クレジットカード・セキュリティガイドライン　新旧対照表 *（2021 年 3 月改定、4 月適用開始／関連部分のみ抜粋）*

<table>
<tr><th>頁</th><th>現行【1.0 版】</th><th>改定版　※2020 年 12 月 28 日より変更した部分のみ下線</th></tr>
<tr><td>用語集
P.5
～8</td><td><table><tr><td>PSP</td><td>Payment Service Provider の略。
インターネット上の取引において EC 加盟店にクレジットカード決済スキームを提供し、クレジットカード情報を処理する事業者をいう。
注　割賦販売法におけるクレジットカード番号等取扱契約締結事業者の登録を行った事業者はカード会社（アクワイアラー）としての対策等も必要となる。</td></tr></table>
（追加）

（追加）</td><td>（同左）

<table><tr><td>決済代行業者等</td><td>以下のいずれかの業務を行う決済代行業者（PSP 含む）※1、EC モール、EC システム提供会社※2 等の事業者の総称。
①特定のアクワイアラーのために加盟店に立替払いをする業務。
②加盟店のためにクレジットカード情報（以下「カード情報」という。）をアクワイアラーに提供（当該アクワイアラー以外の者を通じた提供を含む。）する業務。

※1　ここでいう決済代行業者は、インターネット上の取引において EC 加盟店にクレジットカードスキームを提供し、カード情報を処理する事業者である PSP と、インターネット以外の取引において加盟店にクレジットカードスキームを提供し、カード情報を処理する事業者をいう。
※2　ここでいう EC システム提供会社は、アクワイアラーとの契約有無にかかわらず、決済システムを運営し EC 加盟店にサービスとして提供する事業者をいう。ASP/SaaS として EC 加盟店にサービス提供する形式や、EC 加盟店に購入プラットフォームを提供する形式等がある。</td></tr><tr><td>コード決済事業者</td><td>以下のいずかの業務を行う事業者。
①カード会員からカード情報の提供を受けて QR コードや決</td></tr></table></td></tr>
</table>

頁	現行【1.0 版】	改定版　※2020 年 12 月 28 日より変更した部分のみ下線
		等　済用の ID※3 など対面取引・非対面取引の決済に用いることができる情報と結び付け、カード会員に当該情報を提供する業務。 ②上記①の事業者から委託を受けてカード情報を他の決済情報により特定できる状態で管理する業務。 ※3　カード会員データ（クレジットカード番号、クレジットカード会員名、サービスコード、有効期限）が事前に登録された際に、カード会員データの代わりにクレジットカード決済が可能となる ID または番号を指す。
P9	本ガイドラインの基本的な考え方 ３．対象となる関係事業者について 現時点ではセキュリティ対策の実施主体者である「加盟店」「カード会社（イシュアー、アクワイアラー）」「PSP* (Payment Service Provider)」及びこれらの事業者が対策を実施するに際し協力等を行う「機器メーカー」「ソリューションベンダー*」「情報処理センター」「セキュリティ事業者」「国際ブランド」「業界団体」等のクレジットカード取引に関係する事業者を「関係事業者」としている。今後新たな決済スキームの進展や新たな事業者が登場し、これらのセキュリティ対策の検証が必要な場合には、関係事業者を追加することとする。	本ガイドラインの基本的な考え方 ３．対象となる関係事業者について 現時点ではセキュリティ対策の実施主体者である「加盟店」「カード会社（イシュアー、アクワイアラー）」「決済代行業者等※」「コード決済事業者等※」及びこれらの事業者が対策を実施するに際し協力等を行う「機器メーカー」「ソリューションベンダー*」「情報処理センター」「セキュリティ事業者」「国際ブランド」「業界団体」等のクレジットカード取引に関係する事業者を「関係事業者」としている。今後新たな決済スキームの進展や新たな事業者が登場し、これらのセキュリティ対策の検証が必要な場合には、関係事業者を追加することとする。
P11	Ⅰ．クレジットカード情報保護対策分野 カード情報注の保護は、クレジットカード取引に関わる全ての事業者の責務である。 企業や個人を狙ったマルウェアや標的型攻撃によって個人情報やカード情報の窃取、またそれらの窃取した情報を利用した特殊詐欺等の事件は引き続き発生しており、特にカード情報の不正利用は国内だけに止まらず、国際的にも甚大な被害をもたらしている。これらは、不正を働いている犯	（同左）

頁	現行【1.0 版】	改定版　※2020 年 12 月 28 日より変更した部分のみ下線
	罪者の大きな資金源になっているとも言われており、犯罪防止の観点からも関係事業者が責任を持って適切な情報管理を行うことが求められる。 　そもそもカード情報を自社で保持していなければ、カード情報を窃取されることがなく、情報漏えいの観点からも有効なセキュリティ対策と考えられる。しかし、カード情報を保持しなくても事業を運営できる事業者と、保持しなければ事業を運営できない事業者があるため、各事業者の実態を踏まえた対策を講じることが重要である。 　カード情報保護対策について具体的には、カード情報を保持しない非保持化や、カード情報を取り扱う場合は、国際ブランド（VISA、Mastercard、JCB、American Express、Discover）が共同で策定したデータセキュリティの国際基準である PCI DSS（Payment Card Industry Data Security Standard）への準拠の取組がある。PCI DSS の準拠においては、事業者が PCI DSS の内容を正しく理解し効率的に対応する必要がある。	
P11	本ガイドラインにおいて加盟店は非保持化（非保持と同等/相当※を含む）又はカード情報を保持する場合は PCI DSS 準拠、カード会社及び PSP は PCI DSS 準拠が求められる。 　各事業者は、本ガイドラインに基づき自社の実態を踏まえたカード情報保護に向けた適切な対策を講じる必要がある。 注 「カード情報」とは、クレジットカード会員データ（クレジットカード番号、クレジットカード会員名、サービスコード、有効期限）及び機密認証データ（カード情報を含む全トラックデータ、CAV2/CVC2/CVV2/CID いわゆるセキュリティコード、PIN*又は PIN ブロック）をいう。 ただし、クレジットカード会員データのうち、クレジットカード番号以外のデータのみであれば「カード情報」ではない。 また、以下の処理がなされたものはクレジットカード番号とは見做さない。 ・トークナイゼーション（自社システムの外でクレジットカード番号を不可逆的に別の番号等に置き換え、自社システム内ではクレジットカ	本ガイドラインにおいて加盟店は非保持化（非保持と同等/相当※を含む）又はカード情報を保持する場合は PCI DSS 準拠、カード会社、決済代行業者等及びコード決済事業者等は PCI DSS 準拠が求められる。 　各事業者は、本ガイドラインに基づき自社の実態を踏まえたカード情報保護に向けた適切な対策を講じる必要がある。 注 「カード情報」とは、カード会員データ（クレジットカード番号、クレジットカード会員名、サービスコード、有効期限）及び機密認証データ（カード情報を含む全トラックデータ、CAV2/CVC2/CVV2/CID いわゆるセキュリティコード、PIN*又は PIN ブロック）をいう。 ただし、カード会員データのうち、クレジットカード番号以外のデータのみであれば「カード情報」ではない。 また、以下の処理がなされたものはクレジットカード番号とは見做さない。 ・トークナイゼーション（自社システムの外でクレジットカード番号を不可逆的に別の番号等に置き換え、自社システム内ではクレジットカ

頁	現行【1.0 版】	改定版　※2020 年 12 月 28 日より変更した部分のみ下線
	ード番号を特定できないもの） ・トランケーション（自社システムの外でクレジットカード番号を、自社システム内では特定できない方法で安全に国際的な第三者機関に認められた桁数を切り落としたもの） ・無効処理されたクレジットカード番号 １．各事業者に求められる対策等 （１）加盟店 ■カード情報を保持しない「非保持化」（非保持と同等/相当を含む）はカード情報を保持する場合は PCI DSS に準拠する。【指針対策】 ■カード情報の窃取を企図する者の最新の攻撃手口等の情報を踏まえ、対策実施後も不断に自社のセキュリティ対策の改善・強化を図る。	ード番号を特定できないもの） ・トランケーション（自社システムの外でクレジットカード番号を、自社システム内では特定できない方法で安全に国際的な第三者機関に認められた桁数を切り落としたもの） ・無効処理されたクレジットカード番号 （同左）
P12	加盟店が非保持化に向けた具体的な取組を進めるにあたっては、対面加盟店と非対面加盟店に分けたアプローチをする必要がある。さらに、非対面加盟店のうち、昨今カード情報漏えい事案が発生している EC 加盟店においてはセキュリティ対策を一層強化することが重要である。 特に、EC 加盟店のウェブサイトの脆弱性や簡易なログインパスワードを設定しているなどの管理画面への不十分なアクセス制御等のウェブサイトの開発・運用段階での設定の不備、EC 加盟店の委託先事業者が提供する決済ソリューション（ショッピングカート機能等）の脆弱性等が悪用された漏えい事案が発生している点を踏まえ、自社システムの定期的な点検やその結果に基づいて追加的な対策等を講じるなどセキュリティレベルを向上させることが重要である。	加盟店が非保持化に向けた具体的な取組を進めるにあたっては、対面加盟店と非対面加盟店に分けたアプローチをする必要がある。さらに、非対面加盟店のうち、昨今カード情報漏えい事案が発生している EC 加盟店においてはセキュリティ対策を一層強化することが重要である。 特に、EC 加盟店のウェブサイトの脆弱性やウェブサイトの開発・運用段階で管理画面に簡易なログインパスワードを設定する等の不適切なアクセス制御、EC 加盟店の委託先事業者が提供する決済ソリューション（ショッピングカート機能等）の脆弱性等が悪用された漏えい事案が発生している点を踏まえ、委託先に必要な対策を求めるとともに、自社システムの定期的な点検やその結果に基づいて追加的な対策等を講じるなどセキュリティレベルを向上させることが重要である。
P23	①非保持化対策 ②PCI DSS 準拠	（同左）

頁	現行【1.0 版】	改定版　※2020 年 12 月 28 日より変更した部分のみ下線
	（２）カード会社（イシュアー・アクワイアラー） ■カード情報を取り扱うカード会社は、外部からの不正侵入やカード情報の外部への漏えい等といった外的脅威によるリスクを極小化し、かつ予見される様々なリスクに厳格に対処するため PCI DSS に準拠し、これを維持・運用する。このほか、関係法令・ガイドライン等を参照し、リスクに応じた必要なセキュリティ対策を講じるとともに、適切な管理運営を行う。【指針対策】 ■カード会社（アクワイアラー）は、PSP 等と連携の上、加盟店に対し非保持化（非保持と同等/相当を含む）又は PCI DSS 準拠を推進するとともに、カード情報保護対策について必要な助言や情報提供等を行う。また、PCI DSS 準拠を完了していない PSP がある場合には可及的速やかに準拠するよう指導を行う。 ■カード会社（イシュアー）は、フィッシングやウイルス感染、EC サイト改ざんによる不正画面への遷移など、カード会員から直接カード情報等を窃取する手口も存在するため、消費者に対する注意喚起及びセキュリティ対策の必要性等の啓発を行う。	（２）カード会社（イシュアー・アクワイアラー） ■カード会社（イシュアー・アクワイアラー）は、外部からの不正侵入やカード情報の外部への漏えい等といった外的脅威によるリスクを極小化し、かつ予見される様々なリスクに厳格に対処するため PCI DSS に準拠し、これを維持・運用する。このほか、関係法令・ガイドライン等を参照し、リスクに応じた必要なセキュリティ対策を講じるとともに、適切な管理運営を行う。【指針対策】 ■カード会社（アクワイアラー）は、契約のある決済代行業者等と連携し、加盟店に対し非保持化（非保持と同等/相当を含む）又は PCI DSS 準拠について必要な助言や情報提供等を行う。 ■カード会社（イシュアー）は、フィッシングやウイルス感染、EC サイト改ざんによる不正画面への遷移など、カード会員から直接カード情報等を窃取する手口について、消費者に対する注意喚起及びセキュリティ対策の必要性等の啓発を行う。
	（３）PSP ■カード情報を取り扱う PSP については、PCI DSS に準拠し、これを維持・運用する。 ■カード会社（アクワイアラー）と協力して、加盟店に対しカード情報保護対策について必要な助言や情報提供等を行い、その取組を支援する。	（３）決済代行業者等 ■決済代行業者等については、PCI DSS に準拠し、これを維持・運用する。【指針対策】 ■非保持化（非保持と同等/相当を含む）の対策を講じている対面取引は、当該対策に加え、リスクに応じた必要なセキュリティ対策を講じるとともに、適切な管理運営を行う。【指針対策】 ■決済代行業者等は、加盟店の取組を支援するため、加盟店に対しカード情報保護対策について必要な助言や情報提供等を実施する。なお、カード会社（アクワイアラー）と契約を有する決済代行業者等については、カード会社（アクワイアラー）と連携して対応する。
	（追加）	

頁	現行【1.0 版】	改定版　※2020 年 12 月 28 日より変更した部分のみ下線
		（４）コード決済事業者等 ■コード決済事業者等については、PCI DSS に準拠し、これを維持・運用する。【指針対策】 ■また、コード決済事業者等から委託を受けてカード情報を他の決済情報により特定できる状態で管理している事業者についても PCI DSS に準拠し、これを維持・運用する。【指針対策】
	（４）その他関係事業者等 ①国際ブランド ②ソリューションベンダー ③行政 ④業界団体等 ■日本クレジット協会は、カード会社（アクワイアラー）と連携し、本ガイドラインに掲げるカード情報保護対策の必要性について加盟店に対する周知活動を徹底するとともに、加盟店の業界団体、消費者団体等との連携を強化し、事業者向けの情報発信に取組む。 ■日本クレジット協会は、行政と連携の上、他の情報セキュリティに係る関係機関との連携・情報共有を図り、クレジット取引に関係する事業者等に対して適時情報発信を行う。 ■政府の情報セキュリティ政策会議において、クレジット分野は、国の重要インフラの一つに指定されており、「重要インフラ情報セキュリティ第 4 次行動計画」（2018 年 7 月 25 日付改定）に基づき、官民連携による重要インフラ防護を推進していく。具体的な取組としては、「クレジット CEPTOAR における情報セキュリティガイドライン」に基づき、重要インフラ事業者における安全基準等の整備・浸透、情報共有体制の強化等を図る。	（５）その他関係事業者等 ①国際ブランド ②ソリューションベンダー ③行政 ④業界団体等 ■日本クレジット協会は、カード会社（アクワイアラー）と連携し、本ガイドラインに掲げるカード情報保護対策の必要性について加盟店に対する周知活動を徹底するとともに、加盟店の業界団体、消費者団体及び関連団体（キャッシュレス推進協議会、EC 決済協議会、Fintech 協会）等との連携を強化し、事業者向けの情報発信に取組む。 （同左） （同左）
P24	２．その他留意事項	２．その他留意事項

頁	現行【1.0 版】	改定版　※2020 年 12 月 28 日より変更した部分のみ下線
	（１）カード情報の取扱い業務を外部委託する場合の留意点と受託者における必要な対策 　関係事業者は、カード情報を取り扱う業務を外部委託する場合は、委託者自身が委託先のセキュリティ状況を確認し、責任を持って PCI DSS 準拠等の必要な対策を求める。 　また、複数の委託者からカード情報を取り扱う業務を受託する又はショッピングカート機能等のシステムを提供する事業者は、自社システムにおけるカード情報の保持状況について確認の上、PCI DSS 準拠等の必要なカード情報保護対策等を行う。	（１）カード情報の取扱い業務を外部委託する場合の留意点と受託者における必要な対策 　セキュリティ対策の実施主体者である関係事業者（加盟店、カード会社、決済代行業者等、コード決済事業者等）は、カード情報を取り扱う業務を外部委託する場合は、委託者自身が委託先のセキュリティ状況を確認し、責任を持って PCI DSS 準拠等の必要な対策を求める。 　また、特に、複数の委託者からカード情報を取り扱う業務を受託する事業者においては、カード情報が漏えいした場合の影響が大きいため、又、ショッピングカート機能等のシステムを提供する事業者においては、ショッピングカート部分の脆弱性からフィッシング等によりカード情報が漏えいする事案が発生していることから、自社システムにおけるカード情報の保持状況について確認の上、PCI DSS 準拠等の必要なカード情報保護対策等を行う。