレジット取引情報を取り扱うブランド会社（AMERICAN EXPRESS、JCB、MasterCard、VISA 等）及びクレジットカード会社を対象とした狭い範囲を指す場合や、それに加えて、クレジットカードで商品やサービスの決済が可能なレストランや百貨店等の加盟店、プロセシング会社を含めた広い範囲を指す場合などです。本ガイドでは、後者の、ブランド会社、クレジットカード会社、加盟店、プロセシング会社を含めて「クレジット産業」と表現します。

１．２　何故、クレジット産業において情報セキュリティが必要なのか

（１）与信（個人信用）情報を取扱う業界としての責務

クレジット産業は、日常の活動において消費者に対する与信業務に携わっており、大量の個人情報を取得、保有、利用しています。また、取扱う情報の内容は、消費者の購買情報や借入情報等の支払い能力に関する情報であることから、これら情報の保護については特段の措置を講じることが求められています。また与信情報は、消費者に対する与信業者の過剰な与信を排除し、適切な与信を行うことを目的として使用される情報（個人信用情報）であり、その情報については厳格な正確性が求められていると言えます。

こうした社会的要請を受け、「認定個人情報保護団体クレジット個人情報保護推進協議会」は「クレジット産業における個人信用情報保護・利用に関する自主ルール」を制定するとともに、情報保護のための安全管理対策指針を定め、業界として情報セキュリティの向上に取り組んでいます。

（２）国民の消費経済を支える社会インフラとしての責務

クレジット産業はクレジットカードをはじめとして、その取引において情報システムに大きく依存しており、まさに装置産業であると言えます。こうした情報システムは、国民の消費経済活動に対して大きな役割を担っており、万が一、情報システムが機能しないという事態が生じれば、日本における経済活動に重大な影響を及ぼす可能性があります。クレジット産業は、その使命として情報システムの安定的な稼動が必須であると言えます。

（3）クレジット犯罪の防止

クレジット産業においては、クレジットカードの不正使用をはじめとして、クレジット犯罪があとを断ちません。過去においては、クレジットカードの盗難等による犯罪が中心でしたが、最近では加盟店等に設置したクレジット端末器等から情報を盗む方法（スキミング）により、クレジットカード会員情報（クレジットカード番号や有効期限等）を盗み、偽造カードを作成して、加盟店等で不正使用するケースが増加しています。これに対してクレジット産業では、クレジットカードの IC 化をはじめとしたセキュリティの向上を目指す等、国内外において情報セキュリティ向上に取り組んでいます。

しかしながら、インターネットを中心としたネットワークの利用拡大等は、クレジット取引の利便性の向上とともに、物理的な店舗が要らないことなどから商取引への参入がしやすくなりました。一方で、セキュリティ対策の不十分な者、悪意をもった者等がクレジット取引に参加する可能性が増え、クレジット産業における情報セキュリティに対する脅威となっています。また、悪意をもった者等がクレジットカード会社に成りすまし、消費者から直接クレジットカード会員情報を騙し取り（フィッシング）、インターネット加盟店から商品を詐取したり、不正に情報サービスを受けたりする等の犯罪が発生しています。これらに対抗するために、国際ペイメントカードブランド各社を中心にインターネット取引セキュリティの共同規格の導入等にも取り組んでいます。

しかしながら、情報技術の向上だけで情報が守れるものではありません。技術的安全管理に加え、組織的、人的、物理的観点からの情報保護が、クレジットカード会社に留まらず、加盟店、プロセシング会社等も含めたクレジット産業全体で必要となっています。クレジット産業は、過去のセキュリティ対策に加え、新たに発生するこれらの犯罪を根絶して、消費者が安心してクレジット取引を行えるよう取り組みを推進していかなければなりません。

１．３　与信情報セキュリティの目標

情報セキュリティを実施する際に重要なのは、「何のために情報セキュリティを実施するのか」を明確にすることです。情報セキュリティの目標を明確に定義し、その目標達成のためのマネジメントを実践することが重要となります。特に重要と思われる目標の例を以下に示します。

（1） 与信情報及びクレジット取引情報の保護

与信情報は個人情報のなかでも特に重要な情報であり、与信情報の漏洩は本人のプライバシーを著しく侵害することとなります。またクレジット取引情報の中でも、クレジットカード番号情報の漏洩はそれらの情報を不正に用いて商品を騙し取る等の犯罪に繋がるものであり、クレジット産業は取り扱う情報の重要性を認識し、適切に管理しなければな

りません。

特に重要な対策（管理策）例としては、以下のようなものが挙げられます。

与信情報及びクレジット取引情報の機密性の維持：

個人情報保護及び犯罪防止の観点から与信情報の機密性の維持を行うこと

（2）過剰与信防止

与信情報の完全性が維持されない場合、誤った情報に基づく与信が実施される恐れがあります。クレジット産業は、過剰与信防止の観点から与信情報の完全性の維持に努めなければなりません。

特に重要な対策（管理策）例としては、以下のようなものが挙げられます。

与信情報の完全性の維持：

適切な与信を行う観点から与信情報の完全性[1]の維持を行うこと

（3）信用取引の継続

クレジット取引に係るネットワークは、災害が発生した場合でも、社会インフラとして継続して信用取引を行えるように速やかに機能回復する必要があります。また、悪意を持った攻撃に対する適切な防御手段を用意し、サイバーテロなどに対処できるようにしなければなりません。

特に重要な対策（管理策）例としては、以下のようなものが挙げられます。

情報システムの可用性の維持：

事業継続を目的とした機能維持のために情報システムの可用性の維持を行うこと

１．４　情報セキュリティと情報セキュリティマネジメントシステム

IT の発展速度は極めて速いため、ある時に講じた最高の情報セキュリティ対策が、将来にわたっても最高のものとして永続することは一般的には期待できません。その時々のハードウェア、ソフトウェアの導入は、導入時には適切な対策となっているかもしれませんが、継続性は保証されていません。情報セキュリティ対策は、ある瞬間に考えられるリスクに対応した対策を実施することによって完結する一過性の取り組みではなく、情報セキュリティ基本方針の策定、及びそれに続く日々の継続的な取り組みによって管理される性質のものであることを十分に認識することが大切です。情報セキュリティ対策の継続的な管理のことを情報セキュリティマネジメントシステム（以下、ISMS（Information Security Management System）という。）といいます。

情報セキュリティマネジメントの方針となる「情報セキュリティ基本方針」には、継続

[1] ここでいう完全性の維持の対象として、データの処理等も含みます。

的な情報収集及びセキュリティ確保の体制を構築しておくこと、また「いかにセキュリティが破られないか」のみならず、「破られたときにどうするか」についての対策も適切に規定し、当該規定に基づいた対策を十分に実施しておくことが重要です。

さらには、情報セキュリティ基本方針、及び情報セキュリティ基本方針に関連する実施手順等の規定類を定期的に見直すことによって、所有する資産に対して新たな脅威が発生していないか、環境の変化はないかを確認し、継続的に対策を講じていくことが必要です。特に情報セキュリティの分野では、技術の進歩や不正アクセスの手口の巧妙化に鑑み、早いサイクルで見直しを行っていくことも重要です。

１．５　情報セキュリティマネジメントシステム（ISMS）を確立するには

クレジット産業に係る情報に関連する資産に対して、ISMS を確立するには、様々な脅威から情報に関連する資産を守らなければなりません（脅威の詳細については後述）。一般的なクレジットカード会社が保有する情報に関連する資産の例としては、以下のものが挙げられます。

表 1-1　資産の例示

資産の種類	例示
情報	カード番号、コンピュータシステム内の個人情報、与信情報など申込書、売上伝票、個人信用情報機関から取得した情報など
ソフトウェア資産	業務アプリケーション、システムプログラムなど
物理的資産	コンピュータ装置：コンピュータ、プリンタなど 記憶媒体：MO、磁気テープなど 通信設備：ネットワーク、電話、通信回線など 電気設備：電源ケーブル、発電機、CVCF など
サービス	計算処理サービス、通信サービス、一般ユーティリティ（例えば、暖房、照明、電源、空調）
人（知識）	知識としての個人情報、業務ノウハウ、パスワードなど

これら情報に関連する資産を管理するために資産分類を実施し、資産の整理を行った上で管理を実施する必要があります。資産分類の例としては JIS Q 27002:2006「７．資産管理」が参考になります。

１．６　クレジット産業における情報セキュリティに関する脅威とぜい弱性

クレジット産業における情報セキュリティに関する脅威とぜい弱性について説明します。

（１） 脅威とは

リスクが発生する要因のことを「脅威」といいます。より厳密に言えば、「資産や組織に損失や損害をもたらす不測の事態の潜在的な要因」のことです。

情報セキュリティの脅威は大きく以下の３つに分類されます。

① 物理的・環境的脅威

② 技術的脅威

③ 人為的脅威

以下に脅威の例を示します。

表 1-2　脅威の例

脅威の分類	脅威の例
物理的・環境的脅威	・自然災害（地震・火事・落雷・水害など） ・破壊行為（テロなど） ・停電 ・故障、部品の劣化 ・非権限者、非認証者の侵入
技術的脅威	・プログラムの誤動作・停止 ・コンピュータウイルス ・バックドア ・不正アクセス ・盗聴 ・情報の改ざんおよび消失（消去） ・なりすまし ・IT 技術の進歩（例：暗号の解読が容易になる）
人為的脅威	・情報の持ち出しなどの不正行為 ・搬送中の事故、盗難 ・誤操作、不正操作

これらの脅威はあくまで「不測の事態の潜在的な要因」であり、脅威があるだけでは問題とはなりません。これらの脅威を顕在化し、具体的な損害を与える要因があって初めて脅威が問題となります。

（2） ぜい弱性とは

資産が保有する脅威を顕在化させる弱点のことを「ぜい弱性」といいます。情報セキュリティのぜい弱性も大きく以下の３つに分類されます。

① 物理面・環境面におけるぜい弱性
② 技術におけるぜい弱性
③ 人為的ぜい弱性

以下にぜい弱性の例を示します。

表 1-3　ぜい弱性の例

ぜい弱性の分類	ぜい弱性の例
物理面・環境面におけるぜい弱性	・建築上の問題 ・建物の立地の問題 ・復旧対応、応急対応の不備（バックアップ電源など） ・監視装置の不備
技術におけるぜい弱性	・ハードウェアの欠陥 ・ソフトウェアのバグ ・仕様上の欠陥 ・情報の非暗号化 ・通信ネットワークの安全性の欠如 ・復旧対応、応急対応の不備 （情報のバックアップ、迂回回線、代替システムの不備）
人為的ぜい弱性	・標準化され、文書化された情報セキュリティポリシーやシステム導入手順が存在しないこと ・事故発生時の対応手順が存在しないこと ・発生した問題の追跡手段が存在しないこと ・教育プログラムの不備、そこに起因する担当者の理解不足

ぜい弱性は、その存在自体が障害となるわけではありません。脅威とぜい弱性が組み合わさることでリスクの顕在化につながります。

１．７　与信情報セキュリティとリスクマネジメント

リスクに対処する方法（リスク対応）はいくつかあり、次のように分類できます。

表 1-4　リスクに対処する方法

リスクに対処する方法

リスクコントロール
積極的に損害を小さくする対策
・リスク予防
脅威やぜい弱性を少なくするための対策を実施する
・損害の極小化
リスクが発生したときの損害を少なくするための対策を実施する

リスク移転
契約等により他社に移転する対策
・リスクファイナンス
損害保険や責任賠償保険などに加入しリスクを移転する
・アウトソーシング
情報資産そのものや情報セキュリティ対策を外部に委託する

リスク保有
組織としてリスクを受容する対応
・リスクファイナンス
引当金を積むなどの対応を行う
・何もしない

リスク回避
適切な対策が見出せない場合の対応
・業務の廃止
業務そのものをやめてしまう
・情報資産の破壊
管理対象物をなくしてしまう

注意：JIS Q 27001：2006 の記載とは、以下のように整理付けすることが可能です。

表 1-5　本ガイドの表示と JIS Q 27001:2006 の記載

本ガイドの表示（上表）	JIS Q 27001：2006
リスクコントロール	適切な管理策の適用
リスク保有	組織の方針及びリスク受容基準を明確に満たすリスクの、意識的、かつ、客観的な受容
リスク移転	他者（例えば、保険業者、供給者）への移転
リスク回避	リスクの回避

通常のリスクマネジメントにおいては、リスク対応として、これらのうちのどれか一つだけを選択するということではなく、リスクの重要度や対策の容易性などから総合的に判

断し、これらの対策を組み合わせて実施します。この中で、一般的に情報セキュリティ対策として認識されているのは「リスクコントロール」の中の「リスク予防」です。リスク予防はリスクが発生しないようにする予防的な対策であるため、金銭的に補償することが難しいリスクに対して特に有効です。情報漏洩した企業は信用を失墜し、また、それがクレジット産業全体の信用失墜に拡大すれば、経済活動にも重大な影響を及ぼしかねません。

また、「リスク移転」の中の「アウトソーシング」、すなわち、「外部委託」もリスク対応として、よくとられる手段です。クレジット産業界においても、複雑なトランザクションや与信等の管理を外部業者に委託して運用しているケースは少なくありません。一方、外部委託業者の不十分なセキュリティ対策に起因する事件・事故（インシデント）も多数報告されており、安易な外部委託ではリスク移転にならないことも知られています。リスク移転として外部業者に業務委託する場合、委託元の責任である業務に係るリスクの特定、業者選定、情報セキュリティ事項を含む契約の締結、委託業務監督などを遂行しなければなりません。

外部委託業者の選定等に関しては、日本情報処理開発協会発行の「外部委託における ISMS 適合性評価制度の活用方法」を参照してください。

管理者にとっては費用対効果を念頭に置いた上で最も有効な対策の組合せを検討することも重要なリスクマネジメントの要素です。

１．８　クレジット産業における情報セキュリティ基準

クレジット産業における関係者を次の図に示し、求められるセキュリティ要件を説明します。

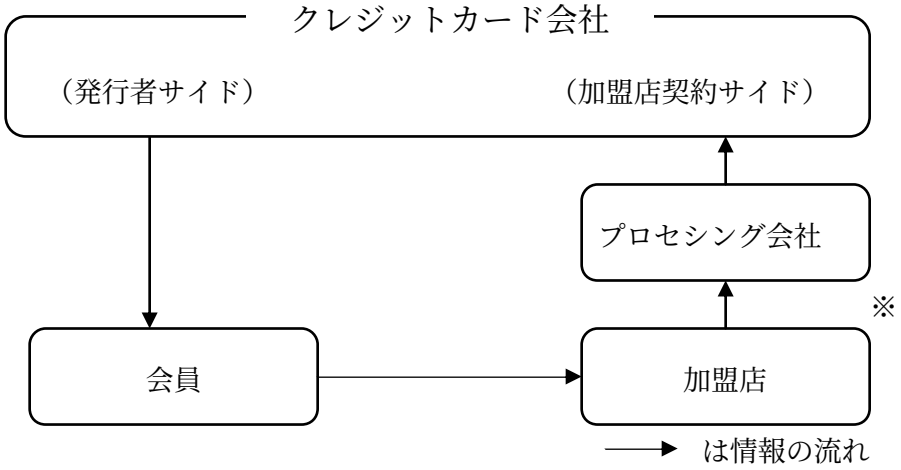

図 1-1 クレジット産業における関係者

クレジット産業では、各関係者が保有する情報によって、求められるセキュリティ基準が異なります。クレジットカードのアカウント情報や取引情報を取扱う事業者に対しては、それらを保護するための基準の順守が求められ、個人のプライバシーに関わる情報を取扱う事業者に対しては、それらを適切に管理するための基準の順守が求められます。これらの要求は、アカウント情報や取引情報を委託している加盟店にも同等に課せられています。

ISMS においては、組織の保護すべき情報に関連する資産に関して、機密性、完全性、可用性（CIA）が維持されたマネジメントシステムを構築することを目的としています。ISMS を構築していく上で、識別されたリスクを最適化するために、最適慣行を管理策として示したものが「JIS Q 27001 :2006 の附属書 A「管理目的と管理策」」となります。管理目的及び管理策は 11 個のカテゴリ分け（A5 から A15 までのカテゴリ分け）がされております。

クレジット産業にとって有用なセキュリティ基準としては、国際ペイメントカードブランドが共同で策定した PCI DSS といった、クレジットカードなどのアカウント情報および取引情報を保護するための要件を示した基準や、国内クレジットカード産業を始めとする与信業者向けに策定された「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」および「クレジット産業における個人信用情報保護・利用に関する自主ルール」といった、個人信用情報を保護するためのルールが認知されています。

なお、本ガイドでは便宜的に前者のアカウント情報および取引情報を保護するための要件のことを情報処理系のセキュリティ要件、後者の個人信用情報を保護するためのルールのことをコンプライアンス系のセキュリティ要件と表現しています。

また、情報セキュリティの分野にかかるマネジメントを対象とした ISMS と、これらのセキュリティ基準をあわせて順守することで、バランスのとれた情報セキュリティを構築し、維持することにつながります。その際、ISMS とその他のセキュリティ基準を一括して検討できることは、事業者の負担を軽減することができメリットが大きいといえます。そのため、本ガイドでは ISMS とその他のセキュリティ基準とのマッピング表を作成しました。

PCI DSS に関しては２章を、「経済産業分野における個人情報保護ガイドライン」及び「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」に関しては３章をそれぞれ参照してください。

また、これらの基準の相関をイメージしたものが図 1-2 です。

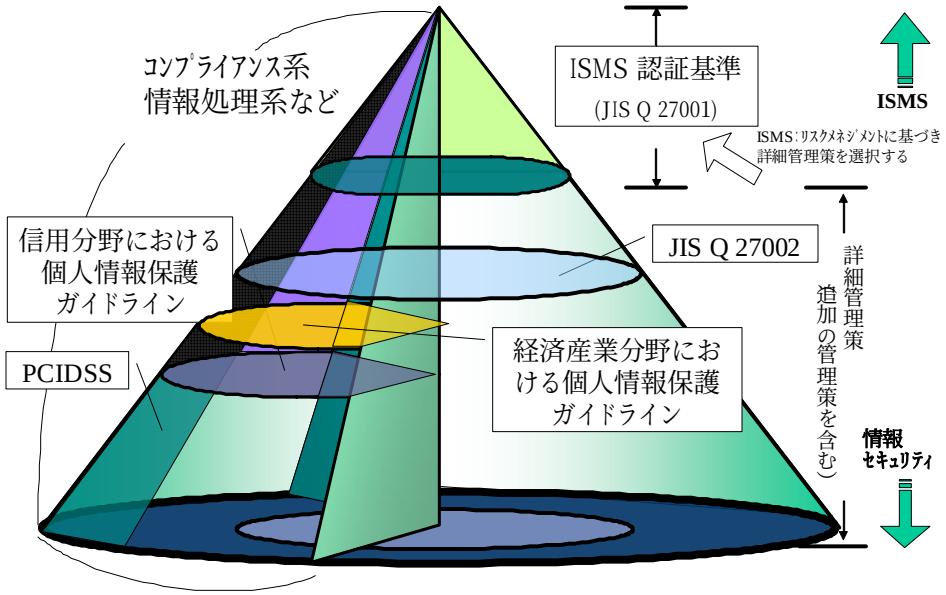

図 1-2　基準間の相関（イメージ）

１.９　カード会員情報の流出例と国際ペイメントカードブランドの対応

下図はカード会員情報の保管主体を分類し、どのようにしてカード会員情報が盗まれるかを図式化したものです。カード会員情報を所持しているのは「カード会員」ですが、カード会員情報を取り扱う事業者には、「加盟店」「アクワイアラー（加盟店契約会社）」「プロセシング会社」等があります。データが盗まれる手口としてはハッキングをはじめとして、PC やサーバーの盗難、フィッシング、カード会員の暗証番号を盗む行為、スキミング（カードの磁気データを特殊な機械で擦り取る行為）等です。

事業体がこのような攻撃を受けると、実際の不正被害の引き金となり、経済的損害はもちろん、信用失墜、経営危機に陥る危険さえあるのです。

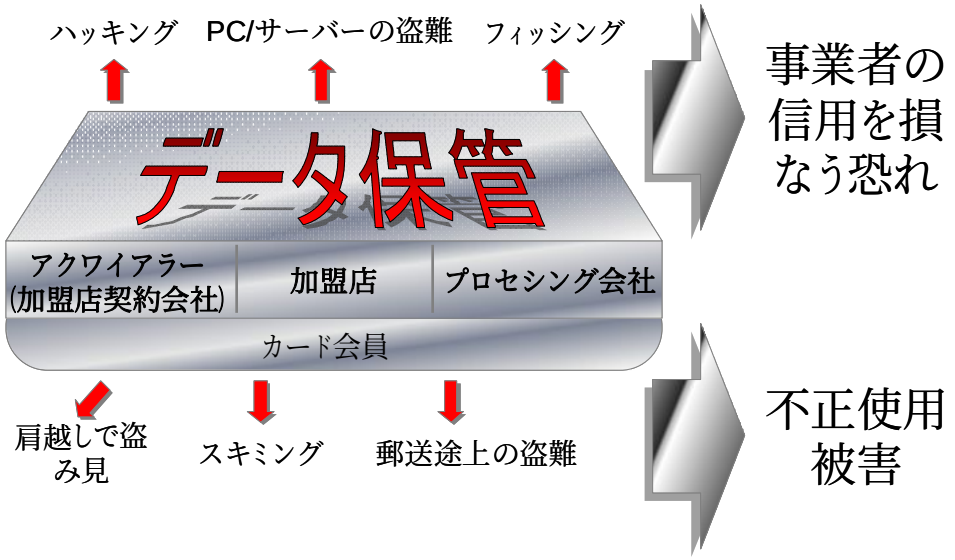

図 1-3　不必要なカード会員情報を保管することが問題

このような事態に対する効果的な対策には、データ保管についての教育、データ保管に関するルール変更、法令順守の徹底、データ保管主体の特定等が掲げられます。国際ペイメントカードブランドでは PCI DSS を共同で作成し、カード会員情報の共通の安全基準として採択しています。

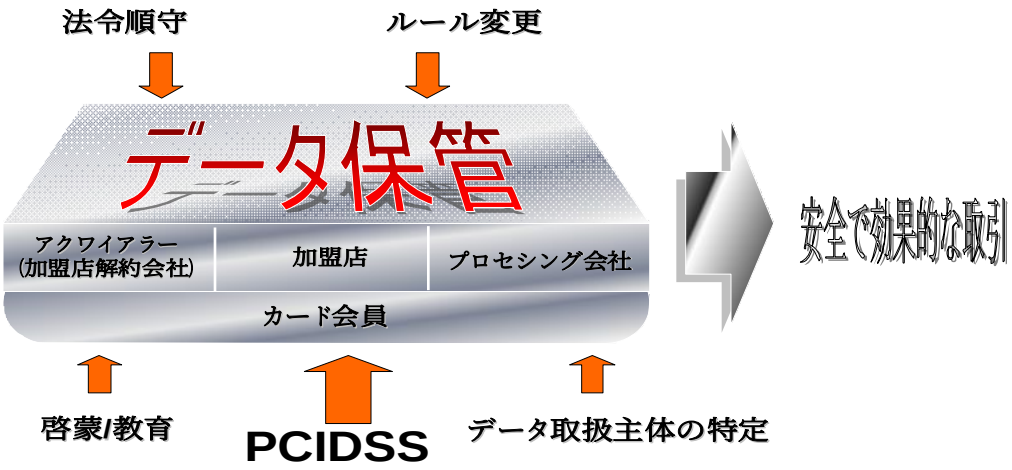

図 1-4　カード会員情報流出に対する効果的対策

１．１０　情報セキュリティに対するカード加盟店の意識

2008 年 9 月、サイボウズ・メディアアンドテクノロジー株式会社とＮＴＴデータ・セキュリティ株式会社は共同で全国のオンラインショッピングの運営に携わる 322 名に対し PCI DSS の認知度調査を実施しました。その結果、オンラインショッピング従事者の約 4 割が PCI DSS の概要を知っているか、詳しく内容を知っていた。見聞きしたレベルでの認知度は 6 割であった。一方で十分な予算と人員をセキュリテイ対策に振り向けることのできる事業者は限られており、人員も予算も十分に割けない小規模ＥＣサイトがオンライン犯罪の脆弱点になることが懸念されます。

■主な調査結果

1. 実施されているセキュリテイ対策
2. 情報セキュリテイ認証取得状況
3. PCI データセキュリティ基準 (PCI DSS) の認知度と対応状況

■調査方法

2008 年 9 月、広くインターネットで物品やサービスの販売に携わる広義のオンラインショッピング従事者に対しインターネットを利用しアンケートを実施した。アンケートでは PCI DSS の認知度の他、その対応状況や全般的なセキュリティ対策状況等も併せて調査した。調査対象の詳細は表 1-6 の通り。

表 1-6　　アンケート回答者のプロフィール

年齢

	n	12歳未満	12歳～19歳	20歳～24歳	25歳～29歳	30歳～34歳	35歳～39歳	40歳～44歳	45歳～49歳
n	322	0	0	12	76	83	64	48	39
(%)	100.0%	0.0%	0.0%	3.7%	23.6%	25.8%	19.9%	14.9%	12.1%

オンラインショップでの職種

	n	社長・経営者	運営責任者（店長、マネージャー、Webマス	受付問い合わせ窓口・カスタマーサポート	Webサイト運営管理	経理・総務	マーケティング・営業	情報システム部門	その他
n	322	59	49	27	65	47	32	31	12
(%)	100.0%	18.3%	15.2%	8.4%	20.2%	14.6%	9.9%	9.6%	3.7%

オンラインショップ規模

	n	1～10名	11～50名	51～100名	101名以上
n	322	192	68	31	31
(%)	100.0%	59.6%	21.1%	9.6%	9.6%

（1）実施しているセキュリティ対策

表 1-7　　実施しているセキュリティ対策

	全体(n/%)		1～10名		11～50名		51～100名		101名以上	
ウイルス対策	218	67.7%	113	58.9%	55	80.9%	24	77.4%	26	83.9%
スパイウエア対策	165	51.2%	83	43.2%	42	61.8%	19	61.3%	21	67.7%
ファイアウォール	151	46.9%	77	40.1%	33	48.5%	22	71.0%	19	61.3%
フィッシング対策	139	43.2%	68	35.4%	34	50.0%	21	67.7%	16	51.6%
スパムメール対策	128	39.8%	65	33.9%	33	48.5%	15	48.4%	15	48.4%
暗号化	100	31.1%	40	20.8%	35	51.5%	10	32.3%	15	48.4%
ログ管理	90	28.0%	43	22.4%	17	25.0%	12	38.7%	18	58.1%
ネットワーク監視	62	19.3%	26	13.5%	15	22.1%	11	35.5%	10	32.3%
認証・アクセス制御・PKI	53	16.5%	19	9.9%	16	23.5%	8	25.8%	10	32.3%
3Dセキュア	48	14.9%	18	9.4%	12	17.6%	6	19.4%	12	38.7%
モール標準機能	48	14.9%	46	24.0%	1	1.5%	1	3.2%	0	0.0%
入退室管理	42	13.0%	10	5.2%	15	22.1%	8	25.8%	9	29.0%
VPN	40	12.4%	15	7.8%	11	16.2%	8	25.8%	6	19.4%
IDS／IPS	39	12.1%	15	7.8%	10	14.7%	6	19.4%	8	25.8%
脆弱性診断	26	8.1%	7	3.6%	8	11.8%	7	22.6%	4	12.9%
検疫ネットワーク	25	7.8%	12	6.3%	7	10.3%	5	16.1%	1	3.2%
シンクライアント	25	7.8%	7	3.6%	8	11.8%	4	12.9%	6	19.4%
監視カメラ	23	7.1%	6	3.1%	4	5.9%	6	19.4%	7	22.6%
ワンタイムパスワード	20	6.2%	9	4.7%	8	11.8%	2	6.5%	1	3.2%
アイデンティティ管理	16	5.0%	2	1.0%	3	4.4%	5	16.1%	6	19.4%
フォレンジック	12	3.7%	4	2.1%	5	7.4%	2	6.5%	1	3.2%
その他	2	0.6%	2	1.0%	0	0.0%	0	0.0%	0	0.0%
わからない	19	5.9%	13	6.8%	5	7.4%	0	0.0%	1	3.2%
やっていない	5	1.6%	4	2.1%	1	1.5%	0	0.0%	0	0.0%
計	322		192		68		31		31	

現在実施しているセキュリティ対策と人数によるショップ規模の 2 つの条件でクロス集計を行った。運営規模が大きいほどセキュリティ対策が実施されている傾向が明確に認められた。

(2) 情報セキュリティ認証取得状況

表 1-8　オンラインショップ規模別の情報セキュリティ認証取得状況

	全体(n/%)		1～10名		11～50名		51～100名		101名以上	
ISO27001／ISMS	94	29.2%	32	16.7%	26	38.2%	17	54.8%	19	61.3%
JISQ15001(プライバシーマーク)	76	23.6%	21	10.9%	26	38.2%	13	41.9%	16	51.6%
TRUSTe	27	8.4%	8	4.2%	6	8.8%	7	22.6%	6	19.4%
その他	4	1.2%	2	1.0%	2	2.9%	0	0.0%	0	0.0%
取得していない	167	51.9%	139	72.4%	19	27.9%	6	19.4%	3	9.7%
計	322		192		68		31		31	

約3割の企業がISMSを取得した企業であった。運営規模が大きいほど認証取得が顕著である。

（3） PCI DSSの認知度と対応状況

表1-9　PCI DSS認知度

	n	（%）
詳しく知っている	44	13.7%
概要を知っている	81	25.2%
見たこと、聞いたことがある程度	81	25.2%
知らない	116	36.0%
計	322	100.0%

「PCI DSSを知っていますか？」という質問に対し、「詳しく知っている」「概要を知っている」を合わせた数字は38.9%で約4割が認知しているという結果を得た。「見た、聞いた」レベルまで合わせると64.1%となり6割を超える高い認知度という結果になった。

表1-10　オンラインショップ規模別のPCI DSS対応状況

	全体(n/%)		1～10名		11～50名		51～100名		101名以上	
既に対応し準拠認定を受けた	25	12.1%	10	9.7%	5	9.6%	4	16.0%	6	23.1%
対応中	59	28.6%	17	16.5%	20	38.5%	12	48.0%	10	38.5%
情報収集・検討段階	49	23.8%	23	22.3%	13	25.0%	6	24.0%	7	26.9%
対応予定はあるがまだ具体的に着手していない	31	15.0%	18	17.5%	9	17.3%	1	4.0%	3	11.5%
対応予定は無い	21	10.2%	17	16.5%	3	5.8%	1	4.0%	0	0.0%
わからない	21	10.2%	18	17.5%	2	3.8%	1	4.0%	0	0.0%
総数	206	100.0%	103	100.0%	52	100.0%	25	100.0%	26	100.0%

表1-9　にて「詳しく知っている」「概要を知っている」と回答した206人に対しショップ規模別にクロス集計を行った。「すでに対応し準拠認定を受けた」オンラインショップは101名以上の規模が最多で23.1%となり、ここでも運営規模との関連が認められる。

２．情報処理系のセキュリティ要件

本章では、クレジットカード等のカード会員情報や取引情報を取り扱う事業者に対して、それらを保護するための情報処理系セキュリティ基準の１つである、国際ペイメントカードブランドが共同で策定した PCI DSS と ISMS との関係について解説します。

２．１　PCI データセキュリティ基準　（PCI DSS）と ISMS

PCI DSS は、国際ペイメントカードブランドが共同で策定した、カードビジネス関連事業者向けの情報セキュリティ基準です。また、PCI DSS は、クレジットに限らずデビッド及びプリペイドのカード会員情報セキュリティや電子決済のセキュリティも含みます。

この基準は、機密として扱うべきカード会員情報やカード取引情報の保護に関して、ビジネス上の最低基準を確立するために策定されました。PCI DSS は 2006 年 9 月に国際ペイメントカードブランドが共同で設立した国際機関「PCI セキュリティ・スタンダード・カウンシル（以降「PCI SSC」）」により管理されています。

（１）PCI DSS の適用対象

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、カード会員情報、取引情報のいずれかまたは両方の処理、保管、送信を行なっているすべての企業が対象となっています。

（２）PCI DSS の要約

PCI DSS は、国際ペイメントカードブランドのカード・決済関連情報を保護するための 12 の要件で構成されています。

PCI DSS の要件

安全なネットワークの構築と維持

要件 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こと
要件 2	システムパスワードおよびその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こと

カード会員データの保護

要件 3	保存されるカード会員データの保護
要件 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、暗号化すること

脆弱性管理プログラムの整備

要件 5	アンチウィルスソフトウェアを使用し、定期的に更新すること
要件 6	安全性の高いシステムとアプリケーションを開発し、保守すること

強固なアクセス制御手法の導入

要件 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こと
要件 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
要件 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

要件 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
要件 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

情報セキュリティにポリシーの整備

要件 12	情報セキュリティポリシーを整備する

保護すべき会員データ

	データ要素	保存の可否	保護の必要性	暗号化の必要性
カード会員データ	カード会員番号（PAN)	可	必須	必須
	カード会員名(＊)	可	必須	任意
	サービスコード(＊)	可	必須	任意
	有効期限(＊)	可	必須	任意
センシテイブ認証データ	完全な磁気ストライプデータ	不可	―	―
	CAV2/CVC2/CVV2/CID	不可	―	―
	PIN/PIN ブロック	不可	―	―

(＊)ｶｰﾄﾞ番号と関連付けて保管する場合には保護が必要

――■PCI DSS（Ver1.2）のリンク先：

https://www.pcisecuritystandards.org/security_standards/pci_dss_download.html

ISMS と PCI DSS は共に情報セキュリティ基準ですが、内容的に異なる点があります。PCI DSS はカード番号と認証データの保護を目的として設計されていますが、これに対し

ISMS は業種を問わず広範な領域への適用を目的として設計されています。また、ISMS が経営の観点から「経営陣の責任」および「マネジメントレビュー」など情報セキュリティマネージメントのフレームワークを規定している本文と具体的な管理策から構成されているのに対し、PCI DSS は、カード会員情報の暗号化手法やファイアウォールの要件など、より実装レベルの詳細な規定となっています。本ガイドの２．６節では JIS Q 27001:2006 と PCI DSS（Ver.1.2）とのマッピングを図ります。

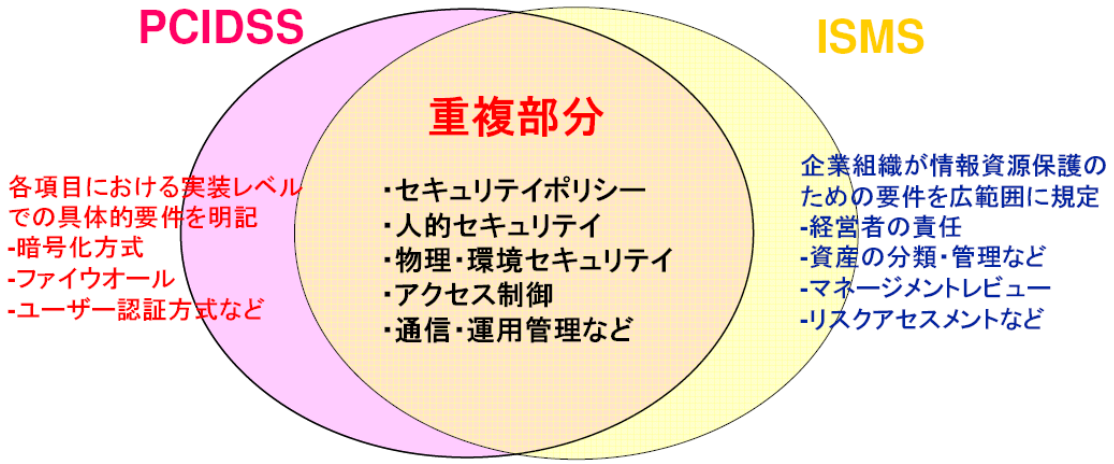

図 2-1　ISMS と PCI DSS の相関関係イメージ

２．２　国際ペイメントカードブランドの制度と PCI DSS

（１）PCI DSS 基準実施のための国際ペイメントカードブランドの制度

PCI DSS はカード会員情報のセキュリティ基準です。この基準を実現する制度として AIS（Account Information Security）プログラムと SDP（Site Data Protection）プログラムなど各国際ペイメントカードブランドが設定した制度（プログラム）があります。これらの制度はいずれもカード加盟店・プロセシング（以下「事業者」）が、PCI DSS を適確に順守することを目的に設計されたもので、カード会員情報の安全性を確保するために、事業者に起因するデータ管理に関する脆弱性の特定・対策内容と手続を定めています。

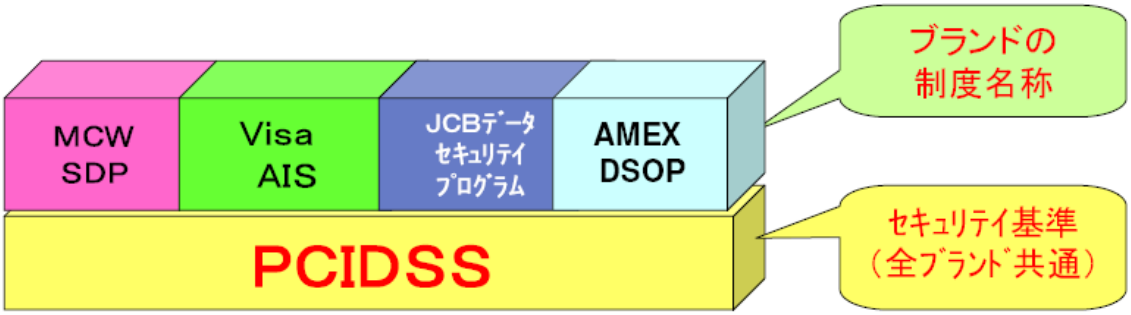

図 2-2　PCI DSS（基準）と国際ﾍﾟｲﾒﾝﾄｶｰﾄﾞﾌﾞﾗﾝﾄﾞの各制度

AMERICAN EXPRESS / JCB / MasterCard / Visa の国際ペイメントカードブランドのカードを取扱う事業者は PCI DSS の順守状況を確認し、ブランドのルールに従ってその取扱規模に応じた検証作業を行う必要があります。どのような取扱規模に応じてどのような検証作業が必要かについては、次のウェブサイトを参照してください。

■AMERICAN EXPRESS
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

（2）PCI SSC と認定審査機関（QSA）/認定スキャニングベンダー（ASV）

2006 年 9 月 8 日国際ペイメントカードブランド 5 社（AMERICAN EXPRESS、DISCOVER、JCB、MasterCard、Visa）は共同で「PCI セキュリティ・スタンダード・カウンシル（PCI SSC）」を設立いたしました。PCI SSC が PCI DSS の要件の管理の他、PCI DSS の普及を推進するための訪問審査機関（QSA）の認定と脆弱性スキャニングベンダー（ASV）の認定を行います。国際ペイメントカードブランド 5 社は既に PCI SSC の認定審査機関（QSA）の審査結果、認定スキャニングベンダー（ASV）のスキャニング結果を受け入れることに合意しています。

- PCI DSS の検証作業項目は共通です。以下の 3 項目です。
  - 事業者による自己診断
  - ASV によるスキャニングテスト
  - QSA によるオンサイトレビュー（訪問審査）

認定スキャニングベンダー及び認定審査機関の一覧表は次のウェブサイトに掲載されます。

■認定スキャニングベンダーの一覧表
https://pcisecuritystandards.org/pdfs/asv_report.html
■認定審査機関の一覧表
https://pcisecuritystandards.org/pdfs/pci_qsa_list.pdf

（3）国際ペイメントカードブランドの各制度の流れ

事業者は、PCI SSC 認定審査機関（QSA)、認定スキャニングベンダー（ASV）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、事業者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。

アクワイアラー（加盟店契約会社）は契約先の加盟店等の事業者に対して PCI DSS 準拠についての情報提供と啓蒙・教育する立場にあります。またアクワイアラーは、加盟店等の事業者が検証の結果 PCI DSS に準拠していることが判明した時は、各国際ペイメントカードブランドに対して証明書の提出をして、事業者のセキュリティレベルを報告する必要があります。

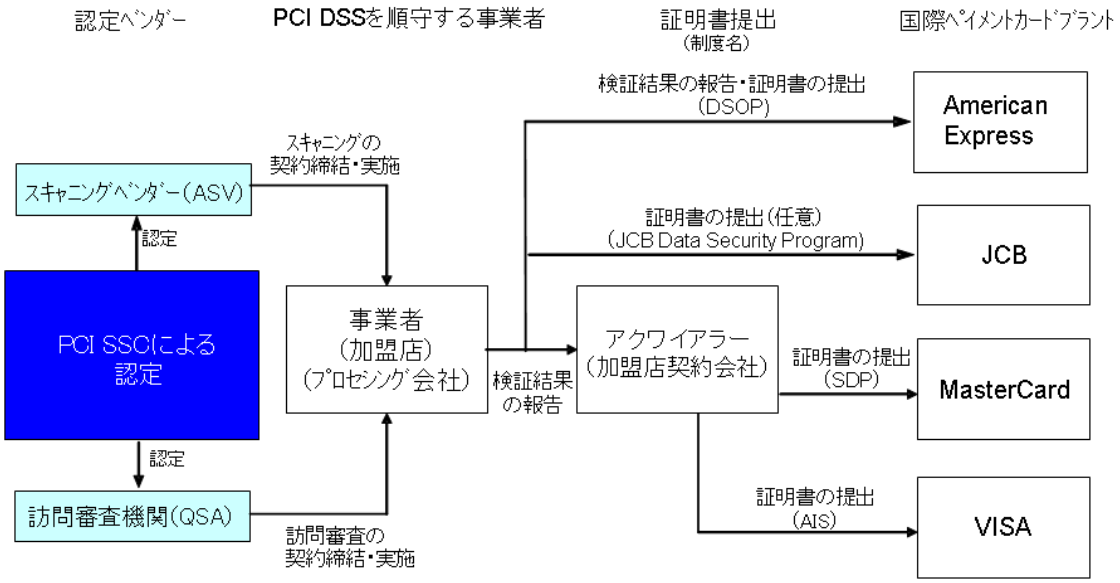

図 2-3　国際ペイメントカードブランドの各制度手続き

（４）カード会員情報が流出してしまった場合の AIS/SDP の保険的効果

AIS/SDP 順守義務を怠ったことに起因するセキュリティ侵害や情報流出が発生し、その結果カード発行会社等が被害を被った場合、事業者は損害補償を求められることがあります。しかし、AIS/SDP の検証作業が完了し各ブランドに対してアクワイアラーが AIS/SDP の証明書を提出していたものの、カード会員情報が流出してしまった場合には、しかるべき調査の実施後、カード発行会社等が蒙った費用の一部または全部の賠償責任の免除を受けられる可能性があります。これは、AIS/SDP の証明書を取得することに基づいて与えられる、一種の保険的効果を事業者に付与するものです。言い換えれば、事業者は AIS/SDP の証明書を取得しておくことによって、不測の事態による損害賠償責任を事前に担保する効果が期待できます。

２．３　PCI DSS の導入実績と課題

（１）これまでの活動実績

2005 年 9 月に「クレジット産業向け ISMS ユーザーズガイド（初版）」が発行され、ISMS と AIS 双方の年次オンサイトレビュー受診企業が一括対応もしくは AIS の差分審査などコスト・作業負荷を軽減するため活用されています。同年 10 月、ビザ・インターナショナル（以下、「Visa」）は JCB とともに AIS プログラムにおいて加盟店/サービスプロバイダーなどが自ら PCI DSS の順守状況を確認できるようにするため、オンラインによる無料の自己診断サービスの提供を開始しました。またさらに、Visa は 2006 年 4 月より独自にオンラインによる無料の脆弱性スキャニングテストのサービスを提供しています。これにより情報セキュリティに対する意識の高い企業は手軽に自社のセキュリティレベルが、国際ペイメントカードブランドが求めている基準に達しているかどうかを確認・評価できるようになりました。

Visa およびメンバーカード会社では 2005 年 6 月に発覚した米国プロセシング会社の情報流出事件を教訓に、大量のカード会員情報が集中管理されるプロセシング会社に優先順位を置き、各国の大手プロセシング会社に AIS プログラムへの参加を呼びかけてきました。その結果、1 年間に日本においては主要 35 社（市場の約 80%シェア）のご理解とご賛同を得ることができました。また、一方カード加盟店においては取扱い規模の大きい大手１０社を始め、各種の広報活動を通じ一般加盟店からの自主的な参加も見られました。

（２）今後の課題

2008 年 9 月にオンラインショップ加盟店に対する PCI DSS の認知度調査が実施されました（本ガイド 1.10「情報セキュリティに対するカード加盟店の意識」を参照)。この調査結果によると日本のオンラインショップ加盟店の PCI DSS の認知度は 4 割と必ずしも十分でないことがわかりました。この点において国際ペイメントカードブランドは各ブランドの情報セキュリティプログラムの一層の普及を通じ関連企業の PCI DSS に対する理解と順守を求めてゆくことが課題となっています。

そのためには事業者が自社のセキュリティレベルをより簡易・安価に評価・確認できる制度や仕組みを充実させことが肝要です。本ガイドは事業者が ISMS と PCI DSS の順守状況をより簡易に評価・確認できるように設計されております。

一方、カード会員情報を保管・管理する加盟店・プロセシング会社については、国内外のカードが国境を意識されることなく日常的に使われている現在、情報セキュリティ問題はもはや個社・国内固有の問題ではなく、広く国際統一基準（PCI DSS）を順守した対応が求められています。米国で発生した情報流出事件を教訓とした早期な対応が求められています。

２．４　ISMS と PCI DSS に適合した事例

ISMS と PCI DSS に適合した事例について紹介します。
なお、㈱NTT データ様では、PCI DSS への準拠に関して AIS プログラムで実施されたので、本文中では AIS と記載しています。

組織の概要
事業者名称　株式会社 NTT データ
部門名称　　決済ソリューション事業本部　カード＆ペイメントビジネスユニット
登録範囲　CAFIS※を中心としたカード決済総合サービスに関するお客様対応窓口業務及び保守・運用業務
ISMS 初回登録日　　２００５年４月７日
PCI DSS 初回登録日　２００６年６月２６日

Q１　ISMS と AIS の登録範囲は？

・ ISMS では、CAFIS を取り巻く決済ソリューション全体を登録範囲としている。この単位での認証取得については、NTT データ全社的な取得単位である。AIS では、ISMS の登録範囲である決済ソリューションの中で提供している CAFIS を対象としている。

Q２　審査の実施は？

・ ２００５年３月に ISMS
・ ２００６年３月に ISMS＋AIS（同時に実施）

Q３　AIS の構築について体制と進め方は？

・ ISMS の体制を活用して構築していった。なお、構築にあたっては主に AIS と ISMS との差分を洗い出して、その差分を確認し、補強していく作業を中心に実施していった。

Q４　AIS と ISMS との違いは（イメージ）？

・ AIS は、各々のセキュリティに対する対策が具体的に詳細なレベルまで定められているイメージ。ある意味悩むことなく対策内容が把握できるものであるが、実際の構築済みのシステムに照らし合わせた場合に、対策と実行可能範囲との乖離に悩む部分もある。
・ ISMS は､組織が主体性をもってセキュリティに対する対策のレベルを決めるといった意味で、ある意味、幅があるイメージ。しかし、具体的な対策内容は検討し、取捨選択する必要がある。

Q５　AIS の詳細なレベルについて、これは ISMS でいう追加の管理策という位置付け？

・ 追加の管理策というよりかは、むしろ ISMS で適用している管理策を更に詳細に規定した位置付け

Q６　両方の制度の審査/診断の同時審査で良かった点は？

・ 審査/診断を同時に行ったため、効率的であった。また、同じ審査/診断員であるため、重複説明（組織や事業内容に関する説明等）の必要が無かった。
また、対策自体も網羅的に一元管理できた。

Q７　両方の制度の審査/診断を受けて苦労した点は？

・ 切り口や切り込み方が ISMS と AIS で異なるので、審査員の質問への回答方法に苦労した。ISMS は基準に基づく管理の方式の確認となるが、AIS では具体的なシステムの設定内容の質問になったりする点。

Q８　両方の基準に適合できた成功要因は？

・ 運営組織トップの積極的な関与である

Q９　その他、クレジット産業のセキュリティ全般に関するご意見は？

・ 加盟店へセキュリティ運用の推進を行うためには、決済後の加盟店側の運用にてカード会員情報が必要とならなくなるような、カード会社と加盟店での運用全体を含めた検討が必要であると思います。

※ CAFIS … Credit And Finance Information System の略。1984 年 2 月よりサービス開始。
クレジットカード会社（約 120 社）・金融機関（約 1600 社）・企業・加盟店（約 1500 社）などの相互間で、クレジット情報（与信照会、売上など）、および資金移動情報（デビット・サービス、コンビニ CD サービスなどにおける資金移動情報）のオンライン・トランザクションを中継する、日本最大のカード決済総合ネットワークシステム。

■インタビュアー感想

NTT データ様は、まず ISMS を構築して、その後 AIS に取り組まれている事例であり、AIS に適合される際は、ISMS の体制を活用されたということ、また審査/診断も同時に受けることができたという点で、組織にとってメリットがありました。

また、AIS と ISMS との差分を補強するといった形で AIS に適合していったとの点については、現在 ISMS を認証取得され今後 AIS に取り組もうとしている事業者にとって参考になると思います。

最後に、運営組織のトップが積極的に関与されたとのことで、ISMS と AIS にうまく適合できたと強く認識され、推進されているという心証を得ました。ISMS と AIS の構築と運用の成功要因としてトップダウンによる推進が重要と思われますが、それを実施している良い事例と思います。

（駒瀬　彰彦、井原　亮二）

取材協力者（取材日　2006.8.17）

株式会社 NTT データ　決済ソリューション事業本部	
カード＆ペイメントビジネスユニット	
カードネットワーク担当　課長	金子 優一 様
カードネットワーク担当　課長代理	西岡 敦子 様
カードネットワーク担当　課長代理	市川 健美 様
NTT データ・セキュリティ株式会社	小沼 茂 様

２．５　JIS Q 27001／ISMS と PCI DSS 両方に取り組むことのメリット

JIS Q 27001／ISMS と PCI DSS 両方に取り組むことのメリットとしては、次の点が挙げられます。

１）セキュリティ面でのメリット

JIS Q 27001:2006 は、事業者として、広範な業界、領域に対して、経営的観点で企業・組織での基準管理および具体的管理策を規定した認証基準です。また、PCI DSS は加盟店、プロセシング会社、インターネット決済事業者などカード会員情報、取引情報のいずれかまたは両方の処理、保管、送信を行っている企業を対象としたより実装的対策となるクレジット産業界の世界標準セキュリティ基準です。これら両者を順守／取得することで、より強固でバランスのとれた情報セキュリティ環境を実現することができます。

両者を順守／取得することは、技術の進歩や不正アクセス手口の巧妙化が著しい情報セキュリティ分野において、定期的サイクルでの見直しおよび評価を実施していくことができ、リスクコントロールにおいて重要なリスク予防につながる理想的な運営の形であり、重要な取り組みであります。

また、企業にとって両者を順守／取得することは、カード会員情報、取引情報の管理を厳格に実施しているという点から、セキュリティに対して真剣に取り組んでいる企業であるという姿勢を顧客にアピールでき、また、顧客からの更なる信頼の獲得も期待できるという営業的な観点からも大きな意義ある取り組みとなるでしょう。

２）リソース面でのメリット

「JIS Q 27001:2006 と PCI DSS（Ver.1.2）とのマッピング」表を活用することにより、一方の取得を検討する際に、併せてもう一方への取り組みがしやすくなり、同時並行での効率的な検討が可能となっています。また、ISMS および PCI SSC の認定機関であれば審査自体も並行して実施することができ、マッピング表を用いた審査項目の一部免除も実施されるなど認定にかかる負荷、コストを軽減することが可能です。

さらに、ISMS に準拠、認定を取得している企業が PCI DSS の訪問審査を受診する場合は、審査機関によっては優遇措置がとられるケースもあります。

２．６　ISMS と PCI DSS とのマッピング

「関連性の程度」欄に付されている記号について

◎　－　関連性が高い

○　－　関連性がある

JIS Q 27001:2006 と PCI DSS の対応関係の詳細については、「ISMS と PCI DSS とのマッピング」を参照してください。

３．コンプライアンス系のセキュリティ要件

本章では、個人信用情報を保護するためのガイドラインで国内クレジットカード産業を始めとする与信業者向けに策定された「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」と ISMS とのマッピングを図ります。なお、個人情報保護と ISMS との関連については、「法規適合性に関する ISMS ユーザーズガイド（URL：http://www.isms.jipdec.jp/doc/JIP-ISMS115-10.pdf ）平成 17 年 4 月発行」を参照して下さい。

「ISMS と個人情報系ガイドラインとのマッピング」は、JIS Q 27001:2006 と信用分野ガイドラインの対応関係の概要の理解の促進のために参考として示すものです。JIS Q 27001:2006 及び信用分野ガイドラインの対象とする範囲がそれぞれ異なること、信用分野ガイドラインに規定されている項目の中には、JIS Q 27001:2006 では規定されていない項目があること、またその逆もあることより、JIS Q 27001:2006 に準拠することにより、信用分野ガイドラインを遵守していることにはなりません。また、その逆も同様です。

JIS Q 27001:2006、PCI DSS（Ver.1.2）、自主ルールなどは民間が自主的に定める任意規格又はルールですが、信用分野ガイドラインの「しなければならない」とされる規定は、個人情報保護法の解釈基準であり、その遵守状況を政府が直接判断する強制規定であることに留意してください。

なお、割賦販売法の改正に伴う割賦販売法施行規則の改正によりクレジットカード等購入あつせん業者又は立替払取次業者は、経済産業省令で定める基準に従い、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こととなったことに留意する必要があります。

例えば、この法律の施行に必要な限度において、クレジットカード番号等の安全管理の状況に関する報告を経済産業大臣に提出することなども留意点のひとつになります。本ガイドが示す両基準を満たすための活動は、このような場合においても有効であると考えられます。

JIS Q 27001:2006 と信用分野ガイドラインの対応関係の詳細については、「ISMS と個人情報系ガイドラインとのマッピング」を参照してください。

ISMS と PCI DSS とのマッピング

マッピング表の補足

・本マッピング表は、あくまでも参考という位置付けでご利用いただけますよう
お願い申し上げます。

・例えば、JIS Q 27001や27002の1つの項目に対して必ずしも1対1対応をしているの
ではない場合もあり、複数の項目に関連している場合もあり、その逆もあります
ので、参考レベルでご覧いただければ幸いです。

※ マッピング表で比較対象とした項目は両基準に関連した部分を抽出したものであり、
クレジット産業におけるセキュリティ要件をすべて網羅しているものではないことに
ご留意ください。

・「関連性の程度」欄に付されている記号について

◎ － 関連性が高い

○ － 関連性がある

※ 一部でも 関連性がある場合は○、関連性が高い場合は◎を採用しました。

JIS Q 27001:2006 (附属書A)		JIS Q 27002:2006		PCIデータセキュリティスタンダード(Ver.1.2)※	関連性の程度
項番		項番	条文		
	管理目的及び管理策				
	表A.1に規定した管理目的及び管理策は，JIS Q 27002: 2006の箇条5～15までに掲げられているものをそのまま取り入れて配列したものである。この表は，管理目的及び管理策のすべてを網羅してはいないので，組織は，管理目的及び管理策の追加が必要であると考えてよい。この表の中の管理目的及び管理策は，本体の4.2.1に規定するISMSのプロセスの一部として，選択しなければならない。				
	JIS Q 27002: 2006の箇条5～15までは，A.5～A.15までに規定した管理策を支える，導入への助言及び最適な実施のための手引を提供している。				
A.5	**セキュリティ基本方針**	**5**	**情報セキュリティ基本方針**		
A.5.1	**A.5.1 情報セキュリティ基本方針** 目的：情報セキュリティのための経営陣の方向性及び支持を，事業上の要求事項，関連する法令及び規制に従って規定するため。	5.1	**5.1 情報セキュリティ基本方針**		
A.5.1.1	A.5.1.1 **情報セキュリティ基本方針文書**	5.1.1	**5.1.1 情報セキュリティ基本方針文書**	12.1 以下を実現するセキュリティポリシーを確立、公開、維持、および周知する。 12.1.1 すべての PCI DSS 要件に対応する。 12.1.2 脅威、脆弱性、結果を識別する年に一度のプロセスを正式なリスク評価に含める。 12.1.3 レビューを少なくとも年に一度含め、環境の変化に合わせて更新する。 12.5.1 セキュリティポリシーおよび手順を確立、文書化、および周知する。	◎
A.5.1.2	A.5.1.2 **情報セキュリティ基本方針のレビュー**	5.1.2	**5.1.2 情報セキュリティ基本方針のレビュー**	12.1.3 レビューを少なくとも年に一度含め、環境の変化に合わせて更新する。 12.3 従業員に公開されている重要なテクノロジ（リモートアクセステクノロジ、無線テクノロジ、リムーバブル電子メディア、ラップトップ、携帯情報端末（PDA）、電子メールの使用、インターネットの使用など）に関する使用ポリシーを作成して、すべての従業員および派遣社員向けにこれらのテクノロジの適切な使用を定義する。これらの使用ポリシーでは以下を要求します。 12.3.1 管理者による明示的な承認	◎
A.6	**A.6 情報セキュリティのための組織**	**6**	**情報セキュリティのための組織**		
A.6.1	**A.6.1 内部組織** 目的：組織内の情報セキュリティを管理するため。	6.1	**6.1 内部組織**		
A.6.1.1	A.6.1.1 **情報セキュリティに対する経営陣の責任**	6.1.1	**6.1.1 情報セキュリティに対する経営陣の責任**		
A.6.1.2	A.6.1.2 **情報セキュリティの調整**	6.1.2	**6.1.2 情報セキュリティの調整**		
A.6.1.3	A.6.1.3 **情報セキュリティ責任の割当て**	6.1.3	**6.1.3 情報セキュリティ責任の割当て**	12.5 個人またはチームに以下の情報セキュリティ管理責任を割り当てる。 12.5.1 セキュリティポリシーおよび手順を確立、文書化、および周知する。 12.5.2 セキュリティに関する警告および情報を監視して分析し、該当する担当者に通知する。 12.5.3 セキュリティインシデントの対応およびエスカレーション手順を確立、文書化、および周知して、あらゆる状況をタイムリーかつ効果的に処理する。 12.5.4 追加、削除、変更を含め、ユーザアカウントを管理する 12.5.5 データへのすべてのアクセスを監視および管理する。	◎
A.6.1.4	A.6.1.4 **情報処理設備の認可プロセス**	6.1.4	**6.1.4 情報処理設備の認可手続**		
A.6.1.5	A.6.1.5 **秘密保持契約**	6.1.5	**6.1.5 機密保持契約**		
A.6.1.6	A.6.1.6 **関係当局との連絡**	6.1.6	**6.1.6 関係当局との連絡**		
A.6.1.7	A.6.1.7 **専門組織との連絡**	6.1.7	**6.1.7 専門組織との連絡**	2.2 すべてのシステムコンポーネントについて、構成基準を作成する。この基準は、すべての既知のセキュリティ脆弱性をカバーし、また業界で認知されたシステム強化基準と一致している必要がある。	◎
A.6.1.8	A.6.1.8 **情報セキュリティの独立したレビュー**	6.1.8	**6.1.8 情報セキュリティの独立したレビュー**	11.1 無線アナライザを少なくとも四半期に一度使用して、または使用中のすべての無線デバイスを識別するための無線IDS/IPS を導入し、無線アクセスポイントの存在をテストする。 11.2 内部および外部ネットワークの脆弱性スキャンを少なくとも四半期に一度およびネットワークでの大幅な変更（新しいシステムコンポーネントのインストール、ネットワークトポロジの変更、ファイアウォール規則の変更、製品アップグレードなど）後に実行する。 注: 四半期に一度の外部の脆弱性スキャンは、PCI（Payment Card Industry）セキュリティ基準審議会（PCI SSC）によって資格を与えられた Approved Scanning Vendor(ASV)によって実行される必要があります。ネットワーク変更後に実施されるスキャンは、会社の内部スタッフによって実行することができます。 11.3 外部および内部のペネトレーションテストを少なくとも年に一度および大幅なインフラストラクチャまたはアプリケーションのアップグレードや変更（オペレーティングシステムのアップグレード、環境へのサブネットワークの追加、環境への Web サーバの追加など）後に実行する。これらのペネトレーションテストには以下を含める必要がある。 11.3.1 ネットワーク層のペネトレーションテスト 11.3.2 アプリケーション層のペネトレーションテスト	○
A.6.2	**A.6.2 外部組織** 目的：外部組織によってアクセス，処理，通信，又は管理される組織の情報及び情報処理施設のセキュリティを維持するため。	6.2	**6.2 外部組織**		
A.6.2.1	A.6.2.1 **外部組織に関係したリスクの識別**	6.2.1	**6.2.1 外部組織に関係したリスクの識別**		
A.6.2.2	A.6.2.2 **顧客対応におけるセキュリティ**	6.2.2	**6.2.2 顧客対応におけるセキュリティ**		

JIS Q 27001:2006 (附属書A)		JIS Q 27002:2006		PCIデータセキュリティスタンダード(Ver.1.2)※	関連性の程度
項番		項番	条文		
A.6.2.3	A.6.2.3 **第三者との契約におけるセキュリティ**	6.2.3	**6.2.3 第三者との契約におけるセキュリティ**	12.8 カード会員データをサービスプロバイダと共有する場合は、サービスプロバイダを管理するためのポリシーと手順を維持および実施して、以下を含める。 12.8.1 サービスプロバイダのリストを維持する。 12.8.2 サービスプロバイダが自社の所有するカード会員データのセキュリティに対して責任を負うことに同意した、書面での契約を維持する。	◎
				12.8.3 契約前の適切なデューディリジェンスを含め、サービスプロバイダとの契約に関するプロセスが確立されている。 12.8.4 サービスプロバイダの PCIDSS 準拠ステータスを監視するプログラムを維持する。	
A.7	**A.7 資産の管理**	**7**	**資産の管理**		
A.7.1	**A.7.1 資産に対する責任** 目的: 組織の資産を適切に保護し, 維持するため。	7.1	**7.1 資産に対する責任**		
A.7.1.1	A.7.1.1 **資産目録**	7.1.1	**7.1.1 資産目録**	9.9.1 すべての媒体の在庫ログを適切に保持し、少なくとも年に一度メディアの在庫調査を実施する。 12.3.3 このようなすべてのデバイスおよびアクセスできる担当者のリスト	◎
A.7.1.2	A.7.1.2 **資産の管理責任者**	7.1.2	**7.1.2 資産の管理責任者**		
A.7.1.3	A.7.1.3 **資産利用の許容範囲**	7.1.3	**7.1.3 資産利用の許容範囲**	4.2 暗号化されていない PAN をエンドユーザメッセージングテクノロジ (電子メール、インスタントメッセージング、チャットなど) で送信しない。 12.3.5 テクノロジの許容される利用法 12.3.6 テクノロジの許容されるネットワーク上の場所 12.8.1 サービスプロバイダのリストを維持する。 12.8.2 サービスプロバイダが自社の所有するカード会員データのセキュリティに対して責任を負うことに同意した、書面での契約を維持する。 12.8.3 契約前の適切なデューディリジェンスを含め、サービスプロバイダとの契約に関するプロセスが確立されている。 12.8.4 サービスプロバイダの PCIDSS 準拠ステータスを監視するプログラムを維持する。	◎
A.7.2	**A.7.2 情報の分類** 目的: 情報の適切なレベルでの保護を確実にするため。	7.2	**7.2 情報の分類**		
A.7.2.1	A.7.2.1 **分類の指針**	7.2.1	**7.2.1 分類の指針**		
A.7.2.2	A.7.2.2 **情報のラベル付け及び取扱い**	7.2.2	**7.2.2 情報のラベル付け及び取扱い**	9.7.1 秘密であると識別できるように、媒体を分類する。	◎
A.8	**A.8 人的資源のセキュリティ**	**8**	**8 人的資源のセキュリティ**		
A.8.1	**A.8.1 雇用前** 目的: 従業員, 契約相手及び第三者の利用者がその責任を理解し, 求められている役割にふさわしいことを確実にするとともに, 盗難, 不正行為, 又は施設の不正使用のリスクを低減するため。	8.1	**8.1 雇用前**		
A.8.1.1	A.8.1.1 **役割及び責任**	8.1.1	**8.1.1 役割及び責任**	12.4 セキュリティポリシーおよび手順に、すべての従業員および派遣社員の情報セキュリティに対する責任を明確に定義する。 1.1.4 ネットワークコンポーネントの論理的管理のためのグループ、役割、責任に関する記述	◎
A.8.1.2	A.8.1.2 **選考**	8.1.2	**8.1.2 選考**	12.7 雇用する前に、可能性のある従業員 (上述の 9.2 の "従業員" の定義を参照) を選別して、内部ソースからの攻撃リスクを最小限に抑える。 トランザクションを進めるときに一度に 1つのカード番号にしかアクセスできない、店のレジ係などの従業員については、この要件は推奨のみです。	◎
A.8.1.3	A.8.1.3 **雇用条件**	8.1.3	**8.1.3 雇用条件**		
A.8.2	**A.8.2 雇用期間中** 目的: 従業員, 契約相手及び第三者の利用者の, 情報セキュリティの脅威及び諸問題, 並びに責任及び義務に対する認識を確実なものとし, 通常の業務の中で組織の情報セキュリティ基本方針を維持し, 人による誤りのリスクを低減できるようにすることを確実にするため。	8.2	**8.2 雇用期間中**		
A.8.2.1	A.8.2.1 **経営陣の責任**	8.2.1	**8.2.1 経営陣の責任**	12.6 正式なセキュリティに関する認識を高めるプログラムを実施して、すべての従業員がカード会員データセキュリティの重要性を認識するようにする。	◎
A.8.2.2	A.8.2.2 **情報セキュリティの意識向上, 教育及び訓練**	8.2.2	**8.2.2 情報セキュリティの意識向上, 教育及び訓練**	12.6.1 雇用時および少なくとも年に一度従業員を教育する。 12.6.2 会社のセキュリティポリシーおよび手順に目を通して理解したことについての同意を、少なくとも年に一度従業員に求める。	◎
A.8.2.3	A.8.2.3 **懲戒手続**	8.2.3	**8.2.3 懲戒手続**		
A.8.3	**A.8.3 雇用の終了又は変更** 目的: 従業員, 契約相手及び第三者の利用者の組織からの離脱又は雇用の変更を所定の方法で行うことを確実にするため。	8.3	**8.3 雇用の終了又は変更**		
A.8.3.1	A.8.3.1 **雇用の終了又は変更に関する責任**	8.3.1	**8.3.1 雇用の終了又は変更に関する責任**		
A.8.3.2	A.8.3.2 **資産の返却**	8.3.2	**8.3.2 資産の返却**		
A.8.3.3	A.8.3.3 **アクセス権の削除**	8.3.3	**8.3.3 アクセス権の削除**		
A.9	**A.9 物理的及び環境的セキュリティ**	**9**	**物理的及び環境的セキュリティ**		
A.9.1	**A.9.1 セキュリティを保つべき領域** 目的: 組織の施設及び情報に対する認可されていない物理的アクセス, 損傷及び妨害を防止するため。	9.1	**9.1 セキュリティを保つべき領域**		
A.9.1.1	A.9.1.1 **物理的セキュリティ境界**	9.1.1	**9.1.1 物理的セキュリティ境界**	9.1 適切な施設入館管理を使用して、カード会員データ環境内のシステムへの物理アクセスを制限および監視する。	◎

JIS Q 27001:2006 (附属書A)		JIS Q 27002:2006		PCIデータセキュリティスタンダード(Ver.1.2)※	関連性の程度
項番		項番	条文		
				9.1.1 ビデオカメラやその他のアクセス管理メカニズムを使用して、機密エリアへの個々の物理アクセスを監視する。収集されたデータを確認し、その他のエントリと相関付ける。法律によって別途定められていない限り、少なくとも 3 カ月間保管する。注: "機密エリア" とは、データセンタ、サーバルーム、またはカード会員データを保存、処理、または伝送するシステムが設置されているエリアのことです。これには、小売店のレジなど、POS 端末のみが存在するエリアは含まれません。 9.1.3 無線アクセスポイント、ゲートウェイ、およびハンドヘルドデバイスへの物理アクセスを制限する。	
A.9.1.2	A.9.1.2 **物理的入退管理策**	9.1.2	**9.1.2 物理的入退管理策**	9.1 適切な施設入館管理を使用して、カード会員データ環境内のシステムへの物理アクセスを制限および監視する。 9.2 カード会員データにアクセス可能なエリアでは特に、すべての担当者が従業員と訪問者を容易に区別できるような手順を開発する。この要件において、"従業員" とは、フルタイムおよびパートタイムの従業員、一時的な従業員および要員、事業体の敷地内に "常駐" している請負業者やコンサルタントのことです。"訪問者" は、ベンダ、従業員の客、サービス要員、または短時間（通常は 1 日以内）施設に入る必要がある人として定義されます。 9.4 訪問者ログを使用して、訪問者の行動の物理的な監査証跡を保持する。訪問者の名前、所属会社、物理アクセスを承認した従業員をログに記録する。法律によって別途定められていない限り、このログを少なくとも 3 カ月間保管する。 9.3 すべての訪問者が次のように処理されることを確認する。 9.3.1 カード会員データが処理または保守されているエリアに入る前に承認が行われる 9.3.2 有効期限があり、訪問者を非従業員として識別する物理トークン（バッジ、アクセスデバイスなど）が与えられる 9.3.3 施設を出る前、または期限切れの日に物理トークンの返却を求められる	◎
A.9.1.3	A.9.1.3 **オフィス, 部屋及び施設のセキュリティ**	9.1.3	**9.1.3 オフィス, 部屋及び施設のセキュリティ**		
A.9.1.4	A.9.1.4 **外部及び環境の脅威からの保護**	9.1.4	**9.1.4 外部及び環境の脅威からの保護**		
A.9.1.5	A.9.1.5 **セキュリティを保つべき領域での作業**	9.1.5	**9.1.5 セキュリティを保つべき領域での作業**		
A.9.1.6	A.9.1.6 **一般の人の立寄り場所及び受渡場所**	9.1.6	**9.1.6 一般の人の立寄り場所及び受渡場所**		
A.9.2	**A.9.2 装置のセキュリティ** 目的: 資産の損失, 損傷, 盗難又は劣化, 及び組織の活動に対する妨害を防止するため。	9.2	**9.2 装置のセキュリティ**		
A.9.2.1	A.9.2.1 **装置の設置及び保護**	9.2.1	**9.2.1 装置の設置及び保護**	9.6 カード会員データを含むすべての紙および電子媒体を物理的にセキュリティで保護する。	◎
A.9.2.2	A.9.2.2 **サポートユーティリティ**	9.2.2	**9.2.2 サポートユーティリティ**		
A.9.2.3	A.9.2.3 **ケーブル配線のセキュリティ**	9.2.3	**9.2.3 ケーブル配線のセキュリティ**	9.1.2 誰でもアクセス可能なネットワークジャックへの物理アクセスを制限する。	○
A.9.2.4	A.9.2.4 **装置の保守**	9.2.4	**9.2.4 装置の保守**		
A.9.2.5	A.9.2.5 **構外にある装置のセキュリティ**	9.2.5	**9.2.5 構外にある装置のセキュリティ**		
A.9.2.6	A.9.2.6 **装置の安全な処分又は再利用**	9.2.6	**9.2.6 装置の安全な処分又は再利用**		
A.9.2.7	A.9.2.7 **資産の移動**	9.2.7	**9.2.7 資産の移動**		
A.10	**A.10 通信及び運用管理**	**10**	**通信及び運用管理**		
A.10.1	**A.10.1 運用の手順及び責任** 目的: 情報処理設備の正確, かつ, セキュリティを保った運用を確実にするため。	10.1	**10.1 運用の手順及び責任**		
A.10.1.1	A.10.1.1 **操作手順書**	10.1.1	**10.1.1 操作手順書**	12.2 この仕様の要件と整合する日常的な運用上のセキュリティ手順を作成する（たとえば、ユーザアカウント保守手順、ログレビュー手順）。	◎
A.10.1.2	A.10.1.2 **変更管理**	10.1.2	**10.1.2 変更管理**	1.1.1 すべてのネットワーク接続およびファイアウォール/ルーター構成への変更を承認およびテストする正式なプロセス 1.1.2 ワイヤレスネットワークを含む、カード会員データへのすべての接続を示す最新ネットワーク図 6.4 システムコンポーネントへのすべての変更において、変更管理手順に従う。手順には以下を含める必要がある。 6.4.1 影響の文書化 6.4.2 適切な管理者による承認 6.4.3 運用機能のテスト 6.4.4 回復手順	◎
A.10.1.3	A.10.1.3 **職務の分割**	10.1.3	**10.1.3 職務の分割**	6.3.3 開発/テスト環境と本番環境での責務の分離	◎
A.10.1.4	A.10.1.4 **開発施設, 試験施設及び運用施設の分離**	10.1.4	**10.1.4 開発施設, 試験施設及び運用施設の分離**	6.3.2 開発/テスト環境と本番環境の分離 6.3.3 開発/テスト環境と本番環境での責務の分離	◎
A.10.2	**A.10.2 第三者が提供するサービスの管理** 目的: 第三者の提供するサービスに関する合意に沿った, 情報セキュリティ及びサービスの適切なレベルを実現し, 維持するため。	10.2	**10.2 第三者が提供するサービスの管理**		
A.10.2.1	A.10.2.1 **第三者が提供するサービス**	10.2.1	**10.2.1 第三者が提供するサービス**	2.4 共有ホスティングプロバイダは、各事業体のホスト環境およびカード会員データを保護する必要がある。「付録 A: 共有ホスティングプロバイダ向けの PCI DSS 追加要件」に詳しく説明されている要件を満たす必要がある。	○
A.10.2.2	A.10.2.2 **第三者が提供するサービスの監視及びレビュー**	10.2.2	**10.2.2 第三者が提供するサービスの監視及びレビュー**		
A.10.2.3	A.10.2.3 **第三者が提供するサービスの変更に対する管理**	10.2.3	**10.2.3 第三者が提供するサービスの変更に対する管理**		
A.10.3	**A.10.3 システムの計画作成及び受入れ** 目的: システム故障のリスクを最小限に抑えるため。	10.3	**10.3 システムの計画作成及び受入れ**		
A.10.3.1	A.10.3.1 **容量・能力の管理**	10.3.1	**10.3.1 容量・能力の管理**		
A.10.3.2	A.10.3.2 **システムの受入れ**	10.3.2	**10.3.2 システムの受入れ**	6.4.3 運用機能のテスト	◎

JIS Q 27001:2006 (附属書A)		JIS Q 27002:2006		PCIデータセキュリティスタンダード(Ver.1.2)※	関連性の程度
項番		項番	条文		
A.10.4	**A.10.4 悪意のあるコード及びモバイルコード[9]からの保護** 目的：ソフトウェア及び情報の完全性を保護するため。 注3) モバイルコードとはコンピュータから別のコンピュータへ移動するソフトウェアであって，利用者とのやり取りがほとんどない，又はまったくない状態で自動的に起動し，特定の機能を実行するものをいう。	10.4	**10.4 悪意のあるコード及びモバイルコードからの保護**		
A.10.4.1	A.10.4.1 **悪意のあるコードに対する管理策**	10.4.1	**10.4.1 悪意のあるコードに対する管理策**	5.2 すべてのアンチウィルスメカニズムが最新で、有効に実行されており、監査ログが生成できる。 5.1 悪意のあるソフトウェアの影響を受けやすいすべてのシステム（特にパーソナルコンピュータとサーバ）に、アンチウィルスソフトウェアを導入する。 5.1.1 すべてのアンチウィルスプログラムは、すべての既知のタイプの悪意のあるソフトウェアに対して検知、駆除、保護が可能でなければならない。 6.3.7 コーディングの脆弱性がないことを確認するために、本番または顧客へのリリースの前に、カスタムコードをレビューする 注: このコードレビュー要件は、PCI DSS要件 6.3 で要求されるシステム開発ライフサイクルの一環として、すべてのカスタムコード（内部および公開）に適用される。コードレビューは、知識を持つ社内担当者または第三者が実施できる。一般に公開されているWeb アプリケーションは、実装後の脅威および脆弱性に対処するために、PCIDSS 要件 6.6 に定義されている追加コントロールの対象となる。	◎
A.10.4.2	A.10.4.2 **モバイルコードに対する管理策**	10.4.2	**10.4.2 モバイルコードに対する管理策**		
A.10.5	**A.10.5 バックアップ** 目的：情報及び情報処理設備の完全性及び可用性を維持するため。	10.5	**10.5 バックアップ**		
A.10.5.1	A.10.5.1 **情報のバックアップ**	10.5.1	**10.5.1 情報のバックアップ**	9.5 メディアバックアップを安全な場所に保管する（代替またはバックアップサイト、商用ストレージ施設などのオフサイト施設が望ましい）。保管場所のセキュリティを少なくとも年に一度確認する。 3.4 以下の手法を使用して、すべての保存場所でPAN を少なくとも読み取り不能にする（ポータブルデジタルメディア、バックアップメディア、ログを含む）。 ・強力な暗号化技術をベースにしたワンウェイハッシュ ・トランケーション ・インデックストークンとパッド（パッドは安全に保存する必要がある） ・関連するキー管理プロセスおよび手順を伴う、強力な暗号化 アカウント情報のうち、少なくとも PANは読み取り不能にする必要がある。	◎
A.10.6	**A.10.6 ネットワークセキュリティ管理** 目的：ネットワークにおける情報の保護，及びネットワークを支える基盤の保護を確実にするため。	10.6	**10.6 ネットワークセキュリティ管理**		
A.10.6.1	A.10.6.1 **ネットワーク管理策**	10.6.1	**10.6.1 ネットワーク管理策**	1.1.1 すべてのネットワーク接続およびファイアウォール/ルーター構成への変更を認およびテストする正式なプロセス 1.1.2 ワイヤレスネットワークを含む、カード会員データへのすべての接続を示す新ネットワーク図 1.1.3 各インターネット接続、および DMZ（demilitarized zone）と内部ネットワークゾーンとの間のファイアウォール要件 1.1.4 ネットワークコンポーネントの論理的管理のためのグループ、役割、責任にする記述 1.1.5 使用が許可されているすべてのサービス、プロトコル、ポートの文書化。および使用が許可されている業務上の理由（安全でないとみなされているプロトコルに実装されているセキュリティ機能の文書化など） 1.1.6 ファイアウォールおよびルーターのルールセットは少なくとも 6 カ月ごとにビューされる必要がある 1.2.3 すべてのワイヤレスネットワークとカード会員データ環境の間に境界ファイアウォールをインストールし、ワイヤレス環境からカード会員データ環境へのすべてのトラフィックを拒否または制御（そのようなトラフィックが業務上必要な場合）するようにファイアウォールを構成する。 2.2 すべてのシステムコンポーネントについて、構成基準を作成する。この基準は、すべての既知のセキュリティ脆弱性をカバーし、また業界で認知されたシステム強化基準と一致している必要がある。 4.1.1 カード会員データを伝送する、またはカード会員データ環境に接続しているワイヤレスネットワークには、業界のベストプラクティス（IEEE 802.11i など）を使用して、認証および伝送用に強力な暗号化を実装する。 ・新しいワイヤレス実装において、2009 年 3 月 31 日以降は WEP を実装できない。 ・現在のワイヤレス実装において、2010 年 6 月 30 日以降は WEP を使用できない。	◎
A.10.6.2	A.10.6.2 **ネットワークサービスのセキュリティ**	10.6.2	**10.6.2 ネットワークサービスのセキュリティ**	1.1.5 使用が許可されているすべてのサービス、プロトコル、ポートの文書化。および使用が許可されている業務上の理由（安全でないとみなされているプロトコルに実装されているセキュリティ機能の文書化など） 1.2 信頼できないネットワークとカード会員データ環境内のすべてのシステムコンポーネントとの接続を制限する、ファイアウォール構成を構築する。 1.3 インターネットとカード会員データ環境 内のすべてのシステムコンポーネント間の、直接的なパブリックアクセスを禁止する。 2.2.1 1 つのサーバには、主要機能を 1つだけ実装する。	○
A.10.7	**A.10.7 媒体の取扱い** 目的：資産の認可されていない開示，改ざん，除去又は破壊，及びビジネス活動の中断を防止するため。	10.7	**10.7 媒体の取扱い**	9.7 カード会員データを含むあらゆる種類の媒体の内部または外部での配布に関して、以下を含め、厳格な管理を維持する。	◎

JIS Q 27001:2006 (附属書A)		JIS Q 27002:2006		PCIデータセキュリティスタンダード(Ver.1.2)※	関連性の程度
項番		項番	条文		
A.10.7.1	A.10.7.1 **取外し可能な媒体の管理**	10.7.1	**10.7.1 取外し可能な媒体の管理**	9.10 次のように、ビジネスまたは法律上の理由で不要になったカード会員データを含む媒体を破棄する。 9.6 カード会員データを含むすべての紙および電子媒体を物理的にセキュリティで保護する。 9.8 安全なエリアから移動されるカード会員データを含むすべての媒体を管理者が承認するようにする（特に媒体が個人に配布される場合）。 9.9.1 すべての媒体の在庫ログを適切に保持し、少なくとも年に一度メディアの在庫調査を実施する。 9.5 メディアバックアップを安全な場所に保管する（代替またはバックアップサイト、商用ストレージ施設などのオフサイト施設が望ましい）。保管場所のセキュリティを少なくとも年に一度確認する。	◎
A.10.7.2	A.10.7.2 **媒体の処分** 管理策 媒体が不要になった場合は，正式な手順を用いて，セキュリティを保ち，かつ，安全に処分しなければならない。	10.7.2	**10.7.2 媒体の処分**	9.10.1 カード会員データを再現できないよう、ハードコピー資料を裁断、焼却、またはパルプ化する。 9.10.2 カード会員データを再現できないように、電子媒体上のカード会員データを回復不能にする。	◎
A.10.7.3	A.10.7.3 **情報の取扱手順**	10.7.3	**10.7.3 情報の取扱手順**	9.6 カード会員データを含むすべての紙および電子媒体を物理的にセキュリティで保護する。 9.9 カード会員データを含む媒体の保管およびアクセスに関して厳格な管理を維持する。 3.2 承認後にセンシティブ認証データを保存しない（暗号化されている場合でも）。センシティブ認証データには、以降の要件 3.2.1～ 3.2.3 で言及されているデータを含む。 3.2.1 磁気ストライプのいかなるトラックのいかなる内容も保存しない（カードの裏面、チップ内、その他に存在する）。このデータは、全トラック、トラック、トラック1、トラック2、磁気ストライプデータとも呼ばれる。 注: 通常の業務範囲では、磁気ストライプの以下のデータ要素を保存する必要が生じる場合がある。 ・ カード会員名 ・ プライマリアカウント番号（PAN） ・ 有効期限 ・ サービスコード リスクを最小限に抑えるため、業務上必要なデータ要素のみを保存する。 注: 詳細については、「PCI DSS Glossary of Terms, Abbreviations, and Acronyms」を参照。 3.2.2 カードを提示しない取引の確認に使用されるカード検証コードまたは値（ペイメントカードの前面または裏面に印字された 3 桁または 4 桁の数字）を保存しない。 注: 詳細については、「PCI DSS Glossary of Terms, Abbreviations, and Acronyms」を参照。 3.2.3 個人識別番号（PIN）または暗号化された PIN ブロックを保存しない。 3.3 表示する際に PAN をマスクする（最大でも最初の 6 桁と最後の 4 桁のみを表示）。 注: ・ 従業員およびその他の関係者が、業務上の合法的なニーズにより PAN全体を見る必要がある場合、この要 件は適用されない。 ・ カード会員データの表示に関するこれより厳しい要件（POS レシートなど）がある場合は、そちらに置き換えられる。	◎
A.10.7.4	A.10.7.4 **システム文書のセキュリティ**	10.7.4	**10.7.4 システム文書のセキュリティ**		
A.10.8	**A.10.8 情報の交換** 目的: 組織内部で交換した及び外部と交換した，情報及びソフトウェアのセキュリティを維持するため。	10.8	**10.8 情報の交換**		
A.10.8.1	A.10.8.1 **情報交換の方針及び手順**	10.8.1	**10.8.1 情報交換の方針及び手順**		
A.10.8.2	A.10.8.2 **情報交換に関する合意**	10.8.2	**10.8.2 情報交換に関する合意**		
A.10.8.3	A.10.8.3 **配送中の物理的媒体**	10.8.3	**10.8.3 配送中の物理的媒体**	9.7.2 安全な配達業者または正確に追跡できるその他の配送方法によって媒体を送付する。	◎
A.10.8.4	A.10.8.4 **電子的メッセージ通信**	10.8.4	**10.8.4 電子的メッセージ通信**	4.2 暗号化されていない PAN をエンドユーザメッセージングテクノロジ（電子メール、インスタントメッセージング、チャットなど）で送信しない。	○
A.10.8.5	A.10.8.5 **業務用情報システム**	10.8.5	**10.8.5 業務用情報システム**		
A.10.9	**A.10.9 電子商取引サービス** 目的: 電子商取引サービスのセキュリティ，及びそれらサービスのセキュリティを保った利用を確実にするため。	10.9	**10.9 電子商取引サービス**		
A.10.9.1	A.10.9.1 **電子商取引**	10.9.1	**10.9.1 電子商取引**		
A.10.9.2	A.10.9.2 **オンライン取引**	10.9.2	**10.9.2 オンライン取引**	4.1 オープンな公共ネットワーク経由で機密性の高いカード会員データを伝送する場合、強力な暗号化と SSL/TLS またはIPSEC などのセキュリティプロトコルを使用する。 PCI DSS では、オープンな公共ネットワークの例として以下が挙げられる。 ・インターネット ・ワイヤレステクノロジ ・Global System for Mobile communications（GSM） 1.3 インターネットとカード会員データ環境内のすべてのシステムコンポーネント間の、直接的なパブリックアクセスを禁止する。 1.3.5 カード会員データ環境からインターネットへの発信トラフィックが、DMZ 内の IP アドレスにのみアクセス可能なように制限する。	○
A.10.9.3	A.10.9.3 **公開情報**	10.9.3	**10.9.3 公開情報**		
A.10.10	**A.10.10 監視** 目的: 認可されていない情報処理活動を検知するため。	10.10	**10.10 監視**		

JIS Q 27001:2006 (附属書A)		JIS Q 27002:2006		PCIデータセキュリティスタンダード(Ver.1.2)※	関連性の程度
項番		項番	条文		
A.10.10.1	A.10.10.1 **監査ログ取得**	10.10.1	**10.10.1 監査ログ取得**	10.2 以下のイベントを再現するためにすべてのシステムコンポーネントの自動監査証跡を実装する。 10.2.1 カード会員情報に対するすべての個人ユーザーによるアクセス。 10.2.3 すべての監査証跡へのアクセス。 10.2.4 無効な論理的アクセス試行。 10.3 イベントごとに、すべてのシステムコンポーネントについて少なくとも以下の監査証跡エントリを記録する。 10.3.1 ユーザ識別 10.3.3 日付と時刻 10.3.4 成功または失敗を示す情報 12.5.5 データへのすべてのアクセスを監視および管理する. 10.3.5 イベントの発生元 10.3.6 影響を受けるデータ、システムコンポーネント、またはリソースの ID または名前 5.2 すべてのアンチウィルスメカニズムが最新で、有効に実行されており、監査ログが生成できる。	◎
A.10.10.2	A.10.10.2 **システム使用状況の監視**	10.10.2	**10.10.2 システム使用状況の監視**	10.1 システムコンポーネントへのすべてのアクセス(特に、ルートなどの管理権限を使用して行われたアクセス)を各ユーザにリンクするプロセスを確立する。 10.2.2 ルート権限または管理権限を持つ個人によって行われたすべてのアクション 10.2 5 識別および認証メカニズムの使用 10.2.6 監査ログの初期化 10.2.7 システムレベルオブジェクトの作成および削除 10.3.2 イベントの種類 12.5.2 セキュリティに関する警告および情報を監視して分析し、該当する担当者に通知する。 12.5.5 データへのすべてのアクセスを監視および管理する。	◎
A.10.10.3	A.10.10.3 **ログ情報の保護**	10.10.3	**10.10.3 ログ情報の保護**	10.5 変更できないよう、監査証跡をセキュリティで保護する。 10.5.1 監査証跡の表示を、仕事関連のニーズを持つ人物のみに制限する。 10.5.2 監査証跡ファイルを不正な変更から保護する。 10.5.3 監査証跡ファイルを、変更が困難な一元管理ログサーバまたは媒体に即座にバックアップする。 10.5.4 外部に公開されているテクノロジのログを内部 LAN 上のログサーバに書き込む. 10.5.5 ログに対してファイル整合性監視または変更検出ソフトウェアを使用して、既存のログデータを変更すると警告が生成されるようにする (ただし、新しいデータの追加は警告を発生させない)。 10.6 少なくとも日に一度、すべてのシステムコンポーネントのログを確認する。ログの確認には、侵入検知システム (IDS) や認証、 認可、アカウンティングプロトコル (AAA) サーバ (RADIUS など) のようなセキュリティ機能を実行するサーバを含める必要がある。 注: 要件 10.6 に準拠するために、ログの収集、解析、および警告ツールを使用することができます。 10.7 監査証跡の履歴を少なくとも 1 年間保持する。少なくとも 3 カ月はすぐに分析できる状態にしておく (オンライン、アーカイブ、 バックアップから復元可能など)。	◎
A.10.10.4	A.10.10.4 **実務管理者及び運用担当者の作業ログ**	10.10.4	**10.10.4 実務管理者及び運用担当者の作業ログ**	10.2 以下のイベントを再現するためにすべてのシステムコンポーネントの自動監査証跡を実装する。 10.2.1 カード会員情報に対するすべての個人ユーザーによるアクセス。 10.2.2 ルート権限または管理権限を持つ個人によって行われたすべてのアクション	◎
A.10.10.5	A.10.10.5 **障害のログ取得**	10.10.5	**10.10.5 障害のログ取得**		
A.10.10.6	A.10.10.6 **クロックの同期**	10.10.6	**10.10.6 クロックの同期**	10.4 すべての重要なシステムクロックおよび時間を同期する。	◎
A.11	**A.11 アクセス制御**	**11**	**アクセス制御**		
A.11.1	**A.11.1 アクセス制御に対する業務上の要求事項** 目的: 情報へのアクセスを制御するため。	11.1	**11.1 アクセス制御に対する業務上の要求事項**		
A.11.1.1	A.11.1.1 **アクセス制御方針**	11.1	**11.1.1 アクセス制御方針**	12.3.3 このようなすべてのデバイスおよびアクセスできる担当者のリスト 1.1.6 ファイアウォールおよびルーターのルールセットは少なくとも 6 カ月ごとにレビューされる必要がある	◎
A.11.2	**A.11.2 利用者アクセスの管理** 目的: 情報システムへの, 認可された利用者のアクセスを確実にし, 認可されていないアクセスを防止するため。	11.2	**11.2 利用者アクセスの管理**	7.1 システムコンポーネントとカード会員データへのアクセスを、業務上必要な人に限定する。アクセス制限には以下を含める必要がある。 12.5.4 追加、削除、変更を含め、ユーザアカウントを管理する	◎
A.11.2.1	A.11.2.1 **利用者登録**	11.2.1	**11.2.1 利用者登録**	7.1 システムコンポーネントとカード会員データへのアクセスを、業務上必要な人に限定する。アクセス制限には以下を含める必要がある。 7.1.3 管理職により署名され、必要な特権を特定する承認フォームが要求される 7.1.4 自動アクセス制御システムを実装する 8.1 システムコンポーネントまたはカード会員データへのアクセスを許可する前に、すべてのユーザに一意の ID を割り当てる。 7.2 複数のユーザーを持つシステムコンポーネントに対して、ユーザーの必要な範囲に基づいてアクセスを制限し、特に許可されていない限り「すべてを拒否」に設定した、アクセス制御システムを確立する。アクセス制御システムには以下を含める必要がある。 7.2.1 すべてのシステムコンポーネントを対象に含む 7.2.2 職種と職能に基づく、個人への特権の付与 7.2.3 デフォルトでは「すべてを拒否」の設定 8.5.4 契約終了したユーザのアクセスは直ちに取り消す。 8.5.5 少なくとも 90 日ごとに非アクティブのユーザアカウントを削除/無効化する。 8.5.6 リモート保守のためにベンダが使用するアカウントは、必要な期間のみ有効にする。	◎

JIS Q 27001:2006 (附属書A)		JIS Q 27002:2006		PCIデータセキュリティスタンダード(Ver.1.2)※	関連性の程度
項番		項番	条文		
A.11.2.2	A.11.2.2 **特権管理**	11.2.2	**11.2.2 特権管理**	7.1.1 特権ユーザー ID に関するアクセス権が、職務の実行に必要な最小限の特権に制限されていること 7.1.2 特権の付与は、個人の職種と職能に基づくこと	◎
A.11.2.3	A.11.2.3 **利用者パスワードの管理**	11.2.3	**11.2.3 利用者パスワードの管理**		
				8.2 一意の ID の割り当てに加え、以下の方法の少なくとも 1 つを使用してすべてのユーザを認証する。 Ÿ パスワードまたはパスフレーズ Ÿ 2 因子認証（トークンデバイス、スマートカード、生体認証、公開鍵など） 8.5.2 パスワードのリセットを実行する前にユーザ ID を確認する。 8.5.3 初期パスワードをユーザごとに一意の値に設定し、初回使用後に直ちに変更する。	◎
				2.1 システムをネットワーク上に導入する前に、ベンダ提供のデフォルト値を必ず変更する（パスワード、簡易ネットワーク管理プロトコル（SNMP）コミュニティ文字列の変更、不必要なアカウントの削除など）。 2.1.1 カード会員データ環境に接続されている、またはカード会員データを伝送するワイヤレス環境の場合、ワイヤレスベンダのデフォルト値を変更する。これには、デフォルトのワイヤレス暗号化キー、パスワード、SNMP コミュニティ文字列が含まれる（ただし、これらに限定されない）。認証および伝送のために、強力な暗号化技術のワイヤレスデバイスセキュリティ設定が有効になっていることを確認する。	
A.11.2.4	A.11.2.4 **利用者アクセス権のレビュー**	11.2.4	**11.2.4 利用者アクセス権のレビュー**	8.5.4 契約終了したユーザのアクセスは直ちに取り消す。 8.5.5 少なくとも 90 日ごとに非アクティブのユーザアカウントを削除/無効化する。	○
A.11.3	**A.11.3 利用者の責任** 目的：認可されていない利用者のアクセス，並びに情報及び情報処理設備の損傷又は盗難を防止するため。	11.3	**11.3 利用者の責任**	8.5.7 パスワード手順およびポリシーを、カード会員データにアクセスできるすべてのユーザに伝達する。	◎
A.11.3.1	A.11.3.1 **パスワードの利用**	11.3.1	**11.3.1 パスワードの利用**	8.5.10 パスワードに 7 文字以上が含まれることを要求する。 8.5.11 数字と英文字の両方を含むパスワードを使用する。 8.5.9 少なくとも 90 日ごとにユーザパスワードを変更する。 8.5.12 ユーザが新しいパスワードを送信する際、最後に使用した 4 つのパスワードと同じものを使用できないようにする。 8.5.13 最大 6 回の試行後にユーザ IDをロックアウトして、アクセス試行の繰り返しを制限する。 8.5.14 ロックアウトの期間を、最小 30分または管理者がユーザ ID を有効にするまで、に設定する。	○
A.11.3.2	A.11.3.2 **無人状態にある利用者装置**	11.3.2	**11.3.2 無人状態にある利用者装置**		
A.11.3.3	A.11.3.3 **クリアデスク・クリアスクリーン方針**	11.3.3	**11.3.3 クリアデスク・クリアスクリーン方針**		
A.11.4	**A.11.4 ネットワークのアクセス制御** 目的：ネットワークを利用したサービスへの認可されていないアクセスを防止するため。	11.4	**11.4 ネットワークのアクセス制御**		
A.11.4.1	A.11.4.1 **ネットワークサービスの利用についての方針**	11.4.1	**11.4.1 ネットワークサービスの利用についての方針**	1.2 信頼できないネットワークとカード会員データ環境内のすべてのシステムコンポーネントとの接続を制限する、ファイアウォール構成を構築する。 1.3 インターネットとカード会員データ環境内のすべてのシステムコンポーネント間の、直接的なパブリックアクセスを禁止する。 1.3.2 着信インターネットトラフィックをDMZ 内の IP アドレスに制限する。 1.3.4 インターネットから DMZ 内へ通過できる内部インターネットアドレスを禁止する。 1.3.6 動的パケットフィルタリングとも呼ばれる、ステートフルインスペクションを実装する。（ネットワーク内へは、「確立された」接続のみ許可される。） 1.3.8 RFC 1918 アドレス領域を使用して、IP マスカレードを実装し、内部アドレスが変換されインターネット上で露出することを防ぐ。ポート アドレス変換（PAT）などのネットワークアドレス変換（NAT）テクノロジを使用する。	○
A.11.4.2	A.11.4.2 **外部から接続する利用者の認証**	11.4.2	**11.4.2 外部から接続する利用者の認証**	2.1.1 カード会員データ環境に接続されている、またはカード会員データを伝送するワイヤレス環境の場合、ワイヤレスベンダのデフォルト値を変更する。これには、デフォルトのワイヤレス暗号化キー、パスワード、SNMP コミュニティ文字列が含まれる（ただし、これらに限されない）。認証および伝送のために、強力な暗号化技術のワイヤレスデバイスセキュリティ設定が有効になっていることを確認する。 4.1.1 カード会員データを伝送する、またはカード会員データ環境に接続しているワイヤレスネットワークには、業界のベストプラクティス（IEEE 802.11i など）を使用して、認証および伝送用に強力な暗号化を実装する。 Ÿ 新しいワイヤレス実装において、2009 年 3 月 31 日以降は WEP を実装できない。 Ÿ 現在のワイヤレス実装において、2010 年 6 月 30 日以降は WEP を使用できない。 8.3 従業員、管理者、および第三者によるネットワークへのリモートアクセスネットワーク外部からのネットワークレベルアクセス）には 2 因子認証を組み込む。RADIUS（Remote Authentication and Dial-InService）、TACACS（Terminal Access Controller Acceess Control System）とトークン、または VPN（SSL/TLS または IPSECベース）と個々の証明書などのテクノロジを使用する。	◎
A.11.4.3	A.11.4.3 **ネットワークにおける装置の識別**	11.4.3	**11.4.3 ネットワークにおける装置の識別**		

JIS Q 27001:2006 (附属書A)		JIS Q 27002:2006		PCIデータセキュリティスタンダード(Ver.1.2)※	関連性の程度
項番		項番	条文		
A.11.4.4	A.11.4.4 **遠隔診断用及び環境設定用ポートの保護**	11.4.4	**11.4.4 遠隔診断用及び環境設定用ポートの保護**	1.1.5 使用が許可されているすべてのサービス、プロトコル、ポートの文書化。および使用が許可されている業務上の理由（安全でないとみなされているプロトコルに実装されているセキュリティ機能の文書化など） 1.2 信頼できないネットワークとカード会員データ環境内のすべてのシステムコンポーネントとの接続を制限する、ファイアウォール構成を構築する。 2.1 システムをネットワーク上に導入する前に、ベンダ提供のデフォルト値を必ず変更する（パスワード、簡易ネットワーク管理プロトコル（SNMP）コミュニティ文字列の変更、不必要なアカウントの削除など）。 2.2 すべてのシステムコンポーネントについて、構成基準を作成する。この基準は、すべての既知のセキュリティ脆弱性をカバーし、また業界で認知されたシステム強化基準と一致している必要がある。 2.2.2 安全性の低い不必要なサービスおよびプロトコルはすべて無効にする（デバイスの特定機能を実行するのに直接必要でないサービスおよびプロトコル）。 2.2.3 システムの誤用を防止するためにシステムセキュリティパラメータを構成する。	◎
A.11.4.5	A.11.4.5 **ネットワークの領域分割**	11.4.5	**11.4.5 ネットワークの領域分割**	1.1 以下を含むファイアウォールおよびルーター構成基準を確立する	◎
				1.1.3 各インターネット接続、および DMZ（demilitarized zone）と内部ネットワークゾーンとの間のファイアウォール要件 1.1.5 使用が許可されているすべてのサービス、プロトコル、ポートの文書化。および使用が許可されている業務上の理由（安全でないとみなされているプロトコルに実装されているセキュリティ機能の文書化など）	
				1.2.1 着信および発信トラフィックを、カード会員データ環境に必要なトラフィックに制限する。 1.2.2 ルーター構成ファイルをセキュリティ保護および同期化する。 1.2.3 すべてのワイヤレスネットワークとカード会員データ環境の間に境界ファイアウォールをインストールし、ワイヤレス環境からカード会員データ環境へのすべてのトラフィックを拒否または制御（そのようなトラフィックが業務上必要な場合）するようにファイアウォールを構成する。 1.3.7 DMZ から分離された内部ネットワークゾーンに、データベースを配置する。 1.2.3 すべてのワイヤレスネットワークとカード会員データ環境の間に境界ファイアウォールをインストールし、ワイヤレス環境からカード会員データ環境へのすべてのトラフィックを拒否または制御（そのようなトラフィックが業務上必要な場合）するようにファイアウォールを構成する。	
A.11.4.6	A.11.4.6 **ネットワークの接続制御**	11.4.6	**11.4.6 ネットワークの接続制御**	1.3 インターネットとカード会員データ環境内のすべてのシステムコンポーネント間の、直接的なパブリックアクセスを禁止する。 7.1 システムコンポーネントとカード会員データへのアクセスを、業務上必要な人に限定する。アクセス制限には以下を含める必要がある。 8.1 システムコンポーネントまたはカード会員データへのアクセスを許可する前に、すべてのユーザに一意の ID を割り当てる。 1.3.1 DMZ を実装し、着信および発信トラフィックを、カード会員データ環境に必要なトラフィックに制限する。 1.3.3 インターネットとカード会員データ環境間トラフィックの、すべての直接経路（着信/発信）を使用不可にする。 1.3.5 カード会員データ環境からインターネットへの発信トラフィックが、DMZ 内の IP アドレスにのみアクセス可能なように制限する。	◎
A.11.4.7	A.11.4.7 **ネットワークルーティング制御**	11.4.7	**11.4.7 ネットワークルーティング制御**	1.1.1 すべてのネットワーク接続およびファイアウォール/ルーター構成への変更を承認およびテストする正式なプロセス 1.1.6 ファイアウォールおよびルーターのルールセットは少なくとも 6 カ月ごとにレビューされる必要がある 1.3.8 RFC 1918 アドレス領域を使用して、IP マスカレードを実装し、内部アドレスが変換されインターネット上で露出することを防ぐ。ポート アドレス変換（PAT）などのネットワークアドレス変換（NAT）テクノロジを使用する。	◎
A.11.5	**A.11.5 オペレーティングシステムのアクセス制御** 目的：オペレーティングシステムへの，認可されていないアクセスを防止するため。	11.5	**11.5 オペレーティングシステムのアクセス制御**		
A.11.5.1	A.11.5.1 **セキュリティに配慮したログオン手順**	11.5.1	**11.5.1 セキュリティに配慮したログオン手順**		
A.11.5.2	A.11.5.2 **利用者の識別及び認証**	11.5.2	**11.5.2 利用者の識別及び認証**	8.5.8 グループ、共有、または汎用のアカウントおよびパスワードを使用しない。 8.5.16 カード会員データを含むデータベースへのすべてのアクセスを認証する。これには、アプリケーション、管理者、およびその他のすべてのユーザによるアクセスが含まれる。 8.3 従業員、管理者、および第三者によるネットワークへのリモートアクセス（ネットワーク外部からのネットワークレベルアクセス）には 2 因子認証を組み込む。RADIUS（Remote Authentication and Dial-InService）、TACACS（Terminal Access Controller Acceess Control System）とトークン、または VPN（SSL/TLS または IPSECベース）と個々の証明書などのテクノロジを使用する。 8.5 すべてのシステムコンポーネントで、以下のように、消費者以外のユーザおよび管理者に対して適切なユーザ認証とパスワード管理を確実に行う。	◎

JIS Q 27001:2006 (附属書A)		JIS Q 27002:2006		PCIデータセキュリティスタンダード(Ver.1.2)※	関連性の程度
項番		項番	条文		
A.11.5.3	A.11.5.3 **パスワード管理システム**	11.5.3	**11.5.3 パスワード管理システム**	8.4 (「PCI DSS Glossary of Terms, Abbreviations, and Acronyms」で定義されている) 強力な暗号化を使用して、すべてのシステムコンポーネントでの伝送および保存中にすべてのパスワードを読み取り不能にする。 8.5 すべてのシステムコンポーネントで、以下のように、消費者以外のユーザおよび管理者に対して適切なユーザ認証とパスワード管理を確実に行う。	◎
A.11.5.4	A.11.5.4 **システムユーティリティの使用**	11.5.4	**11.5.4 システムユーティリティの使用**		
A.11.5.5	A.11.5.5 **セッションのタイムアウト**	11.5.5	**11.5.5 セッションのタイムアウト**	8.5.15 セッションが 15 分を超えてアイドル状態の場合、端末を再有効化するためにユーザにパスワードの再入力を要求する。 12.3.8 非アクティブ状態が特定の期間続いた後のリモートアクセステクノロジのセッションの自動切断	◎
A.11.5.6	A.11.5.6 **接続時間の制限**	11.5.6	**11.5.6 接続時間の制限**		
A.11.6	**A.11.6 業務用ソフトウェア及び情報のアクセス制御** 目的: 業務用ソフトウェアシステムが保有する情報への認可されていないアクセスを防止するため。	11.6	**11.6 業務用ソフトウェア及び情報のアクセス制御**		
A.11.6.1	A.11.6.1 **情報へのアクセス制限**	11.6.1	**11.6.1 情報へのアクセス制限**	8.5.1 ユーザ ID、資格情報、およびその他の識別子オブジェクトの追加、削除、変更を管理する。	◎
A.11.6.2	A.11.6.2 **取扱いに慎重を要するシステムの隔離**	11.6.2	**11.6.2 取扱いに慎重を要するシステムの隔離**		
A.11.7	**A.11.7 モバイルコンピューティング及びテレワーキング**注5) 目的:モバイルコンピューティング及びテレワーキングの設備を用いるときの情報セキュリティを確実にするため。 注5) モバイルコンピューティングとは，移動中又は外出先でコンピュータを利用することであり，テレワーキングとは，要員が，自分の所属する組織の外の決まった場所で，通信技術を用いて作業することである。	11.7	**11.7 モバイルコンピューティング及びテレワーキング**		
A.11.7.1	A.11.7.1 **モバイルのコンピューティング及び通信**	11.7.1	**11.7.1 モバイルのコンピューティング及び通信**	1.4 インターネットに直接接続するすべてのモバイルコンピュータまたは従業員所有のコンピュータ (あるいはその両方) で、企業ネットワークへのアクセスに使用されるものに (従業員が使用するラップトップなど)、パーソナルファイアウォールソフトウェアをインストールする。 8.5 すべてのシステムコンポーネントで、以下のように、消費者以外のユーザおよび管理者に対して適切なユーザ認証とパスワード管理を確実に行う。 12.3 従業員に公開されている重要なテクノロジ (リモートアクセステクノロジ、無線テクノロジ、リムーバブル電子メディア、ラップトップ、携帯情報端末 (PDA)、電子メールの使用、インターネットの使用など) に関する使用ポリシーを作成して、すべての従業員および派遣社員向けにこれらのテクノロジの適切な使用を定義する。これらの使用ポリシーでは以下を要求します。 12.3.1 管理者による明示的な承認 12.3.2 テクノロジの使用に対する認証 12.3.3 このようなすべてのデバイスおよびアクセスできる担当者のリスト 12.3.4 デバイスへの所有者、連絡先情報、目的を記載したラベルの添付 12.3.5 テクノロジの許容される利用法 12.3.6 テクノロジの許容されるネットワーク上の場所 12.3.7 会社が承認した製品のリスト 12.3.8 非アクティブ状態が特定の期間続いた後のリモートアクセステクノロジのセッションの自動切断 12.3.9 ベンダには必要とする場合にのみリモートアクセステクノロジをアクティブ化し、使用後直ちに非アクティブ化する 12.3.10 リモートアクセステクノロジ経由でカード会員データにアクセスする場合、ローカルハードドライブおよびリムーバブル電子メディアへのカード会員データのコピー、移動、保存を禁止する。	◎
A.11.7.2	A.11.7.2 **テレワーキング**	11.7.2	**11.7.2 テレワーキング**		
A.12	**A.12 情報システムの取得，開発及び保守**	12	**情報システムの取得，開発及び保守**		
A.12.1	**A.12.1 情報システムのセキュリティ要求事項** 目的: セキュリティは情報システムの欠くことのできない部分であることを確実にするため。	12.1	**12.1 情報システムのセキュリティ要求事項**		
A.12.1.1	A.12.1.1 **セキュリティ要求事項の分析及び仕様化**	12.1.1	**12.1.1 セキュリティ要求事項の分析及び仕様化**	6.5 すべての Web アプリケーション (内部、外部、アプリケーションへの Web 管理アクセス) を、「Open Web Application Security Project Guide」などの安全なコーディングガイドラインに基づいて開発する。ソフトウェア開発プロセスに共通するコーディングの脆弱性の防止対応して、以下を含める。 注: PCI DSS v1.2 が発行されたときに6.5.1 ～ 6.5.10 に挙げられている脆弱性は、現在 OWASP ガイドに掲載されている。ただし、OWASP ガイドが更新されている場合、これらの要件には現在のバージョンを使用する必要がある。 6.5.1 クロスサイトスクリプティング (XSS) 6.5.2 インジェクションの不具合 (特にSQL インジェクション) LDAP と Xpath のインジェクションの不具合、その他のインジェクションの不具合も考慮する。 6.5.3 悪意のあるファイル実行 6.5.4 安全でないオブジェクトの直接参照 6.5.5 クロスサイトリクエスト偽造 (CSRF) 6.5.6 情報漏洩と不適切なエラー処理 6.5.7 不完全な認証管理とセッション管理 6.5.8 安全でない暗号化保存 6.5.9 安全でない通信 6.5.10 URL アクセスの制限失敗 6.3 PCI DSS (安全な認証やロギングな ど) に従い、業界のベストプラクティスに基づいてソフトウェアアプリケーションを開発し、ソフトウェア開発ライフサイクル全体を通して情報セキュリティを実現する。これらのプロセスには、以下を含める必要がある。 6.3.1.5 適切な役割ベースのアクセス制御 (RBAC) の検証	◎
A.12.2	**A.12.2 業務用ソフトウェアでの正確な処理** 目的: 業務用ソフトウェアにおける情報の誤り，消失，認可されていない変更又は不正使用を防止するため。	12.2	**12.2 業務用ソフトウェアでの正確な処理**		

JIS Q 27001:2006 (附属書A)		JIS Q 27002:2006		PCIデータセキュリティスタンダード(Ver.1.2)※	関連性の程度
項番		項番	条文		
A.12.2.1		12.2.1	**12.2.1 入力データの妥当性確認**	6.5.7 不完全な認証管理とセッション管理 6.5.1 クロスサイトスクリプティング（XSS） 6.5.2 インジェクションの不具合（特にSQL インジェクション）LDAP と Xpath のインジェクションの不具合、その他のインジェクションの不具合も考慮する。 6.5.6 情報漏洩と不適切なエラー処理 6.3.1.1 すべての入力の検証（クロスサイトスクリプティング、インジェクションの不具合、悪意のあるファイル実行などを防止するため）	○
A.12.2.2	A.12.2.2 **内部処理の管理**	12.2.2	**12.2.2 内部処理の管理**	6.3.1.2 適切なエラー処理の検証	◎
A.12.2.3	A.12.2.3 **メッセージの完全性**	12.2.3	**12.2.3 メッセージの完全性**		
A.12.2.4	A.12.2.4 **出力データの妥当性確認**	12.2.4	**12.2.4 出力データの妥当性確認**		
A.12.3	**A.12.3 暗号による管理策** 目的: 暗号手段によって，情報の機密性，真正性又は完全性を保護するため。	12.3	**12.3 暗号による管理策**		
A.12.3.1	A.12.3.1 **暗号による管理策の利用方針**	12.3.1	**12.3.1 暗号による管理策の利用方針**	2.3 すべてのコンソール以外の管理アクセスを暗号化する。Web ベースの管理やその他のコンソール以外の管理アクセスについては、SSH、VPN、または SSL/TLS などのテクノロジを使用する。 3.4 以下の手法を使用して、すべての保存場所で PAN を少なくとも読み取り不能にする（ポータブルデジタルメディア、バックアップメディア、ログを含む）。 ・強力な暗号化技術をベースにしたワンウェイハッシュ ・トランケーション ・インデックストークンとパッド（パッドは安全に保存する必要がある） ・関連するキー管理プロセスおよび手順を伴う、強力な暗号化 アカウント情報のうち、少なくとも PAN は読み取り不能にする必要がある。 3.5 カード会員データの暗号化に使用される暗号化キーを、漏洩と誤使用から保護する。 3.5.1 暗号化キーへのアクセスを、必要最小限の管理者に制限する。 3.5.2 暗号化キーの保存場所と形式を最小限にし、安全に保存する。 3.6 カード会員データの暗号化に使用されるキーの管理プロセスおよび手順をすべて文書化し、実装する。これには、以下が含まれる。 6.3.1.3 暗号化による安全な保存の検証 6.3.1.4 安全な通信の検証	◎
A.12.3.2	A.12.3.2 **かぎ（鍵）管理**	12.3.2	**12.3.2 かぎ（鍵）管理**	3.6 カード会員データの暗号化に使用されるキーの管理プロセスおよび手順をすべて文書化し、実装する。これには、以下が含まれる。 3.6.1 強力な暗号化キーの生成 3.6.2 安全な暗号化キーの配布 3.6.3 安全な暗号化キーの保存 3.6.4 定期的な暗号化キーの変更 ・関連するアプリケーションで必要とされる場合、自動的に行われることが望ましい（再キー入力など）。 ・少なくとも年 1 回 3.6.5 古いキーまたは危険にさらされた疑いのあるキーの破棄または取替 3.6.6 暗号化キーの知識分割と二重管理 3.6.7 暗号化キーの不正置換の防止 3.6.8 暗号化キー管理者が自身の責務を理解し、それを受諾したことを示す書面への署名 3.4.1（ファイルまたは列レベルのデータベース暗号化ではなく）ディスク暗号化が使用される場合、論理アクセスはネイティブなオペレーティングシステムのアクセス制御メカニズムとは別に管理する必要がある（ローカルユーザーアカウントデータベースを使用しないなどの方法で）。暗号解除キーをユーザアカウントに結合させてはいけない。	◎
A.12.4	**A.12.4 システムファイルのセキュリティ** 目的: システムファイルのセキュリティを確実にするため。	12.4	**12.4 システムファイルのセキュリティ**		
A.12.4.1	A.12.4.1 **運用ソフトウェアの管理**	12.4.1	**12.4.1 運用ソフトウェアの管理**	6.1 すべてのシステムコンポーネントとソフトウェアに、ベンダ提供の最新セキュリティパッチを適用する。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。注: 組織は、パッチインストールの優先順位を付けるために、リスクに基づくアプローチの適用を検討できる。たとえば、重要なインフラストラクチャ（一般に公開されているデバイス、システム、データベースなど）に重要性の低い内部デバイスよりも高い優先順位を付けることで、優先順位の高いシステムおよびデバイスは 1 カ月以内に対処し、重要性の低いシステムおよびデバイスは 3 カ月以内に対処するようにする。 6.4.4 回復手順	◎
A.12.4.2	A.12.4.2 **システム試験データの保護**	12.4.2	**12.4.2 システム試験データの保護**	2.2.4 スクリプト、ドライバ、機能、サブシステム、ファイルシステム、不要な Web サーバなど、不要な機能をすべて削除する。 6.3.4 テストまたは開発に本番環境データ（実際の PAN）を使用しない 6.3.5 本番環境システムがアクティブになる前にテストデータとテストアカウントを削除する 6.3.6 アプリケーションがアクティブになる前、または顧客にリリースされる前に、カスタムアプリケーションアカウント、ユーザー ID、パスワードを削除する	○
A.12.4.3	A.12.4.3 **プログラムソースコードへのアクセス制御**	12.4.3	**12.4.3 プログラムソースコードへのアクセス制御**		
A.12.5	**A.12.5 開発及びサポートプロセスにおけるセキュリティ** 目的: 業務用ソフトウェアシステムのソフトウェア及び情報のセキュリティを維持するため。	12.5	**12.5 開発及びサポートプロセスにおけるセキュリティ** 目的: 業務用ソフトウェアシステムのソフトウェア及び情報のセキュリティを維持するため。 プロジェクト及びサポート環境は，厳しく管理することが望ましい。 業務用ソフトウェアシステムに責任をもつ管理者は，プロジェクト又はサポート環境のセキュリティにも責任を負うことが望ましい。変更によってシステム又は運用環境のセキュリティが損なわれないことを点検するために，管理者は，提案されているすべてのシステム変更のレビューを，確実にすることが望ましい。		

JIS Q 27001:2006 (附属書A)		JIS Q 27002:2006		PCIデータセキュリティスタンダード(Ver.1.2)※	関連性の程度
項番		項番	条文		
A.12.5.1	A.12.5.1 **変更管理手順**	12.5.1	12.5.1 **変更管理手順**	6.3.1 導入前にすべてのセキュリティパッチ、システムとソフトウェア構成の変更をテストする（以下のテストが含まれるが、これらに限定されない）。 6.4 システムコンポーネントへのすべての変更において、変更管理手順に従う。手順には以下を含める必要がある。 6.4.1 影響の文書化 6.4.2 適切な管理者による承認	◎
A.12.5.2	A.12.5.2 **オペレーティングシステム変更後の業務用ソフトウェアの技術的レビュー**	12.5.2	**12.5.2 オペレーティングシステム変更後の業務用ソフトウェアの技術的レビュー**		
A.12.5.3	A.12.5.3 **パッケージソフトウェアの変更に対する制限**	12.5.3	**12.5.3 パッケージソフトウェアの変更に対する制限**	6.1 すべてのシステムコンポーネントとソフトウェアに、ベンダ提供の最新セキュリティパッチを適用する。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。注: 組織は、パッチインストールの優先順位を付けるために、リスクに基づくアプローチの適用を検討できる。たとえば、重要なインフラストラクチャ（一般に公開されているデバイス、システム、データベースなど）に重要性の低い内部デバイスよりも高い優先順位を付けることで、優先順位の高いシステムおよびデバイスは 1 カ月以内に対処し、重要性の低いシステムおよびデバイスは 3 カ月以内に対処するようにする。	○
A.12.5.4	A.12.5.4 **情報の漏えい**	12.5.4	**12.5.4 情報の漏えい**	12.5.2 セキュリティに関する警告および情報を監視して分析し、該当する担当者に通知する。 12.5.5 データへのすべてのアクセスを監視および管理する。	◎
A.12.5.5	A.12.5.5 **外部委託によるソフトウェア開発**	12.5.5	**12.5.5 外部委託によるソフトウェア開発**	6.3.7 コーディングの脆弱性がないことを確認するために、本番または顧客へのリリースの前に、カスタムコードをレビューする 注: このコードレビュー要件は、PCI DSS要件 6.3 で要求されるシステム開発ライフサイクルの一環として、すべてのカスタムコード（内部および公開）に適用される。コードレビューは、知識を持つ社内担当者または第三者が実施できる。一般に公開されている Web アプリケーションは、実装後の脅威および脆弱性に対処するために、PCIDSS 要件 6.6 に定義されている追加コントロールの対象となる。	◎
A.12.6	**A.12.6 技術的ぜい弱性の管理** 目的：公開された技術的ぜい弱性の悪用によって生じるリスクを低減するため。	12.6	**12.6 技術的ぜい弱性管理**		
A.12.6.1	A.12.6.1 **技術的ぜい弱性の管理**	12.6.1	**12.6.1 技術的ぜい弱性の管理**	6.1 すべてのシステムコンポーネントとソフトウェアに、ベンダ提供の最新セキュリティパッチを適用する。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。注: 組織は、パッチインストールの優先順位を付けるために、リスクに基づくアプローチの適用を検討できる。たとえば、重要なインフラストラクチャ（一般に公開されているデバイス、システム、データベースなど）に重要性の低い内部デバイスよりも高い優先順位を付けることで、優先順位の高いシステムおよびデバイスは 1 カ月以内に対処し、重要性の低いシステムおよびデバイスは 3 カ月以内に対処するようにする。 6.2 新たに発見された脆弱性を特定するためのプロセスを確立する（インターネット上で無料で入手可能な警告サービスに加入するなど）。新たな脆弱性の問題に対処するために、PCI DSS 要件 2.2 で要求されているとおりに構成基準を更新する。 6.6 一般公開されている Web アプリケーションは、常時、新しい脅威と脆弱性に対処し、以下のいずれかの手法によって既知の攻撃から保護する必要がある。 ・一般公開されている Web アプリケーションは、アプリケーションのセキュリティ脆弱性を手動/自動で評価するツールまたは手法によって、少なくとも年 1 回および何らかの変更を加えた後にレビューする ・一般公開されている Web アプリケーションの手前に、Web アプリケーションファイアウォールをインストールする 6.3.1 導入前にすべてのセキュリティパッチ、システムとソフトウェア構成の変更をテストする（以下のテストが含まれるが、これらに限定されない）。	◎
A.13	**A.13 情報セキュリティインシデントの管理**	**13**	**13 情報セキュリティインシデントの管理**		
A.13.1	**A.13.1 情報セキュリティの事象及び弱点の報告** 目的：情報システムに関連する情報セキュリティの事象及び弱点を，時機を失しない是正処置をとることができるやり方で連絡することを確実にするため。	13.1	**13.1 情報セキュリティの事象及び弱点の報告**		
A.13.1.1	A.13.1.1 **情報セキュリティ事象の報告**	13.1.1	**13.1.1 情報セキュリティ事象の報告**	12.9 インシデント対応計画を実施する。システム違反に直ちに対応できるよう準備する。 12.9.1 システム違反が発生した場合に実施されるインシデント対応計画を作成する。計画では、最低限、以下に対応する。 Ÿ ペイメントブランドへの通知を最低限含む、侵害が発生した場合の役割、責任、および伝達と連絡に関する戦略 ・具体的なインシデント対応手順 ・ビジネスの復旧および継続手順 ・データバックアッププロセス ・侵害の報告に関する法的要件の分析 ・すべての重要なシステムコンポーネントを対象とした対応 ・ペイメントブランドによるインシデント対応手順の参照または包含	◎
A.13.1.2	A.13.1.2 **セキュリティ弱点の報告**	13.1.2	**13.1.2 セキュリティ弱点の報告**		

JIS Q 27001:2006 (附属書A)		JIS Q 27002:2006		PCIデータセキュリティスタンダード(Ver.1.2)※	関連性の程度
項番		項番	条文		
A.13.2	**A.13.2 情報セキュリティインシデントの管理及びその改善** 目的：情報セキュリティインシデントの管理に，一貫性のある効果的な取組み方法を用いることを確実にするため。	13.2	**13.2 情報セキュリティインシデントの管理及びその改善** 目的：情報セキュリティインシデントの管理に，一貫性のある効果的な取組み方法を用いることを確実にするため。 情報セキュリティの事象及び弱点の報告があったとき直ちに，それらを効果的に取り扱える責任体制及び手順を備えることが望ましい。情報セキュリティインシデントへの対応，並びに情報セキュリティインシデントの監視，評価及び包括的管理に対して，継続的改善の手続をとることが望ましい。 証拠が必要となる場合は，法的要求事項を順守することを確実にするために，証拠を収集することが望ましい。	12.5 個人またはチームに以下の情報セキュリティ管理責任を割り当てる。 12.5.2 セキュリティに関する警告および情報を監視して分析し、該当する担当者に通知する。 12.9.6 得られた教訓を踏まえてインシデント対応計画を変更および改善し、産業の発展を組み込むプロセスを作成する	◎
A.13.2.1	A.13.2.1 **責任及び手順**	13.2.1	**13.2.1 責任及び手順**	12.5.3 セキュリティインシデントの対応およびエスカレーション手順を確立、文書化、および周知して、あらゆる状況をタイムリーかつ効果的に処理する。 12.9.4 セキュリティ違反への対応を担当するスタッフに適切なトレーニングを提供する。 12.9.5 侵入検知、侵入防止、およびファイル整合性監視システムからの警告を含める。	◎
A.13.2.2	A.13.2.2 **情報セキュリティインシデントからの学習**	13.2.2	**13.2.2 情報セキュリティインシデントからの学習**	12.9.6 得られた教訓を踏まえてインシデント対応計画を変更および改善し、産業の発展を組み込むプロセスを作成する。	◎
A.13.2.3	A.13.2.3 **証拠の収集**	13.2.3	**13.2.3 証拠の収集**	10.5 変更できないよう、監査証跡をセキュリティで保護する。	◎
				10.5.1 監査証跡の表示を、仕事関連のニーズを持つ人物のみに制限する。 10.5.2 監査証跡ファイルを不正な変更から保護する。 10.5.3 監査証跡ファイルを、変更が困難な一元管理ログサーバまたは媒体に即座にバックアップする。 10.5.4 外部に公開されているテクノロジのログを内部 LAN 上のログサーバに書き込む。 10.5.5 ログに対してファイル整合性監視または変更検出ソフトウェアを使用して、既存のログデータを変更すると警告が生成されるようにする（ただし、新しいデータの追加は警告を発生させない）。	○
A.14	**A.14 事業継続管理**	**14**	**事業継続管理**		
A.14.1	**A.14.1 事業継続管理における情報セキュリティの側面** 目的：情報システムの重大な故障又は災害の影響からの事業活動の中断に対処するとともに，それらから重要な業務プロセスを保護し，また，事業活動及び重要な業務プロセスの時機を失しない再開を確実にするため。	14.1	**14.1 事業継続管理における情報セキュリティの側面**		
A.14.1.1	A.14.1.1 **事業継続管理手続への情報セキュリティの組込み**	14.1.1	**14.1.1 事業継続管理手続への情報セキュリティの組込み**	12.9 インシデント対応計画を実施する。システム違反に直ちに対応できるよう準備する。 12.9.1 システム違反が発生した場合に実施されるインシデント対応計画を作成する。計画では、最低限、以下に対応する。 ・ペイメントブランドへの通知を最低限含む、侵害が発生した場合の役割、責任、および伝達と連絡に関する戦略 ・具体的なインシデント対応手順 ・ビジネスの復旧および継続手順 ・データバックアッププロセス ・侵害の報告に関する法的要件の分析 ・すべての重要なシステムコンポーネントを対象とした対応 ・ペイメントブランドによるインシデント対応手順の参照または包含 12.9.2 計画を少なくとも年に一度テストする。 12.9.3 警告に 24 時間体制で対応できる担当者を指定する。 12.5.3 セキュリティインシデントの対応およびエスカレーション手順を確立、文書化、および周知して、あらゆる状況をタイムリーかつ効果的に処理する。	◎
A.14.1.2	A.14.1.2 **事業継続及びリスクアセスメント**	14.1.2	**14.1.2 事業継続及びリスクアセスメント**		
A.14.1.3	A.14.1.3 **情報セキュリティを組み込んだ事業継続計画の策定及び実施**	14.1.3	**14.1.3 情報セキュリティを組み込んだ事業継続計画の策定及び実施**		
A.14.1.4	A.14.1.4 **事業継続計画策定の枠組み**	14.1.4	**14.1.4 事業継続計画策定の枠組み**	12.9.1 システム違反が発生した場合に実施されるインシデント対応計画を作成する。計画では、最低限、以下に対応する。 ・ペイメントブランドへの通知を最低限含む、侵害が発生した場合の役割、責任、および伝達と連絡に関する戦略 ・具体的なインシデント対応手順 ・ビジネスの復旧および継続手順 ・データバックアッププロセス ・侵害の報告に関する法的要件の分析 ・すべての重要なシステムコンポーネントを対象とした対応 ・ペイメントブランドによるインシデント対応手順の参照または包含	◎
A.14.1.5	A.14.1.5 **事業継続計画の試験，維持及び再評価**	14.1.5	**14.1.5 事業継続計画の試験，維持及び再評価**	12.9.2 計画を少なくとも年に一度テストする。	◎
A.15	**A.15 順守**	**15**	**順守**		
A.15.1	**A.15.1 法的要求事項の順守** 目的：法令，規制又は契約上のあらゆる義務，及びセキュリティ上のあらゆる要求事項に対する違反を避けるため。 注記 法的順守は，しばしば，コンプライアンスといわれることがある。	15.1	**15.1 法的要求事項の順守**		
A.15.1.1	A.15.1.1 **適用法令の識別**	15.1.1	**15.1.1 適用法令の識別**		
A.15.1.2	A.15.1.2 **知的財産権（IPR）**	15.1.2	**15.1.2 知的財産権（IPR）**		

JIS Q 27001:2006 (附属書A)		JIS Q 27002:2006		PCIデータセキュリティスタンダード(Ver.1.2)※	関連性の程度
項番		項番	条文		
A.15.1.3	A.15.1.3 **組織の記録の保護**	15.1.3	**15.1.3 組織の記録の保護**	3.1 保存するカード会員データは最小限に抑える。 データの保存と廃棄に関するポリシーを作成する。 データ保存ポリシーに従って、保存するデータ量と保存期間を、業務上、法律上、規則上必要な範囲に限定する。 10.5 変更できないよう、監査証跡をセキュリティで保護する。 10.5.1 監査証跡の表示を、仕事関連のニーズを持つ人物のみに制限する。 10.5.2 監査証跡ファイルを不正な変更から保護する。 10.5.3 監査証跡ファイルを、変更が困難な一元管理ログサーバまたは媒体に即座にバックアップする。 10.5.4 外部に公開されているテクノロジのログを内部LAN 上のログサーバに書き込む。 10.5.5 ログに対してファイル整合性監視または変更検出ソフトウェアを使用して、既存のログデータを変更すると警告が生成されるようにする（ただし、新しいデータの追加は警告を発生させない）。	◎
A.15.1.4	A.15.1.4 **個人データ及び個人情報の保護**	15.1.4	**15.1.4 個人データ及び個人情報の保護**		
A.15.1.5	A.15.1.5 **情報処理施設の不正使用防止**	15.1.5	**15.1.5 情報処理施設の不正使用防止**		
A.15.1.6	A.15.1.6 **暗号化機能に対する規制**	15.1.6	**15.1.6 暗号化機能に対する規制**		
A.15.2	**A.15.2 セキュリティ方針及び標準の順守, 並びに技術的順守** 目的: 組織のセキュリティ方針及び標準類へのシステムの順守を確実にするため。	15.2	**15.2 セキュリティ方針及び標準の順守, 並びに技術的順守**	10.6 少なくとも日に一度、すべてのシステムコンポーネントのログを確認する。ログの確認には、侵入検知システム（IDS）や認証、認可、アカウンティングプロトコル（AAA）サーバ（RADIUS など）のようなセキュリティ機能を実行するサーバを含める必要がある。 注: 要件 10.6 に準拠するために、ログの収集、解析、および警告ツールを使用することができます。	○
A.15.2.1	A.15.2.1 **セキュリティ方針及び標準の順守**	15.2.1	**15.2.1 セキュリティ方針及び標準の順守**	12.1.1 すべての PCI DSS 要件に対応する。 12.1.3 レビューを少なくとも年に一度含め、環境の変化に合わせて更新する。	◎
A.15.2.2	A.15.2.2 **技術的順守の点検**	15.2.2	**15.2.2 技術的順守点検**	11.1 無線アナライザを少なくとも四半期に一度使用して、または使用中のすべての無線デバイスを識別するための無線IDS/IPS を導入し、無線アクセスポイントの存在をテストする。 11.2 内部および外部ネットワークの脆弱性スキャンを少なくとも四半期に一度およびネットワークでの大幅な変更（新しいシステムコンポーネントのインストール、ネットワークトポロジの変更、ファイアウォール規則の変更、製品アップグレードなど）後に実行する。 注: 四半期に一度の外部の脆弱性スキャンは、PCI（Payment Card Industry）セキュリティ基準審議会（PCI SSC）によって資格を与えられた Approved Scanning Vendor(ASV)によって実行される必要があります。ネットワーク変更後に実施されるスキャンは、会社の内部スタッフによって実行することができます。 11.3 外部および内部のペネトレーションテストを少なくとも年に一度および大幅なインフラストラクチャまたはアプリケーションのアップグレードや変更（オペレーティングシステムのアップグレード、環境へのサブネットワークの追加、環境への Web サーバの追加など）後に実行する。これらのペネトレーションテストには以下を含める必要がある。 11.3.1 ネットワーク層のペネトレーションテスト 11.3.2 アプリケーション層のペネトレーションテスト	◎
				11.4 侵入検知システムや侵入防止システムを使用して、カード会員データ環境内のすべてのトラフィックを監視し、侵害の疑いがある場合は担当者に警告する。すべての侵入検知および防止エンジンを最新状態に保つ。 11.5 ファイル整合性監視ソフトウェアを導入して重要なシステムファイル、構成ファイル、またはコンテンツファイルの不正な変更を担当者に警告し、重要なファイルの比較を少なくとも週に一度実行するようにソフトウェアを構成する。 注: ファイル整合性監視において、重要なファイルとは通常、定期的に変更されないが、その変更がシステムの侵害や侵害のリスクを示す可能性があるファイルのことです。ファイル整合性監視製品では通常、関連オペレーティングシステム用の重要なファイルがあらかじめ構成されています。カスタムアプリケーション用のファイルなど、その他の重要なファイルは、事業体（つまり、加盟店またはサービスプロバイダ）による評価および定義が必要です。	
A.15.3	**A.15.3 情報システムの監査に対する考慮事項** 目的: 情報システムに対する監査手続の有効性を最大限にするため, 及びシステムの監査プロセスへの干渉及び／又はシステムの監査プロセスからの干渉を最小限にするため。	15.3	**15.3 情報システムの監査に対する考慮事項**		
A.15.3.1	A.15.3.1 **情報システムの監査に対する管理策**	15.3.1	**15.3.1 情報システムの監査に対する管理策**	10.5.1 監査証跡の表示を、仕事関連のニーズを持つ人物のみに制限する。 10.5.2 監査証跡ファイルを不正な変更から保護する。 10.5.3 監査証跡ファイルを、変更が困難な一元管理ログサーバまたは媒体に即座にバックアップする。 10.5.4 外部に公開されているテクノロジのログを内部LAN 上のログサーバに書き込む。 10.5.5 ログに対してファイル整合性監視または変更検出ソフトウェアを使用して、既存のログデータを変更すると警告が生成されるようにする（ただし、新しいデータの追加は警告を発生させない）。	◎
A.15.3.2	A.15.3.2 **情報システムの監査ツールの保護**	15.3.2	**15.3.2 情報システムの監査ツールの保護**		

ISMS と個人情報系ガイドラインとのマッピング

マッピング表の補足

・本マッピング表は、あくまでも参考という位置付けでご利用いただけますよう
お願い申し上げます。

・例えば、JIS Q 27001や27002の1つの項目に対して必ずしも1対1対応をしているの
ではない場合もあり、複数の項目に関連している場合もあり、その逆もあります
ので、参考レベルでご覧いただければ幸いです。

JIS Q 27001:2006 (附属書A)		JIS Q 27002:2006		経済産業分野のうち	経済産業分野を対象とする
項番		項番	条文	信用分野におけるガイドライン	ガイドライン (H20.2)
	管理目的及び管理策				
	表A.1に規定した管理目的及び管理策は，JIS Q 27002: 2006の箇条5～15までに掲げられているものをそのまま取り入れて配列したものである。この表は，管理目的及び管理策のすべてを網羅してはいないので，組織は，管理目的及び管理策の追加が必要であると考えてよい。この表の中の管理目的及び管理策は，本体の4.2.1に規定するISMSのプロセスの一部として，選択しなければならない。				
	JIS Q 27002: 2006の箇条5～15までは，A.5～A.15までに規定した管理策を支える，導入への助言及び最適な実施のための手引を提供している。				
A.5	**セキュリティ基本方針**	**5**	**情報セキュリティ基本方針**		
A.5.1	**A.5.1 情報セキュリティ基本方針** 目的：情報セキュリティのための経営陣の方向性及び支持を，事業上の要求事項，関連する法令及び規制に従って規定するため。	5.1	**5.1 情報セキュリティ基本方針**		
A.5.1.1	A.5.1.1 **情報セキュリティ基本方針文書**	5.1.1	**5.1.1 情報セキュリティ基本方針文書**	【組織①】 与信事業者等は、個人データの安全管理に関する事項を含んだ個人情報保護に関する考え方や方針に関する宣言を策定し、公表しなければならない。 ※「個人データの安全管理に関する事項を含んだ個人情報保護に関する考え方や方針に関する宣言」には、例えば、いわゆるプライバシーポリシー、プライバシーステートメント等が該当する。 【組織②】 与信事業者等は、本ガイドラインに従った個人データの安全管理措置を定めた規程や手順書等（以下「規程等」という。）を整備しなければならない。	【組織②】個人データの取扱いに関する規程等の整備とそれらに従った運用 【組織②】個人データを取り扱う情報システムの安全管理措置に関する規程等の整備とそれらに従った運用 【組織②】個人データの取扱いに係る建物、部屋、保管庫等の安全管理に関する規程等の整備とそれらに従った運用 【組織②】個人データの取扱いを委託する場合における委託先の選定基準、委託契約書のひな型、委託先における委託した個人データの取扱状況を確認するためのチェックリスト等の整備とそれらに従った運用
A.5.1.2	A.5.1.2 **情報セキュリティ基本方針のレビュー**	5.1.2	**5.1.2 情報セキュリティ基本方針のレビュー**	【組織⑨】 与信事業者等は、個人データの安全管理措置の評価、見直し及び改善をしなければならない。	【組織④】監査責任者から受ける監査報告、個人データに対する社会通念の変化及び情報技術の進歩に応じた定期的な安全管理措置の見直し及び改善
A.6	**A.6 情報セキュリティのための組織**	**6**	**情報セキュリティのための組織**		
A.6.1	**A.6.1 内部組織** 目的：組織内の情報セキュリティを管理するため。	6.1	**6.1 内部組織**		
A.6.1.1	A.6.1.1 **情報セキュリティに対する経営陣の責任**	6.1.1	**6.1.1 情報セキュリティに対する経営陣の責任**		
A.6.1.2	A.6.1.2 **情報セキュリティの調整**	6.1.2	**6.1.2 情報セキュリティの調整**		
A.6.1.3	A.6.1.3 **情報セキュリティ責任の割当て**	6.1.3	**6.1.3 情報セキュリティ責任の割当て**	【組織③】 与信事業者等は、個人データの安全管理に関する従業者の役割及び責任を明確にしなければならない。 その際、与信事業者等は、職務分掌規程、契約書その他の従業者に関する規程類において個人データの安全管理に関する従業者の役割及び責任を具体的に定めなければならない。 なお、「従業者」とは、個人情報取扱事業者の組織内にあって直接間接に事業者の指揮監督を受けて事業者の業務に従事している者をいい、雇用関係にある従業員（正社員、契約社員、嘱託社員、パート社員、アルバイト社員等）のみならず、取締役、執行役、理事、監事役、監事、派遣社員等も含まれる。 【組織④】 与信事業者等は、個人情報保護に関する責任者を設置しなければならない。 ※上記には、例えば、いわゆる、チーフ・プライバシー・オフィサー（CPO）等が該当する。 ※個人データの取扱いにおける作業責任者の設置及び作業担当者の限定、個人データを取り扱う情報システム運用責任者の設置及び担当者（システム管理者を含む。）の限定を行うこととする。 【組織⑤】 与信事業者等は、個人データの管理をする者を、個人データを取り扱う部署等ごとに設置しなければならない。	【組織①】従業者の役割・責任の明確化 【組織①】個人情報保護管理者（いわゆる、チーフ・プライバシー・オフィサー（ＣＰＯ））の設置 【組織①】個人データの取扱い（取得・入力、移送・送信、利用・加工、保管・バックアップ、消去・廃棄等の作業）における作業責任者の設置及び作業担当者の限定 【組織①】個人データを取り扱う情報システム運用責任者の設置及び担当者（システム管理者を含む。）の限定 【組織①】個人データの取扱いにかかわるそれぞれの部署の役割と責任の明確化 【組織①】監査責任者の設置 【組織①】監査実施体制の整備 【取得①】個人データを取得する際の作業責任者の明確化 【取得①】取得した個人データを情報システムに入力する際の作業責任者の明確化（以下、併せて「取得・入力」という。） 【移送①】個人データを移送・送信する際の作業責任者の明確化 【利用①】個人データを利用・加工する際の作業責任者の明確化 【保管①】個人データを保管・バックアップする際の作業責任者の明確化 【消去①】個人データを消去する際の作業責任者の明確化 【消去①】個人データを保管している機器、記録している媒体を廃棄する際の作業責任者の明確化
A.6.1.4	A.6.1.4 **情報処理設備の認可プロセス**	6.1.4	**6.1.4 情報処理設備の認可手続**		
A.6.1.5	A.6.1.5 **秘密保持契約**	6.1.5	**6.1.5 機密保持契約**	【人①】 与信事業者等は、雇用契約時及び委託契約時において、非開示契約その他の個人データの安全管理措置に関する事項を盛り込んだ契約を締結しなければならない。 ※雇用契約又は委託契約等における非開示条項は、一定期間ごとに確認することとし、また、契約終了後も一定期間有効であるようにすることとする。 ※個人データを取り扱う従業者ではないが、個人データを保有する建物等に立ち入る可能性がある者、個人データを取り扱う情報システムにアクセスする可能性がある者についてもアクセス可能な関係者の範囲及びアクセス条件について契約書等に明記することとする。なお、個人データを取り扱う従業者以外の者には、情報システムの開発・保守関係者、清掃担当者、警備員等が含まれる。	【人①】従業者の採用時又は委託契約時における非開示契約の締結
A.6.1.6	A.6.1.6 **関係当局との連絡** 管理策 関係当局との適切な連絡体制を維持しなければならない。	6.1.6	**6.1.6 関係当局との連絡** 実施の手引 組織は，法が破られたと疑われる場合に，いつ，だれが関係当局（例えば，法の執行機関，監督官庁）に連絡するか，また，特定した情報セキュリティインシデントをいかにして時機を失せずに報告するかの手順を備えることが望ましい。 インターネットからの攻撃下にある組織は，外部の第三者（例えば，インターネットサービス提供者，通信事業者）が攻撃元に対して対策をとることを必要とする場合もある。	【組織③】 与信事業者等は、個人データの安全管理に関する従業者の役割及び責任を明確にしなければならない。 その際、与信事業者等は、職務分掌規程、契約書その他の従業者に関する規程類において個人データの安全管理に関する従業者の役割及び責任を具体的に定めなければならない。 なお、「従業者」とは、個人情報取扱事業者の組織内にあって直接間接に事業者の指揮監督を受けて事業者の業務に従事している者をいい、雇用関係にある従業員（正社員、契約社員、嘱託社員、パート社員、アルバイト社員等）のみならず、取締役、執行役、理事、監査役、監事、派遣社員等も含まれる。	【組織①】漏えい等の事故発生時における主務大臣及び認定個人情報保護団体等に対する報告体制の整備.
A.6.1.7	A.6.1.7 **専門組織との連絡**	6.1.7	**6.1.7 専門組織との連絡**		

JIS Q 27001:2006 (附属書A)		JIS Q 27002:2006		経済産業分野のうち	経済産業分野を対象とするガイドライン (H20.2)
項番		項番	条文	個用分野におけるガイドライン	
A.6.1.8	A.6.1.8 **情報セキュリティの独立したレビュー**	6.1.8	**6.1.8 情報セキュリティの独立したレビュー**	【組織⑧】 与信事業者等は、外部監査その他の本ガイドラインに従った安全管理措置が実施されていることを確認する仕組みを導入しなければならない。 （別紙） 4．外部監査 個人信用情報機関は、本ガイドラインに従った取組が確実に実施されていることを確認する仕組みとして、外部監査を行うこととする。	【組織④】監査計画の立案と、計画に基づく監査（内部監査又は外部監査）の実施 【取得④】手続の明確化と手続に従った実施及び作業担当者の識別、認証、権限付与の実施状況の確認 【取得④】アクセスの記録、保管と、権限外作業の有無の確認 【移送④】手続の明確化と手続に従った実施及び作業担当者の識別、認証、権限付与の実施状況の確認 【移送④】アクセスの記録、保管と、権限外作業の有無の確認 【利用④】手続の明確化と手続に従った実施及び作業担当者の識別、認証、権限付与の実施状況の確認 【利用④】アクセスの記録、保管と権限外作業の有無の確認 【保管④】手続の明確化と手続に従った実施及び作業担当者の識別、認証、権限付与の実施状況の確認 【保管④】アクセスの記録、保管と権限外作業の有無の確認 【消去④】手続の明確化と手続に従った実施及び作業担当者の識別、認証、権限付与の実施状況の確認 【消去④】アクセスの記録、保管、権限外作業の有無の確認
A.6.2	**A.6.2 外部組織** 目的：外部組織によってアクセス，処理，通信，又は管理される組織の情報及び情報処理施設のセキュリティを維持するため。	6.2	**6.2 外部組織**		
A.6.2.1	A.6.2.1 **外部組織に関係したリスクの識別**	6.2.1	**6.2.1 外部組織に関係したリスクの識別**	（別紙） 2．個人信用情報機関による会員管理 2－1 入会審査等 2－1－1 個人信用情報機関は、新たに入会する会員について、当該個人信用情報機関の個人情報データベース等にアクセスする会員の照会端末の設置状況及びアクセス権限の設定状況の確認を行うこととする。そのほか、個人情報データベース等にアクセスすることについて適正な事業者のみ会員となるようあらかじめ定めた入会審査基準に基づき、厳正に入会審査を行うこととする。 2－1－2 個人信用情報機関は、会員が入会審査基準を満たし続けているかどうか定期的に確認することとする。 2－1－3 個人信用情報機関は、法の制定に伴い入会審査基準を改定している場合には、改定前の入会審査基準により入会した会員を改定後の入会審査基準に基づいて再審査をすることとする。 2－1－4 会員においては、入会後も個人信用情報機関によるモニタリングに協力することが求められ、個人信用情報機関からの求めに応じて必要な情報を提供できるよう、与信申込書や契約書等、個人信用情報機関の個人情報データベース等へのアクセスが正当なものであることを証明することができる資料等を保管しておくよう必要があるところ、個人信用情報機関は、これらの事項を入会審査基準や会員規約に盛り込む等必要なルールを定めることとする。 2－2 会員モニタリング 個人信用情報機関は、会員が、消費者からの与信申込みがないにもかかわらず任意の個人について個人信用情報機関の個人情報データベース等にアクセスして情報を入手する等の不正利用をすることのないよう、会員に対する必要かつ適切なモニタリングを行うこととする。そのほか、個人信用情報機関は、会員が、個人信用情報機関の個人情報データベース等に適正にアクセスして入手した個人の支払能力に関する情報を支払能力調査目的以外の目的に不正利用することのないよう、会員に対する必要かつ適切なモニタリングを行うこととする。また、個人信用情報機関は、会員モニタリングの運用基準についても整理することとする。 2－3 不正利用に対する処分 2－3－1 個人信用情報機関は、会員による上記の不正利用があった場合、あらかじめ定めた処分に関する規程に基づき、公表、利用停止、退会その他の処分をすることとする。 2－3－2 個人信用情報機関は、どのような不正についてどの処分をするか、また、処分をするか否かの判断基準、その判断を行うための組織体制・意思決定プロセスを予め明確に定めておくこととする。	
A.6.2.2	A.6.2.2 **顧客対応におけるセキュリティ**	6.2.2	**6.2.2 顧客対応におけるセキュリティ**		
A.6.2.3	A.6.2.3 **第三者との契約におけるセキュリティ**	6.2.3	**6.2.3 第三者との契約におけるセキュリティ**	【人①】 与信事業者等は、雇用契約時及び委託契約時において、非開示契約その他の個人データの安全管理措置に関する事項を盛り込んだ契約を締結しなければならない。 ※雇用契約又は委託契約等における非開示条項は、一定期間ごとに確認することとし、また、契約終了後も一定期間有効であるようにすること。 ※個人データを取り扱う従業者ではないが、個人データを保有する建物等に立ち入る可能性がある者、個人データを取り扱う情報システムにアクセスする可能性がある者についてもアクセス可能な関係者の範囲及びアクセス条件について契約書等に明記することとする。なお、個人データを取り扱う従業者以外の者には、情報システムの開発・保守関係者、清掃担当者、警備員等が含まれる。 【委託②】 与信事業者等は、委託契約において、個人データの取扱いに関して委託者、受託者双方が同意した内容を契約に盛り込まなければならない。 （別紙） 1．個人信用情報機関自らの安全管理措置 1－1 複数の個人信用情報機関が各々の保有個人データを共通の情報処理会社に委託してその個人情報データベース等に集約して管理している場合には、当該個人情報データベース等にアクセス可能なすべての個人信用情報機関は、同様の高い水準の安全管理措置を講じなければならない。また、当該個人情報データベース等へのアクセスと情報保護に関してそれぞれの責任関係を明確にしておかなければならない。	【人①】従業者の採用時又は委託契約時における非開示契約の締結 【組織②】個人データの取扱いを委託する場合における委託先の選定基準、委託契約書のひな型、委託先における委託した個人データの取扱状況を確認するためのチェックリスト等の整備とそれらに従った運用
A.7	**A.7 資産の管理**	7	**資産の管理**		
A.7.1	**A.7.1 資産に対する責任** 目的：組織の資産を適切に保護し，維持するため。	7.1	**7.1 資産に対する責任**		

JIS Q 27001:2006 (附属書A)		JIS Q 27002:2006		経済産業分野のうち	経済産業分野を対象とする
項番		項番	条文	信用分野におけるガイドライン	ガイドライン (H20.2)
A.7.1.1	A.7.1.1 **資産目録**	7.1.1	**7.1.1 資産目録**	【組織⑦】 与信事業者等は、個人データの取扱状況を一覧できる手段を整備し、最新の状態となるように維持しなければならない。	【組織③】個人データについて、取得する項目、明示・公表等を行った利用目的、保管場所、保管方法、アクセス権限を有する者、利用期限、その他個人データの適正な取扱いに必要な情報を記した個人データ取扱台帳の整備 【組織③】個人データ取扱台帳の内容の定期的な確認による最新状態の維持
A.7.1.2	A.7.1.2 **資産の管理責任者**	7.1.2	**7.1.2 資産の管理責任者**		
A.7.1.3	A.7.1.3 **資産利用の許容範囲**	7.1.3	**7.1.3 資産利用の許容範囲**		
A.7.2	**A.7.2 情報の分類** 目的: 情報の適切なレベルでの保護を確実にするため。	7.2	**7.2 情報の分類**		
A.7.2.1	A.7.2.1 **分類の指針**	7.2.1	**7.2.1 分類の指針**		
A.7.2.2	A.7.2.2 **情報のラベル付け及び取扱い**	7.2.2	**7.2.2 情報のラベル付け及び取扱い**	【組織②】 与信事業者等は、本ガイドラインに従った個人データの安全管理措置を定めた規程や手順書等（以下「規程等」という。）を整備しなければならない。 【技術⑥】 与信事業者等は、個人データの移送・送信時における適切な対策を実施しなければならない。 ・個人データを含む電子媒体を移送する場合、暗号化又はパスワードロックを行うこと。 ・インターネットを経由して電子メールに添付して個人データを送信する場合に、電子メール自体を暗号化すること。 ※なお、暗号鍵の長さ、使用する暗号アルゴリズム、パスワードの文字数や複雑性については、個人データを含む電子媒体を紛失した場合に本人が被る権利利益の大きさを考慮し適切に設定することが望ましい。	【組織②】個人データの取扱いに関する規程等の整備とそれらに従った運用 【取得②】取得・入力する際の手続の明確化 【移送②】個人データを移送・送信する際の手続の明確化 【利用②】個人データを利用・加工する際の手続の明確化 【保管②】個人データを保管・バックアップする際の手続の明確化 【消去②】消去・廃棄する際の手続の明確化 【物理②】氏名、住所、メールアドレス等を記載した個人データとそれ以外の個人データの分離保管
A.8	**A.8 人的資源のセキュリティ**	8	**8 人的資源のセキュリティ**		
A.8.1	**A.8.1 雇用前** 目的: 従業員，契約相手及び第三者の利用者がその責任を理解し，求められている役割にふさわしいことを確実にするとともに，盗難，不正行為，又は施設の不正使用のリスクを低減するため。	8.1	**8.1 雇用前**		
A.8.1.1	A.8.1.1 **役割及び責任**	8.1.1	**8.1.1 役割及び責任**	【組織③】 与信事業者等は、個人データの安全管理に関する従業者の役割及び責任を明確にしなければならない。 その際、与信事業者等は、職務分掌規程、契約書その他の従業者に関する規程類において個人データの安全管理に関する従業者の役割及び責任を具体的に定めなければならない。 なお、「従業者」とは、個人情報取扱事業者の組織内にあって直接間接に事業者の指揮監督を受けて事業者の業務に従事している者をいい、雇用関係にある従業員（正社員、契約社員、嘱託社員、パート社員、アルバイト社員等）のみならず、取締役、執行役、理事、監査役、監事、派遣社員等も含まれる。	【組織①】従業者の役割・責任の明確化 【取得②】定められた手続による取得・入力の実施 【移送②】定められた手続による移送・送信の実施 【利用②】定められた手続による利用・加工の実施 【保管②】定められた手続による保管・バックアップの実施 【消去②】定められた手続による消去・廃棄の実施
A.8.1.2	A.8.1.2 **選考**	8.1.2	**8.1.2 選考**		
A.8.1.3	A.8.1.3 **雇用条件**	8.1.3	**8.1.3 雇用条件**	【人①】 与信事業者等は、雇用契約時及び委託契約時において、非開示契約その他の個人データの安全管理措置に関する事項を盛り込んだ契約を締結しなければならない。 ※雇用契約又は委託契約等における非開示条項は、一定期間ごとに確認することとし、また、契約終了後も一定期間有効であるようにすることとする。 ※個人データを取り扱う従業者ではないが，個人データを保有する建物等に立ち入る可能性がある者，個人データを取り扱う情報システムにアクセスする可能性がある者についてもアクセス可能な関係者の範囲及びアクセス条件について契約書等に明記することとする。なお，個人データを取り扱う従業者以外の者には，情報システムの開発・保守関係者、清掃担当者、警備員等が含まれる。	【人①】従業者の採用時又は委託契約時における非開示契約の締結 【人①】非開示契約に違反した場合の措置に関する規程の整備
A.8.2	**A.8.2 雇用期間中** 目的: 従業員，契約相手及び第三者の利用者の，情報セキュリティの脅威及び諸問題，並びに責任及び義務に対する認識を確実なものとし，通常の業務の中で組織の情報セキュリティ基本方針を維持し，人による誤りのリスクを低減できるようにすることを確実にするため。	8.2	**8.2 雇用期間中**		
A.8.2.1	A.8.2.1 **経営陣の責任**	8.2.1	**8.2.1 経営陣の責任**		
A.8.2.2	A.8.2.2 **情報セキュリティの意識向上，教育及び訓練**	8.2.2	**8.2.2 情報セキュリティの意識向上，教育及び訓練**	【人③】 与信事業者等は、従業者に対し、個人データの安全管理に関する教育・訓練を継続的に実施しなければならない。	【人②】個人データ及び情報システムの安全管理に関する従業者の役割及び責任を定めた内部規程等についての周知 【人②】個人データ及び情報システムの安全管理に関する従業者の役割及び責任についての教育・訓練の実施 【人②】従業者に対する必要かつ適切な教育・訓練が実施されていることの確認
A.8.2.3	A.8.2.3 **懲戒手続**	8.2.3	**8.2.3 懲戒手続**	【人②】 与信事業者等は、職務規程等に、個人データの安全管理措置に関する事項を盛り込まなければならない。	【人①】非開示契約に違反した場合の措置に関する規程の整備
A.8.3	**A.8.3 雇用の終了又は変更** 目的: 従業員，契約相手及び第三者の利用者の組織からの離脱又は雇用の変更を所定の方法で行うことを確実にするため。	8.3	**8.3 雇用の終了又は変更**		
A.8.3.1	A.8.3.1 **雇用の終了又は変更に関する責任**	8.3.1	**8.3.1 雇用の終了又は変更に関する責任**		
A.8.3.2	A.8.3.2 **資産の返却**	8.3.2	**8.3.2 資産の返却**		
A.8.3.3	A.8.3.3 **アクセス権の削除**	8.3.3	**8.3.3 アクセス権の削除**		
A.9	**A.9 物理的及び環境的セキュリティ**	9	**物理的及び環境的セキュリティ**		
A.9.1	**A.9.1 セキュリティを保つべき領域** 目的: 組織の施設及び情報に対する認可されていない物理的アクセス，損傷及び妨害を防止するため。	9.1	**9.1 セキュリティを保つべき領域**		
A.9.1.1	A.9.1.1 **物理的セキュリティ境界**	9.1.1	**9.1.1 物理的セキュリティ境界**	【物理③】 与信事業者等は、機器・装置等を物理的に保護しなければならない。 （別紙） 1．個人信用情報機関自らの安全管理措置 1－2 個人信用情報機関は、個人情報データベース等へのアクセスを伴う業務を取り扱うフロア（以下「業務フロア」という）については、消費者への開示スペース等、他のフロアとは構造的に隔離されているようにしなければならない。	【組織②】個人データの取扱いに係る建物、部屋、保管庫等の安全管理に関する規程等の整備とそれらに従った運用

JIS Q 27001:2006 (附属書A)		JIS Q 27002:2006		経済産業分野のうち	経済産業分野を対象とする
項番		項番	条文	個別分野におけるガイドライン	ガイドライン (H20.2)
				〔別紙〕 1. 個人信用情報機関自らの安全管理措置 1－4 個人信用情報機関は、業務フロア内については、監視カメラにより定常的に室内状況を記録し、その映像を一定期間保存することとし、管理責任者が定期的に記録をチェックしなければならない。	
A.9.1.2	A.9.1.2 **物理的入退管理策**	9.1.2	**9.1.2 物理的入退管理策**	【物理①】 与信事業者等は、個人データを取り扱う施設に応じて、以下の管理を行わなければならない。 〔事業施設及び個人データ処理施設における管理〕 ・施錠等による施設及び室の管理 〔個人データ処理施設における管理〕 ・入退館〔室〕をする者の資格付与及び認証 ・入退館〔室〕の記録 ※「事務施設」とは、例えば本社、支社、営業店等の執務室を含み、「個人データ処理施設」とは、例えば電算センター、コールセンター、サーバルーム等を含む。 〔別紙〕 1. 個人信用情報機関自らの安全管理措置 1－3 個人信用情報機関は、業務フロアの出入り口については、ICカード認証等により電子的に入退室の認証管理を行い、その入退室記録が電子的に一定期間保存される仕組みを採用しなければならない。	【物理①】個人データを取り扱う情報システム等の、入退館〔室〕管理を実施している物理的に保護された室内等への設置
A.9.1.3	A.9.1.3 **オフィス，部屋及び施設のセキュリティ**	9.1.3	**9.1.3 オフィス，部屋及び施設のセキュリティ**	【物理③】 与信事業者等は、機器・装置等を物理的に保護しなければならない。	【組織②】個人データの取扱いに係る建物、部屋、保管庫等の安全管理に関する規程等の整備とそれらに従った運用 【保管②】個人データを記録している媒体の遠隔地保管
A.9.1.4	A.9.1.4 **外部及び環境の脅威からの保護**	9.1.4	**9.1.4 外部及び環境の脅威からの保護**		
A.9.1.5	A.9.1.5 **セキュリティを保つべき領域での作業**	9.1.5	**9.1.5 セキュリティを保つべき領域での作業**		【物理①】個人データを取り扱う業務の、入退館〔室〕管理を実施している物理的に保護された室内での実施 【取得②】権限を与えられていない者が立ち入れない建物、部屋（以下「建物等」という。）での入力作業の実施 【利用②】権限を与えられていない者が立ち入れない建物等での利用・加工の実施 【消去②】権限を与えられていない者が立ち入れない建物等での消去・廃棄作業の実施
A.9.1.6	A.9.1.6 **一般の人の立寄り場所及び受渡場所**	9.1.6	**9.1.6 一般の人の立寄り場所及び受渡場所**	【物理①】 与信事業者等は、個人データを取り扱う施設に応じて、以下の管理を行わなければならない。 〔事業施設及び個人データ処理施設における管理〕 ・施錠等による施設及び室の管理 〔個人データ処理施設における管理〕 ・入退館〔室〕をする者の資格付与及び認証 ・入退館〔室〕の記録 ※「事務施設」とは、例えば本社、支社、営業店等の執務室を含み、「個人データ処理施設」とは、例えば電算センター、コールセンター、サーバルーム等を含む。	【物理①】個人データを取り扱う業務の、入退館〔室〕管理を実施している物理的に保護された室内での実施
A.9.2	**A.9.2 装置のセキュリティ** 目的：資産の損失，損傷，盗難又は劣化，及び組織の活動に対する妨害を防止するため。	9.2	**9.2 装置のセキュリティ**		
A.9.2.1	A.9.2.1 **装置の設置及び保護**	9.2.1	**9.2.1 装置の設置及び保護**	【物理②】 与信事業者等は、個人データ自体、又は個人データを含む書類、磁気媒体等の盗難を防止するための対策を行わなければならない。	【物理③】個人データを取り扱う機器・装置等の、安全管理上の脅威（例えば、盗難、破壊、破損）や環境上の脅威（例えば、漏水、火災、停電）からの物理的な保護
A.9.2.2	A.9.2.2 **サポートユーティリティ**	9.2.2	**9.2.2 サポートユーティリティ**	【物理③】 与信事業者等は、機器・装置等を物理的に保護しなければならない。	【物理③】個人データを取り扱う機器・装置等の、安全管理上の脅威（例えば、盗難、破壊、破損）や環境上の脅威（例えば、漏水、火災、停電）からの物理的な保護
A.9.2.3	A.9.2.3 **ケーブル配線のセキュリティ**	9.2.3	**9.2.3 ケーブル配線のセキュリティ**	【物理②】 与信事業者等は、個人データ自体、又は個人データを含む書類、磁気媒体等の 盗難を防止するための対策を行わなければならない。 【物理③】 与信事業者等は、機器・装置等を物理的に保護しなければならない。	【物理③】個人データを取り扱う機器・装置等の、安全管理上の脅威（例えば、盗難、破壊、破損）や環境上の脅威（例えば、漏水、火災、停電）からの物理的な保護
A.9.2.4	A.9.2.4 **装置の保守**	9.2.4	**9.2.4 装置の保守**		
A.9.2.5	A.9.2.5 **構外にある装置のセキュリティ**	9.2.5	**9.2.5 構外にある装置のセキュリティ**	【技術⑥】 与信事業者等は、個人データの移送・送信時における適切な対策を実施しなければならない。 ・個人データを含む電子媒体を移送する場合、暗号化又はパスワードロックを行うこと。 ・インターネットを経由して電子メールに添付して個人データを送信する場合に、電子メール自体を暗号化すること。 ※なお、暗号鍵の長さ、使用する暗号アルゴリズム、パスワードの文字数や複雑性については、個人データを含む電子媒体を紛失した場合に本人が被る権利利益の大きさを考慮し適切に設定することが望ましい。	【技術⑥】移送時における紛失・盗難が生じた際の対策（例えば、媒体に保管されている個人データの暗号化等の秘匿化）
A.9.2.6	A.9.2.6 **装置の安全な処分又は再利用**	9.2.6	**9.2.6 装置の安全な処分又は再利用**	【組織②】 与信事業者等は、本ガイドラインに従った個人データの安全管理措置を定めた規程や手順書等（以下「規程等」という。）を整備しなければならない。	【消去②】個人データが記録された媒体や機器をリース会社に返却する前の、データの完全消去（例えば、意味のないデータを媒体に1回又は複数回上書きする。）
A.9.2.7	A.9.2.7 **資産の移動**	9.2.7	**9.2.7 資産の移動**	【物理③】 与信事業者等は、機器・装置等を物理的に保護しなければならない。	【移送②】定められた手続による移送・送信の実施
A.10	**A.10 通信及び運用管理**	**10**	**通信及び運用管理**		
A.10.1	**A.10.1 運用の手順及び責任** 目的：情報処理設備の正確，かつ，セキュリティを保った運用を確実にするため。	10.1	**10.1 運用の手順及び責任**		
A.10.1.1	A.10.1.1 **操作手順書**	10.1.1	**10.1.1 操作手順書**	【組織②】 与信事業者等は、本ガイドラインに従った個人データの安全管理措置を定めた規程や手順書等（以下「規程等」という。）を整備しなければならない。	【組織②】個人データを取り扱う情報システムの安全管理措置に関する規程等の整備とそれらに従った運用
A.10.1.2	A.10.1.2 **変更管理**	10.1.2	**10.1.2 変更管理**	【技術⑦】 与信事業者等は、個人データを取り扱う情報システムの動作確認時の対策を行わなければならない。	【技術⑦】情報システムの変更時に、それらの変更によって情報システム又は運用環境のセキュリティが損なわれないことの検証

JIS Q 27001:2006 (附属書A)		JIS Q 27002:2006		経済産業分野のうち	経済産業分野を対象とする
項番		項番	条文	個別分野におけるガイドライン	ガイドライン (H20.2)
A.10.1.3	A.10.1.3 **職務の分割**	10.1.3	**10.1.3 職務の分割**	[技術②] 与信事業者等は、個人データへのアクセス制御を行わなければならない。 [技術③] 与信事業者等は、個人データへのアクセス権限の管理を行わなければならない。	[技術②] 個人データへのアクセス権限を付与すべき者の最小化 [技術②] アクセス権限を有する者に付与する権限の最小化
A.10.1.4	A.10.1.4 **開発施設, 試験施設及び運用施設の分離**	10.1.4	**10.1.4 開発施設, 試験施設及び運用施設の分離**		
A.10.2	**A.10.2 第三者が提供するサービスの管理** 目的: 第三者の提供するサービスに関する合意に沿った, 情報セキュリティ及びサービスの適切なレベルを実現し, 維持するため。	10.2	**10.2 第三者が提供するサービスの管理**		
A.10.2.1	A.10.2.1 **第三者が提供するサービス**	10.2.1	**10.2.1 第三者が提供するサービス**	[委託②] 与信事業者等は、委託契約において、個人データの取扱いに関して委託者、受託者双方が同意した内容を契約に盛り込まなければならない。	[組織②] 個人データの取扱いを委託する場合における委託先の選定基準、委託契約書のひな型、委託先における委託した個人データの取扱状況を確認するためのチェックリスト等の整備とそれらに従った運用
A.10.2.2	A.10.2.2 **第三者が提供するサービスの監視及びレビュー**	10.2.2	**10.2.2 第三者が提供するサービスの監視及びレビュー**		
A.10.2.3	A.10.2.3 **第三者が提供するサービスの変更に対する管理**	10.2.3	**10.2.3 第三者が提供するサービスの変更に対する管理**		
A.10.3	**A.10.3 システムの計画作成及び受入れ** 目的: システム故障のリスクを最小限に抑えるため。	10.3	**10.3 システムの計画作成及び受入れ**		
A.10.3.1	A.10.3.1 **容量・能力の管理**	10.3.1	**10.3.1 容量・能力の管理**		
A.10.3.2	A.10.3.2 **システムの受入れ**	10.3.2	**10.3.2 システムの受入れ**	[技術⑦] 与信事業者等は、個人データを取り扱う情報システムの動作確認時の対策を行わなければならない。	
A.10.4	**A.10.4 悪意のあるコード及びモバイルコード[3]からの保護** 目的: ソフトウェア及び情報の完全性を保護するため。 注3) モバイルコードとはコンピュータから別のコンピュータへ移動するソフトウェアであって, 利用者とのやり取りがほとんどない, 又はまったくない状態で自動的に起動し, 特定の機能を実行するものをいう。	10.4	**10.4 悪意のあるコード及びモバイルコードからの保護**		
A.10.4.1	A.10.4.1 **悪意のあるコードに対する管理策**	10.4.1	**10.4.1 悪意のあるコードに対する管理策**	[技術⑤] 与信事業者等は、個人データを取り扱う情報システムに対する不正ソフトウェア対策を行わなければならない。	[技術⑤] ウイルス対策ソフトウェアの導入 [技術⑤] オペレーティングシステム（OS）、アプリケーション等に対するセキュリティ対策用修正ソフトウェア（いわゆる、セキュリティパッチ）の適用 [技術⑤] 不正ソフトウェア対策の有効性・安定性の確認（例えば、パターンファイルや修正ソフトウェアの更新の確認）
A.10.4.2	A.10.4.2 **モバイルコードに対する管理策**	10.4.2	**10.4.2 モバイルコードに対する管理策**		
A.10.5	**A.10.5 バックアップ** 目的: 情報及び情報処理設備の完全性及び可用性を維持するため。	10.5	**10.5 バックアップ**		
A.10.5.1	A.10.5.1 **情報のバックアップ**	10.5.1	**10.5.1 情報のバックアップ**		[保管②] 個人データを記録している媒体を保管する場合の施錠管理 [保管②] 個人データを記録している媒体を保管する部屋、保管庫等の鍵の管理 [保管②] 個人データを記録している媒体の遠隔地保管 [保管②] 個人データのバックアップから迅速にデータが復元できることのテストの実施
A.10.6	**A.10.6 ネットワークセキュリティ管理** 目的: ネットワークにおける情報の保護, 及びネットワークを支える基盤の保護を確実にするため。	10.6	**10.6 ネットワークセキュリティ管理**		
A.10.6.1	A.10.6.1 **ネットワーク管理策**	10.6.1	**10.6.1 ネットワーク管理策**	[技術⑥] 与信事業者等は、個人データの移送・送信時における適切な対策を実施しなければならない。 ・個人データを含む電子媒体を移送する場合、暗号化又はパスワードロックを行うこと。 ・インターネットを経由して電子メールに添付して個人データを送信する場合に、電子メール自体を暗号化すること。 ※なお、暗号鍵の長さ、使用する暗号アルゴリズム、パスワードの文字数や複雑性については、個人データを含む電子媒体を紛失した場合に本人が被る権利利益の大きさを考慮し適切に設定することが望ましい。	[技術⑥] 盗聴される可能性のあるネットワーク（例えば、インターネットや無線LAN等）で個人データを送信（例えば、本人及び従業者による入力やアクセス、メールに添付してファイルを送信する等を含むデータの転送等）する際の、個人データの暗号化等の秘匿化
A.10.6.2	A.10.6.2 **ネットワークサービスのセキュリティ**	10.6.2	**10.6.2 ネットワークサービスのセキュリティ**		
A.10.7	**A.10.7 媒体の取扱い** 目的: 資産の認可されていない開示, 改ざん, 除去又は破壊, 及びビジネス活動の中断を防止するため。	10.7	**10.7 媒体の取扱い**		
A.10.7.1	A.10.7.1 **取外し可能な媒体の管理**	10.7.1	**10.7.1 取外し可能な媒体の管理**	[技術②] 与信事業者等は、個人データへのアクセス制御を行わなければならない。	[物理②] 個人データを含む媒体の施錠保管 [保管②] 個人データを記録している媒体を保管する場合の施錠管理 [保管②] 個人データを記録している媒体を保管する部屋、保管庫等の鍵の管理 [保管②] 個人データを記録している媒体の遠隔地保管
A.10.7.2	A.10.7.2 **媒体の処分**	10.7.2	**10.7.2 媒体の処分**		[消去②] 個人データが記録された媒体の物理的な破壊（例えば、シュレッダー、メディアシュレッダー等で破壊する。）
A.10.7.3	A.10.7.3 **情報の取扱手順**	10.7.3	**10.7.3 情報の取扱手順**	[組織②] 与信事業者等は、本ガイドラインに従った個人データの安全管理措置を定めた規程や手順書等（以下「規程等」という。）を整備しなければならない。 [技術②] 与信事業者等は、個人データへのアクセス制御を行わなければならない。 [技術⑥] 与信事業者等は、個人データの移送・送信時における適切な対策を実施しなければならない。 ・個人データを含む電子媒体を移送する場合、暗号化又はパスワードロックを行うこと。 ・インターネットを経由して電子メールに添付して個人データを送信する場合に、電子メール自体を暗号化すること。 ※なお、暗号鍵の長さ、使用する暗号アルゴリズム、パスワードの文字数や複雑性については、個人データを含む電子媒体を紛失した場合に本人が被る権利利益の大きさを考慮し適切に設定することが望ましい。	[取得②] 定められた手続による取得・入力の実施 [取得②] 個人データを入力できる端末の、業務上の必要性に基づく限定 [移送②] 個人データを移送・送信する場合の個人データの暗号化等の秘匿化（例えば、公衆回線を利用して個人データを送信する場合） [移送②] 移送時におけるあて先確認と受領確認（例えば、配達記録郵便等の利用） [移送②] FAX等におけるあて先番号確認と受領確認 [移送②] 個人データを記した文書をFAX機等に放置することの禁止 [利用②] 個人データを利用・加工できる端末の、業務上の必要性に基づく限定 [保管②] 個人データを保管・バックアップする場合の個人データの暗号化等の秘匿化 [消去②] 個人データを消去できる端末の、業務上の必要性に基づく限定
A.10.7.4	A.10.7.4 **システム文書のセキュリティ**	10.7.4	**10.7.4 システム文書のセキュリティ**		[物理②] 個人データを取り扱う情報システムの操作マニュアルの机上等への放置の禁止
A.10.8	**A.10.8 情報の交換** 目的: 組織内部で交換した及び外部と交換した, 情報及びソフトウェアのセキュリティを維持するため。	10.8	**10.8 情報の交換**		

JIS Q 27001:2006 (附属書A)		JIS Q 27002:2006		経済産業分野のうち	経済産業分野を対象とする
項番		項番	条文	個別分野におけるガイドライン	ガイドライン(H20.2)
A.10.8.1	A.10.8.1 **情報交換の方針及び手順**	10.8.1	**10.8.1 情報交換の方針及び手順**	[技術⑥] 与信事業者等は、個人データの移送・送信時における適切な対策を実施しなければならない。 ・個人データを含む電子媒体を移送する場合、暗号化又はパスワードロックを行うこと。 ・インターネットを経由して電子メールに添付して個人データを送信する場合に、電子メール自体を暗号化すること。 ※なお、暗号鍵の長さ、使用する暗号アルゴリズム、パスワードの文字数や複雑性については、個人データを含む電子媒体を紛失した場合に本人が被る権利利益の大きさを考慮し適切に設定することが望ましい。 [物理③] 与信事業者等は、機器・装置等を物理的に保護しなければならない。	[技術⑥]盗聴される可能性のあるネットワーク(例えば、インターネットや無線LAN等)で個人データを送信(例えば、本人及び従業者による入力やアクセス、メールに添付してファイルを送信する等を含むデータの転送等)する際の、個人データの暗号化等の秘匿化 [移送②]FAX等におけるあて先番号確認と受領確認 [移送②]個人データを記した文書をFAX機等に放置することの禁止
A.10.8.2	A.10.8.2 **情報交換に関する合意**	10.8.2	**10.8.2 情報交換に関する合意**	[技術⑥] 与信事業者等は、個人データの移送・送信時における適切な対策を実施しなければならない。 ・個人データを含む電子媒体を移送する場合、暗号化又はパスワードロックを行うこと。 ・インターネットを経由して電子メールに添付して個人データを送信する場合に、電子メール自体を暗号化すること。 ※なお、暗号鍵の長さ、使用する暗号アルゴリズム、パスワードの文字数や複雑性については、個人データを含む電子媒体を紛失した場合に本人が被る権利利益の大きさを考慮し適切に設定することが望ましい。	[技術⑥]盗聴される可能性のあるネットワーク(例えば、インターネットや無線LAN等)で個人データを送信(例えば、本人及び従業者による入力やアクセス、メールに添付してファイルを送信する等を含むデータの転送等)する際の、個人データの暗号化等の秘匿化
A.10.8.3	A.10.8.3 **配送中の物理的媒体**	10.8.3	**10.8.3 配送中の物理的媒体**	[技術⑥] 与信事業者等は、個人データの移送・送信時における適切な対策を実施しなければならない。 ・個人データを含む電子媒体を移送する場合、暗号化又はパスワードロックを行うこと。 ・インターネットを経由して電子メールに添付して個人データを送信する場合に、電子メール自体を暗号化すること。 ※なお、暗号鍵の長さ、使用する暗号アルゴリズム、パスワードの文字数や複雑性については、個人データを含む電子媒体を紛失した場合に本人が被る権利利益の大きさを考慮し適切に設定することが望ましい。	[技術⑥]移送時における紛失・盗難が生じた際の対策(例えば、媒体に保管されている個人データの暗号化等の秘匿化)
A.10.8.4	A.10.8.4 **電子的メッセージ通信**	10.8.4	**10.8.4 電子的メッセージ通信**	[技術⑥] 与信事業者等は、個人データの移送・送信時における適切な対策を実施しなければならない。 ・個人データを含む電子媒体を移送する場合、暗号化又はパスワードロックを行うこと。 ・インターネットを経由して電子メールに添付して個人データを送信する場合に、電子メール自体を暗号化すること。 ※なお、暗号鍵の長さ、使用する暗号アルゴリズム、パスワードの文字数や複雑性については、個人データを含む電子媒体を紛失した場合に本人が被る権利利益の大きさを考慮し適切に設定することが望ましい。	[技術⑥]盗聴される可能性のあるネットワーク(例えば、インターネットや無線LAN等)で個人データを送信(例えば、本人及び従業者による入力やアクセス、メールに添付してファイルを送信する等を含むデータの転送等)する際の、個人データの暗号化等の秘匿化
A.10.8.5	A.10.8.5 **業務用情報システム**	10.8.5	**10.8.5 業務用情報システム**		
A.10.9	**A.10.9 電子商取引サービス** 目的: 電子商取引サービスのセキュリティ，及びそれらサービスのセキュリティを保った利用を確実にするため。	10.9	**10.9 電子商取引サービス**		
A.10.9.1	A.10.9.1 **電子商取引**	10.9.1	**10.9.1 電子商取引**	[技術⑥] 与信事業者等は、個人データの移送・送信時における適切な対策を実施しなければならない。 ・個人データを含む電子媒体を移送する場合、暗号化又はパスワードロックを行うこと。 ・インターネットを経由して電子メールに添付して個人データを送信する場合に、電子メール自体を暗号化すること。 ※なお、暗号鍵の長さ、使用する暗号アルゴリズム、パスワードの文字数や複雑性については、個人データを含む電子媒体を紛失した場合に本人が被る権利利益の大きさを考慮し適切に設定することが望ましい。	[技術⑥]盗聴される可能性のあるネットワーク(例えば、インターネットや無線LAN等)で個人データを送信(例えば、本人及び従業者による入力やアクセス、メールに添付してファイルを送信する等を含むデータの転送等)する際の、個人データの暗号化等の秘匿化
A.10.9.2	A.10.9.2 **オンライン取引**	10.9.2	**10.9.2 オンライン取引**		
A.10.9.3	A10.9.3 **公開情報**	10.9.3	**10.9.3 公開情報**		
A.10.10	**A.10.10 監視** 目的: 認可されていない情報処理活動を検知するため。	10.10	**10.10 監視**		
A.10.10.1	A.10.10.1 **監査ログ取得**	10.10.1	**10.10.1 監査ログ取得**	[技術④] 与信事業者等は、個人データのアクセスの記録を行わなければならない。 [技術⑧] 与信事業者等は、個人データを取り扱う情報システムを監視しなければならない。 ※個人データを取り扱う情報システムを監視した結果の記録が個人情報に該当する場合があることに留意する。 [組織②] 与信事業者等は、本ガイドラインに従った個人データの安全管理措置を定めた規程や手順書等(以下「規程等」という。)を整備しなければならない。 (別紙) 1. 個人信用情報機関自らの安全管理措置 1－5 個人信用情報機関は、個人情報データベース等にアクセスするパソコン端末については、指紋認証など起動時及び一定時間離席時のアクセス認証を行い、そのアクセス記録を一定期間保存することとする仕組みにしなければならない。	[技術④]個人データへのアクセスや操作の成功と失敗の記録(例えば、個人データへのアクセスや操作を記録できない場合には、情報システムへのアクセスの成功と失敗の記録) [技術⑧]個人データへのアクセス状況(操作内容も含む。)の監視 [組織②]定められた規程等に従って業務手続が適切に行われたことを示す監査証跡の保持 [取得③]個人データの取得・入力業務を行う作業担当者に付与した権限の記録 [取得④]アクセスの記録、保管と、権限外作業の有無の確認 [移送③]個人データの移送・送信業務を行う作業担当者に付与した権限の記録 [移送④]アクセスの記録、保管と、権限外作業の有無の確認 [利用③]個人データを利用・加工する作業担当者に付与した権限(例えば、複写、複製、印刷、削除、変更等)の記録 [利用④]アクセスの記録、保管と権限外作業の有無の確認 [保管③]個人データの保管・バックアップ業務を行う作業担当者に付与した権限(例えば、バックアップの実行、保管庫の鍵の管理等)の記録 [保管④]アクセスの記録、保管と権限外作業の有無の確認 [消去③]個人データの消去・廃棄を行う作業担当者に付与した権限の記録 [消去④]アクセスの記録、保管、権限外作業の有無の確認

JIS Q 27001:2006 (附属書A)		JIS Q 27002:2006		経済産業分野のうち	経済産業分野を対象とする
項番		項番	条文	個用分野におけるガイドライン	ガイドライン(H20.2)
A.10.10.2	A.10.10.2 **システム使用状況の監視**	10.10.2	**10.10.2 システム使用状況の監視**	【技術④】 与信事業者等は、個人データのアクセスの記録を行わなければならない。 【技術⑧】 与信事業者等は、個人データを取り扱う情報システムを監視しなければならない。 ※個人データを取り扱う情報システムを監視した結果の記録が個人情報に該当する場合があることに留意する。 【組織②】 与信事業者等は、本ガイドラインに従った個人データの安全管理措置を定めた規程や手順書等（以下「規程等」という。）を整備しなければならない。	【保管②】個人データのバックアップに関する各種事象や障害の記録 【技術④】個人データへのアクセスや操作の成功と失敗の記録（例えば、個人データへのアクセスや操作を記録できない場合には、情報システムへのアクセスの成功と失敗の記録） 【技術⑧】個人データを取り扱う情報システムの使用状況の定期的な監視
A.10.10.3	A.10.10.3 **ログ情報の保護**	10.10.3	**10.10.3 ログ情報の保護**		
A.10.10.4	A.10.10.4 **実務管理者及び運用担当者の作業ログ**	10.10.4	**10.10.4 実務管理者及び運用担当者の作業ログ**	【技術④】 与信事業者等は、個人データのアクセスの記録を行わなければならない。	【保管②】個人データのバックアップに関する各種事象や障害の記録 【技術④】個人データへのアクセスや操作の成功と失敗の記録（例えば、個人データへのアクセスや操作を記録できない場合には、情報システムへのアクセスの成功と失敗の記録）
A.10.10.5	A.10.10.5 **障害のログ取得**	10.10.5	**10.10.5 障害のログ取得**	【技術④】 与信事業者等は、個人データのアクセスの記録を行わなければならない。	【保管②】個人データのバックアップに関する各種事象や障害の記録 【技術④】個人データへのアクセスや操作の成功と失敗の記録（例えば、個人データへのアクセスや操作を記録できない場合には、情報システムへのアクセスの成功と失敗の記録）
A.10.10.6	A.10.10.6 **クロックの同期**	10.10.6	**10.10.6 クロックの同期**		
A.11	**A.11 アクセス制御**	**11**	**アクセス制御**		
A.11.1	**A.11.1 アクセス制御に対する業務上の要求事項** 目的：情報へのアクセスを制御するため。	11.1	**11.1 アクセス制御に対する業務上の要求事項**		
A.11.1.1	A.11.1.1 **アクセス制御方針**	11.1.1	**11.1.1 アクセス制御方針**	【組織②】 与信事業者等は、本ガイドラインに従った個人データの安全管理措置を定めた規程や手順書等（以下「規程等」という。）を整備しなければならない。 【技術②】 与信事業者等は、個人データへのアクセス制御を行わなければならない。	【取得③】個人データを取得・入力できる作業担当者の、業務上の必要性に基づく限定 【取得③】作業担当者に付与する権限の限定 【移送③】個人データを移送・送信できる作業担当者の、業務上の必要性に基づく限定 【移送③】作業担当者に付与する権限の限定（例えば、個人データを、コンピュータネットワークを介して送信する場合、送信する者は個人データの内容を閲覧、変更する権限は必要ない。） 【利用③】個人データを利用・加工する作業担当者の、業務上の必要性に基づく限定 【利用③】作業担当者に付与する権限の限定（例えば、個人データを閲覧することのみが業務上必要とされる作業担当者に対し、個人データの複写、複製を行う権限は必要ない。） 【保管③】個人データを保管・バックアップする作業担当者の、業務上の必要性に基づく限定 【保管③】作業担当者に付与する権限の限定（例えば、個人データをバックアップする場合、その作業担当者は個人データの内容を閲覧、変更する権限は必要ない。） 【消去③】個人データを消去・廃棄できる作業担当者の、業務上の必要性に基づく限定 【消去③】作業担当者に付与する権限の限定 【技術②】個人データを格納した情報システムへの同時利用者数の制限
A.11.2	**A.11.2 利用者アクセスの管理** 目的：情報システムへの，認可された利用者のアクセスを確実にし，認可されていないアクセスを防止するため。	11.2	**11.2 利用者アクセスの管理**		
A.11.2.1	A.11.2.1 **利用者登録**	11.2.1	**11.2.1 利用者登録**	【技術①】 与信事業者等は、個人データへのアクセスにおける識別と認証を行わなければならない。 【技術③】 与信事業者等は、個人データへのアクセス権限の管理を行わなければならない。	【技術③】個人データにアクセスできる者を許可する権限管理の適切かつ定期的な実施（例えば、定期的に個人データにアクセスする者の登録を行う作業担当者が適当であることを十分に審査し、その者だけが、登録等の作業を行えるようにする。） 【技術③】個人データを取り扱う情報システムへの必要最小限のアクセス制御の実施
A.11.2.2	A.11.2.2 **特権管理**	11.2.2	**11.2.2 特権管理**	【技術①】 与信事業者等は、個人データへのアクセスにおける識別と認証を行わなければならない。 【技術③】 与信事業者等は、個人データへのアクセス権限の管理を行わなければならない。	【技術③】個人データにアクセスできる者を許可する権限管理の適切かつ定期的な実施（例えば、定期的に個人データにアクセスする者の登録を行う作業担当者が適当であることを十分に審査し、その者だけが、登録等の作業を行えるようにする。）
A.11.2.3	A.11.2.3 **利用者パスワードの管理** 管理策 パスワードの割当ては，正式な管理プロセスによって管理しなければならない。	11.2.3	**11.2.3 利用者パスワードの管理**	【技術①】 与信事業者等は、個人データへのアクセスにおける識別と認証を行わなければならない。	【移送②】暗号鍵やパスワードの適切な管理
A.11.2.4	A.11.2.4 **利用者アクセス権のレビュー**	11.2.4	**11.2.4 利用者アクセス権のレビュー**	【技術③】 与信事業者等は、個人データへのアクセス権限の管理を行わなければならない。	【技術③】個人データにアクセスできる者を許可する権限管理の適切かつ定期的な実施（例えば、定期的に個人データにアクセスする者の登録を行う作業担当者が適当であることを十分に審査し、その者だけが、登録等の作業を行えるようにする。）
A.11.3	**A.11.3 利用者の責任** 目的：認可されていない利用者のアクセス，並びに情報及び情報処理設備の損傷又は盗難を防止するため。	11.3	**11.3 利用者の責任**		
A.11.3.1	A.11.3.1 **パスワードの利用**	11.3.1	**11.3.1 パスワードの利用**	【技術③】 与信事業者等は、個人データへのアクセス権限の管理を行わなければならない。	【移送②】暗号鍵やパスワードの適切な管理 【保管②】暗号鍵やパスワードの適切な管理
A.11.3.2	A.11.3.2 **無人状態にある利用者装置**	11.3.2	**11.3.2 無人状態にある利用者装置**	（別紙） 1．個人信用情報機関自らの安全管理措置 1－5 個人信用情報機関は、個人情報データベース等にアクセスするパソコン端末については、指紋認証など起動時及び一定時間離席時のアクセス認証を行い、そのアクセス記録を一定期間保存することとする仕組みにしなければならない。	
A.11.3.3	A.11.3.3 **クリアデスク・クリアスクリーン[5]方針**	11.3.3	**11.3.3 クリアデスク・クリアスクリーン方針**	【技術②】 与信事業者等は、個人データへのアクセス制御を行わなければならない。	【物理②】個人データを記した書類、媒体、携帯可能なコンピュータ等の机上及び車内等への放置の禁止 【物理②】離席時のパスワード付きスクリーンセイバ等の起動によるのぞき見等の防止
A.11.4	**A.11.4 ネットワークのアクセス制御** 目的：ネットワークを利用したサービスへの認可されていないアクセスを防止するため。	11.4	**11.4 ネットワークのアクセス制御**		

JIS Q 27001:2006 (附属書A)		JIS Q 27002:2006		経済産業分野のうち	経済産業分野を対象とする
項番		項番	条文	個別分野におけるガイドライン	ガイドライン (H20.2)
A.11.4.1	A.11.4.1 **ネットワークサービスの利用についての方針**	11.4.1	**11.4.1 ネットワークサービスの利用についての方針**	【技術②】 与信事業者等は、個人データへのアクセス制御を行わなければならない。	
A.11.4.2	A.11.4.2 **外部から接続する利用者の認証**	11.4.2	**11.4.2 外部から接続する利用者の認証**	【技術②】 与信事業者等は、個人データへのアクセス制御を行わなければならない。	
A.11.4.3	A.11.4.3 **ネットワークにおける装置の識別**	11.4.3	**11.4.3 ネットワークにおける装置の識別**	【技術①】 与信事業者等は、個人データへのアクセスにおける識別と認証を行わなければならない。	【技術①】個人データへのアクセス権限を有する者が使用できる端末又はアドレス等の識別と認証（例えば、MAC アドレス認証、IP アドレス認証、電子証明書や秘密分散技術を用いた認証等）の実施
A.11.4.4	A.11.4.4 **遠隔診断用及び環境設定用ポートの保護**	11.4.4	**11.4.4 遠隔診断用及び環境設定用ポートの保護**	【技術②】 与信事業者等は、個人データへのアクセス制御を行わなければならない。	
A.11.4.5	A.11.4.5 **ネットワークの領域分割**	11.4.5	**11.4.5 ネットワークの領域分割**	【技術②】 与信事業者等は、個人データへのアクセス制御を行わなければならない。	
A.11.4.6	A.11.4.6 **ネットワークの接続制御**	11.4.6	**11.4.6 ネットワークの接続制御**	【技術②】 与信事業者等は、個人データへのアクセス制御を行わなければならない。	
A.11.4.7	A.11.4.7 **ネットワークルーティング制御**	11.4.7	**11.4.7 ネットワークルーティング制御**	【技術②】 与信事業者等は、個人データへのアクセス制御を行わなければならない。	
A.11.5	**A.11.5 オペレーティングシステムのアクセス制御** 目的：オペレーティングシステムへの，認可されていないアクセスを防止するため。	11.5	**11.5 オペレーティングシステムのアクセス制御**		
A.11.5.1	A.11.5.1 **セキュリティに配慮したログオン手順**	11.5.1	**11.5.1 セキュリティに配慮したログオン手順**		
A.11.5.2	A.11.5.2 **利用者の識別及び認証**	11.5.2	**11.5.2 利用者の識別及び認証**	【技術①】 与信事業者等は、個人データへのアクセスにおける識別と認証を行わなければならない。 【技術④】 与信事業者等は、個人データのアクセスの記録を行わなければならない。	【技術①】個人データに対する正当なアクセスであることを確認するために正当なアクセス権限を有する者であることの識別と認証（例えば、ID とパスワードによる認証、生体認証等）の実施 【取得③】IDとパスワードによる認証、生体認証等による作業担当者の識別 【移送③】IDとパスワードによる認証、生体認証等による作業担当者の識別 【利用③】IDとパスワードによる認証、生体認証等による作業担当者の識別 【保管③】IDとパスワードによる認証、生体認証等による作業担当者の識別 【消去③】IDとパスワードによる認証、生体認証等による作業担当者の識別
A.11.5.3	A.11.5.3 **パスワード管理システム**	11.5.3	**11.5.3 パスワード管理システム**		
A.11.5.4	A.11.5.4 **システムユーティリティの使用**	11.5.4	**11.5.4 システムユーティリティの使用**		
A.11.5.5	A.11.5.5 **セッションのタイムアウト**	11.5.5	**11.5.5 セッションのタイムアウト**		
A.11.5.6	A.11.5.6 **接続時間の制限**	11.5.6	**11.5.6 接続時間の制限**		【技術②】個人データを格納した情報システムの利用時間の制限（例えば、休業日や業務時間外等の時間帯には情報システムにアクセスできないようにする等）
A.11.6	**A.11.6 業務用ソフトウェア及び情報のアクセス制御** 目的：業務用ソフトウェアシステムが保有する情報への認可されていないアクセスを防止するため。	11.6	**11.6 業務用ソフトウェア及び情報のアクセス制御**		
A.11.6.1	A.11.6.1 **情報へのアクセス制限**	11.6.1	**11.6.1 情報へのアクセス制限**	【技術②】 与信事業者等は、個人データへのアクセス制御を行わなければならない。	【取得②】個人データを入力できる端末に付与する機能の、業務上の必要性に基づく限定（例えば、個人データを入力できる端末では、CD-R、USBメモリ等の外部記録媒体を接続できないようにする。） 【利用②】個人データを利用・加工できる端末に付与する機能の、業務上の必要性に基づく、限定（例えば、個人データを閲覧だけできる端末では、CD-R、USBメモリ等の外部記録媒体を接続できないようにする。） 【技術②】識別に基づいたアクセス制御（パスワード設定をしたファイルがだれでもアクセスできる状態は、アクセス制御はされているが、識別がされていないことになる。このような場合には、パスワードを知っている者が特定され、かつ、アクセスを許可する者に変更があるたびに、適切にパスワードを変更する必要がある。）の実施 【技術②】個人データにアクセス可能なアプリケーションの無権限利用の防止（例えば、アプリケーションシステムに認証システムを実装する、業務上必要となる者が利用するコンピュータのみに必要なアプリケーションシステムをインストールする、業務上必要な機能のみメニューに表示させる等）
A.11.6.2	A.11.6.2 **取扱いに慎重を要するシステムの隔離**	11.6.2	**11.6.2 取扱いに慎重を要するシステムの隔離**		
A.11.7	**A.11.7 モバイルコンピューティング及びテレワーキング**[5] 目的：モバイルコンピューティング及びテレワーキングの設備を用いるときの情報セキュリティを確実にするため。 注5) モバイルコンピューティングとは，移動中又は外出先でコンピュータを利用することであり，テレワーキングとは，要員が，自分の所属する組織の外の決まった場所で，通信技術を用いて作業することである。	11.7	**11.7 モバイルコンピューティング及びテレワーキング**		
A.11.7.1	A.11.7.1 **モバイルのコンピューティング及び通信**	11.7.1	**11.7.1 モバイルのコンピューティング及び通信**		
A.11.7.2	A.11.7.2 **テレワーキング**	11.7.2	**11.7.2 テレワーキング**		
A.12	**A.12 情報システムの取得，開発及び保守**	**12**	**情報システムの取得，開発及び保守**		
A.12.1	**A.12.1 情報システムのセキュリティ要求事項** 目的：セキュリティは情報システムの欠くことのできない部分であることを確実にするため。	12.1	**12.1 情報システムのセキュリティ要求事項**		
A.12.1.1	A.12.1.1 **セキュリティ要求事項の分析及び仕様化**	12.1.1	**12.1.1 セキュリティ要求事項の分析及び仕様化**		
A.12.2	**A.12.2 業務用ソフトウェアでの正確な処理** 目的：業務用ソフトウェアにおける情報の誤り，消失，認可されていない変更又は不正使用を防止するため。	12.2	**12.2 業務用ソフトウェアでの正確な処理**		
A.12.2.1	A.12.2.1 **入力データの妥当性確認**	12.2.1	**12.2.1 入力データの妥当性確認**		【取得②】取得・入力する際の手続の明確化 【取得②】定められた手続による取得・入力の実施
A.12.2.2	A.12.2.2 **内部処理の管理**	12.2.2	**12.2.2 内部処理の管理**	【技術⑧】 与信事業者等は、個人データを取り扱う情報システムを監視しなければならない。	【取得②】取得・入力する際の手続の明確化 【取得②】定められた手続による取得・入力の実施
A.12.2.3	A.12.2.3 **メッセージの完全性**	12.2.3	**12.2.3 メッセージの完全性**		【取得②】取得・入力する際の手続の明確化 【取得②】定められた手続による取得・入力の実施
A.12.2.4	A.12.2.4 **出力データの妥当性確認**	12.2.4	**12.2.4 出力データの妥当性確認**		【取得②】取得・入力する際の手続の明確化 【取得②】定められた手続による取得・入力の実施

JIS Q 27001:2006 (附属書A)		JIS Q 27002:2006		経済産業分野のうち	経済産業分野を対象とする
項番		項番	条文	信用分野におけるガイドライン	ガイドライン (H20.2)
A.12.3	**A.12.3 暗号による管理策** 目的: 暗号手段によって, 情報の機密性, 真正性又は完全性を保護するため。	12.3	**12.3 暗号による管理策**		
A.12.3.1	A.12.3.1 **暗号による管理策の利用方針**	12.3.1	**12.3.1 暗号による管理策の利用方針**	【組織②】 与信事業者等は、本ガイドラインに従った個人データの安全管理措置を定めた規程や手順書等（以下「規程等」という。）を整備しなければならない。 【技術⑥】 与信事業者等は、個人データの移送・送信時における適切な対策を実施しなければならない。 ・個人データを含む電子媒体を移送する場合、暗号化又はパスワードロックを行うこと。 ・インターネットを経由して電子メールに添付して個人データを送信する場合に、電子メール自体を暗号化すること。 ※なお、暗号鍵の長さ、使用する暗号アルゴリズム、パスワードの文字数や複雑性については、個人データを含む電子媒体を紛失した場合に本人が被る権利利益の大きさを考慮し適切に設定することが望ましい。	【移送②】個人データを移送・送信する場合の個人データの暗号化等の秘匿化（例えば、公衆回線を利用して個人データを送信する場合） 【移送②】移送時におけるあて先確認と受領確認（例えば、配達記録郵便等の利用） 【保管②】個人データを保管・バックアップする場合の個人データの暗号化等の秘匿化 【技術⑥】盗聴される可能性のあるネットワーク（例えば、インターネットや無線LAN等）で個人データを送信（例えば、本人及び従業者による入力やアクセス、メールに添付してファイルを送信する等を含むデータの転送等）する際の、個人データの暗号化等の秘匿化
A.12.3.2	A.12.3.2 **かぎ（鍵）管理**	12.3.2	**12.3.2 かぎ（鍵）管理**	【組織②】 与信事業者等は、本ガイドラインに従った個人データの安全管理措置を定めた規程や手順書等（以下「規程等」という。）を整備しなければならない。 【技術⑥】 与信事業者等は、個人データの移送・送信時における適切な対策を実施しなければならない。 ・個人データを含む電子媒体を移送する場合、暗号化又はパスワードロックを行うこと。 ・インターネットを経由して電子メールに添付して個人データを送信する場合に、電子メール自体を暗号化すること。 ※なお、暗号鍵の長さ、使用する暗号アルゴリズム、パスワードの文字数や複雑性については、個人データを含む電子媒体を紛失した場合に本人が被る権利利益の大きさを考慮し適切に設定することが望ましい。	【移送②】暗号鍵やパスワードの適切な管理 【保管②】暗号鍵やパスワードの適切な管理
A.12.4	**A.12.4 システムファイルのセキュリティ** 目的: システムファイルのセキュリティを確実にするため。	12.4	**12.4 システムファイルのセキュリティ**		
A.12.4.1	A.12.4.1 **運用ソフトウェアの管理**	12.4.1	**12.4.1 運用ソフトウェアの管理**	【技術⑤】 与信事業者等は、個人データを取り扱う情報システムに対する不正ソフトウェア対策を行わなければならない。	【技術⑤】オペレーティングシステム（OS）、アプリケーション等に対するセキュリティ対策用修正ソフトウェア（いわゆる、セキュリティパッチ）の適用
A.12.4.2	A.12.4.2 **システム試験データの保護**	12.4.2	**12.4.2 システム試験データの保護**	【技術⑦】 与信事業者等は、個人データを取り扱う情報システムの動作確認時の対策を行わなければならない。	【技術⑦】情報システムの動作確認時のテストデータとして個人データを利用することの禁止
A.12.4.3	A.12.4.3 **プログラムソースコードへのアクセス制御**	12.4.3	**12.4.3 プログラムソースコードへのアクセス制御**		
A.12.5	**A.12.5 開発及びサポートプロセスにおけるセキュリティ** 目的: 業務用ソフトウェアシステムのソフトウェア及び情報のセキュリティを維持するため。	12.5	**12.5 開発及びサポートプロセスにおけるセキュリティ**		
A.12.5.1	A.12.5.1 **変更管理手順**	12.5.1	**12.5.1 変更管理手順**	【技術③】 与信事業者等は、個人データへのアクセス権限の管理を行わなければならない。	【技術⑦】情報システムの変更時に、それらの変更によって情報システム又は運用環境のセキュリティが損なわれないことの検証
A.12.5.2	A.12.5.2 **オペレーティングシステム変更後の業務用ソフトウェアの技術的レビュー**	12.5.2	**12.5.2 オペレーティングシステム変更後の業務用ソフトウェアの技術的レビュー**		
A.12.5.3	A.12.5.3 **パッケージソフトウェアの変更に対する制限**	12.5.3	**12.5.3 パッケージソフトウェアの変更に対する制限**		
A.12.5.4	A.12.5.4 **情報の漏えい**	12.5.4	**12.5.4 情報の漏えい**	【技術③】 与信事業者等は、個人データを取り扱う情報システムに対する不正ソフトウェア対策を行わなければならない。	【技術⑤】オペレーティングシステム（OS）、アプリケーション等に対するセキュリティ対策用修正ソフトウェア（いわゆる、セキュリティパッチ）の適用
A.12.5.5	A.12.5.5 **外部委託によるソフトウェア開発**	12.5.5	**12.5.5 外部委託によるソフトウェア開発**		
A.12.6	**A.12.6 技術的ぜい弱性の管理** 目的: 公開された技術的ぜい弱性の悪用によって生じるリスクを低減するため。	12.6	**12.6 技術的ぜい弱性管理**		
A.12.6.1	A.12.6.1 **技術的ぜい弱性の管理**	12.6.1	**12.6.1 技術的ぜい弱性の管理**		【技術②】個人データを取り扱う情報システムに導入したアクセス制御機能の有効性の検証（例えば、ウェブアプリケーションのぜい弱性有無の検証）
A.13	**A.13 情報セキュリティインシデントの管理**	**13**	**13 情報セキュリティインシデントの管理**		
A.13.1	**A.13.1 情報セキュリティの事象及び弱点の報告** 目的: 情報システムに関連する情報セキュリティの事象及び弱点を, 時機を失しない是正処置をとることができるやり方で連絡することを確実にするため。	13.1	**13.1 情報セキュリティの事象及び弱点の報告**		
A.13.1.1	A.13.1.1 **情報セキュリティ事象の報告**	13.1.1	**13.1.1 情報セキュリティ事象の報告**	【組織⑥】 与信事業者等は、個人データの漏えい等の事故が発生した場合に対処するための以下の報告連絡体制を整備しなければならない。 ・個人情報保護に関する責任者等、社内での報告連絡体制。 ※なお、個人データの漏えい等の事故が発生した場合の報告連絡体制のみならず、発生する可能性が高い場合に対応するための報告連絡体制についても整備しておくこととする。 ・漏えい等の事故による影響を受ける可能性のある本人への情報提供体制（本人に通知し、又は本人が容易に知り得る状態にするための体制） ・経済産業省への報告連絡体制 （別紙） 3. 透明性確保等 3－1 個人信用情報機関は、1. の安全管理措置、2. の会員管理の状況や、監査の内容、結果について、行政に報告し、セキュリティ上支障のある部分を除いて一般に公表することとする。 3－2 個人信用情報機関は、自社からの情報漏洩や会員からの許容された利用目的を逸脱した利用については、行政への報告、一般への実績の公表を行うこと及び被害にあった個人への通知がなされるようにすることとする。 3－3 個人信用情報機関は、行政に対して定期的に安全管理措置の履行状況について報告することとする。	【組織①】個人データの取扱いに関する規程等に違反している事実又は兆候があることに気づいた場合の、代表者等への報告連絡体制の整備 【組織①】個人データの漏えい等（漏えい、滅失又はき損）の事故が発生した場合、又は発生の可能性が高いと判断した場合の、代表者等への報告連絡体制の整備 【組織①】漏えい等の事故による影響を受ける可能性のある本人への情報提供体制の整備 【組織①】漏えい等の事故発生時における主務大臣及び認定個人情報保護団体等に対する報告体制の整備 【組織⑤】以下の(ア)から(カ)までの手順の整備 ただし、書店で誰もが容易に入手できる市販名簿等（事業者において全く加工をしていないもの）を紛失等した場合には、以下の対処をする必要はないものと考えられる。 (ア)事実調査、原因の究明 (イ)影響範囲の特定 (ウ)再発防止策の検討・実施 (エ)影響を受ける可能性のある本人への連絡 事故又は違反について本人へ謝罪し、二次被害を防止するために、可能な限り本人へ連絡することが望ましい。 ただし、例えば、以下のように、本人の権利利益が侵害されておらず、今後も権利利益の侵害の可能性がない又は極めて小さいと考えられる場合には、本人への連絡を省略しても構わないものと考えられる。 ・紛失等した個人データを、第三者に見られることなく、速やかに回収した場合 ・高度な暗号化等の秘匿化が施されている場合

JIS Q 27001:2006 (附属書A)		JIS Q 27002:2006		経済産業分野のうち	経済産業分野を対象とする
項番		項番	条文	信用分野におけるガイドライン	ガイドライン (H20.2)
					・漏えい等をした事業者以外では、特定の個人を識別することができない場合（事業者が所有する個人データと照合することによって、はじめて個人データとなる場合） (オ)主務大臣等への報告 a．個人情報取扱事業者が認定個人情報保護団体の対象事業者の場合 認定個人情報保護団体の業務の対象となる個人情報取扱事業者（以下「対象事業者」という。）は、経済産業大臣（主務大臣）への報告に代えて、自己が所属する認定個人情報保護団体に報告を行うことができる。認定個人情報保護団体は、対象事業者の事故又は違反の概況を経済産業省に定期的に報告する。 ただし、以下の場合は、経済産業大臣（主務大臣）に、逐次速やかに報告を行うことが望ましい。 ・機微にわたる個人データ（(a)思想、信条又は宗教に関する事項、(b)人種、民族、門地、本籍地（所在都道府県に関する情報のみの場合を除く。）、身体・精神障害、犯罪歴その他社会的差別の原因となる事項、(c)勤労者の団結権、団体交渉その他団体行動の行為に関する事項、(d)集団示威行為への参加、請願権の行使その他の政治的権利の行使に関する事項、(e)保健医療又は性生活に関する事項等）を漏えいした場合 ・信用情報、クレジットカード番号等を含む個人データが漏えいした場合であって、二次被害が発生する可能性が高い場合 ・同一事業者において漏えい等の事故（特に同種事案）が繰り返し発生した場合 ・その他認定個人情報保護団体が必要と考える場合 b．個人情報取扱事業者が認定個人情報保護団体の対象事業者でない場合 経済産業大臣（主務大臣）に報告を行う。 なお、認定個人情報保護団体の対象事業者であるか否かにかかわらず、主務大臣に報告するほか、所属する業界団体等の関係機関に報告を行うことが望ましい。” (カ)事実関係、再発防止策等の公表 二次被害の防止、類似事案の発生回避等の観点から、個人データの漏えい等の事案が発生した場合は、可能な限り事実関係、再発防止策等を公表することが重要である。 ただし、例えば、以下のように、二次被害の防止の観点から公表の必要性がない場合には、事実関係等の公表を省略しても構わないものと考えられる。なお、そのような場合も、類似事案の発生回避の観点から、同業種間等で、当該事案に関する情報が共有されることが望ましい。 ・影響を受ける可能性のある本人すべてに連絡がついた場合 ・紛失等した個人データを、第三者に見られることなく、速やかに回収した場合 ・高度な暗号化等の秘匿化が施されている場合 ・漏えい等をした事業者以外では、特定の個人を識別することができない場合 （事業者が所有する個人データと照合することによって、はじめて個人データとなる場合）
A.13.1.2	A.13.1.2 **セキュリティ弱点の報告**	13.1.2	**13.1.2 セキュリティ弱点の報告**		【組織①】個人データの漏えい等（漏えい、滅失又はき損）の事故が発生した場合、又は発生の可能性が高いと判断した場合の、代表者等への報告連絡体制の整備
A.13.2	**A.13.2 情報セキュリティインシデントの管理及びその改善** 目的：情報セキュリティインシデントの管理に，一貫性のある効果的な取組み方法を用いることを確実にするため。	13.2	**13.2 情報セキュリティインシデントの管理及びその改善**		
A.13.2.1	A.13.2.1 **責任及び手順**	13.2.1	**13.2.1 責任及び手順**	[組織⑨] 与信事業者等は、個人データの安全管理措置の評価、見直し及び改善をしなければならない。 [組織⑩] 与信事業者等は、自己の取り扱う個人データ（受託者が取り扱うものを含む。）の漏洩に係る二次被害の防止、類似事案の発生回避等の観点から以下のような適切な対処を行わなければならない。 ・事実関係を本人に速やかに通知し又は本人が容易に知り得る状態に置くこと。 ・可能な限り事実関係等を遅滞なく公表すること。 ・事実関係、発生原因、対応策その他の漏えいに関する事項を可能な限り速やかに経済産業省に報告すること。	【組織①】個人データの漏えい等（漏えい、滅失又はき損）の事故が発生した場合、又は発生の可能性が高いと判断した場合の、代表者等への報告連絡体制の整備 【組織①】漏えい等の事故による影響を受ける可能性のある本人への情報提供体制の整備 【組織①】漏えい等の事故発生時における主務大臣及び認定個人情報保護団体等に対する報告体制の整備 【組織⑤】以下の(ア)から(カ)までの手順の整備 ただし、書店で誰もが容易に入手できる市販名簿等（事業者において全く加工をしていないもの）を紛失等した場合には、以下の対処をする必要はないものと考えられる。 (ア)事実調査、原因の究明 (イ)影響範囲の特定 (ウ)再発防止策の検討・実施 (エ)影響を受ける可能性のある本人への連絡 事故又は違反について本人へ謝罪し、二次被害を防止するために、可能な限り本人へ連絡することが望ましい。 ただし、例えば、以下のように、本人の権利利益が侵害されておらず、今後も権利利益の侵害の可能性がない又は極めて小さいと考えられる場合には、本人への連絡を省略しても構わないものと考えられる。 ・紛失等した個人データを、第三者に見られることなく、速やかに回収した場合 ・高度な暗号化等の秘匿化が施されている場合 ・漏えい等をした事業者以外では、特定の個人を識別することができない場合（事業者が所有する個人データと照合することによって、はじめて個人データとなる場合） (オ)主務大臣等への報告 a．個人情報取扱事業者が認定個人情報保護団体の対象事業者の場合 認定個人情報保護団体の業務の対象となる個人情報取扱事業者（以下「対象事業者」という。）は、経済産業大臣（主務大臣）への報告に代えて、自己が所属する認定個人情報保護団体に報告を行うことができる。認定個人情報保護団体は、対象事業者の事故又は違反の概況を経済産業省に定期的に報告する。 ただし、以下の場合は、経済産業大臣（主務大臣）に、逐次速やかに報告を行うことが望ましい。 ・機微にわたる個人データ（(a)思想、信条又は宗教に関する事項、(b)人種、民族、門地、本籍地（所在都道府県に関する情報のみの場合を除く。）、身体・精神障害、犯罪歴その他社会的差別の原因となる事項、(c)勤労者の団結権、団体交渉その他団体行動の行為に関する事項、(d)集団示威行為への参加、請願権の行使その他の政治的権利の行使に関する事項、(e)保健医療又は性生活に関する事項等）を漏えいした場合

JIS Q 27001:2006 (附属書A)		JIS Q 27002:2006		経済産業分野のうち	経済産業分野を対象とする
項番		項番	条文	個別分野におけるガイドライン	ガイドライン (H20.2)
					・信用情報、クレジットカード番号等を含む個人データが漏えいした場合であって、二次被害が発生する可能性が高い場合 ・同一事業者において漏えい等の事故（特に同種事案）が繰り返し発生した場合 ・その他認定個人情報保護団体が必要と考える場合 b. 個人情報取扱事業者が認定個人情報保護団体の対象事業者でない場合 経済産業大臣（主務大臣）に報告を行う。 なお、認定個人情報保護団体の対象事業者であるか否かにかかわらず、主務大臣に報告するほか、所属する業界団体等の関係機関に報告を行うことが望ましい。" (カ)事実関係、再発防止策等の公表 二次被害の防止、類似事案の発生回避等の観点から、個人データの漏えい等の事案が発生した場合は、可能な限り事実関係、再発防止策等を公表することが重要である。 ただし、例えば、以下のように、二次被害の防止の観点から公表の必要性がない場合には、事実関係等の公表を省略しても構わないものと考えられる。なお、そのような場合も、類似事案の発生回避の観点から、同業種間等で、当該事案に関する情報が共有されることが望ましい。 ・影響を受ける可能性のある本人すべてに連絡がついた場合 ・紛失等した個人データを、第三者に見られることなく、速やかに回収した場合 ・高度な暗号化等の秘匿化が施されている場合 ・漏えい等をした事業者以外では、特定の個人を識別することができない場合 （事業者が所有する個人データと照合することによって、はじめて個人データとなる場合）
A.13.2.2	A.13.2.2 **情報セキュリティインシデントからの学習** 管理策 情報セキュリティインシデントの形態，規模及び費用を定量化し監視できるようにする仕組みを備えなければならない。	13.2.2	**13.2.2 情報セキュリティインシデントからの学習** 実施の手引 情報セキュリティインシデントの評価から得た情報は，再発する又は影響の大きいインシデントを特定するために利用することが望ましい。		
A.13.2.3	A.13.2.3 **証拠の収集**	13.2.3	**13.2.3 証拠の収集**		
A.14	**A.14 事業継続管理**	**14**	**事業継続管理**		
A.14.1	**A.14.1 事業継続管理における情報セキュリティの側面** 目的：情報システムの重大な故障又は災害の影響からの事業活動の中断に対処するとともに，それらから重要な業務プロセスを保護し，また，事業活動及び重要な業務プロセスの時機を失しない再開を確実にするため。	14.1	**14.1 事業継続管理における情報セキュリティの側面**		
A.14.1.1	A.14.1.1 **事業継続管理手続への情報セキュリティの組込み**	14.1.1	**14.1.1 事業継続管理手続への情報セキュリティの組込み**		
A.14.1.2	A.14.1.2 **事業継続及びリスクアセスメント**	14.1.2	**14.1.2 事業継続及びリスクアセスメント**		
A.14.1.3	A.14.1.3 **情報セキュリティを組み込んだ事業継続計画の策定及び実施**	14.1.3	**14.1.3 情報セキュリティを組み込んだ事業継続計画の策定及び実施**		
A.14.1.4	A.14.1.4 **事業継続計画策定の枠組み**	14.1.4	**14.1.4 事業継続計画策定の枠組み**		
A.14.1.5	A.14.1.5 **事業継続計画の試験，維持及び再評価**	14.1.5	**14.1.5 事業継続計画の試験，維持及び再評価**		
A.15	**A.15 順守**	**15**	**順守**		
A.15.1	**A.15.1 法的要求事項の順守** 目的：法令，規制又は契約上のあらゆる義務，及びセキュリティ上のあらゆる要求事項に対する違反を避けるため。 注記　法的順守は，しばしば，コンプライアンスといわれることがある。	15.1	**15.1 法的要求事項の順守**		
A.15.1.1	A.15.1.1 **適用法令の識別**	15.1.1	**15.1.1 適用法令の識別**		
A.15.1.2	A.15.1.2 **知的財産権（IPR）**	15.1.2	**15.1.2 知的財産権（IPR）**		
A.15.1.3	A.15.1.3 **組織の記録の保護**	15.1.3	**15.1.3 組織の記録の保護**	【組織②】 与信事業者等は、本ガイドラインに従った個人データの安全管理措置を定めた規程や手順書等（以下「規程等」という。）を整備しなければならない。 【技術④】 与信事業者等は、個人データのアクセスの記録を行わなければならない。 ※個人データを取り扱う情報システムの記録が個人情報に該当する場合があることに留意する。	【技術④】採取した記録の漏えい、滅失及びき損からの適切な保護 【組織②】定められた規程等に従って業務手続が適切に行われたことを示す監査証跡の保持
A.15.1.4	A.15.1.4 **個人データ及び個人情報の保護**	15.1.4	**15.1.4 個人データ及び個人情報の保護**	『他に該当しないものすべて』	『他に該当しないものすべて』
A.15.1.5	A.15.1.5 **情報処理施設の不正使用防止**	15.1.5	**15.1.5 情報処理施設の不正使用防止**		
A.15.1.6	A.15.1.6 **暗号化機能に対する規制**	15.1.6	**15.1.6 暗号化機能に対する規制**		
A.15.2	**A.15.2 セキュリティ方針及び標準の順守，並びに技術的順守** 目的：組織のセキュリティ方針及び標準類へのシステムの順守を確実にするため。	15.2	**15.2 セキュリティ方針及び標準の順守，並びに技術的順守**		
A.15.2.1	A.15.2.1 **セキュリティ方針及び標準の順守**	15.2.1	**15.2.1 セキュリティ方針及び標準の順守**	【組織④】 与信事業者等は、個人情報保護に関する責任者を設置しなければならない。 ※上記には、例えば、いわゆる、チーフ・プライバシー・オフィサー（CPO）等が該当する。 ※個人データの取扱いにおける作業責任者の設置及び作業担当者の限定、個人データを取り扱う情報システム運用責任者の設置及び担当者（システム管理者を含む。）の限定を行うこととする。	【組織④】監査計画の立案と、計画に基づく監査（内部監査又は外部監査）の実施 【組織④】監査実施結果の取りまとめと、代表者への報告 【組織④】監査責任者から受ける監査報告、個人データに対する社会通念の変化及び情報技術の進歩に応じた定期的な安全管理措置の見直し及び改善
A.15.2.2	A.15.2.2 **技術的順守の点検**	15.2.2	**15.2.2 技術的順守点検**	【技術②】 与信事業者等は、個人データへのアクセス制御を行わなければならない。 【技術③】 与信事業者等は、個人データを取り扱う情報システムに対する不正ソフトウェア対策を行わなければならない。	【技術②】個人データを取り扱う情報システムに導入したアクセス制御機能の有効性の検証（例えば、ウェブアプリケーションのぜい弱性有無の検証） 【技術③】不正ソフトウェア対策の有効性・安定性の確認（例えば、パターンファイルや修正ソフトウェアの更新の確認）
A.15.3	**A.15.3 情報システムの監査に対する考慮事項** 目的：情報システムに対する監査手続の有効性を最大限にするため，及びシステムの監査プロセスへの干渉及び／又はシステムの監査プロセスからの干渉を最小限にするため。	15.3	**15.3 情報システムの監査に対する考慮事項**		
A.15.3.1	A.15.3.1 **情報システムの監査に対する管理策**	15.3.1	**15.3.1 情報システムの監査に対する管理策**		A.15.3.1
A.15.3.2	A.15.3.2 **情報システムの監査ツールの保護**	15.3.2	**15.3.2 情報システムの監査ツールの保護**		A.15.3.2

おわりに

本ガイドがクレジット産業における ISMS 構築の一助になれば幸いです。また、ISMS を構築することがクレジット産業におけるセキュリティ要件を順守するために非常に有効な方法であることをご理解いただければ幸いです。

クレジット産業向け“PCI DSS”/ISMS ユーザーズガイド検討作業部会メンバー

氏名	所属／役職
メンバー	
荒川　明良	マスターカード・ワールドワイド　ジャパンオフィス セキュリティー・リスクサービス　日本／韓国／グァム　ビジネスリーダー
五十嵐　浩志	ビザ・ワールドワイド・ジャパン㈱ カントリー リスクマネジメント／リスク　マネージャー
石渡　洋平	マスターカード・ワールドワイド　ジャパンオフィス セキュリティー・リスクサービス 日本／韓国／グァム プログラム・マネージャー
井上　憲司	㈱ジェーシービー　国際本部　国際インフラ推進部 プロダクト統括グループ担当　部長代理
井原　亮二	ビザ・ワールドワイド・ジャパン㈱　カントリー リスク ダイレクター リスクマネージメント
大沼　靖秀	KPMG ビジネスアシュアランス㈱　執行役員　ディレクター
駒瀬　彰彦	㈱アズジェント　取締役　技術本部長
近藤　由紀子	アメリカン・エキスプレス・インターナショナル, Inc. 加盟店事業部門　国際提携推進本部　本部長
日辻　治彦	㈱ジェーシービー　専任マネージャー（品質管理グループ担当）
松尾　正浩	㈱三菱総合研究所　経営コンサルティング本部　研究部長　主席研究員
丸山　満彦	監査法人トーマツ　エンタープライズ リスク サービス部　パートナー
オブザーバー	
浅野　優子	経済産業省　商務情報政策局　商務流通グループ　取引信用課　係長
秋貞　幸雄	経済産業省　商務情報政策局　情報セキュリティ政策室　技術係長

2009 年 3 月

ISMS 適合性評価制度技術専門部会
財団法人日本情報処理開発協会