

クレジットカード・セキュリティガイドライン 【6.0版】

クレジットカード取引セキュリティ対策協議会

事務局 一般社団法人日本クレジット協会

2025年3月

目次

第1章 はじめに	7
1-1 クレジットカード情報保護対策	8
1-2 不正利用対策	8
1-2-1 対面取引におけるクレジットカードの不正利用対策	8
1-2-2 非対面取引におけるクレジットカードの不正利用対策	8
第2章 用語集	11
第3章 附属文書・関係文書	17
3-1 附属文書一覧	17
3-2 関係文書一覧	18
3-3 附属文書に記載の対策一覧	19
第4章 本ガイドラインの基本的な考え方	20
4-1 本ガイドラインにおけるセキュリティ対策の対象	20
4-2 割賦販売法との関係性	20
4-3 対象となる関係事業者	20
4-4 対象となるクレジットカード	20
4-5 関係事業者間の情報連携等	21
4-6 消費者への情報提供	21
第5章 各事業者が講じる対策等	22
5-1 カード会社（イシューア）	22
5-1-1 対面取引・非対面取引共通	22
5-1-1-1 カード情報保護対策	22
①カード会社（イシューア）の指針対策（1号事業者）	22
a. PCI DSS 準拠	22
②委託先管理	22
③加盟店におけるカード情報漏えい時の対応	22
5-1-2 対面取引	22
5-1-2-1 不正利用対策	22
①発行カードのIC化	22
②IC取引時のオペレーションルール	22
5-1-3 非対面取引	23
5-1-3-1 不正利用対策	23
①EMV 3-D セキュア	23
a.発行カードのEMV 3-D セキュアの導入	24
b.リスクベース認証（RBA）の精度向上	24
c. 動的（ワンタイム）パスワードの送付先の登録情報の最新化	24
d. システムの安定稼働	24
②オーソリモニタリング	24
a.精度向上	24

b. 不正に入手したカード番号の有効性確認への対策.....	24
③カード会員に対するカード利用時の通知の導入及び登録推進	25
④真正利用照会対応.....	25
⑤コード決済等連携時の対策	25
5-1-4 周知・啓発	25
①発行カードの IC 化.....	25
a. PIN.....	25
i .認知度向上	25
ii .「サインの取得による本人確認」及び「PIN バイパスの廃止」	25
②情報管理リテラシー向上.....	25
a. フィッシング対策等	25
b. 「なりすまし」対策	26
c. 利用明細の確認.....	26
5-2 加盟店	26
5-2-1 対面取引	26
5-2-1-1 カード情報保護対策	26
①対面取引加盟店の指針対策（2号事業者）	26
a. 非保持化	26
i .非保持化の定義.....	26
ii .非保持化の実現方法.....	27
iii .非保持と同等/相当（内回り方式）の要件.....	27
iv .非保持化を実現した加盟店の留意点	27
b. PCI DSS 準拠.....	28
②委託先管理.....	28
③カード情報漏えい時の対応	28
5-2-1-2 不正利用対策	28
①対面取引加盟店の指針対策	28
a. 決済端末機の IC 対応.....	28
i 決済専用端末（CCT）	28
ii .POS	29
iii .特定業界	29
②IC 取引時のオペレーションルール	29
a. 接触 IC 取引	30
b. 非接触 IC 取引.....	30
c. サインの取得による本人確認.....	31
d. PIN バイパスの廃止.....	31
③情報共有要請.....	32
5-2-1-3 周知・啓発	32
①決済端末機の IC 対応.....	32
a. PIN.....	32
i .認知度向上	32
ii .「サインの取得による本人確認」及び「PIN バイパスの廃止」	32

5-2-2 非対面取引 (EC 加盟店)	32
5-2-2-1 カード情報保護対策	32
①EC 加盟店の指針対策 (2号事業者)	32
a.非保持化	32
i .非保持化の定義	32
ii .非保持化の実現方法	33
iii .非保持化を実現した加盟店の留意点	33
b.PCI DSS 準拠	34
c.脆弱性対策	34
②委託先管理	35
③カード情報漏えい時の対応	36
5-2-2-2 不正利用対策	36
①EC 加盟店の指針対策	36
a.不正利用対策導入の基本的な考え方	36
b.EC 加盟店が講じる具体的な対策	38
i .オーソリゼーション処理の体制整備	38
ii .善管注意義務	38
iii .EMV 3-D セキュア	38
iv .不正ログイン対策	39
v .不正顕在化加盟店が講じる具体的な対策	39
②情報共有	40
5-2-2-3 周知・啓発	41
①情報管理リテラシー向上	41
a.フィッシング対策	41
b.「なりすまし」対策	41
5-2-3 非対面取引 (MO・TO 取引取扱加盟店)	41
5-2-3-1 カード情報保護対策	41
①MO・TO 取引取扱加盟店の指針対策 (2号事業者)	41
a.非保持化	41
i .非保持化の定義	41
ii .非保持化の実現方法	42
iii .非保持と同等/相当 (内回り方式) の要件	42
iv .非保持化を実現した加盟店の留意点	42
b.PCI DSS 準拠	42
②委託先管理	43
③カード情報漏えい時の対応	43
5-2-3-2 不正利用対策	43
①MO・TO 取引取扱加盟店の指針対策	43
a.不正利用対策導入の考え方	43
②情報共有	44
5-2-4 加盟店のカード情報保護対策及び不正利用対策の概要	44
①カード情報保護対策	44
②対面取引加盟店における不正利用対策	45

③EC加盟店における不正利用対策の指針対策	46
④MO・TO取引取扱加盟店における不正利用対策の指針対策	46
5-3 カード会社（アクワイアラー）	46
5-3-1 対面取引・非対面取引共通	46
5-3-1-1 カード情報保護対策	46
①カード会社（アクワイアラー）の指針対策（3号事業者）	46
a.PCI DSS 準拠	46
②委託先管理	46
③加盟店におけるカード情報漏えい時の対応	47
5-3-2 対面取引	47
5-3-2-1 カード情報保護対策	47
①加盟店サポート	47
5-3-2-2 不正利用対策	47
①決済端末機のIC対応	47
②加盟店サポート	47
a.ガイドラインの周知及びベンダーとの連携	47
③IC取引時のオペレーションルール	47
a.接触IC取引	48
b.非接触IC取引	48
c.サインの取得による本人確認	49
d.PINバイパスの廃止	49
5-3-2-3 周知・啓発	50
①決済端末機のIC対応	50
a.PIN	50
i.認知度向上	50
ii.「サインの取得による本人確認」及び「PINバイパスの廃止」	50
5-3-3 非対面取引	50
5-3-3-1 カード情報保護対策	50
①加盟店サポート	50
②脆弱性対策	50
5-3-3-2 不正利用対策	51
①加盟店サポート	51
a.EMV 3-D セキュア	51
i.導入及び運用サポート	51
ii.AReq設定項目の充実	52
iii.システムの安定稼働	52
b.不正ログイン対策	52
i.導入及び運用サポート	52
c.不正顕在化加盟店	52
d.情報提供	53
i.情報共有	53
ii.真正利用照会対応	53

②コード決済ガイドライン等の準拠の確認	53
5-4 決済代行業者等・PSP	54
5-4-1 対面取引	54
5-4-1-1 カード情報保護対策	54
①決済代行業者等の指針対策（4号事業者）	54
a.PCI DSS 準拠	54
②委託先管理	54
③加盟店サポート	54
④加盟店におけるカード情報漏えい時の対応	54
5-4-1-2 不正利用対策	55
①決済端末機の IC 対応	55
5-4-1-3 周知・啓発	55
①決済端末機の IC 対応	55
a.PIN	55
i .認知度向上	55
ii .「サインの取得による本人確認」及び「PIN バイパスの廃止」	55
5-4-2 非対面取引	55
5-4-2-1 カード情報保護対策	55
①決済代行業者等の指針対策（4号事業者）	55
a.PCI DSS 準拠	55
②委託先管理	56
③加盟店サポート	56
④脆弱性対策	56
⑤加盟店におけるカード情報漏えい時の対応	57
5-4-2-2 不正利用対策	58
①加盟店サポート	58
a.EMV 3-D セキュア	58
i .導入及び運用サポート	58
ii .AReq 設定項目の充実	58
iii .システムの安定稼働	58
b.不正ログイン対策	58
i .導入及び運用サポート	58
c.不正顕在化加盟店	59
d.情報提供	60
i .情報共有	60
ii .真正利用照会対応	60
e.不正利用対策提供のための体制整備	60
5-5 コード決済事業者等	60
5-5-1 対面取引・非対面取引共通	60
5-5-1-1 カード情報保護対策	60
①コード決済事業者等の指針対策（5号事業者）	60

a.PCI DSS 準拠.....	60
②コード決済ガイドライン等の遵守.....	60
③委託先管理.....	61
5-6 コード決済事業者等の委託先及びECシステム提供会社等.....	61
5-6-1 対面取引・非対面取引共通.....	61
5-6-1-1 カード情報保護対策.....	61
①コード決済事業者等の委託先及びECシステム提供会社等の指針対策 (6号事業者及び7号事業者).....	61
a.PCI DSS 準拠.....	61
②委託先管理.....	61
5-6-1-2 カード情報保護対策・不正利用対策共通 (ECシステム提供会社のみ).....	62
①加盟店へのシステム等の提供及びサポート.....	62
5-7 その他の関係事業者等の具体的な対策.....	62
5-7-1 国際ブランド.....	62
①各事業者サポート.....	62
②周知・啓発.....	62
5-7-2 ソリューションベンダー.....	62
①加盟店へのシステム等の提供及びサポート.....	62
5-7-3 機器メーカー.....	63
①加盟店へのシステム等の提供及びサポート.....	63
②各事業者サポート.....	63
③周知・啓発.....	63
5-7-4 行政.....	63
①各事業者サポート.....	63
②周知・啓発.....	63
5-7-5 業界団体.....	64
①各事業者サポート.....	64
②周知・啓発.....	64
第6章 その他関係事項.....	66
6-1 消費者及び事業者等への周知・啓発.....	66
6-1-1 消費者への周知・啓発.....	66
6-1-2 事業者等への周知・啓発.....	66
【履歴】.....	67

第1章 はじめに

「クレジットカード取引におけるセキュリティ対策の強化に向けた実行計画（以下「実行計画」という。）」がその実施期限である2020年3月末に終了し、クレジットカード取引の関係事業者が実施すべきセキュリティ対策を「クレジットカード・セキュリティガイドライン（以下「本ガイドライン」という。）」として2020年3月にとりまとめて以降、5回目の改訂となる。

我が国では、政府の政策としてキャッシュレス化を推進し、2025年6月までにキャッシュレス決済比率40%を目指す目標を打ち立てている。2023年現在、我が国のキャッシュレス決済比率は39.3%に増加しており、多様なキャッシュレス決済がある中で、クレジットカード決済は依然として圧倒的なウェイト（83.5%）を占めている。一方、クレジットカード情報の盗用による非対面不正利用の被害は依然として高い水準で推移している。このような状況は、カード情報の保持又は非保持化に関わらず、加盟店のECサイトの設定不備や既知の脆弱性を悪用した第三者による不正アクセス、大量かつ連続する不正アタックによる有効性確認により窃取されたクレジットカード情報、フィッシング等の手段によりカード会員等から窃取されたセキュリティコードを含むクレジットカード情報やECサイト利用者のログインID・パスワード等が、コード決済やEC加盟店において悪用されているものと考えられる。

このようなクレジットカード情報の窃取や不正利用を防止するため、EC加盟店におけるカード情報保護対策及び本人認証を強化するための取組である不正利用対策が喫緊の課題である。加えて、キャッシュレス化の進展に伴い、カードレスやモバイルの利用が拡大しており、新たな決済の仕組みに応じた取引ルールの見直しや、消費者に対するフィッシングへの注意喚起、クレジットカードの安全・安心な利用に関する周知・啓発等の円滑な取組も重要となっている。

本協議会としてはこれまでも、非対面取引のカード情報保護対策としての「脆弱性対策」の強化や、不正利用対策としての本人認証を強化するために、EMV 3-Dセキュアの導入推進や多面的・重層的な対策の導入の必要性を本ガイドラインに掲載し、クレジットカード取引関係事業者が取組を求めてきたところであるが、上述のような不正利用被害の状況を踏まえ、実効性のあるセキュリティ対策を実現するため、今般、クレジットカード・セキュリティガイドライン【6.0版】として取りまとめたものである。

各関係事業者がクレジットカード決済環境の変化を踏まえ、本ガイドラインに基づくセキュリティ対策を実施し、クレジットカードを利用する消費者が安全・安心に利用できる環境の整備に一層取り組まれることを引き続き期待する。

なお、本ガイドラインでは各事業者ごとに講じる対策をまとめているが、その対策は「カード情報保護対策」「不正利用対策」「周知・啓発」であり、それぞれの対策等の基本的な考え方はこの後に記載する。

2025年3月

1-1 クレジットカード情報保護対策

カード情報の保護は、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及び標的型攻撃による個人情報やカード情報の窃取、さらには EC サイトの脆弱性やフィッシングによるカード会員からの窃取、そしてそれらの窃取したカード情報を利用した不正利用は国内に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カード情報の管理を行うことが求められる。

カード情報の漏えいは主に加盟店において発生していることから、カード情報を加盟店で保持しないこと（非保持化）が有効なセキュリティ対策と考えられてきたが、最近の漏えい事故の傾向として、非保持化を実現した EC 加盟店であっても Web サイトの脆弱性等を原因としたカード情報の窃取が発生している。このため、EC 加盟店には、カード情報の保持又は非保持にかかわらず、EC 加盟店の自社システム及び Web サイトの定期的な点検を行い、この点検結果に基づき、追加的な対策を導入するなどの適切な対策を講じることが求められる。

これまで本ガイドラインでは、割賦販売法第 35 条の 16 第 1 項第 2 号に定める事業者（2 号事業者＝加盟店）の指針対策は、「カード情報の非保持化（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」、また、同条同項第 1 号及び第 3 号から第 7 号の各事業者は「PCI DSS 準拠」を指針対策としてきた。本ガイドライン【6.0 版】からは、2 号事業者のうち EC 加盟店に対しては、カード情報保護対策として EC 加盟店のシステム及び Web サイトの「脆弱性対策」を講じることが指針対策に追加した。

この「脆弱性対策」は、割賦販売法で義務付けられているクレジットカード番号等の漏えい等の事故を防止するための措置の指針対策の一つであるが、これを適切に実施するためには、EC 加盟店のみならず関係事業者が「脆弱性対策」の内容を理解し、EC 加盟店の導入・運用に対してサポートを行うことが必要である。

なお、本ガイドラインと割賦販売法との関係性については、後記の「4-2 割賦販売法との関係性」を参照すること。

1-2 不正利用対策

1-2-1 対面取引におけるクレジットカードの不正利用対策

対面取引の不正利用対策については、割賦販売法によるセキュリティ対策の義務化及び本協議会の取組により、加盟店の決済端末の IC 対応、カードの IC 化が普及、定着し、偽造カードによる不正利用被害は減少傾向が続いている。このことから、現時点においても対面取引の不正利用対策としては IC 取引が最も効果的な対策である。

1-2-2 非対面取引におけるクレジットカードの不正利用対策

非対面取引の加盟店には、EC 加盟店と MO・TO 取引取扱加盟店があるが、不正利用被害のほとんどは EC 加盟店において発生しており、被害額は近年増加し続けている。日本クレジット協会の調査によると、2023 年のクレジットカード不正利用被害額は約 541 億円にのぼり、そのうちの約 9 割を EC 加盟店において「いずれかで窃取されたカード情報等を当該カードの会員本人になりすまして利用し商品等を購入する（以下「なりすまし」という。）」不正利用による被害が占めている。

EC 加盟店における不正利用被害が増加している背景としては、EC 加盟店からの情報漏えいが断続的に発生していることに加え、カード会員からのクレジットカード番号やセキュリ

ティコード、EC サイト利用者のログイン ID・パスワード等を巧みに窃取する手口である「フィッシング」、クレジットカード番号の採番の規則性を悪用して機械的に生成する手法（クレジットカードマスター）によって大量にカード番号を生成し、それらを EC 加盟店での利用を通じて実際に利用できるカード番号かを確認する手口等、カード番号等を窃取等する手口が年々巧妙化すると共に増加し続けているためである。これまで EC 加盟店における不正利用対策としては、「4つの方策」を個々に導入することを指針としてきたが、前述の手口により窃取されたカード情報や属性情報等による「なりすまし」の不正利用が増加しており、その「なりすまし」による手口は、EC 加盟店の取扱商品やスキーム等により異なることから、実効的な抑止効果が得られにくくなってきた。

また、EC 加盟店における不正利用は、カード決済のタイミングだけではなく、顧客が EC 加盟店の Web サイトの利用を開始してから商品の受け渡し完了するまでの間に様々な手口により行われている。

例えば、「カード決済前」には窃取された属性情報、ID・パスワード等による不正ログインが行われ、「カード決済時」にはなりすましによるカードの不正利用が行われ、「カード決済後」には、不正に購入された商品が配送・転売されるといった取引の一連の流れの中で、不正利用につながる複数の攻撃が行われている。このため、クレジットカード取引の流れを「線」として捉え、その線上の各タイミングにおいて適切な不正利用対策を講じることが、不正利用防止の実効性を高めることとなる。本ガイドラインでは、これを「線の考え方」に基づく対策の導入とし、EC 加盟店の不正利用対策の基本的な考え方とする。

【「線の考え方」の概念図】



本ガイドライン【6.0版】では、EC 加盟店の指針対策は「線の考え方」を基本として、従前の「オーソリゼーション処理の体制整備」「加盟店契約上の善良なる管理者の注意義務の履行」に加え、カード決済前の対策として「適切な不正ログイン対策の実施」、カード決済時の対策として「EMV 3-Dセキュアの導入」を求めることとしている。さらに、不正顕在化

加盟店に対しては、これに加え「類似の不正利用の発生を防止するために、適切な不正利用対策を追加導入する」ことを指針対策としている。

この「不正利用対策」は、割賦販売法で義務付けられている不正利用を防止するための措置の指針対策であるが、これを適切に実施するためには、EC加盟店のみならず関係事業者が「不正利用対策」の内容を理解し、EC加盟店の導入・運用に対してサポートを行うことが必要である。

なお、本ガイドラインと割賦販売法との関係性については、後記の「4-2 割賦販売法との関係性」を参照すること。



第2章 用語集

本ガイドラインにおける用語の説明は以下のとおり。

用語	説明
2段階認証	認証する回数を1回ではなく2段階に分けて行うことをいう。例えば、Webサイトにログインする際に、ID/パスワードを入力して認証した後、SMS、メール等で取得した認証コードを指定された画面に入力して追加の認証をすることでセキュリティを高める方式。2段階でそれぞれ異なる認証要素を用いる場合、多要素認証（後記参照）にもなり得る。
CCT	<u>C</u> redit <u>C</u> enter <u>T</u> erminalの略。 共同利用端末として運営される情報処理センターの信用照会端末。
CVM リミット金額	CVMとは、 <u>C</u> ardholder <u>V</u> erification <u>M</u> ethodの略。 クレジットカードに対するカード保有者を認証する本人確認方法。カードを提示した者が当該カードを使用する権利を有する者かを検証する。 CVMリミット金額とは、カード会社が定める本人確認を不要とする上限額。
EMV 3-D セキュア	オンラインショッピング時にクレジットカード番号等の情報の盗用による不正利用を防ぎ、安全にクレジットカード決済を行うために国際ブランドが推奨する本人認証サービス。 利用者がカード会員本人であることを確認する仕組みであり、各カード会社（イシューア）が、カード会員のデバイス情報等を用いて不正利用のリスク判断を行うとともに、必要に応じてパスワード入力を要求することで当該取引における安全性を確保する。 【EMV 3-D セキュア仕様の特徴について】 リスクベース認証で判定されたリスク度合いに応じて、認証処理は下記の通りフローが異なる。 ・低：フリクションレスフローとしてパスワード等の入力なしに認証が完結する。 ・中：チャレンジフローとして会員に対して追加の認証（パスワード等）を要求する。 ・高：認証拒否 詳細は、「EMV 3-D セキュア導入ガイド【附属文書 14】」参照。
IC化	ICは <u>I</u> ntegrated <u>C</u> ircuitの略。 クレジットカードにICチップを組み込むこと。構造上ICカードの複製は極めて困難であるとともに、演算機能を利用してオフラインで、偽造カードの検知やカード使用者の本人確認が可能であり、セキュリティ面で磁気カードより格段に優れる。ICチップのインターフェースによって接触型と非接触型に大別される。
IC対応	加盟店に設置するクレジットカード決済端末にICチップ読取機能を持たせること。
IC取引	カード情報をICチップに暗号化して格納したICカードを、加盟店に設置されたICチップ読取機能を持ったカード決済端末で処理する取引。
IPアドレス	IPアドレスとは「 <u>I</u> nternet <u>P</u> rotocol <u>A</u> ddress」の略で、PCやスマホなどのネットワークに接続する機器に割り振られる識別番号のこと。
MO・TO取引取扱加盟店	カタログやテレビを見て、はがきや電話で注文するいわゆるメールオーダー・テレフォンオーダーによる通信販売を取り扱う非対面取引加盟店。

用語	説明
PCI DSS	<p><u>P</u>ayment <u>C</u>ard <u>I</u>ndustry <u>D</u>ata <u>S</u>ecurity <u>S</u>tandard の略。 カード情報を取り扱う全ての事業者に対して国際ブランド（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。 安全なネットワークの構築やカード会員データの保護等、12の要件に基づいて約400の要求事項から構成されており、「準拠」とは、このうち該当する要求事項に全て対応できていることをいう。PCI DSS 準拠の検証方法としては、①オンサイトレビュー（認定セキュリティ評価機関（QSA）による訪問審査）又は②自己問診（SAQ、自己評価によってPCI DSS 準拠の度合いを評価し、報告することができるツール）による方法がある。 ※ Diners Club は Discover のグループであり、PCI DSS においては Discover の基準を適用している。</p>
PCI PTS	<p><u>P</u>ayment <u>C</u>ard <u>I</u>ndustry <u>P</u>IN <u>T</u>ransaction <u>S</u>ecurity の略。 PCI SSC が定めた、PIN 取引を保護する PIN 入力装置に関わる国際的なセキュリティ基準。PIN 取得時は PCI PTS に準拠した機器の利用が必要となる。機器メーカーが PCI SSC に申請し、個体ごとにその認定を受ける。物理的なキーボードやタッチスクリーン等、PIN を入力して伝送する端末を対象とし、端末の不正開封行為に対する強度（耐タンパー性）や、端末の操作時に発生する信号の保護、PIN 伝送時の暗号化等を定める。</p>
PCI P2PE	<p><u>P</u>CI <u>P</u>oint <u>t</u>o <u>P</u>oint <u>E</u>ncryption の略。 カードリーダーデバイスから決済処理ポイントまでカード会員データを安全に伝送処理する仕組みで、PCI SSC に認定されたソリューション。 ※ 詳細は、「メールオーダー・テレフォンオーダー加盟店における非保持化対応ソリューションについて【附属文書1】」を参照。</p>
PCI SSC	<p><u>P</u>ayment <u>C</u>ard <u>I</u>ndustry <u>S</u>ecurity <u>S</u>tandards <u>C</u>ouncil の略。 国際ブランド（VISA、Mastercard、JCB、American Express、Discover）が共同で設立した PCI セキュリティ基準の開発、管理、教育、認知を担当する、グローバル規模の開かれた協議会。 ※ 現在、UnionPay International（銀聯国際）がストラテジックメンバーとして参加している。</p>
PIN	<p><u>P</u>ersonal <u>I</u>dentification <u>N</u>umber の略。 カード入会時にカード会社（イシューア）に登録する暗証番号で、IC 取引時にカード会員が IC 対応決済端末に入力する数字。</p>
PIN パッド	<p>IC 取引に必要な PIN（暗証番号）を入力するためのパッド。</p>
PIN バイパス	<p>PIN（暗証番号）不知の一時的な救済措置として、カード会員に認められている PIN スキップ機能であり、「PIN」の代替として「サイン」による本人確認を行うものをいう。2025年3月をもって廃止した。</p>
PSP	<p><u>P</u>ayment <u>S</u>ervice <u>P</u>rovider 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、カード情報を処理する事業者をいう。 ※ 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。</p>

用語	説明
QSA	<u>Qualified Security Assessor</u> の略。 PCI SSCに認定されたセキュリティ評価機関。加盟店やPSPへのインタビューやドキュメント、サーバー等の訪問審査を正式に行うことができる認定セキュリティ評価機関。
SAQ	<u>Self-Assessment Questionnaire</u> の略。 自己問診。PCI DSS 準拠の自己評価を支援することを目的とした検証ツール。
SDK	<u>Software Development Kit</u> の略。 スマートフォンのアプリ等のソフトウェアの開発にあたり、必要なプログラムや文書、サンプルコードなどをパッケージ化したもの。
SQLインジェクション	データベースと連携したウェブアプリケーションの多くは、利用者からの入力情報を基にSQL文（データベースへの命令文）を組み立てている。ここでSQL文の組立方法に問題がある場合、攻撃によってデータベースの不正利用をまねく可能性がある。このような問題を「SQLインジェクションの脆弱性」と呼び、この問題を悪用した攻撃を、「SQLインジェクション攻撃」という。
アカウント/パスワードクラッキング	データを解析して他人のアカウントやパスワードを不正に割り出すこと。攻撃者は総当たり攻撃などさまざまな手法を使ってアカウントやパスワードを解読し、システムやWebサービスへの不正アクセスを試みている。
オーソリモニタリング	カード会社がオーソリゼーション情報等により不正利用を検知する仕組み。「不正検知システム」とも呼ばれるが、属性・行動分析ベンダーが提供するサービスとの混同を避ける観点から、本ガイドラインでは「オーソリモニタリング」と表記する。
オフライン PIN	IC 対応決済端末に IC カードが読み込まれ、カード利用時にカード会員が入力した数字と、カードの IC チップ内に記録された PIN とを照合するもの。 一方、IC 対応決済端末上での照合ではなく、オンラインネットワークを経由してカード会社（イシューア）のシステム上で照合するオンライン PIN がある。
カード会社（イシューア・アクワイアラ）	イシューアとはクレジットカード番号等取扱業者（割賦販売法第 35 条の 16 第 1 項第）の 1 号事業者ことをいう。 アクワイアラとは、クレジットカード番号等取扱業者（割賦販売法第 35 条の 16 第 1 項）の 3 号事業者又はクレジットカード番号等取扱契約締結事業者（割賦販売法第 35 条の 17 の 2）をいう。
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、有効期限で構成されるデータをいう。
カード情報	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。カード仕様の一部を構成する機密認証データは、PCI DSS によりそれ単体での保持も認められていない。 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ード番号を特定できないもの）

用語	説明
	<ul style="list-style-type: none"> ・ 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 <p>上記にかかわらず、2号事業者以外の事業者には PCI DSS 準拠が求められる。</p>
<p>共通シンボルマーク等</p>	<p>ICクレジットカードの暗証番号の認知度向上及び IC 取引における本人確認では暗証番号が必要であることの周知活動に活用するために、一般社団法人日本クレジット協会（以下「日本クレジット協会」という。）が策定したもの。</p> <p>「クレジットカードの暗証番号の認知度向上のための共通シンボルマーク」 「IC取引における本人確認方法の周知・啓発デザイン」</p> <div style="display: flex; justify-content: space-around; align-items: center;">   </div> <p>※ 「共通シンボルマーク」は日本クレジット協会の登録商標（平成30年7月27日登録）</p> <p>使用方法は「クレジットカードの暗証番号の認知度向上のためのシンボルマーク・デザインマニュアル」及び「IC取引における本人確認方法の周知・啓発デザインマニュアル」を参照（日本クレジット協会のホームページに掲載）。</p>
<p>クレジットマスター</p>	<p>クレジットカード番号等の採番の規則性を悪用し、機械的にクレジットカード番号を生成すること。</p>
<p>クロスサイト・スクリプティング</p>	<p>ウェブアプリケーションの中には、検索のキーワードの表示画面や個人情報登録時の確認画面等、ユーザーからの入力内容や HTTP ヘッダの情報を処理し、ウェブページとして出力するものがある。ここで、ウェブページへの出力処理に問題がある場合、そのウェブページにスクリプト（簡易なプログラム）等を埋め込まれてしまう。この問題を「クロスサイト・スクリプティングの脆弱性」と呼び、この問題を悪用した攻撃手法を「クロスサイト・スクリプティング攻撃」という。</p>
<p>決済専用端末</p>	<p>CCT（Credit Center Terminal）及びそれと同等以上のセキュリティレベルのものをいう。</p>
<p>シグネチャー</p>	<p>マルウェアを検出するためのデータベースファイル。「パターンファイル」や「定義ファイル」とも呼ばれる。ウイルス対策ソフト等のベンダーによって提供される。</p>
<p>スロットリング</p>	<p>同一 IP アドレスからの一定時間内に受信可能なリクエスト数を制限し、上回るリクエストがなされた際には受信を拒否しエラーコードを返却すること。</p>
<p>接触 IC 取引</p>	<p>決済端末に IC カードを挿入しカード券面上に露出した IC チップの接触端子からカード情報を読み込んで処理を行うものをいう。</p>

用語	説明
ソリューションベンダー	非保持化や非保持と同等/相当を実現するためのソリューション（仕組み）を提供するシステム会社等をいう。
多要素認証(2要素認証)	認証の3要素である「知識情報」「所持情報」「生体情報」のうち、異なる2つ以上の要素を組み合わせることで、認証のセキュリティが強化される。異なるパスワードを2回求める場合は、どちらも「知識情報」であるため多要素認証とされない。
データディレクトリ	ディレクトリとは、階層構造を持ったファイルを保管するための場所の総称であり、コンピュータ全般で使う用語であるが、Windowsではフォルダのことを指す。そのうちデータディレクトリとは、システムやアプリケーションのデータを保管している場所のことを指す。
デバイスフィンガープリント	アクセス元のデバイスを特定するためにウェブブラウザを通して情報を収集するプロセス。デバイス情報は主に、タイムスタンプ、IPアドレス、画面解像度、インストール済みプラグイン、Cookie、HTTPヘッダーを使って同一デバイスの特定をする仕組み。
非接触 IC 取引	決済端末に IC カードをかざす通信により、カード券面の内部に搭載された IC チップ内のカード情報を読み取り処理を行うものをいう。
非保持化	加盟店におけるカード情報保護対策の一つ。 自社で保有する機器・ネットワークにおいて「カード情報」を「保存」「処理」「通過」しないこと。
非保持と同等/相当	POS 内システム又は社内システムを介してカード情報を処理等するが、クレジットカード番号を特定できない状態とし、自社内で復号できない仕組み。 ※ 詳細については、「メールオーダー・テレフォンオーダー加盟店における非保持化対応ソリューションについて【附属文書 1】」及び「対面取引加盟店における非保持化対応ソリューションについて【附属文書 2】」を参照。
ブランドテスト	国際ブランドを介した取引に利用する決済システムの導入時に、国際ブランドごとに当該ブランドについて国際的な相互運用性が確保できることを確認するためのテスト。
ペネトレーションテスト	特定の脆弱性や問題点を発見することを主眼に、悪意のある攻撃者が意図する特定の攻撃を想定し、それが成功するか否かを検証するもの。システム全体に存在する脆弱性やセキュリティ上の不備を診断する「脆弱性診断」は、攻撃成功の実証を行わない点で異なる。
マルウェア	「悪意のある」という意味の英語「Malicious」と「software」を組み合わせた造語（malware）。様々な脆弱性を利用して攻撃を仕掛けるソフトウェアの総称として使われる。 ウイルスをはじめ、ワーム、スパイウェア、フィッシング、スパム、ボット、キーロガー（キーストロークロガー）、トロイの木馬等、種類は様々ある。
リスクベース認証	利用者が決済に使用するデバイスの設定情報や利用者から提供される個人情報等の様々なデータを活用して本人の利用であるかを確認し、認証をする仕組み。

[カード情報保護対策の対象事業者の定義]

対象事業者	定義
1号事業者	割賦販売法第35条の16第1項第1号に規定されるクレジットカード等購入あっせん業者であり、具体的にはカード発行会社（イシューア）を指す。
2号事業者	割賦販売法第35条の16第1項第2号に規定されるクレジットカード等購入あっせん関係販売業者又はクレジットカード等購入あっせん関係役務提供事業者であり、具体的には加盟店を指す。
3号事業者	割賦販売法第35条の16第1項第3号に規定される立替払取次業者であり、具体的にはアクワイアラーを指す。
4号事業者	割賦販売法第35条の16第1項第4号に規定されるアクワイアラー（3号事業者）のために、加盟店（2号事業者）にカード決済の代金相当額を交付（立替払い）する事業者を指す。 対象事業者の例としては、以下の通り。 ○決済代行業者（包括代理加盟事業者） ○ECモール事業者（デジタルプラットフォーム等） ○SC、百貨店（消化仕入れを除く）、ショッピングモール等 ○商店街組合（包括代理加盟事業者）
5号事業者	割賦販売法第35条の16第1項第5号に規定されるカード情報を別の決済用情報と結び付け、当該決済用情報で後払い決済を提供する事業者であり、具体的にはコード決済事業者等を指す。 対象事業者の例としては、以下の通り。 ○QRコード決済事業者 ○スマートフォン決済事業者 ○ID決済事業者等
6号事業者	割賦販売法第35条の16第1項第6号に規定されるコード決済事業者等（5号事業者）からの委託により、決済用情報に結びつけたカード情報を特定可能な状態で管理する事業者であり、具体的にはコード決済事業者等のカード情報管理業務受託事業者を指す。
7号事業者	割賦販売法第35条の16第1項第7号及び同法施行規則第132条の2に規定される事業者であり、具体的には加盟店が決済代行業者又はアクワイアラーにカード会員データを提供するために、クレジットカード決済機能を有するシステム及びそのサービスを提供する事業者を指す。この事業者には、カード会員データの伝送処理保存を行っている事業者、決済代行業者又はアクワイアラーに接続できる決済モジュールを提供している事業者も含まれる。 対象事業者の例としては、以下の通り。 ○ECシステム提供会社（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。 ASP/SaaSとしてEC事業者にサービス提供する事業者、EC事業者に購入プラットフォームを提供する事業者、これらに限らない。）

第3章 附属文書・関係文書

本ガイドラインにおけるセキュリティ対策の各方策等については、本協議会が策定した以下の附属文書及び本協議会事務局の日本クレジット協会が策定した関係文書の中で詳述している。

3-1 附属文書一覧

文書名	目的・概要
メールオーダー・テレフォンオーダー加盟店における非保持化対応ソリューションについて【附属文書1】	メールオーダー・テレフォンオーダー（MO・TO）加盟店における「非保持化（非保持と同等/相当を含む）」のため、具体的な方策例について取りまとめたもの。
対面取引加盟店における非保持化対応ソリューションについて【附属文書2】	対面取引加盟店における「非保持化（非保持と同等/相当を含む）」の実現方法及び具体的な技術要件について取りまとめたもの。
非保持化実現加盟店における過去のカード情報保護対策【附属文書3】	電子計算機を使用して作成する国税関係帳簿書類の保存方法等の特例に関する法律に基づき、過去のカード情報を含む電子帳簿について非保持化が困難な場合があることを踏まえ、「スタンドアローン環境」での保管・利用等の措置内容を取りまとめたもの。
国内ガソリンスタンドにおけるクレジットカード取引対応指針【附属文書4】	国内のガソリンスタンドにおける商慣習上の制約を考慮し、当面の対応として、実現可能な代替策を取りまとめたもの。
オートローディング式自動精算機のIC対応指針と自動精算機の本人確認方法について【附属文書5】	オートローディング式自動精算機の国際的なセキュリティ準拠が技術的に困難なことから、当面の対応として実現可能な自動精算機のIC対応とそれに伴うセキュリティリスク及び代替コントロール策を示したもの。
ICカード対応 POS ガイドライン（第I部 取引処理編）【附属文書6】	POS 加盟店での IC 対応を円滑に進めるため、磁気・接触 IC・非接触 IC ごとに端末要件や業務要件等について具体的な方策として策定したもの。
ICカード対応 POS ガイドライン（第II部 接続運用編）【附属文書7】	加盟店センター等が IC カード対応する際のシステム対応及び運用ガイドについて説明したもの。
ICカード対応 POS ガイドライン（第III部 非接触 EMV Kernel 処理編）【附属文書8】	非接触 EMV の各ブランド固有の Kernel 処理についての概要や注意事項をとりまとめたもの。
ICカード対応 POS 導入の手引き～認定・試験プロセス概要～【附属文書9】	加盟店、POS ベンダーを対象に、接触/非接触 EMV 対応有人型 POS の導入・修正において考慮していただきたい要件や認定・試験プロセスを整理したもの。
ブランドテスト要否一覧【附属文書10】	「ICカード対応 POS 導入の手引き～認定・試験プロセス概要～」の附属文書であり、同手引きに記載される「シナリオ別ブランドテスト要否一覧」の詳細を記したもの。
ICカード対応 POS 導入の手引き～全体概要編～【附属文書11】	POS 導入を計画するシステム企画担当者、売場の POS 運用担当者、POS のシステム・ネットワーク保守管理担当者を対象とし、IC クレジットカードの受入れの為に必要な基礎知識を磁気・接触 IC・非接触 IC ごとに紹介するもの。
ICカード対応 POS 導入の手引き～取引処理フロー解説編～【附属文書12】	加盟店の POS 端末システム企画担当者、POS 端末保守運用管理担当者を対象に、EMV 仕様書で規定されている IC カードと IC 対応端末の間、IC カードとカード会社ホストの間で行われる処理内容やそのフローを解説したもの。

文書名	目的・概要
【附属文書 13】 旧：不正利用対策 4 方策の具体的な基準・考え方について	廃止
EMV 3-D セキュア導入ガイド 【附属文書 14】	EMV 3-D セキュアの円滑な導入・運用を目的として、概要やシステム要件等、各ステークホルダーに必要な情報を取りまとめたもの。
<関連資料> ・【EMV 3-D セキュア】統合版_AReq 設定項目及び 3RI の仕様・ユースケース ・EMV 3-D セキュア導入ガイドに関する FAQ	
クレジット取引における本人確認方法に係るガイドライン 【附属文書 15】	IC 取引時のオペレーションルールとして、国内加盟店での IC 取引における本人確認方法の業界統一的な考え方を示すとともに、加盟店の円滑な IC 対応に資するよう、日本クレジット協会が策定し、2023 年度より協議会の附属文書として移管されたもの。
クレジットカード売上票の作成・保管に関するガイドライン 【附属文書 16】	「サイン」を取得しない加盟店の運用変更が円滑に進むことや運用の統一を目指し、クレジットカード取引における売上票の作成・保管に関しての運用を取りまとめたもの。
スマートフォン・タブレット等のアプリを利用した決済に関するセキュリティ対策等について 【附属文書 17】	スマートフォンやタブレット等の汎用デバイスを用いた決済及びスマホアプリ等の SDK を利用する決済について、「非保持化（非保持と同等/相当を含む）」の取組を推進するため、具体的な対策例について取りまとめたもの。
EC 加盟店における非保持化対応ソリューションについて 【附属文書 18】	EC 加盟店における「非保持化」の取組を推進するための実現方法等について取りまとめたもの。
属性・行動分析ガイダンス【附属文書 19】	属性・行動分析を効果的に導入・運用するにあたっての共通の考え方を示すもの
EC 加盟店におけるセキュリティ対策 導入ガイド 【附属文書 20】	EC 加盟店やその他非対面取引加盟店においてセキュリティ意識の向上と講じるべき対策についての理解を深め、カード情報漏えい対策及び不正利用対策に資するよう具体的な対策について解説したもの。
<関連資料> ・〔別紙 a〕 EC 加盟店におけるセキュリティ対策一覧 ・〔別紙 b〕 EC 加盟店におけるセキュリティ対策 導入ガイド 補足資料 （旧：セキュリティ・チェックリスト【附属文書 21】） ・〔別紙 c〕 EC サイトのセキュリティ対策実施状況申告書（例）	
【附属文書 21】 旧：セキュリティ・チェックリスト	廃止（附属文書 20 別紙 b に変更）

3-2 関係文書一覧

文書名	目的・概要
クレジットカード情報の漏えい時及び漏えい懸念時の対応要領 【関係文書 1】	クレジットカード取扱加盟店からクレジットカード情報が漏えいした、又は漏えいの懸念がある場合の対応ポイントをまとめたもの。

3-3 附属文書に記載の対策一覧

附属文書番号	別紙	附属文書名	該当指针对策						一般公開資料 (○: JCA一般HP掲載)
			カード情報保護		不正利用対策				
			非保持化	脆弱性	IC化	EMV3DS	不正ログイン	不正顕在化	
附属文書1		メールオーダー・テレフォンオーダー加盟店における非保持化対応ソリューションについて	○						
附属文書2		対面取引加盟店における非保持化対応ソリューションについて	○						
附属文書3		非保持化実現加盟店における過去のカード情報保護対策	○						
附属文書4		国内ガソリンスタンドにおけるICクレジットカード取引対応指針			○				
附属文書5		オートローディング式自動精算機のIC対応指針と自動精算機の本人確認方法について			○				
附属文書6		ICカード対応POSガイドライン（第I部 取引処理編）			○				
附属文書7		ICカード対応POSガイドライン（第II部 接続運用編）			○				
附属文書8		ICカード対応POSガイドライン（第III部 非接触EMV Kernel 処理編）			○				
附属文書9		ICカード対応POS導入の手引き ～認定・試験プロセス概要～			○				
附属文書10		ブランドテスト要否一覧			○				
附属文書11		ICカード対応POS導入の手引き ～全体概要編～			○				
附属文書12		ICカード対応POS導入の手引き ～取引処理フロー解説編～			○				
附属文書13		廃版（旧不正利用対策4方策の具体的な基準・考え方について（2024年改訂版））							
附属文書14		EMV 3-Dセキュア導入ガイド				○		○	○
		【EMV 3-Dセキュア】統合版_AReq設定項目及び3RIの仕様・ユースケース（公表版）				○		○	○
		【EMV 3-Dセキュア】統合版_AReq設定項目及び3RIの仕様・ユースケース（関係者版）				○		○	○
		EMV 3-Dセキュア導入ガイドに関するFAQ				○		○	○
附属文書15		クレジット取引における本人確認方法に係るガイドライン（関係者版）			○				
		クレジット取引における本人確認方法に係るガイドライン（公表版）			○				○
		「クレジット取引における本人確認方法に係るガイドライン」関係者版・公表版における記載の違いについて			○				
附属文書16		クレジットカード売上票の作成・保管に関するガイドライン			○				
附属文書17		スマートフォン・タブレット等のアプリを利用した決済に関するセキュリティ対策等について		○			○	○	
附属文書18		EC加盟店における非保持化対応ソリューションについて	○						
附属文書19		属性・行動分析ガイダンス（公開版は、附属文書20の文中に記載）				○	○	○	
附属文書20		EC加盟店におけるセキュリティ対策 導入ガイド		○		○	○	○	○
	別紙 a	EC加盟店におけるセキュリティ対策一覧		○		○	○	○	○
	別紙 b	EC加盟店におけるセキュリティ対策 導入ガイド 補足資料		○		○	○	○	○
	別紙 c	ECサイトのセキュリティ対策実施状況申告書（例）		○		○	○	○	○
附属文書21		廃版（旧セキュリティ・チェックリスト 附属文書20別紙 bへ統合）							
関係文書1		クレジットカード情報の漏えい時および漏えい懸念時の対応要領	○						

第4章 本ガイドラインの基本的な考え方

4-1 本ガイドラインにおけるセキュリティ対策の対象

本ガイドラインでは、クレジットカード取引の関係事業者ごとに、対面取引と非対面取引別に「カード情報保護」と「不正利用防止」のために講じるセキュリティ対策を定めるとともに、その対策を有効に機能させるために取り組むべき事項を記載している。

なお、対面取引と非対面取引とは以下の定義による。

取引形態	定義
対面取引	カード会員から提示を受けたカードのカード情報を端末機により読取り、当該カード情報をアクワイアラーに提供する取引
非対面取引	カード会員から、インターネット、電話等のカードの提示を受けない方法によりカード情報の通知を受け、アクワイアラーに提供する取引
EC加盟店	インターネットによりカード情報の通知を受ける加盟店（非保持化を実現した加盟店も含む）
MO・TO取引取扱加盟店	電話・FAX・はがき等によりカード情報の通知を受ける加盟店

4-2 割賦販売法との関係性

「割賦販売法（後払分野）に基づく監督の基本方針」において、本ガイドラインに掲げられる措置が割賦販売法で義務付けられているクレジットカード番号等の漏えい等の事故及び不正利用を防止するための措置の実務上の指針として位置付けられている。本ガイドラインに掲げる措置又はそれと同等以上の措置を適切に講じている場合には、クレジットカード番号等の漏えい等の事故及び不正利用を防止する措置として、割賦販売法に規定する「必要かつ適切な措置」が講じられているとみなされており、本ガイドラインにおいては、【指針対策】としてこれらの措置を記載している。

なお、割賦販売法においては、【指針対策】が実務指針となっている漏えい等の事故及び不正利用を防止するための措置のみならず、実施すべき措置が義務付けられていることに留意する。

4-3 対象となる関係事業者

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（イシューアークワイアラー）」「決済代行業者等（4号事業者）」「コード決済事業者等（5号事業者）」「コード決済事業者等の委託会社（6号事業者）」「加盟店向け決済システム提供事業者（7号事業者）」並びに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」及び「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。

4-4 対象となるクレジットカード

本ガイドラインの対象となるクレジットカードは、世界中で利用され、不正利用のリスクが高い「国際ブランド付きのクレジットカード」としている。

「国際ブランドが付いていないクレジットカード」は、利用できる範囲が限定され不正

利用のリスクも低いことから本ガイドラインの対象とはしていないが、不正利用等のリスクに応じたセキュリティ対策を講じる必要がある。

4－5 関係事業者間の情報連携等

本ガイドラインのセキュリティ対策は、関係事業者間による緊密な連携、協力体制の下で実施されなければ実効性のあるものにはならないため、各関係事業者は、本ガイドラインに基づく対策を講じる場合には相互に必要なサポートや情報提供を行う体制を構築する必要がある。

4－6 消費者への情報提供

本ガイドラインのセキュリティ対策の実効性確保のためには、クレジットカード利用者である消費者自らの取組の実施が必要である。このため、各関係事業者は、消費者の理解及び取組の推進に向けた情報提供及び周知活動に取り組む必要がある。

第5章 各事業者が講じる対策等

5-1 カード会社（イシューア）

5-1-1 対面取引・非対面取引共通

5-1-1-1 カード情報保護対策

①カード会社（イシューア）の指針対策（1号事業者）

【指針対策】

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。

a. PCI DSS 準拠

PCI DSS は、安全なネットワークの構築や、カード会員データの保護等の 12 の要件から構成されているが、各事業者の業態、システム・ネットワーク構成によって要求事項が異なることから、自社が対応すべき事項を検証し、準拠する必要がある。

「PCI DSS v4.0.1 基準書およびサポート文書」（「v4.0」から「v4.0.1」への変更の概要）は、PCI SSC（PCI Security Standards Council）のホームページ

（<https://www.pcisecuritystandards.org/lang/ja-ja/>）からダウンロードできる。

また、国内の PCI DSS 認定セキュリティ評価機関（QSA）のほとんどが参加している団体である、日本カード情報セキュリティ協議会（以下「JCDCS」という。）が、PCI DSS 準拠の取組をサポートするため、各種資料の提供や相談窓口を設置しており活用されたい（JCDCS ホームページ <https://www.jcdsc.org/>）。

②委託先管理

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く、標的型攻撃や既知の脆弱性等により不正侵入を許し、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。

③加盟店におけるカード情報漏えい時の対応

加盟店等からカード情報が漏えいした際は、被害の拡大を防ぐために早急に行動を起こす必要がある。具体的には、日本クレジット協会において策定した「クレジットカード情報漏えい時及び漏えい懸念時の対応要領【関係文書 1】」を有事の際の参考にしつつ、二次被害の防止のために必要な措置を講じる。

5-1-2 対面取引

5-1-2-1 不正利用対策

①発行カードの IC 化

発行するカードの全てを IC 化する。

②IC 取引時のオペレーションルール

IC 取引の円滑な運用に資するため、「接触 IC 取引」及び「非接触 IC 取引」の本人確認方法を IC 取引時のオペレーションルールとして、下表のとおり定めている。

[IC 取引時のオペレーションルール]

□取引形態別（接触 IC 取引/非接触 IC 取引）の本人確認方法

◆接触 IC 取引

- ・原則、「オフライン PIN」とする。
- ・CVM リミット金額以下の場合、本人確認を不要とすることができる。

◆非接触 IC 取引

- ・CVM リミット金額以下の場合、本人確認を不要とすることができる。
- ・「カード型」における CVM リミット金額超過時は「接触 IC 取引」へ切り替える。
- ・「モバイル型等」における CVM リミット金額超過時は Consumer Device CVM（モバイル PIN/生体認証等）とする。

CVM リミット金額	取引形態		
	接触 IC 取引	非接触 IC 取引	
		カード型	モバイル型等
CVM リミット以下	本人確認を「不要」とすることが可能		
CVM リミット超	原則オフライン PIN	[接触 IC 取引へ切替え] 原則オフライン PIN	Consumer Device CVM（モバイル PIN/生体認証等）

なお、オフライン PIN をサポートしていない海外発行カードや接触 IC 取引への切替を許容しないカード等については、「クレジット取引における本人確認方法に係るガイドライン【附属文書 15】」を参照すること。

対面取引における本人確認方法を、これまで行ってきた「サインの取得」から原則「PIN の入力」に変更することは、紛失・盗難カードの不正利用を防止するために実施するものである。

また、各国際ブランドのルールにおいても、これまで本人確認方法としてきた「サインの取得」は本人確認としての有効性が認められておらず、加盟店の業務上の必要性に応じて実施するもの（任意化）とされている。

このような状況を踏まえ、本協議会では、2022 年より「カード取引において本人確認としてのサインの取得を行わない運用とすることを推奨」し、「2025 年 4 月以降本人確認として PIN の入力が必要になる」旨の周知・啓発活動をクレジット業界全体で実施してきた。

また、PIN バイパス（PIN 入力スキップ機能）についても、2022 年より、2025 年 3 月をもって廃止する方針を本ガイドラインに記載し、周知・啓発活動を行ってきた。

よって、カード会社（イシューア）はカード会員に対しては、PIN の周知・啓発を継続的に行う必要がある。

詳細は「クレジット取引における本人確認方法に係るガイドライン【附属文書 15】」を、自動精算機については「オートローディング式自動精算機の IC 対応指針と自動精算機の本人確認方法について【附属文書 5】」を参照すること。

5-1-3 非対面取引

5-1-3-1 不正利用対策

①EMV 3-D セキュア

EMV 3-D セキュアは、カード会員のデバイス情報等を用いて「なりすまし」による不正利用のリスク判断を行うとともに、必要に応じて動的（ワンタイム）パスワードの入力等を要求することにより、当該取引がカード会員本人によるものかを確認する仕組みであること

から、取引の安全性を確保するための対策である。

具体的には、カード会社（イシューア）は、EMV 3-D セキュアにおけるリスクベース認証（RBA）により「なりすまし」のリスク判定を行い、本人確認が必要な取引と判断した場合は、動的（ワンタイム）パスワードの入力又は生体認証を求めるチャレンジフローの追加認証を行う。動的（ワンタイム）パスワードの場合は、カード会社（イシューア）に登録されているカード会員の携帯電話番号やメールアドレス等への動的（ワンタイム）パスワードの送付を行い、カード会員が受信した動的（ワンタイム）パスワードをその有効時間内に Web サイト画面に入力することにより本人認証を行う。

なお、後述する「b. リスクベース認証（RBA）の精度向上」及び「c. 動的（ワンタイム）パスワードの送付先の登録情報の最新化」も含め、「EMV 3-D セキュア導入ガイド【附属文書 14】」を参照すること。

a. 発行カードの EMV 3-D セキュアの導入

カード会社（イシューア）は、自社カード会員の EMV 3-D セキュアの登録を行う。

b. リスクベース認証（RBA）の精度向上

自社カード会員取引のリスク度合いを適切に判定するために、データ処理能力の向上や認証精度の分析及びルール設定等の最適化を常に行い、リスクベース認証の精度向上に継続的に取り組むことが求められる。

c. 動的（ワンタイム）パスワードの送付先の登録情報の最新化

カード会社（イシューア）は、自社カード会員に対して、EMV 3-D セキュアを導入した EC 加盟店から決済の際に動的（ワンタイム）パスワードの入力等を要求されることがあることの周知・啓発を行い、EC 加盟店における円滑な取引等がされるように対応する。

また、カード会社（イシューア）は、カード会員にその動的（ワンタイム）パスワードが確実に届くために、携帯電話番号やメールアドレス等の登録情報が常に最新化されているように対応することが求められる。

d. システムの安定稼働

EMV 3-D セキュアの安定稼働のための対応に関係事業者と連携し継続的に取り組む。

②オーソリモニタリング

a. 精度向上

過去の取引履歴等の様々な情報から、不正取引か否かを判断するオーソリモニタリングの検知精度の向上・強化を図る。

b. 不正に入手したカード番号の有効性確認への対策

EC 加盟店からの情報漏えい及びフィッシング等で窃取したカード番号やクレジットカードで生成したカード番号を利用し、EC 加盟店での利用を通じて実際に利用できるカード番号かを確認する手口が依然として発生していることから、このようなカード決済を早期に検知し、当該カード番号による取引を停止させる対策を講じることが必要である。

③カード会員に対するカード利用時の通知の導入及び登録推進

「カード会員に対するカード利用時の通知」とは、カード会員がカードを利用した際に、カード会社（イシューア）がメールやアプリ等により、カードの利用内容を通知することである。第三者による不正利用が発生した場合、当該通知によりカード会員が不正利用の発生を認知することができ、カード会社（イシューア）に連絡することで、迅速に決済の取消やカードの無効処理等の不正利用被害の抑止のための対応が可能となる。このため、カード会社（イシューア）は「カード会員に対するカード利用時の通知」の実施とカード会員に対して当該通知の利用のための携帯電話番号やメールアドレス等の登録を推進することが必要である。

④真正利用照会対応

非対面取引加盟店からの真正利用確認照会（オフアス取引の場合はアクワイアラー経由の照会）に応じるべく情報連携強化に取り組む。

⑤コード決済等連携時の対策

クレジットカードを、コード決済事業者等が提供する他の決済サービスと連携（紐づけ）する取引は、「なりすまし」によりクレジットカードを連携された場合、反復的に不正なチャージや決済利用がされることにより、高額な不正利用被害が発生する蓋然性がある。

このため、クレジットカードと連携する取引の時点で、カード会社（イシューア）は EMV 3-D セキュアによる認証やオーソリモニタリング等の対策を講じる必要がある。

5-1-4 周知・啓発

①発行カードの IC 化

a. PIN

i. 認知度向上

IC 取引では、本人確認のため「PIN の入力」が必要になることから、引き続き PIN の認知度向上のための周知活動を行うとともに、PIN を認知していないカード会員に対しては、PIN の重要性や PIN の確認方法等について、分かりやすく丁寧に説明する。

また、PIN 不知による利用阻害を生じさせないように、カード会員に速やかに PIN を通知するよう努める。

ii. 「サインの取得による本人確認」及び「PIN バイパスの廃止」

IC 取引において、「サインの取得」については、本人確認の効果を有していない。また、PIN バイパスは廃止されているため、引き続きカード会員への周知・啓発に取り組む。

②情報管理リテラシー向上

a. フィッシング対策等

カード会員に対して、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等の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、具体的な事例等の紹介を交えて注意喚起をするとともに、所持する電子機器のセキュリティ対策の必要性等について積極的に周知・啓発する。

また、自社カード会員における EMV 3-D セキュアの認証方法はフィッシングによって窃取されたカード情報等が不正利用される対策としても有効である動的（ワンタイム）パスワードを利用するため、カード会員の円滑な取引のために周知・啓発をする。

さらに、自社のサイトに似せたフィッシングサイトを確認したときは、当該フィッシングサイトの無効化等の手続をすることとする。

b. 「なりすまし」対策

カード会員自らの不正利用対策の実施を促進するため、カード利用時に入力求められることがあるセキュリティコードや動的（ワンタイム）パスワードの説明を行うとともに、EC サイトのログイン ID・パスワードの使い回しの危険性等について注意喚起を行う。

c. 利用明細の確認

カード会員が利用明細を確認することは、利用覚えのない取引の認知、カード会社（イシューア）に対する不正利用の事実確認の依頼、不正利用であることが確認された場合のカードの無効・再発行処理等の不正利用被害の拡大防止につながる。このため、カード会員に対して、利用明細を確認することの必要性について周知・啓発する。

5-2 加盟店

5-2-1 対面取引

5-2-1-1 カード情報保護対策

①対面取引加盟店の指針対策（2号事業者）

【指針対策】

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）、又はカード情報を保持する場合は PCI DSS に準拠する。

a. 非保持化

i. 非保持化の定義

加盟店におけるカード情報保護のための取組として「非保持化」を推進する。

非保持化は PCI DSS 準拠とイコールではないものの、カード情報保護という観点では同等の効果があるものと認められるため、本ガイドラインにおいては、PCI DSS 準拠に並ぶ措置とする。

本ガイドラインで示す加盟店における「非保持化」とは、「自社で保有する機器・ネットワークにおいて『カード情報』を『保存』『処理』『通過』しないこと」を言い、カード情報に含まれる「機密認証データ」の保持も認められない。

また、加盟店が POS システムでクレジットカード決済を行わず「IC 対応した決済専用端末」のみを使用し、カード情報を直接外部の情報処理センター等に伝送している場合も「非保持化」に該当する。

対面取引では、決済端末の IC 対応とともに外回りによる非保持化が進展している。

なお、以下ア.~ウ.の状態ではカード情報を保存する場合には、「保持」とはならない。

ア.紙（クレジット取引伝票、カード番号を記した FAX、申込書、メモ等）

イ.紙媒体をスキャンした画像データ

ウ.電話での通話記録（音声データを含む）

(注1) 上記ア.～ウ.以外において非保持化（非保持と同等/相当を含む）が実現されていることが前提。

(注2) 本ガイドラインにおいて上記ア.～ウ.の状態でカード情報を保存する場合は「保持」とはならないが、PCI DSS 準拠を目指す加盟店においては、本ガイドラインの内容にかかわらず、PCI DSS 準拠対象になることに留意する必要がある。

ii. 非保持化の実現方法

POS システムを導入している加盟店では POS の機能と決済の機能を分離し、決済専用端末から直接外部の情報処理センター又は ASP/クラウドセンター等に伝送される「外回り方式」を導入することにより非保持化を実現することが可能である。

なお、具体的な非保持化の実現方法については、「対面取引加盟店における非保持化対応ソリューションについて【附属文書 2】」を参照すること。

また、カード会社や ASP/クラウドセンター等を運営する事業者から、カード情報の還元を受け自社で保有する機器・ネットワークにおいて「保存」「処理」「通過」している場合（決済以外の目的の場合も含む）は、カード情報の保持となるため PCI DSS の準拠が必要となることに留意する。

iii. 非保持と同等/相当（内回り方式）の要件

カード会員データを特定できない状態とし、自社内で復号できない仕組みとすれば、仮に窃取されてもカード情報として不正に利用することは極めて困難であるため、PCI P2PE 認定ソリューションの導入又は本協議会が取りまとめたセキュリティ技術要件に適合するセキュリティ基準を満たすことにより（「内回り方式」）、非保持と同等/相当のセキュリティ対策を実現することが可能である。なおこの場合でも、事業者の選択により PCI DSS に準拠することが望ましい。

なお、具体的な非保持と同等/相当の実現方法については、「対面取引加盟店における非保持化対応ソリューションについて【附属文書 2】」を参照すること。

[対面取引加盟店における非保持化（非保持と同等/相当を含む）導入例]

方策		概要
非保持化 (外回り方式)	ア.非保持化	決済専用端末連動型
	イ.非保持化	ASP/クラウド接続型
ウ.非保持と同等/相当 (内回り方式)		PCI P2PE 認定ソリューション又は PCI MPoC 認定ソリューションの導入あるいは本協議会が取りまとめたセキュリティ技術要件に適合するセキュリティ基準を満たしたカード情報の暗号化による内回り方式

iv. 非保持化を実現した加盟店の留意点

非保持化を実現した加盟店においては、①顧客からの照会への対応と、②過去に取り扱ったカード情報の保護対策について留意する。

なお、具体的な対応等は、①顧客からの照会への対応については、「対面取引加盟店における非保持化対応ソリューションについて【附属文書 2】」を、②過去に取り扱ったカード情報の保護対策については、「非保持化実現加盟店における過去のカード情報保護対策【附属文書 3】」を参照すること。

b. PCI DSS 準拠

PCI DSS は、安全なネットワークの構築や、カード会員データの保護等の 12 の要件から構成されているが、各事業者の業態、システム・ネットワーク構成によって要求事項が異なることから、自社が対応すべき事項を検証し、準拠する必要がある。

「PCI DSS v4.0.1 基準書およびサポート文書」（「v4.0」から「v4.0.1」への変更の概要）は、PCI SSC（PCI Security Standards Council）のホームページ

（<https://www.pcisecuritystandards.org/lang/ja-ja/>）からダウンロードできる。

また、国内の PCI DSS 認定セキュリティ評価機関（QSA）のほとんどが参加している団体である、日本カード情報セキュリティ協議会（以下「JCDSC」という。）が、PCI DSS 準拠の取組をサポートするため、各種資料の提供や相談窓口を設置しており活用されたい（JCDSC ホームページ <https://www.jcdsc.org/>）。

②委託先管理

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く、標的型攻撃や既知の脆弱性等により不正侵入を許し、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。

③カード情報漏えい時の対応

カード情報が漏えいした際は、速やかに契約するカード会社（アクワイアラー）又は決済代行業者に連絡するとともに、契約するカード会社（アクワイアラー）又は決済代行業者の要請にしたがって、被害の拡大を防止するための初動対応として、漏えい元（データベース又は決済端末等）のネットワークからの切り離し、カード決済の一時停止等の措置、フォレンジック調査、PCI DSS 準拠等の確認及び再発防止のための適切な措置を講じる。

また、カード決済の再開に当たっては、加盟店は契約するカード会社（アクワイアラー）又は決済代行業者と PCI DSS 準拠等の再発防止のための適切な措置の具体的な内容について協議し、SAQ 等の提出や再発防止のための措置等の対応を十分に講じた上で、契約するカード会社（アクワイアラー）に判断を求める。

5-2-1-2 不正利用対策

①対面取引加盟店の指针对策

【指针对策】

IC 取引を可能とするため、設置する決済端末の全てを IC 対応にする。

a. 決済端末機の IC 対応

i. 決済専用端末（CCT）

POS システムを導入していない加盟店又は POS システムをクレジットカード決済に用いていない加盟店については、IC 対応した決済専用端末（CCT）を導入することで、IC 対応を図ることができる。

ii. POS

IC 対応の実現方法としては、各加盟店の現行システムや店頭オペレーションの特徴を踏まえ、技術面、コスト面から検証・整理を行うと、決済専用端末（CCT）連動型、決済サーバー接続型、ASP/クラウド接続型に大別される。

なお、IC 対応の実現方法は、「IC カード対応 POS 導入の手引き ～全体概要編～【附属文書 11】」「IC カード対応 POS ガイドライン（第 I 部 取引処理編）【附属文書 6】」

「IC カード対応 POS ガイドライン（第 II 部 接続運用編）【附属文書 7】」「IC カード対応 POS ガイドライン（第 III 部 EMV Kernel 処理編）【附属文書 8】」等を参照すること。

iii. 特定業界

7) 石油元売

日本国内のガソリンスタンドにおいては、利用者が乗車したまま決済するサービス（フルサービス）を行うガソリンスタンドの場合、総務省消防庁通知の内容に準拠した PIN 入力可能なハンディ端末の開発・導入が必要となる。

また、セルフサービスのガソリンスタンドにおいては、現行システム・機器の仕様の制約上、現状では国際基準が求める PIN パッドの設置等が困難であり、代替コントロール策の導入が必要となる。このため、同様の課題を抱える一部の業界と合わせた対応の指針として「オートローディング式自動精算機の IC 対応指針と自動精算機の本人確認方法について【附属文書 5】」を取りまとめており、これらの課題が解決するまでの間は、この指針に基づいて対応する。

なお、ガソリンスタンドにおける IC 対応については、上記のような業界固有の課題を踏まえ「国内ガソリンスタンドにおけるクレジットカード取引対応指針【附属文書 4】」に実現可能な方策を取りまとめており、この指針に基づいて IC 対応する。

1) オートローディング式自動精算機

オートローディング式自動精算機に関しては、IC カードリーダーライターと PIN パッドが物理的に分離した構造となるため、現状、PCI SSC が定めた国際的なセキュリティ基準である PCI PTS に準拠することが技術的に難しいという課題がある。

一部の業界（例：ガソリンスタンド、鉄道等）では、PCI PTS への準拠が困難であるオートローディング式により IC 対応を進めることとなったことを受け、「オートローディング式自動精算機の IC 対応指針と自動精算機の本人確認方法について【附属文書 5】」を取りまとめた。この指針では、オートローディング式の自動精算機を IC 対応する場合の PCI PTS 未準拠により生じ得るセキュリティリスクに応じた代替コントロール策の内容等、具体的な対応事例を示している。オートローディング式の自動精算機の IC 対応については、当面の間、この指針に基づいて対応する。

② IC 取引時のオペレーションルール

IC 取引の円滑な運用に資するため、「接触 IC 取引」及び「非接触 IC 取引」の本人確認方法を IC 取引時のオペレーションルールとして取りまとめており、概要は以下のとおり。

詳細は「クレジットカード取引における本人確認方法に係るガイドライン【附属文書 15】」（以下「本人確認ガイドライン」という。）を、自動精算機については「オートローディング式

自動精算機の IC 対応指針と自動精算機の本人確認方法について【附属文書 5】」を参照すること。

a. 接触 IC 取引

接触 IC 取引は、決済端末に IC カードを挿入しカード券面上に露出した IC チップの接触端子からカード情報を読み込んで処理を行うものである。

- ・カード偽造防止のみならず、紛失・盗難カードによる不正利用を防止するため、原則「PIN の入力」による本人確認を行うこととする。
- ・なお、一定条件においては、加盟店は本人確認を不要とすることができる。（※）

b. 非接触 IC 取引

非接触 IC 取引は、決済端末に IC カード等をかざすことにより、カード券面等の内部に搭載された IC チップ内のカード情報を読み取り処理を行うものである。

- ・CVM リミット金額超の取引においては、以下のとおりカード会員が提示する媒体に応じて本人確認を行う。

ア) カード型

CVM リミット金額超の取引については、非接触 IC 取引から接触 IC 取引に切り替え、オフライン PIN による本人確認を行う。

イ) モバイル型等

CVM リミット金額超の取引については、Consumer Device CVM（モバイル型等のパスワードや生体認証等の機能）を用いた本人確認とする。

- ・なお、一定条件においては、加盟店は本人確認を不要とすることができる。（※）

（※）本人確認不要取引

本人確認ガイドラインで規定する「本人確認が必要となる業種/売場/商品等」に該当せず、かつ、「本人確認不要取引の CVM リミット金額」の範囲内については、加盟店は本人確認を不要とすることができる。

本人確認不要取引を行うに当たっては、カード会員の保護及び不正利用発生の防止に留意しなければならない。

なお、加盟店が自主的に本人確認を実施することを妨げるものではない。

詳細については、契約するカード会社（アクワイアラー）又は決済代行会社に確認を行う。

[IC 取引時のオペレーションルール]

□取引形態別（接触 IC 取引/非接触 IC 取引）の本人確認方法

◆接触 IC 取引

- ・原則、「オフライン PIN」とする。
- ・CVM リミット金額以下の場合は、本人確認を不要とすることができる。

◆非接触 IC 取引

- ・CVM リミット金額以下の場合は、本人確認を不要とすることができる。
- ・「カード型」における CVM リミット金額超過時は「接触 IC 取引」へ切り替える。
- ・「モバイル型等」における CVM リミット金額超過時は Consumer Device CVM（モバイル PIN/生体認証等）とする。

CVM リミット金額	取引形態		
	接触 IC 取引	非接触 IC 取引	
		カード型	モバイル型等
CVM リミット以下	本人確認を「不要」とすることが可能		
CVM リミット超	原則オフライン PIN	[接触 IC 取引へ切替え] 原則オフライン PIN	Consumer Device CVM (モバイル PIN/生体認証等)

なお、オフライン PIN をサポートしていない海外発行カードや接触 IC 取引への切替えを許容しないカード等の取扱いについては、「本人確認ガイドライン」を参照すること。

c. サインの取得による本人確認

対面取引における本人確認方法を、これまで行ってきた「サインの取得」から原則「PIN の入力」に変更することは、紛失・盗難カードの不正利用を防止するために実施するものである。

また、各国際ブランドのルールにおいても、これまで本人確認方法としてきた「サインの取得」は本人確認としての有効性が認められておらず、加盟店の業務上の必要性に応じて実施するもの（任意化）とされている。

これらのことから、2022 年より「カード取引において本人確認としてサインの取得を行わない運用とすることを推奨」し、「2025 年 4 月以降本人確認として PIN の入力が必要になる」旨の周知・啓発活動をクレジット業界全体で実施してきた。

なお、加盟店のオペレーション上必要な場合に「サインの取得」を妨げるものではないが、カード取引における本人確認としての効果は有していないことに留意する。

クレジットカード取引の売上票（カード会社控え等）については、カード取引の本人確認としての「サインの取得」をしない運用にすることにより、加盟店においては紙伝票印刷や保管業務の削減等、運用の合理化を図ることが可能となる。「サインの取得」をしない加盟店のクレジットカード売上票の取扱いに関する運用については、「クレジットカード売上票の作成・保管に関するガイドライン【附属文書 16】」を参照すること。

d. PIN バイパスの廃止

本協議会において、PIN バイパス（PIN 入力スキップ機能）については、以下の事由により廃止とし、2022 年より、2025 年 3 月をもって廃止する方針を本ガイドラインに記載し、クレジット業界全体で周知・啓発活動を行ってきた。

- ・紛失・盗難カードの不正利用を防止するために、「PIN の入力」による本人確認が必要である。

- ・海外発行のカードには本機能を許容しないものも存在し利用障害が発生している。

具体的な対応としては、運用面での停止又は決済端末の当該機能の停止をすることにより、PIN バイパスの運用は廃止するものである。

また、「サインの取得」については、本人確認としての効果を有していないため、PIN 失念への救済措置としてきたカード取引の本人確認としての「サインの取得」による代替（PIN バイパス）は存在意義が失われている。

なお、発行主体者と利用される加盟店が同一グループであるなどにより固有の本人確認が行われている場合においては、「サインの取得」による本人確認や「PIN バイパス廃止」への対応は、当該発行主体者と加盟店に委ねられていることに留意する。

③情報共有要請

POS システムでクレジットカード決済を行う加盟店は、自社の IC 対応に係る実現方法を選択する際には、カード会社（アクワイアラー）や機器メーカー等に情報を求める。

5-2-1-3 周知・啓発

①決済端末機の IC 対応

a. PIN

i. 認知度向上

PIN 不知のカード利用者に対しては、PIN 確認のためにカード会社（イシューア）への案内に協力する。

ii. 「サインの取得による本人確認」及び「PIN バイパスの廃止」

対面取引加盟店においては、「5-2-1-2 不正利用対策 ②IC 取引時のオペレーションルール」に記述のとおり、「サインの取得」については、本人確認の効果を有していない。また、PIN バイパスは廃止されているため、カード決済時等におけるカード利用者への案内を行う。

5-2-2 非対面取引（EC 加盟店）

5-2-2-1 カード情報保護対策

①EC 加盟店の指针对策（2号事業者）

【指针对策】

カード情報を保持しない非保持化、又はカード情報を保持する場合は PCI DSS に準拠する。

さらに、EC 加盟店のシステム及び Web サイトの「脆弱性対策」を講じる。

a. 非保持化

i. 非保持化の定義

カード情報保護のための取組として「非保持化」を推進する。

非保持化は PCI DSS 準拠とイコールではないものの、カード情報保護という観点では同等の効果があるものと認められるため、本ガイドラインにおいては、PCI DSS 準拠に並ぶ措置とする。

本ガイドラインで示す加盟店における「非保持化」とは、「自社で保有する機器・ネットワークにおいて『カード情報』を『保存』『処理』『通過』しないこと」を言い、カード情報に含まれる「機密認証データ」の保持も認められない。

また、決済専用端末から直接外部の情報処理センター等に伝送している場合も「非保持化」に該当する。

なお、以下ア～ウの状態ではカード情報を保存する場合には、「保持」とはならない。

ア.紙（クレジット取引伝票、カード番号を記した FAX、申込書、メモ等）

イ.紙媒体をスキャンした画像データ

ウ.電話での通話記録（音声データを含む）

(注 1) 上記ア.～ウ.以外において非保持化が実現されていることが前提。

(注 2) 本ガイドラインにおいて上記ア.～ウ.の状態カード情報を保存する場合は「保持」とはならないが、PCI DSS 準拠を目指す加盟店においては、本ガイドラインの内容にかかわらず、PCI DSS 準拠対象になることに留意する必要がある。

ii. 非保持化の実現方法

PSP を利用する EC 加盟店のカード決済システムにおいては、カード情報が EC 加盟店の機器・ネットワークを通過する「通過型」と、通過しない「非通過型」に大別される。

通過型は、カード情報が EC 加盟店の機器・ネットワークを「通過」して「処理」されるため、EC 加盟店が意図せずにカード情報を「保存」することがある。これらの「通過」して「処理」されたカード情報や「保存」されたカード情報は、外部からの不正アクセスやウイルスの侵入、システムの改ざんや機器の脆弱性により、窃取されるリスクが高い。過去に発生した漏えい事故の多数は、この「通過型」の EC 加盟店において発生したものであった。

一方、非通過型は、カード情報が EC 加盟店ではなく、PSP の機器・ネットワークを「通過」して「処理」され、EC 加盟店はカード情報を「保存」「処理」「通過」することはない。EC 加盟店は、PCI DSS 準拠済みの PSP が提供する非通過型（「リダイレクト（リンク）型」又は「JavaScript 型（トークン型）」）等の決済システムを導入して非保持化を実現することができる。

具体的な非保持化実現方法は、「EC 加盟店における非保持化対応ソリューションについて【附属文書 18】」を参照すること。

また、カード会社や PSP 等から、カード情報の還元を受け自社で保有する機器・ネットワークにおいて「保存」「処理」「通過」している場合（決済以外の目的の場合も含む）は、カード情報の保持となるため PCI DSS の準拠が必要となることに留意する。

なお、自社の決済システムが「通過型」「非通過型」のいずれかであることを認識しておらず、カード情報の漏えい事故が発生した後に、「通過型」であることを認識する事例が見られることから、EC 加盟店は自社の決済システムを確認し、「通過型」を導入している場合には、カード情報を保持しない「非通過型」への移行か、カード情報を保持する必要がある場合は、PCI DSS に準拠しなければならない。

[EC 加盟店における非保持化導入例]

	方策	概要
非通過型	ア.リダイレクト（リンク）型	PSP の決済画面に遷移させカード決済を行う方式
	イ.JavaScript 型（トークン型）	加盟店の決済画面に PSP が提供する JavaScript プログラムを組み込んで利用し、決済を行う方式

iii. 非保持化を実現した加盟店の留意点

非保持化を実現した加盟店においては、①顧客からの照会への対応と、②過去に取り扱ったカード情報の保護対策について留意する。

なお、具体的な対応等は、①顧客からの照会への対応については、「EC 加盟店における非保持化対応ソリューションについて【附属文書 18】」を、②過去に取り扱ったカード情報

の保護対策については、「非保持化実現加盟店における過去のカード情報保護対策【附属文書3】」を参照すること。

b. PCI DSS 準拠

PCI DSS は、安全なネットワークの構築や、カード会員データの保護等の 12 の要件から構成されているが、各事業者の業態、システム・ネットワーク構成によって要求事項が異なることから、自社が対応すべき事項を検証し、準拠する必要がある。

「PCI DSS v4.0.1 基準書およびサポート文書」（「v4.0」から「v4.0.1」への変更の概要）は、PCI SSC（PCI Security Standards Council）のホームページ（<https://www.pcisecuritystandards.org/lang/ja-ja/>）からダウンロードできる。

また、国内の PCI DSS 認定セキュリティ評価機関（QSA）のほとんどが参加している団体である、日本カード情報セキュリティ協議会（以下「JCDSC」という。）が、PCI DSS 準拠の取組をサポートするため、各種資料の提供や相談窓口を設置しており活用されたい（JCDSC ホームページ <https://www.jcdsc.org/>）。

c. 脆弱性対策

EC 加盟店では、EC 加盟店のシステム（※1）や Web サイト（※2）のウイルス対策、管理者の権限の管理、デバイス管理等の「脆弱性対策」の不備を原因としたカード情報の漏えい事案が発生しているほか、大量かつ連続する不正アタックや悪質な有効性確認及び EC 加盟店やカード会社等を模したフィッシングサイトによってカード情報や会員のログインアカウントなどの窃取も見受けられる。これらの対策は、カード情報の保持又は非保持にかかわらず必要なものである。

また、不正に入手した大量のカード会員データやクレジットカード番号の採番の規則性を悪用して生成するクレジットマスターによって生成した大量のカード番号を利用して、EC 加盟店での利用を通じて実際に利用できるカード番号かを確認する手口が依然として発生している。このような手口では、真正なカード会員がカード番号等を入力して決済等を行おうとする場合と比較すると、その速度や連続性の点が明らかに異なることから、EC 加盟店が真正な取引との相違点等により不正な取引を早期に検知し取引を遮断するなど、自社の Web サイトにおいても被害の状況に応じた対策を講じることが必要となる。

このため、これまでは試行として新規加盟店契約前に、自ら EC 加盟店の自社システムや Web サイトの「脆弱性対策」を実施し、その状況をカード会社（アクワイアラー）や PSP に申告してきたが、2025 年 4 月以降は既契約加盟店も含めて、「EC 加盟店におけるセキュリティ対策 導入ガイド【附属文書 20】」（以下「セキュリティ対策導入ガイド【附属文書 20】」という。）の第 2 部「1.脆弱性対策」に記載の対策を実施する。

なお、「脆弱性対策」については、「クレジットカード決済システムのセキュリティ対策強化検討会報告書」（2023 年 1 月 20 日 経済産業省 https://www.meti.go.jp/shingikai/mono_info_service/credit_card_payment/pdf/20230120_1.pdf）においても、EC 加盟店の漏えい対策の強化のための当面の対応として、EC 加盟店のシステム、EC サイト自体の「脆弱性対策」（システム上の設定の不備への対策（PW 管理等）、脆弱性診断・対策、ウイルス対策等）を講ずることと 2024 年度末までにその旨を本ガイドラインに追記することが求められていた。

また、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、不断に自社の

システム及び Web サイトの「脆弱性対策」の改善・強化を図る。

(※1) 商品・サービス・金額等を掲載している Web サイトのセキュリティ対策を含めた管理権限を有するシステム

(※2) 商品・サービス・金額等を掲載し、消費者が閲覧する Web サイト

[導入する「脆弱性対策」] (下記のすべての対策を講じる)

①システム管理画面のアクセス制限と管理者の ID/パスワード管理
システム管理画面のアクセス可能な IP アドレスを制限する。IP アドレスを制限できない場合は管理画面にベーシック認証等のアクセス制限を設ける。
取得されたアカウントを不正使用されないよう 2 段階認証又は多要素認証 (2 要素認証) を採用する。
システム管理画面のログインフォームでは、アカウントロック機能を有効にし、10 回以下(PCI DSS ver4.0.1 基準)のログイン失敗でアカウントをロックする。
②データディレクトリの露見に伴う設定不備への対策
公開ディレクトリには、重要なファイルを配置しない。(特定のディレクトリを非公開にする。公開ディレクトリ以外に重要なファイルを配置する。)
Web サーバーや Web アプリケーションによりアップロード可能な拡張子やファイルを制限する等の設定を行う。
③Web アプリケーションの脆弱性対策
脆弱性診断又はペネトレーションテストを定期的の実施し、必要な修正対応を行う。
SQL インジェクションの脆弱性やクロスサイト・スクリプティングの脆弱性対策として、最新のプラグインの使用やソフトウェアのバージョンアップを行う。
Web アプリケーションを開発又はカスタマイズされている場合には、セキュアコーディング済みであるか、ソースコードレビューを行い確認する。その際は、入力フォームの入力値チェックも行う。
④マルウェア対策としてのウイルス対策ソフトの導入、運用
マルウェア検知/除去などの対策としてウイルス対策ソフトを導入して、シグネチャーの更新や定期的なフルスキャンなどを行う。
⑤悪質な有効性確認、クレジットマスターへの対策
悪質な有効性確認、クレジットマスターに対して、「セキュリティ対策導入ガイド【附属文書 20】」別紙 a 「1.脆弱性対策」⑤に記載の対策を 1 つ以上実施する。

②委託先管理

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。

特に、EC システムや Web サイトの構築・運用を外部委託する場合は、当該委託先に対して、EC 加盟店が行う「脆弱性対策」を理解した上で構築・運用を行うことを求める。

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く、標的型攻撃や既知の脆弱性等により不正侵入を許し、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。

③カード情報漏えい時の対応

カード情報が漏えいした際は、速やかに契約するカード会社（アクワイアラー）又は PSP に連絡するとともに、契約するカード会社（アクワイアラー）又は PSP の要請にしたがって、被害の拡大を防止するための初動対応として、漏えい元（データベース等）のネットワークからの切り離し、カード決済の一時停止等の措置、フォレンジック調査、PCI DSS 準拠等の確認及び再発防止のための適切な措置を講じる。

また、カード決済の再開に当たっては、契約するカード会社（アクワイアラー）又は PSP と PCI DSS 準拠等の再発防止のための適切な措置の具体的な内容について協議し、SAQ 等の提出や再発防止のための措置等の対応を十分に講じた上で、契約するカード会社（アクワイアラー）の判断を求める。

5-2-2-2 不正利用対策

①EC 加盟店の指針対策

【指針対策】

不正利用防止策として、オーソリゼーション処理の体制整備、加盟店契約上の善良なる管理者の注意義務の履行、EMV 3-D セキュアの導入及び適切な不正ログイン対策を実施する。

上記に加え、不正顕在化加盟店は、類似の不正利用の発生を防止するために、不正利用の発生状況等に応じて、本ガイドラインが掲げる不正利用対策から適切な対策を追加導入する。

a. 不正利用対策導入の基本的な考え方

EC 加盟店には、利用者が属性情報やクレジットカード番号等を登録してアカウント（ID）とパスワードを作成し、EC 加盟店の Web サイトにログインをした上で商品購入の申込みとクレジットカード決済を行う「会員登録型」と、商品購入の申込み時にクレジットカード番号を入力して決済を行う「ゲスト購入型」があり、昨今は「会員登録型」の EC 加盟店が主流となってきている。

不正利用に使用する情報は、EC 加盟店等へのサイバー攻撃等による不正アクセスや EC 加盟店やカード会社等を模したフィッシングサイトにより窃取したカード情報、属性情報、アカウント（ID）・パスワード、またクレジットカードマスターにより生成したカード番号である。

その情報を利用した不正利用の手口として「会員登録型」の場合、

- ・ EC 加盟店において、窃取した属性情報・カード情報等を利用し、EC 加盟店において不正なアカウントの登録を行う「不正アカウント作成」
- ・ 窃取した正規のアカウント等のログイン情報等を使用し、EC 加盟店への不正ログインを行う「アカウント乗っ取り」

があり、いずれも Web サイトにおける購入・決済前に行われるため、「決済前の対策」が必要である。

また、「ゲスト購入型」の場合は、不正ログインされることなく、窃取したカード情報等を Web サイトの購入・決済時に利用されるため「決済時の対策」が必要である。

さらに不正利用により購入された商品は、不正利用者が指定した住所に配送されることから、「決済後の対策」が必要である。

このため、EC 加盟店の Web サイトの利用を開始する場面から商品の受け渡し完了する場面までの「カード決済前」「カード決済時」「カード決済後」の取引の流れを「線」として

捉え、その線上の各タイミングにおいて適切な対策を講じることが必要であり、これを「線の考え方」に基づく対策の導入という。

【「線の考え方」の概念図】



具体的には、「不正ログイン対策」を、「カード決済前」の EC 加盟店の Web サイトへの「会員登録時」「会員ログイン時」「属性情報変更時」の対策として実施する。また、「EMV 3-D セキュア」を、「カード決済時」の「イシューアによる本人確認が適切に行われるための対策」として導入する。

なお、EC 加盟店においては、取扱商品（※）やスキーム等により、不正利用の手口が異なることから、不正利用の発生の可能性や被害状況等に応じた適切な対策を導入することが求められる。

また、不正顕在化加盟店についてはこれらの対策に加え、類似の不正利用の発生を防止するための対策を講じる必要がある。カード会社（アクワイアラー）や PSP からの情報提供を受け、不正利用の発生状況を把握し、取扱商品（※）やスキーム等によって異なる不正利用の手口に応じて「適切な対策の追加導入」や既に導入している対策の設定項目の追加・変更や不正判定レベルのチューニングによる「対策の強化」を行う。

この「対策の強化」は、不正顕在化加盟店が、既に導入している EMV 3-D セキュアや属性・行動分析等の対策において、リスク判定や不正判定レベルの分析に基づき、リスク判定項目の追加・変更や不正判定レベルのチューニング等による精度向上を図り、類似の不正利用の発生防止を行うものである。

（※）日本クレジット協会のインフラ整備部会調査によると、「相対的にリスクが高い商材」は、不正利用の発生リスクが高いことから、追加導入する対策や既に導入している対策の設定項目の追加・変更や不正判定レベルのチューニングにおいて、リスクを認識した上での対応が必要である。

詳細は、「セキュリティ対策導入ガイド【附属文書 20】」の第 3 部「2-1.相対的にリスクの高い商材の不正利用対策」を参照すること。

①デジタルコンテンツ（オンラインゲームを含む）、②家電、③電子マネー、④チケット、⑤宿泊予約サービス

なお、ここでいう③電子マネーとは、コード決済事業者等のその他決済サービス（プリペイド機能等）にクレジットカードを紐づけ、その決済サービスにチャージすることにより利用可能となるものは除く。

b. EC 加盟店が講じる具体的な対策

i. オーソリゼーション処理の体制整備

カード会社（イシューア）によるリスク評価を含めた承認判定を得るためのオーソリゼーション処理の体制を整備する。

ii. 善管注意義務

加盟店契約に定める善良なる管理者の注意により不正利用防止措置を実施する。

iii. EMV 3-D セキュア

ア) EMV 3-D セキュアの導入

イシューアによる本人確認が適切に行われるための措置として、EC 加盟店は EMV 3-D セキュアを導入する。

EMV 3-D セキュアは、EC 加盟店における不正利用防止のための本人認証手法の一つで、各カード会社（イシューア）が、カード会員のデバイス情報等を用いて「なりすまし」による不正利用のリスク判断を行うとともに、必要に応じてパスワード入力等を要求することで当該取引の安全性を確保するための対策である。

イ) EMV 3-D セキュアの運用

EC 加盟店は、EMV 3-D セキュアを導入した上で、原則としては決済の都度、EMV 3-D セキュアによる認証を行うことが求められるが、加盟店が EMV 3-D セキュア以外に講じる不正利用対策の内容や抑止効果に応じて、カード番号の登録時に EMV 3-D セキュアによる認証を行う運用や加盟店のリスク判断により EMV 3-D セキュアによる認証を行う運用も認められる。

また、EMV 3-D セキュアの未導入が認められる取引についても別途定めている。

詳細は「EMV 3-D セキュア導入ガイド【附属文書 14】」を参照すること。

ウ) リスクベース認証（RBA）の精度向上のための対応

カード会社（イシューア）におけるリスクベース認証の精度向上のため、「EMV 3-D セキュア導入ガイド【附属文書 14】」を参照し、カード会社（アクワイアラー）や PSP 等と連携しながら、自社の取扱商品や不正利用の被害状況等の実態を踏まえ、カード会員のデバイス情報等の情報をカード会社（イシューア）により多く提供できるよう、また提供する情報を適宜見直せるよう、データ項目の設定等を行える等の体制を整えることが求められる。加えて、後述の「不正顕在化加盟店」等において更なる不正利用対策強化が必要な場合には、カード会社（アクワイアラー）や PSP の要請に応じ、カード会社（イシューア）の認証精度向上に資するデータ項目の設定を行うことが求められる。

iv. 不正ログイン対策

EC加盟店には、利用者が属性情報やクレジットカード番号等を登録してアカウント（ID）とパスワードを作成し、EC加盟店のWebサイトにログインをした上で商品購入の申込みとクレジットカード決済を行う「会員登録型」と、商品購入の申込み時にクレジットカード番号を入力して決済を行う「ゲスト購入型」があり、最近では「会員登録型」のEC加盟店が主流となってきている。

こうした状況から、「会員登録型」のEC加盟店において、アカウント（ID）・パスワード等を悪用されたクレジットカードの不正利用が増加している。

EC加盟店における不正利用の手口としては、「会員登録型」の場合は、窃取した属性情報やカード情報等を利用し、EC加盟店において不正なアカウントの登録を行う「不正アカウント作成」と、窃取した正規のアカウント等のログイン情報等を使用し、EC加盟店への不正ログインを行う「アカウント乗っ取り」の大きく二つの手口がある。

EC加盟店は、不正利用の手口によって導入すべき対策は異なってくることから、その手口による不正利用発生リスクに応じて、決済前の「会員登録時」「会員ログイン時」「属性情報変更時」のそれぞれの場面を考慮した適切な対策を「セキュリティ対策導入ガイド【附属文書20】」の第2部「3.不正ログイン対策（決済前の対策）」に記載の対策から、1つ以上導入する。なお、下表「導入する不正ログイン対策」の①～⑦の対策を優先的に導入することが望ましい。

[導入する不正ログイン対策]

○：有効な対策

対策項目	会員登録時	会員ログイン時	属性情報変更時
①不審なIPアドレスからのアクセス制限	○	○	○
②2段階認証又は多要素認証（2要素認証）による本人確認	—	○	○
③会員登録時の個人情報確認（氏名・住所・電話番号・メールアドレス等）	○	○	—
④ログイン試行回数の制限強化（アカウント/パスワードクラッキングの対応）、スロットリング	—	○	—
⑤会員ログイン時/属性情報変更時のメールやSMS通知	—	○	○
⑥属性・行動分析	○	○	○
⑦デバイスフィンガープリント	○	○	○
⑧その他の対策（「セキュリティ対策導入ガイド【附属文書20】」別紙a「3.不正ログイン対策」（決済前の対策）に記載の対策）			

また、リスト型攻撃（システムを利用し短時間に大量の決済等を行うこと）による不正利用が引き続き発生していることから、カード会社（アクワイアラー）やPSPから、短期間に不正利用が急増し不正利用防止の対応が必要である旨の情報連携を受けた場合は、速やかに適切な対策を追加導入することとする。

v. 不正顕在化加盟店が講じる具体的な対策

カード会社（アクワイアラー）各社が把握する不正利用金額が、「3ヵ月連続50万円超」に該当する加盟店を「不正顕在化加盟店」とする。不正顕在化加盟店は、カード会社（アクワイアラー）やPSPのサポートを受け、類似の不正利用の発生を防止するために、不正利用

の発生状況や取扱商品（※）、スキーム等によって異なる不正利用の手口に応じて「適切な対策の追加導入」や既に導入している対策の設定項目の追加・変更や不正判定レベルのチューニングによる「対策の強化」を行う。

この「適切な対策の追加導入」は、属性・行動分析や配送先情報のチェック、配送停止・配送保留等の「セキュリティ対策導入ガイド【附属文書 20】」に記載の不正利用対策から適切な対策を追加導入することとする。

また、「対策の強化」とは、不正顕在化加盟店が既に導入している EMV 3-D セキュアや属性・行動分析等について、リスク判定や不正判定レベルの分析に基づいてリスク判定項目の追加・変更や不正判定レベルのチューニング等により性能及び実効性の向上を図るものである。

（※）日本クレジット協会のインフラ整備部会調査によると、「相対的にリスクが高い商材」は、不正利用の発生リスクが高いことから、追加導入する対策や既に導入している対策の設定項目の追加・変更や不正判定レベルのチューニングにおいて、リスクを認識した上での対応が必要である。

詳細は「セキュリティ対策導入ガイド【附属文書 20】」の第 3 部「2-1.相対的にリスクの高い商材の不正利用対策」を参照すること。

①デジタルコンテンツ（オンラインゲームを含む）、②家電、③電子マネー、④チケット、⑤宿泊予約サービス

なお、ここでいう③電子マネーとは、コード決済事業者等のその他決済サービス（プリペイド機能等）にクレジットカードを紐づけ、その決済サービスにチャージすることにより利用可能となるものは除く。

なお、EC 加盟店がこれまでに導入している不正利用対策（セキュリティコードや属性・行動分析、配送停止・配送保留等）についても、リスクに応じて継続することとする。

「セキュリティ対策導入ガイド【附属文書 20】」に記載の対策と同等以上の性能を満たしている不正利用対策であれば、その対策を導入することも認められるものとする。ただし、加盟店はカード会社（アクワイアラー）や PSP からその対策が「セキュリティ対策導入ガイド【附属文書 20】」記載の対策と同等以上の性能であることの説明が求められる可能性がある点に留意する必要がある。

②情報共有

自社が導入している不正利用対策の課題を検証し、必要に応じて新たな対策の導入等を検討するため、契約カード会社（アクワイアラー）や PSP との間で迅速な情報共有に努める。

また、自社での不審なカード利用の把握に努めるとともに、不正利用の手口は日々巧妙化することから、カード会社における不正利用対策の更なる向上のため、当該情報（不審利用）や不正利用対策に有効な情報について契約カード会社（アクワイアラー）や PSP と迅速な情報共有に努める。

5-2-2-3 周知・啓発

①情報管理リテラシー向上

a. フィッシング対策

消費者がフィッシング詐欺に遭わないように、フィッシングの手口や自社の名を騙る詐欺サイト等に対する注意喚起を行う。

また、自社の Web サイトを模したフィッシングサイトを確認したときは、当該フィッシングサイトの無効化等の手続をすることとする。

b. 「なりすまし」対策

EC 取引においては、カード利用時に求められる場合のあるセキュリティコードや動的（ワンタイム）パスワードの利用、EC サイト利用者のログイン ID・パスワードの使い回しの危険性等について、注意喚起を行う。

5-2-3 非対面取引（MO・TO 取引取扱加盟店）

5-2-3-1 カード情報保護対策

①MO・TO 取引取扱加盟店の指針対策（2号事業者）

【指針対策】

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）、又はカード情報を保持する場合は PCI DSS に準拠する。

a. 非保持化

i. 非保持化の定義

加盟店におけるカード情報保護のための取組として「非保持化」を推進する。

非保持化は PCI DSS 準拠とイコールではないものの、カード情報保護という観点では同等の効果があるものと認められるため、本ガイドラインにおいては、PCI DSS 準拠に並ぶ措置とする。

本ガイドラインで示す加盟店における「非保持化」とは、「自社で保有する機器・ネットワークにおいて『カード情報』を『保存』『処理』『通過』しないこと」を言い、カード情報に含まれる「機密認証データ」の保持も認められない。

また、決済専用端末から直接外部の情報処理センター等に伝送している場合も「非保持化」に該当する。

なお、以下ア.～ウ.の状態でカード情報を保存する場合には、「保持」とはならない。

ア.紙（クレジット取引伝票、カード番号を記した FAX、申込書、メモ等）

イ.紙媒体をスキャンした画像データ

ウ.電話での通話記録（音声データを含む）

（注 1）上記ア.～ウ.以外において非保持化（非保持と同等/相当を含む）が実現されていることが前提。

（注 2）本ガイドラインにおいて上記ア.～ウ.の状態でカード情報を保存する場合は「保持」とはならないが、PCI DSS 準拠を目指す加盟店においては、本ガイドラインの内容にかかわらず、PCI DSS 準拠対象になることに留意する必要がある。

ii. 非保持化の実現方法

MO・TO 取引取扱加盟店が、顧客から電話・FAX・はがき等でカード情報を入力し、MO・TO 取引取扱加盟店の機器にカード情報を入力して決済を行っている場合には、カード情報を電磁的情報として自社内に「通過」させない外回り方式を導入することにより、非保持化を実現することが可能である。

なお、具体的な実現方法は、「メールオーダー・テレフォンオーダー加盟店における非保持化対応ソリューションについて【附属文書 1】」を参照すること。

また、カード会社等から、カード情報の還元を受け自社で保有する機器・ネットワークにおいて「保存」「処理」「通過」している場合（決済以外の目的の場合も含む）は、カード情報の保持となるため PCI DSS の準拠が必要となることに留意する。

iii. 非保持と同等/相当（内回り方式）の要件

PCI P2PE 認定ソリューションは、カード会員データを特定できない状態とし、自社内で復号できない仕組みであり、仮に情報を窃取されてもカード情報として不正に利用することは極めて困難であることから、PCI P2PE 認定ソリューションを導入することにより、非保持と同等/相当のセキュリティ措置を実現することが可能である。なおこの場合でも、事業者の選択により PCI DSS に準拠することが望ましい。

なお、具体的な実現方法は、「メールオーダー・テレフォンオーダー加盟店における非保持化対応ソリューションについて【附属文書 1】」を参照すること。

[MO・TO 取引取扱加盟店における非保持化（非保持と同等/相当を含む）導入例]

方策	概要	
非通過型 (外回り方式)	ア. 非保持化 イ. 非保持化	決済専用端末を利用した外回り方式 タブレット端末（※）を利用した外回り方式
	ウ. 非保持と同等/相当 (内回り方式)	PCI P2PE 認定ソリューションを導入した内回り方式

（※）非保持化のためにカード情報の取扱いを委託した PSP から提供される端末の例示

iv. 非保持化を実現した加盟店の留意点

非保持化を実現した加盟店においては、①顧客からの照会への対応と、②過去に取り扱ったカード情報の保護対策について留意する。

なお、具体的な対応等は、①顧客からの照会への対応については、「メールオーダー・テレフォンオーダー加盟店における非保持化対応ソリューションについて【附属文書 1】」を、②過去に取り扱ったカード情報の保護対策については、「非保持化実現加盟店における過去のカード情報保護対策【附属文書 3】」を参照すること。

b. PCI DSS 準拠

PCI DSS は、安全なネットワークの構築や、カード会員データの保護等の 12 の要件から構成されているが、各事業者の業態、システム・ネットワーク構成に応じ要求事項が異なることから、自社が対応すべき事項を検証し、準拠する必要がある。

「PCI DSS v4.0.1 基準書およびサポート文書」（「v4.0」から「v4.0.1」への変更の概要）は、PCI SSC（PCI Security Standards Council）のホームページ

（<https://www.pcisecuritystandards.org/lang/ja-ja/>）からダウンロードできる。

また、国内の PCI DSS 認定セキュリティ評価機関（QSA）のほとんどが参加している団体である、日本カード情報セキュリティ協議会（以下「JCDS」という。）が、PCI DSS 準拠の取組をサポートするため、各種資料の提供や相談窓口を設置しており活用されたい（JCDS ホームページ <https://www.jcdsc.org/>）。

②委託先管理

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く、標的型攻撃や既知の脆弱性等により不正侵入を許し、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。

③カード情報漏えい時の対応

カード情報が漏えいした際は、速やかに契約するカード会社（アクワイアラー）又は PSP に連絡するとともに、契約するカード会社（アクワイアラー）又は PSP の要請にしたがって、被害の拡大を防止するための初動対応として、漏えい元（データベース等）のネットワークからの切り離し、カード決済の一時停止等の措置、フォレンジック調査、PCI DSS 準拠等の確認及び再発防止のための適切な措置を講じる。

カード決済の再開に当たっては、契約するカード会社（アクワイアラー）又は PSP と PCI DSS 準拠等の再発防止のための適切な措置の具体的な内容について協議し、SAQ 等の提出や再発防止のための措置等の対応状況を十分に講じた上で、契約するカード会社（アクワイアラー）の判断を求める。

5-2-3-2 不正利用対策

①MO・TO 取引取扱加盟店の指针对策

【指针对策】

オーソリゼーション処理の体制整備と加盟店契約上の善良なる管理者の注意をもって不正利用の発生を防止するとともに、リスクや被害状況に応じた非対面不正利用対策を導入する。

a. 不正利用対策導入の考え方

不正利用防止のための対策として、カード会社（イシューア）の承認判定を得るためのオーソリゼーション処理の体制整備をするとともに、加盟店契約に定める善良なる管理者の注意による不正利用防止措置を実施することが必要である。

また、「相対的にリスクが高い商材」（※）は、不正利用の標的となることから、このような商材を MO・TO 取引で取り扱う場合は、カード会社（アクワイアラー）や PSP のサポートを受け、商材のリスクに応じて適切な不正利用対策を講じるが必要となる。

さらに、カード会社（アクワイアラー）や PSP から、短期間に不正利用が急増し不正利用防止の対応が必要である旨の情報連携を受けた場合は、追加的な対策の導入が必要となる。

なお、MO・TO 取引取扱加盟店がこれまで導入している不正利用対策については、リスクに応じて継続することとする。

（※）日本クレジット協会のインフラ整備部会調査によると、「相対的にリスクが高い商材」は、不正利用の発生リスクが高いことから、追加導入する対策や既に導入してい

る対策の設定項目の追加・変更や不正判定レベルのチューニングにおいては、リスクを認識した上での対応が必要である。

詳細は「セキュリティ対策導入ガイド【附属文書 20】」の第 3 部「2-1.相対的にリスクの高い商材の不正利用対策」を参照すること。

①デジタルコンテンツ（オンラインゲームを含む）、②家電、③電子マネー、④チケット、⑤宿泊予約サービス

なお、ここでいう③電子マネーとは、コード決済事業者等のその他決済サービス（プリペイド機能等）にクレジットカードを紐づけ、その決済サービスにチャージすることにより利用可能となるものは除く。

②情報共有

自社が導入している不正利用対策の課題を検証し、必要に応じて新たな対策の導入等を検討するため、契約カード会社（アクワイアラー）や PSP との間で迅速な情報共有に努める。

また、自社での不審なカード利用の把握に努めるとともに、不正利用の手口は日々巧妙化することから、カード会社における不正利用対策の更なる向上のため、当該情報（不審利用）や不正利用対策に有効な情報について契約カード会社（アクワイアラー）や PSP と迅速な情報共有に努める。

さらに、不正利用対策として、自社で属性・行動分析を導入している場合は、それを有効に活用するために、多くの不正取引の情報や不審なカード利用の把握及び不正利用の手口等の情報の最新化が必要である。このため、カード会社（イシューア）で発生した不正取引の情報について、できるだけ多くのカード会社（アクワイアラー）・PSP 等と迅速な情報共有に努め、自社の不正利用対策の問題の特定とともにその解決を図る。

5-2-4 加盟店のカード情報保護対策及び不正利用対策の概要

①カード情報保護対策

形態		【指针对策】			PCI DSS 準拠
		非保持化			
		外回り（非通過型） カード情報が自社で保有する機器・ネットワークを「保存」「処理」「通過」しない方式	内回り（通過型） カード情報が自社で保有する機器・ネットワークを「保存」「処理」「通過」する方式（非保持と同等/相当）		
対面取引加盟店		決済専用端末利用型	ASP/クラウド接続型	PCI P2PE 認定ソリューション・PCI MPoC ソリューション 本協議会が取りまとめたセキュリティ要件	オンサイトレビュー又は SAQ
非対面取引加盟店	EC 加盟店	リダイレクト型（リンク）型	JavaScript（トークン）型		
	EC 加盟店のシステム及び Web サイトの「脆弱性対策」				
MO・TO 取引取扱加盟店		決済専用端末利用型	タブレット端末利用型	PCI P2PE 認定ソリューション	

（注 1）非保持と同等/相当を実現した場合でも、事業者の選択により PCI DSS に準拠することが望ましい。

(注2) 継続課金加盟店において、カード受付時は対面取引を行い、以降は非対面取引を行う場合には、対面取引加盟店と非対面取引加盟店双方の対策が必要となる。

(注3) 上表は加盟店に求められる対策を示すものであるが、どの対策を採るかは各事業者の選択に委ねられる。

[「①カード情報保護対策」の概要（EC 加盟店の「脆弱性対策」を除く）]

対策項目	非保持化	非保持と同等/相当	PCI DSS 準拠
概要	自社で保有する機器・ネットワークにおいてカード情報を「保存」「処理」「通過」しないこと	自社で保有する機器・ネットワーク外でカード番号を特定できない状態とし、自社内で復号できない仕組み（仮に窃取されてもカード情報として不正に利用することは極めて困難となる）	カード情報を取り扱う全ての事業者に対して国際ブランドが共同で策定したデータセキュリティの国際基準（PCI DSS）に準拠すること
実現方法	本ガイドラインに記載の非保持化実現方策の導入等	本ガイドラインに記載の非保持と同等/相当実現方策の導入	PCI DSS に定められた要件への対応 （12のセキュリティ要件への対応、準拠項目に関する QSA による訪問審査（オンサイトレビュー）又は自己問診（SAQ）の実施）
各々の特徴	非通過型（EC 加盟店）又は外回り方式（対面取引加盟店、MO・TO 取引取扱加盟店）等によりカード情報を一切保持しない	POS 内システム又は自社内システムを介してカード情報を処理等せざるを得ない場合でも、事実上、「非保持化」が可能	カード情報を自社で保有する機器・ネットワークで保持する場合の対策

②対面取引加盟店における不正利用対策

加盟店	指针对策の実現方法
POS システムでクレジットカード決済を行う加盟店	次の実現方式による POS システムでの IC 対応 ア. 決済専用端末（CCT）連動型 イ. 決済サーバー接続型 ウ. ASP/クラウド接続型
POS システム以外でクレジットカード決済を行う加盟店	IC 対応決済専用端末（CCT）の導入
特定業界の加盟店	ア. 「国内ガソリンスタンドにおけるクレジットカード取引対応指針【附属文書 4】」に基づく実現可能な方策による IC 対応 イ. 「オートローディング式自動精算機の IC 対応指針と自動精算機の本人確認方法について【附属文書 5】」に基づく代替コントロール策による IC 対応

③EC 加盟店における不正利用対策の指針対策

EC 加盟店	
◎オーソリゼーション処理の体制整備 ◎加盟店契約上の善良なる管理者の注意義務の履行 ◎EMV 3-D セキュアの導入 ◎適切な不正ログイン対策の実施	
不正顕在化加盟店	
◎類似の不正利用の発生を防止するために、不正利用の発生状況等に応じて、本ガイドラインが掲げる不正利用対策から適切な対策を追加導入	

④MO・TO 取引取扱加盟店における不正利用対策の指針対策

MO・TO 取引取扱加盟店
◎オーソリゼーション処理の体制整備 ◎加盟店契約上の善良なる管理者の注意義務の履行

5-3 カード会社（アクワイアラー）

5-3-1 対面取引・非対面取引共通

5-3-1-1 カード情報保護対策

①カード会社（アクワイアラー）の指針対策（3号事業者）

【指針対策】

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。

a. PCI DSS 準拠

PCI DSS は、安全なネットワークの構築や、カード会員データの保護等の 12 の要件から構成されているが、各事業者の業態、システム・ネットワーク構成によって要求事項が異なることから、自社が対応すべき事項を検証し、準拠する必要がある。

「PCI DSS v4.0.1 基準書およびサポート文書」（「v4.0」から「v4.0.1」への変更の概要）は、PCI SSC（PCI Security Standards Council）のホームページ

（<https://www.pcisecuritystandards.org/lang/ja-ja/>）からダウンロードできる。

また、国内の PCI DSS 認定セキュリティ評価機関（QSA）のほとんどが参加している団体である、日本カード情報セキュリティ協議会（以下「JCDSC」という。）が、PCI DSS 準拠の取組をサポートするため、各種資料の提供や相談窓口を設置しており活用されたい（JCDSC ホームページ <https://www.jcdsc.org/>）。

②委託先管理

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く、標的型攻撃や既知の脆弱性等により不正侵入を許し、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。

③加盟店におけるカード情報漏えい時の対応

加盟店等からカード情報が漏えいした際は、被害の拡大を防ぐために早急に行動を起こす必要がある。具体的には、日本クレジット協会において策定した「クレジットカード情報漏えい時及び漏えい懸念時の対応要領【関係文書 1】」を有事の際の参考にしつつ、二次被害の防止のために必要な措置を講じる。

また、漏えい事案が発生した加盟店等のカード決済の再開に当たっては、SAQ等の提出内容や再発防止のための措置等の対応状況を十分に確認した上で、判断する必要がある。なお、PCI DSS 準拠等の再発防止のための適切な措置の具体的な内容は、当該加盟店等と協議の上、決定する。

5-3-2 対面取引

5-3-2-1 カード情報保護対策

①加盟店サポート

加盟店の指針対策の実行に向けて、契約のある決済代行業者等と連携し、本ガイドライン記載の対面取引加盟店におけるカード情報保護対策を理解の上、加盟店に対し、必要な助言や情報提供、サポート等を行う。

5-3-2-2 不正利用対策

①決済端末機の IC 対応

契約を有する加盟店の決済専用端末の IC 対応を行う。

②加盟店サポート

加盟店の指針対策の実行に向けて、契約のある決済代行業者等と連携し、本ガイドライン記載の対面取引加盟店における不正利用対策を理解の上、加盟店に対し、必要な助言や情報提供、サポート等を行う。

a. ガイドラインの周知及びベンダーとの連携

加盟店に対し、本ガイドラインで整理された各方策について必要に応じて機器メーカーとも連携して情報を提供する。

また、POS システムの接続インターフェース等の共通化や IC 取引オペレーション等を踏まえ作成した「IC カード対応 POS 導入の手引き ～全体概要編～【附属文書 11】」「IC カード対応 POS ガイドライン（第 I 部 取引処理編）【附属文書 6】」「IC カード対応 POS ガイドライン（第 II 部 接続運用編）【附属文書 7】」「IC カード対応 POS ガイドライン（第 III 部 EMV Kernel 処理編）【附属文書 8】」等について、機器メーカーや加盟店等への周知を行う。

③IC 取引時のオペレーションルール

IC 取引の円滑な運用に資するため、「接触 IC 取引」及び「非接触 IC 取引」の本人確認方法を IC 取引時のオペレーションルールとして取りまとめており、概要は以下のとおり。

詳細は「クレジット取引における本人確認方法に係るガイドライン【附属文書 15】」（以下「本人確認ガイドライン」という。）を、自動精算機については「オートローディング式自動精算機の IC 対応指針と自動精算機の本人確認方法について【附属文書 5】」を参照すること。

a. 接触 IC 取引

接触 IC 取引は、決済端末に IC カードを挿入しカード券面上に露出した IC チップの接触端子からカード情報を読み込んで処理を行うものである。

- ・カード偽造防止のみならず、紛失・盗難カードによる不正利用を防止するため、原則「PIN の入力」による本人確認を行うこととする。
- ・なお、一定条件においては、加盟店は本人確認を不要とすることができる。（※）

b. 非接触 IC 取引

非接触 IC 取引は、決済端末に IC カード等をかざすことにより、カード券面の内部に搭載された IC チップ内のカード情報を読み取り処理を行うものである。

- ・CVM リミット金額超の取引においては、以下のとおりカード会員が提示する媒体に応じて本人確認を行う。

ア) カード型

CVM リミット金額超の取引については、非接触 IC 取引から接触 IC 取引に切り替え、オフライン PIN による本人確認を行う。

イ) モバイル型等

CVM リミット金額超の取引については、Consumer Device CVM（モバイル型等のパスワードや生体認証等の機能）を用いた本人確認とする。

- ・なお、一定条件においては、加盟店は本人確認を不要とすることができる。（※）

（※）本人確認不要取引

本人確認ガイドラインで規定する「本人確認が必要となる業種/売場/商品等」に該当せず、かつ、「本人確認不要取引の CVM リミット金額」の範囲内については、加盟店は本人確認を不要とすることができる。

本人確認不要取引を行うに当たっては、カード会員の保護及び不正利用発生の防止に留意しなければならない。

なお、加盟店が自主的に本人確認を実施することを妨げるものではない。

[IC 取引時のオペレーションルール]

□取引形態別（接触 IC 取引/非接触 IC 取引）の本人確認方法

◆接触 IC 取引

- ・原則、「オフライン PIN」とする。
- ・CVM リミット金額以下の場合は、本人確認を不要とすることができる。

◆非接触 IC 取引

- ・CVM リミット金額以下の場合は、本人確認を不要とすることができる。
- ・「カード型」における CVM リミット金額超過時は「接触 IC 取引」へ切り替える。
- ・「モバイル型等」における CVM リミット金額超過時は Consumer Device CVM（モバイル PIN/生体認証等）とする。

CVM リミット金額	取引形態		
	接触 IC 取引	非接触 IC 取引	
		カード型	モバイル型等
CVM リミット以下	本人確認を「不要」とすることが可能		
CVM リミット超	原則オフライン PIN	[接触 IC 取引へ切替え] 原則オフライン PIN	Consumer Device CVM（モバイル PIN/生体認証等）

なお、オフライン PIN をサポートしていない海外発行カードや接触 IC 取引への切替えを許容しないカード等の取扱いについては、「本人確認ガイドライン」を参照すること。

c. サインの取得による本人確認

対面取引における本人確認方法を、これまで行ってきた「サインの取得」から原則「PIN の入力」に変更することは、紛失・盗難カードの不正利用を防止するために実施するものである。

また、各国際ブランドのルールにおいても、これまで本人確認方法としてきた「サインの取得」は本人確認としての有効性が認められておらず、加盟店の業務上の必要性に応じて実施するもの（任意化）とされている。

これらのことから、2022 年より「カード取引において本人確認としてサインの取得を行わない運用とすることを推奨」し、「2025 年 4 月以降本人確認として PIN の入力が必要になる」旨の周知・啓発活動をクレジット業界全体で実施してきた。

なお、加盟店のオペレーション上必要な場合に「サインの取得」を妨げるものではないが、カード取引における本人確認としての効果は有していないことに留意する。

クレジットカード取引の売上票（カード会社控え等）については、カード取引の本人確認としての「サインの取得」をしない運用にすることにより、加盟店においては紙伝票印刷や保管業務の削減等、運用の合理化を図ることが可能となる。「サインの取得」をしない加盟店のクレジットカード売上票の取扱いに関する運用については、「クレジットカード売上票の作成・保管に関するガイドライン【附属文書 16】」を参照すること。

d. PIN バイパスの廃止

本協議会において、PIN バイパス（PIN 入力スキップ機能）については、以下の事由により廃止とし、2022 年より、2025 年 3 月をもって廃止する方針を本ガイドラインに記載し、クレジット業界全体で周知・啓発活動を行ってきた。

- ・紛失・盗難カードの不正利用を防止するために、「PIN の入力」による本人確認が必要である。
- ・海外発行のカードには本機能を許容しないものも存在し利用阻害が発生している。

具体的な対応として、運用面での停止又は決済端末の当該機能の停止をすることにより、PIN バイパスの運用は廃止するものである。

また、「サインの取得」については、本人確認としての効果を有していないため、PIN 失念への救済措置としてきたカード取引の本人確認としての「サインの取得」による代替（PIN バイパス）は存在意義も失われている。

なお、発行主体者と利用される加盟店が同一グループであるなどにより固有の本人確認が行われている場合においては、「サインの取得」による本人確認や「PIN バイパスの廃止」への対応は、当該発行主体者と加盟店に委ねられていることに留意する。

5-3-2-3 周知・啓発

①決済端末機の IC 対応

a. PIN

i. 認知度向上

加盟店と調整の上、必要に応じて加盟店契約内容の改定やカード利用者の PIN 認知度向上のための周知・啓発への協力を依頼する。

ii. 「サインの取得による本人確認」及び「PIN バイパスの廃止」

対面取引加盟店においては、「5-3-2-2 不正利用対策 ③IC 取引時のオペレーションルール」に記述のとおり、「サインの取得」については、本人確認の効果を有していない。また、PIN バイパスは廃止されているため、加盟店に対して、カード決済時等におけるカード利用者への案内についての協力を要請する。

5-3-3 非対面取引

5-3-3-1 カード情報保護対策

①加盟店サポート

非対面取引加盟店の指針対策の実行に向けて、契約のある PSP 等と連携し、本ガイドライン記載の非対面取引加盟店におけるカード情報保護対策を理解の上、加盟店に対し、必要な助言や情報提供、サポート等を行う。

また、EC 加盟店においては、EC 加盟店のシステムや Web サイトの「脆弱性対策」を「EC 加盟店におけるセキュリティ対策 導入ガイド【附属文書 20】（以下「セキュリティ対策導入ガイド【附属文書 20】」という。）」の第 2 部「1.脆弱性対策」を活用して、カード情報保護対策について必要な助言や情報提供、サポート等を行う。

②脆弱性対策

カード会社（アクワイアラー）や PSP は、これまでは試行として EC 加盟店との新規加盟店契約前に、EC 加盟店自ら EC 加盟店のシステム（※1）や Web サイト（※2）の「脆弱性対策」を実施し、その状況の申告を求めていたが、2025 年 4 月以降は既契約 EC 加盟店も含めて「脆弱性対策」の実施を求める。

このため、「セキュリティ対策導入ガイド【附属文書 20】」の第 2 部「1.脆弱性対策」に記載の対策を実施する必要性の周知も合わせて行う。

なお、「脆弱性対策」については、「クレジットカード決済システムのセキュリティ対策強化検討会報告書」（2023 年 1 月 20 日 経済産業省 https://www.meti.go.jp/shingikai/mono_info_service/credit_card_payment/pdf/20230120_1.pdf）においても、EC 加盟店の漏えい対策の強化のための当面の対応として、EC 加盟店のシステム、EC サイト自体の「脆弱性対策」（システム上の設定の不備への対策（PW 管理等）、脆弱性診断・対策、ウイルス対策等）を講ずることと 2024 年度末までにその旨を本ガイドラインに追記することが求められていた。

（※1）商品・サービス・金額等を掲載している Web サイトのセキュリティ対策を含めた管理権限を有するシステム

（※2）商品・サービス・金額等を掲載し、消費者が閲覧する Web サイト

[導入する「脆弱性対策」] (下記のすべての対策を講じる)

①システム管理画面のアクセス制限と管理者の ID/パスワード管理
システム管理画面のアクセス可能な IP アドレスを制限する。IP アドレスを制限できない場合は管理画面にベーシック認証等のアクセス制限を設ける。
取得されたアカウントを不正使用されないよう 2 段階認証又は多要素認証 (2 要素認証) を採用する。
システム管理画面のログインフォームでは、アカウントロック機能を有効にし、10 回以下(PCI DSS ver4.0.1 基準)のログイン失敗でアカウントをロックする。
②データディレクトリの露見に伴う設定不備への対策
公開ディレクトリには、重要なファイルを配置しない。(特定のディレクトリを非公開にする。公開ディレクトリ以外に重要なファイルを配置する。)
Web サーバーや Web アプリケーションによりアップロード可能な拡張子やファイルを制限する等の設定を行う。
③Web アプリケーションの脆弱性対策
脆弱性診断又はペネトレーションテストを定期的実施し、必要な修正対応を行う。
SQL インジェクションの脆弱性やクロスサイト・スクリプティングの脆弱性対策として、最新のプラグインの使用やソフトウェアのバージョンアップを行う。
Web アプリケーションを開発又はカスタマイズされている場合には、セキュアコーディング済みであるか、ソースコードレビューを行い確認する。その際は、入力フォームの入力値チェックも行う。
④マルウェア対策としてのウイルス対策ソフトの導入、運用
マルウェア検知/除去などの対策としてウイルス対策ソフトを導入して、シグネチャーの更新や定期的なフルスキャンなどを行う。
⑤悪質な有効性確認、クレジットマスターへの対策
悪質な有効性確認、クレジットマスターに対して、「セキュリティ対策導入ガイド【附属文書 20】」別紙 a「1.脆弱性対策」⑤に記載の対策を 1 つ以上実施する。

5-3-3-2 不正利用対策

①加盟店サポート

非対面取引加盟店の不正利用による被害を防止するための具体的な対策には、非対面取引加盟店が取扱商品や不正利用の被害状況等のリスクに応じた適切な対策を導入することが必要である。

このため、本ガイドライン記載の非対面取引加盟店の不正利用対策を十分理解した上で、適切な助言・協力を行うための体制を整備するとともに、非対面取引加盟店が適切な対策を確実に導入するために、PSP と連携し、「EMV 3-D セキュア導入ガイド【附属文書 14】」及び「セキュリティ対策導入ガイド【附属文書 20】」を活用して、助言や情報提供、サポートを行う。

a. EMV 3-D セキュア

i. 導入及び運用サポート

EC 加盟店は、EMV 3-D セキュアを導入した上で、原則としては決済の都度、EMV 3-D セキュアによる認証を行うことが求められるが、加盟店が EMV 3-D セキュア以外に講じる不正利用対策の内容や抑止効果に応じて、カード番号の登録時に EMV 3-D セキュアによる

認証を行う運用や加盟店のリスク判断により EMV 3-D セキュアによる認証を行う運用も認められる。

また、EMV 3-D セキュアの未導入が認められる取引についても別途定めている。

カード会社（アクワイアラー）は、「EMV 3-D セキュア導入ガイド【附属文書 14】」を参照して、PSP と連携し、EC 加盟店が適切に導入及び運用をするためのサポートを行う。

ii. AReq 設定項目の充実

カード会社（イシューア）におけるリスクベース認証の精度向上のため、「EMV 3-D セキュア導入ガイド【附属文書 14】」を参照し、EC 加盟店の取扱商品や不正利用発生状況等の実態を踏まえ、EC 加盟店がカード会社（イシューア）にカード会員のデバイス情報等をより多く提供できるようにするために、提供する情報を適宜見直すなど、データ項目の設定等をサポートする。

iii. システムの安定稼働

EMV 3-D セキュアの安定稼働のための対応に関係事業者と連携し継続的に取り組む。

b. 不正ログイン対策

i. 導入及び運用サポート

EC 加盟店における不正利用の手口としては、「会員登録型」の場合は、窃取した属性情報やカード情報等を利用し、EC 加盟店において不正なアカウントの登録を行う「不正アカウント作成」と、窃取した正規のアカウント等のログイン情報等を使用し、EC 加盟店への不正ログインを行う「アカウント乗っ取り」の大きく二つの手口がある。

EC 加盟店は、不正利用の手口によって導入すべき対策は異なってくることから、その手口による不正利用の発生リスクに応じて、決済前の「会員登録時」「会員ログイン時」「属性情報変更時」のそれぞれの場面を考慮した適切な対策を「セキュリティ対策導入ガイド【附属文書 20】」の第 2 部「3.不正ログイン対策（決済前の対策）」に記載の対策から、1 つ以上導入する必要がある。

このため、カード会社（アクワイアラー）は、EC 加盟店の指針対策である「不正ログイン対策」の導入に当たっては、「セキュリティ対策導入ガイド【附属文書 20】」の第 2 部「3. 不正ログイン対策（決済前の対策）」を活用して、PSP と連携し、サポートを行う。

また、リスト型攻撃（システムを利用し短時間に大量の決済等を行うこと）による不正利用が引き続き発生していることから、短期間に不正利用が急増し不正利用防止の対応が必要である旨の情報連携を行い、速やかに適切な対策を追加導入するためのサポートを行う。

c. 不正顕在化加盟店

カード会社（アクワイアラー）各社が把握する不正利用金額が、「3 ヶ月連続 50 万円超」に該当する加盟店を「不正顕在化加盟店」とする。不正顕在化加盟店は、カード会社（アクワイアラー）や PSP のサポートを受け、類似の不正利用の発生を防止するために、不正利用の被害状況や取扱商品（※）、スキーム等による不正利用の手口に応じ、「適切な対策の追加導入」、若しくは既に導入している対策の設定項目の追加・変更や不正判定レベルのチューニングによる「対策の強化」を行う。

このため、カード会社（アクワイアラー）は PSP と連携し、不正顕在化加盟店が「適切な

対策の追加導入」、若しくは「対策の強化」を行うためのサポートを行う。

この「適切な対策の追加導入」は、属性・行動分析や配送先情報のチェック、配送停止・配送保留等の「セキュリティ対策導入ガイド【附属文書 20】」に記載の不正利用対策から適切な対策を追加導入する。

また、「対策の強化」は、不正顕在化加盟店が、既に導入している EMV 3-D セキュアや属性・行動分析等の対策において、リスク判定や不正判定レベルの分析に基づき、リスク判定項目の追加・変更や不正判定レベルのチューニング等による精度向上を図り、類似の不正利用の発生防止を行うものである。

(※) 日本クレジット協会のインフラ整備部会調査によると、「相対的にリスクが高い商材」は、不正利用の発生リスクが高いことから、追加導入する対策や既に導入している対策の設定項目の追加・変更や不正判定レベルのチューニングにおいては、リスクを認識した上で対応が必要であることに留意する。

詳細は「セキュリティ対策導入ガイド【附属文書 20】」の第 3 部「2-1.相対的にリスクの高い商材の不正利用対策」を参照すること。

①デジタルコンテンツ（オンラインゲームを含む）、②家電、③電子マネー、④チケット、⑤宿泊予約サービス

なお、ここでいう③電子マネーとは、コード決済事業者等のその他決済サービス（プリペイド機能等）にクレジットカードを紐づけ、その決済サービスにチャージすることにより利用可能となるものは除く。

なお、EC 加盟店がこれまでに導入している不正利用対策（セキュリティコードや属性・行動分析、配送停止・配送保留等）についても、リスクに応じて継続することを助言する。

「セキュリティ対策導入ガイド【附属文書 20】」に記載の対策と同等以上の性能を満たしている不正利用対策であれば、その対策を導入することも認められるものとする。ただし、その対策が「セキュリティ対策導入ガイド【附属文書 20】」に記載の対策と同等以上の性能であることの説明を必要に応じて加盟店に求めることとする。

d. 情報提供

i. 情報共有

非対面取引加盟店が自社で不正利用対策として、属性・行動分析を導入している場合には、それを有効に活用するために、多くの不正取引の情報や不審なカード利用の把握及び不正利用の手口等の情報の最新化が必要である。このため、カード会社（イシューア）で確認した不正取引の情報について、できるだけ多くの非対面取引加盟店や PSP 等と迅速な情報共有に努め、非対面取引加盟店における不正利用対策の問題の特定とともにその解決を図る。

ii. 真正利用照会対応

非対面取引加盟店からの真正利用確認照会への対応に取り組む。

②コード決済ガイドライン等の準拠の確認

クレジットカードと連携することにより他の決済手段を提供するコード決済事業者等と包括加盟店契約等を締結する場合には、当該事業者は一般社団法人キャッシュレス推進協議会

が取りまとめた「コード決済における不正流出したクレジットカード番号等の不正利用防止対策に関するガイドライン」や一般社団法人日本資金決済業協会が取りまとめた「銀行口座との連携における不正防止に関するガイドライン」等、関係するガイドラインに準拠するなど、十分な安全対策が講じられていることを確認する。

5-4 決済代行業者等・PSP

5-4-1 対面取引

5-4-1-1 カード情報保護対策

①決済代行業者等の指针对策（4号事業者）

【指针对策】

PCI DSS に準拠し、維持・運用する。

ただし、対面取引を取り扱う事業者であって、カード会員データを自社で保有せず、保存・処理・通過を自社以外の業者で行っており、立替払いのみを行っている事業者については本協議会が定める資料「セキュリティ対策チェック項目」に基づき対策を実施し、これを維持・運用する方策も認められる。

a. PCI DSS 準拠

PCI DSS は、安全なネットワークの構築や、カード会員データの保護等の 12 の要件から構成されているが、各事業者の業態、システム・ネットワーク構成によって要求事項が異なることから、自社が対応すべき事項を検証し、準拠する必要がある。

「PCI DSS v4.0.1 基準書およびサポート文書」（「v4.0」から「v4.0.1」への変更の概要）は、PCI SSC（PCI Security Standards Council）のホームページ

（<https://www.pcisecuritystandards.org/lang/ja-ja/>）からダウンロードできる。

また、国内の PCI DSS 認定セキュリティ評価機関（QSA）のほとんどが参加している団体である、日本カード情報セキュリティ協議会（以下「JCDS」という。）が、PCI DSS 準拠の取組をサポートするため、各種資料の提供や相談窓口を設置しており活用されたい（JCDS ホームページ <https://www.jcdsc.org/>）。

②委託先管理

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く、標的型攻撃や既知の脆弱性等により不正侵入を許し、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。

③加盟店サポート

加盟店の指针对策の実行に向けて、契約のあるカード会社（アクワイアラー）と連携し、本ガイドライン記載の対面取引加盟店におけるカード情報保護対策を理解の上、加盟店に対し、必要な助言、情報提供やサポート等を行う。

④加盟店におけるカード情報漏えい時の対応

加盟店等からカード情報が漏えいした際は、被害の拡大を防ぐために早急に行動を起こす必要がある。具体的には、日本クレジット協会において策定した「クレジットカード情報漏

えい時及び漏えい懸念時の対応要領【関係文書 1】」を有事の際の参考にしつつ、二次被害の防止のために必要な措置を講じる。

また、カード情報が漏えいした際は、速やかに契約するカード会社（アクワイアラー）に連絡するとともに、契約するカード会社（アクワイアラー）の要請にしたがって、被害の拡大を防止するための初動対応として、漏えい元（データベース等）のネットワークからの切り離し、カード決済の一時停止等の措置、フォレンジック調査、PCI DSS 準拠等の確認及び再発防止のための適切な措置を講じる。

なお、漏えい事案が発生した加盟店等のカード決済の再開に当たっては、SAQ 等の提出内容や再発防止のための措置等の対応状況を十分に確認した上で、判断する必要がある。なお、PCI DSS 準拠等の再発防止のための適切な措置の具体的な内容は、当該加盟店等と契約するカード会社（アクワイアラー）等で協議の上、決定する。

5-4-1-2 不正利用対策

①決済端末機の IC 対応

契約を有する加盟店の決済専用端末の IC 対応を行う。

5-4-1-3 周知・啓発

①決済端末機の IC 対応

a. PIN

i. 認知度向上

加盟店と調整の上、必要に応じて加盟店契約内容の改定やカード利用者の PIN 認知度向上のための周知・啓発への協力を依頼する。

ii. 「サインの取得による本人確認」及び「PIN バイパスの廃止」

対面取引加盟店においては、「5-3-2-2 不正利用対策 ③IC 取引時のオペレーションルール」に記述のとおり、「サインの取得」については、本人確認の効果を有していない。また、PIN バイパスは廃止されているため、加盟店に対して、カード決済時等におけるカード利用者への案内について協力を要請する。

5-4-2 非対面取引

5-4-2-1 カード情報保護対策

①決済代行業者等の指针对策（4号事業者）

【指针对策】

PCI DSS に準拠し、維持・運用する。

a. PCI DSS 準拠

PCI DSS は、安全なネットワークの構築や、カード会員データの保護等の 12 の要件から構成されているが、各事業者の業態、システム・ネットワーク構成によって要求事項が異なることから、自社が対応すべき事項を検証し、準拠する必要がある。

「PCI DSS v4.0.1 基準書およびサポート文書」（「v4.0」から「v4.0.1」への変更の概要）は、PCI SSC（PCI Security Standards Council）のホームページ

（<https://www.pcisecuritystandards.org/lang/ja-ja/>）からダウンロードできる。

また、国内の PCI DSS 認定セキュリティ評価機関（QSA）のほとんどが参加している団体である、日本カード情報セキュリティ協議会（以下「JCDS」という。）が、PCI DSS 準拠の取組をサポートするため、各種資料の提供や相談窓口を設置しており活用されたい（JCDS ホームページ <https://www.jcdsc.org/>）。

②委託先管理

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事業者及び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、カード情報が漏えいした場合の影響が大きく、標的型攻撃や既知の脆弱性等により不正侵入を許し、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。

③加盟店サポート

非対面取引加盟店による指針対策の実施に向けて、カード会社（アクワイアラー）と連携し、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、情報提供やサポート等を行う。

さらに、EC 加盟店においては、EC 加盟店のシステムや Web サイトの「脆弱性対策」を「EC 加盟店におけるセキュリティ対策 導入ガイド【附属文書 20】（以下「セキュリティ対策導入ガイド【附属文書 20】）」という。）の第 2 部「1.脆弱性対策」を活用して、カード情報保護対策について必要な助言や情報提供、サポート等を行う。

④脆弱性対策

カード会社（アクワイアラー）や PSP は、これまでは試行として EC 加盟店との新規加盟店契約前に、EC 加盟店自ら EC 加盟店のシステム（※1）や Web サイト（※2）の「脆弱性対策」を実施し、その状況の申告を求めていたが、2025 年 4 月以降は既契約 EC 加盟店も含めて「脆弱性対策」の実施を求める。

このため、「セキュリティ対策導入ガイド【附属文書 20】」の第 2 部「1.脆弱性対策」に記載の対策を実施する必要性の周知も合わせて行う。

なお、「脆弱性対策」については、「クレジットカード決済システムのセキュリティ対策強化検討会報告書」（2023 年 1 月 20 日 経済産業省 https://www.meti.go.jp/shingikai/mono_info_service/credit_card_payment/pdf/20230120_1.pdf）において、EC 加盟店の漏えい対策の強化のための当面の対応として、EC 加盟店のシステム、EC サイト自体の「脆弱性対策」（システム上の設定の不備への対策（PW 管理等）、脆弱性診断・対策、ウイルス対策等）を講ずることと 2024 年度末までにその旨を本ガイドラインに追記することが求められていた。

（※1）商品・サービス・金額等を掲載している Web サイトのセキュリティ対策を含めた管理権限を有するシステム

（※2）商品・サービス・金額等を掲載し、消費者が閲覧する Web サイト

[導入する「脆弱性対策」] (下記のすべての対策を講じる)

①システム管理画面のアクセス制限と管理者の ID/パスワード管理
システム管理画面のアクセス可能な IP アドレスを制限する。IP アドレスを制限できない場合は管理画面にベーシック認証等のアクセス制限を設ける。
取得されたアカウントを不正使用されないよう 2 段階認証又は多要素認証 (2 要素認証) を採用する。
システム管理画面のログインフォームでは、アカウントロック機能を有効にし、10 回以下(PCI DSS ver4.0.1 基準)のログイン失敗でアカウントをロックする。
②データディレクトリの露見に伴う設定不備への対策
公開ディレクトリには、重要なファイルを配置しない。(特定のディレクトリを非公開にする。公開ディレクトリ以外に重要なファイルを配置する。)
Web サーバーや Web アプリケーションによりアップロード可能な拡張子やファイルを制限する等の設定を行う。
③Web アプリケーションの脆弱性対策
脆弱性診断又はペネトレーションテストを定期的実施し、必要な修正対応を行う。
SQL インジェクションの脆弱性やクロスサイト・スクリプティングの脆弱性対策として、最新のプラグインの使用やソフトウェアのバージョンアップを行う。
Web アプリケーションを開発又はカスタマイズされている場合には、セキュアコーディング済みであるか、ソースコードレビューを行い確認する。その際は、入力フォームの入力値チェックも行う。
④マルウェア対策としてのウイルス対策ソフトの導入、運用
マルウェア検知/除去などの対策としてウイルス対策ソフトを導入して、シグネチャーの更新や定期的なフルスキャンなどを行う。
⑤悪質な有効性確認、クレジットマスターへの対策
悪質な有効性確認、クレジットマスターに対して、「セキュリティ対策導入ガイド【附属文書 20】」別紙 a「1.脆弱性対策」⑤に記載の対策を 1 つ以上実施する。

⑤加盟店におけるカード情報漏えい時の対応

加盟店等からカード情報が漏えいした際は、被害の拡大を防ぐために早急に行動を起こす必要がある。具体的には、日本クレジット協会において策定した「クレジットカード情報漏えい時及び漏えい懸念時の対応要領【関係文書 1】」を有事の際の参考にしつつ、二次被害の防止のために必要な措置を講じる。

また、カード情報が漏えいした際は、速やかに契約するカード会社 (アクワイアラー) に連絡するとともに、契約するカード会社 (アクワイアラー) の要請にしたがって、被害の拡大を防止するための初動対応として、漏えい元 (データベース等) のネットワークからの切り離し、カード決済の一時停止等の措置、フォレンジック調査、PCI DSS 準拠等の確認及び再発防止のための適切な措置を講じる。

なお、漏えい事案が発生した加盟店等のカード決済の再開に当たっては、SAQ 等の提出内容や再発防止のための措置等の対応状況を十分に確認した上で、判断する必要がある。なお、PCI DSS 準拠等の再発防止のための適切な措置の具体的な内容は、当該加盟店等と契約するカード会社 (アクワイアラー) 等で協議の上、決定する。

5-4-2-2 不正利用対策

①加盟店サポート

非対面取引加盟店の不正利用による被害を防止するための具体的な対策には、非対面取引加盟店が取扱商品や不正利用の被害状況等のリスクに応じた適切な対策を導入することが必要である。

このため、本ガイドライン記載の非対面取引加盟店の不正利用対策を十分理解した上で、適切な助言・協力を行うための体制を整備するとともに、非対面取引加盟店が適切な対策を確実に導入するために、カード会社（アクワイアラー）と連携し、「EMV 3-D セキュア導入ガイド【附属文書 14】」及び「セキュリティ対策導入ガイド【附属文書 20】」を活用して、助言や情報提供、サポートを行う。

a. EMV 3-D セキュア

i. 導入及び運用サポート

EC 加盟店は、EMV 3-D セキュアを導入した上で、原則としては決済の都度、EMV 3-D セキュアによる認証を行うことが求められるが、加盟店が EMV 3-D セキュア以外に講じる不正利用対策の内容や抑止効果に応じて、カード番号の登録時に EMV 3-D セキュアによる認証を行う運用や加盟店のリスク判断により EMV 3-D セキュアによる認証を行う運用も認められる。また、EMV 3-D セキュアの未導入が認められる取引についても別途定めている。

PSP は、「EMV 3-D セキュア導入ガイド【附属文書 14】」を参照して、カード会社（アクワイアラー）と連携し、EC 加盟店が適切に導入及び運用するためのサポートを行う。

ii. AReq 設定項目の充実

カード会社（イシューアー）におけるリスクベース認証の精度向上のため、「EMV 3-D セキュア導入ガイド【附属文書 14】」を参照し、EC 加盟店の取扱商品や不正利用発生状況等の実態を踏まえ、EC 加盟店がカード会社（イシューアー）にカード会員のデバイス情報等をより多く提供できるようにするために、提供する情報を適宜見直すなど、データ項目の設定等をサポートする。

iii. システムの安定稼働

EMV 3-D セキュアの安定稼働のための対応に継続的に取り組む。

b. 不正ログイン対策

i. 導入及び運用サポート

EC 加盟店における不正利用の手口としては、「会員登録型」の場合は、窃取した属性情報やカード情報等を利用し、EC 加盟店において不正なアカウントの登録を行う「不正アカウント作成」と、窃取した正規のアカウント等のログイン情報等を使用し、EC 加盟店への不正ログインを行う「アカウント乗っ取り」の大きく二つの手口がある。

EC 加盟店は、不正利用の手口によって導入すべき対策は異なってくることから、その手口による不正利用発生リスクに応じて、決済前の「会員登録時」「会員ログイン時」「属性情報変更時」のそれぞれの場面を考慮した適切な対策を「セキュリティ対策導入ガイド【附属文書 20】」の第 2 部「3.不正ログイン対策（決済前の対策）」に記載の対策から、1 つ以上導入する必要がある。

このため、PSPは、EC加盟店の指針対策である「不正ログイン対策」の導入に当たっては、「セキュリティ対策導入ガイド【附属文書20】」の第2部「3.不正ログイン対策（決済前の対策）」を活用して、カード会社（アクワイアラー）と連携し、サポートを行う。

また、リスト型攻撃（システムを利用し短時間に大量の決済等を行うこと）による不正利用が引き続き発生していることから、短期間に不正利用が急増し不正利用防止の対応が必要である旨の情報連携を行い、速やかに適切な対策を追加導入するためのサポートを行う。

c. 不正顕在化加盟店

カード会社（アクワイアラー）各社が把握する不正利用金額が、「3ヵ月連続50万円超」に該当する加盟店を「不正顕在化加盟店」とする。不正顕在化加盟店は、カード会社（アクワイアラー）やPSPのサポートを受け、類似の不正利用の発生を防止するために、不正利用の被害状況や取扱商品（※）、スキーム等による不正利用の手口に応じ、「適切な対策の追加導入」、若しくは既に導入している対策の設定項目の追加・変更や不正判定レベルのチューニングによる「対策の強化」を行うこととしている。

このため、PSPはカード会社（アクワイアラー）と連携し、不正顕在化加盟店が「適切な対策の追加導入」、若しくは「対策の強化」を行うためのサポートを行う。

この「適切な対策の追加導入」は、属性・行動分析や配送先情報のチェック、配送停止・配送保留等の「セキュリティ対策導入ガイド【附属文書20】」に記載の不正利用対策から適切な対策を追加導入する。

また、「対策の強化」は、不正顕在化加盟店が、既に導入しているEMV 3-Dセキュアや属性・行動分析等の有効な対策において、リスク判定や不正判定レベルの分析に基づき、リスク判定項目の追加・変更や不正判定レベルのチューニング等による精度向上を図り、類似の不正利用の発生防止を行うものである。

（※）日本クレジット協会のインフラ整備部会調査によると、「相対的にリスクが高い商材」は、不正利用の発生リスクが高いことから、追加導入する対策や既に導入している対策の設定項目の追加・変更や不正判定レベルのチューニングにおいては、リスクを認識した上で対応が必要であることに留意する。

詳細は「セキュリティ対策導入ガイド【附属文書20】」の第3部「2-1.相対的にリスクの高い商材の不正利用対策」を参照すること。

①デジタルコンテンツ（オンラインゲームを含む）、②家電、③電子マネー、④チケット、⑤宿泊予約サービス

なお、ここでいう③電子マネーとは、コード決済事業者等のその他決済サービス（プリペイド機能等）にクレジットカードを紐づけ、その決済サービスにチャージすることにより利用可能となるものは除く。

なお、EC加盟店がこれまでに導入している不正利用対策（セキュリティコードや属性・行動分析、配送停止・配送保留等）についても、リスクに応じて継続することを助言する。

「セキュリティ対策導入ガイド【附属文書20】」に記載の対策と同等以上の性能を満たしている不正利用対策であれば、その対策を導入することも認められるものとする。ただし、その対策が「セキュリティ対策導入ガイド【附属文書20】」記載の対策と同等以上の

性能であることの説明を必要に応じて加盟店に求めることとする。

d. 情報提供

i. 情報共有

非対面取引加盟店が自社で不正利用対策として、属性・行動分析を導入している場合においては、それを有効に活用するために、多くの不正取引の情報や不審なカード利用の把握及び不正利用の手口等の情報の最新化が必要である。このため、カード会社（イシューア）で確認した不正取引の情報について、できるだけ多くの非対面取引加盟店やカード会社（アクワイアラー）等と迅速な情報共有に努め、非対面取引加盟店における不正利用対策の問題の特定とともにその解決を図る。

ii. 真正利用照会対応

非対面取引加盟店からの真正利用確認照会への対応に取り組む。

e. 不正利用対策提供のための体制整備

本ガイドラインに掲げる不正利用対策を提供できる体制を構築し、契約先の非対面取引加盟店における導入の推進に努める。

5-5 コード決済事業者等

5-5-1 対面取引・非対面取引共通

5-5-1-1 カード情報保護対策

①コード決済事業者等の指针对策（5号事業者）

【指针对策】

PCI DSS に準拠し、これを維持・運用する。

a. PCI DSS 準拠

PCI DSS は、安全なネットワークの構築や、カード会員データの保護等の 12 の要件から構成されているが、各事業者の業態、システム・ネットワーク構成によって要求事項が異なることから、自社が対応すべき事項を検証し、準拠する必要がある。

「PCI DSS v4.0.1 基準書およびサポート文書」（「v4.0」から「v4.0.1」への変更の概要）は、PCI SSC（PCI Security Standards Council）のホームページ

（<https://www.pcisecuritystandards.org/lang/ja-ja/>）からダウンロードできる。

また、国内の PCI DSS 認定セキュリティ評価機関（QSA）のほとんどが参加している団体である、日本カード情報セキュリティ協議会（以下「JCDS」という。）が、PCI DSS 準拠の取組をサポートするため、各種資料の提供や相談窓口を設置しており活用されたい（JCDS ホームページ <https://www.jcdsc.org/>）。

②コード決済ガイドライン等の遵守

カード会社（アクワイアラー）には、以下の対策が求められていることに留意する。

「カード会社（アクワイアラー）は、クレジットカードと連携することにより他の決済手段を提供するコード決済事業者等と包括加盟店契約等を締結する場合には、当該事業者は一般社団法人キャッシュレス推進協議会が取りまとめた『コード決済におけ

る不正流出したクレジットカード番号等の不正利用防止対策に関するガイドライン』や一般社団法人日本資金決済業協会が取りまとめた『銀行口座との連携における不正防止に関するガイドライン』等、関係するガイドラインに準拠するなど、十分な安全対策が講じられていることを確認する必要がある。」

③委託先管理

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く、標的型攻撃や既知の脆弱性等により不正侵入を許し、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。

5-6 コード決済事業者等の委託先及び EC システム提供会社等

5-6-1 対面取引・非対面取引共通

5-6-1-1 カード情報保護対策

①コード決済事業者等の委託先及び EC システム提供会社等の指针对策（6号事業者及び7号事業者）

【指针对策】

PCI DSS に準拠し、これを維持・運用する。

a. PCI DSS 準拠

PCI DSS は、安全なネットワークの構築や、カード会員データの保護等の 12 の要件から構成されているが、各事業者の業態、システム・ネットワーク構成に応じ要求事項が異なることから、自社が対応すべき事項を検証し、準拠する必要がある。

「PCI DSS v4.0.1 基準書およびサポート文書」（「v4.0」から「v4.0.1」への変更の概要）は、PCI SSC（PCI Security Standards Council）のホームページ

（<https://www.pcisecuritystandards.org/lang/ja-ja/>）からダウンロードできる。

また、国内の PCI DSS 認定セキュリティ評価機関（QSA）のほとんどが参加している団体である、日本カード情報セキュリティ協議会（以下「JCDSC」という。）が、PCI DSS 準拠の取組をサポートするため、各種資料の提供や相談窓口を設置しており活用されたい（JCDSC ホームページ <https://www.jcdsc.org/>）。

②委託先管理

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く、標的型攻撃や既知の脆弱性等により不正侵入を許し、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。

5-6-1-2 カード情報保護対策・不正利用対策共通（EC システム提供会社のみ）

①加盟店へのシステム等の提供及びサポート

EC 加盟店におけるカード情報保護対策及び不正利用対策の各指針対策を理解した上で、EC 加盟店に対して「対策が具備された EC システムの構築やソリューションの提供」とその維持・管理等を行うとともに、対策に必要な助言や情報提供等を行う。

5-7 その他の関係事業者等の具体的な対策

5-7-1 国際ブランド

①各事業者へのサポート

以下のサポートを行う。

- ・本ガイドラインに掲げるカード情報保護対策の実現に向け、国際ブランドの各種ルール等との調整を行い、各種課題の解決に向けて関係事業者と協働して取り組む。
- ・IC 取引時のオペレーションについて、我が国のクレジットカード業界として制定したルールを推進することに協働して取り組む。また、技術の向上や環境の変化等により新たな措置等が必要になった場合は、カード会社（イシューア・アクワイアラー）と調整を行う。
- ・我が国における非対面取引加盟店でのクレジットカード取引実態を踏まえ、各種課題の解決に向けて関係事業者と協働して取り組む。
- ・グローバルな観点から、海外におけるカード情報保護に関する最新の情報提供に努め、我が国における国際水準のセキュリティ環境の整備について、関係事業者に対し積極的に働きかける。

②周知・啓発

以下の周知・啓発を行う。

- ・グローバルな観点から、海外におけるカード情報保護に関するリスクや各種課題、我が国における国際水準のセキュリティ環境の整備の必要性等について、事業者向けの情報共有・発信に取り組むとともに、海外におけるカード情報保護に関する最新の情報提供に努める。
- ・EMV 3-D セキュアに係るステークホルダーへの影響（運用ルール等）及び EMV 3-D セキュアの導入について、情報提供及び説明を行うとともに EMV 3-D セキュアの安定稼働のための対応を継続的に取り組む。
- ・非対面取引加盟店における不正利用対策の取組を推進するため、海外のカード会社や EC 加盟店における取組事例について情報提供を行うとともに、我が国における国際水準のセキュリティ環境の整備の必要性等について、事業者向けの情報発信に取り組む。

5-7-2 ソリューションベンダー

①加盟店へのシステム等の提供及びサポート

以下のサポート等を行う。

- ・加盟店におけるカード情報保護対策及び不正利用対策の各指針対策を理解した上で、加盟店に対して「対策が具備されたソリューションや決済端末及びシステム構築等のサービス」の提供とその維持・管理等を行うとともに、対策に必要な助言や情報提供等を行う。

5-7-3 機器メーカー

①加盟店へのシステム等の提供及びサポート

以下のサポート等を行う。

- ・加盟店におけるカード情報保護対策及び不正利用対策の各指針対策を理解した上で、加盟店に対して「対策が具備された決済端末や POS システムの構築等のサービス」の提供とその維持・管理等を行うとともに、対策に必要な助言や情報提供等を行う。

②各事業者へのサポート

以下のサポートを行う。

- ・POS システムの接続インターフェース等の共通化や国際ブランドテストの簡略化等を活用し、加盟店における IC 対応 POS システム導入時のコスト低減化に資する技術的解決策の実現に取り組む。
- ・POS システムの IC 対応に当たっては、「IC カード対応 POS 導入の手引き ～全体概要編～【附属文書 11】」「IC カード対応 POS ガイドライン（第 I 部 取引処理編）【附属文書 6】」「IC カード対応 POS ガイドライン（第 II 部 接続運用編）【附属文書 7】」「IC カード対応 POS ガイドライン（第 III 部 EMV Kernel 処理編）【附属文書 8】」等が取りまとめられていることから、これらの各附属文書に留意し、IC 取引実現のための必要な対応を行う。

③周知・啓発

以下の周知・啓発を行う。

- ・加盟店における IC 対応に関し、本ガイドラインで整理された対策についてカード会社（アクワイアラー）とも連携し、加盟店へ必要な情報を提供する。

5-7-4 行政

①各事業者へのサポート

以下のサポートを行う。

- ・関係事業者のセキュリティ対策の実施状況、カード情報の漏えい及び不正利用の被害状況等を把握するとともに、本協議会におけるセキュリティ対策の検討に必要な情報提供、助言を行う。
- ・割賦販売法に基づく監督等を通じ、カード会社及び加盟店等におけるカード情報の適切な管理、対面取引加盟店における紛失・盗難カード等による不正利用防止、非対面取引加盟店における「なりすまし」等による不正利用防止のために必要な措置の適確な実施について指導等を行う。

②周知・啓発

以下の周知・啓発を行う。

- ・本ガイドラインに掲げるカード情報保護対策及び非対面不正利用対策の実施について、事業者向けや消費者向けの情報発信に取り組む。
- ・消費者に対し EMV 3-D セキュア利用の必要性や動的（ワンタイム）パスワード等の認証方法による安全性の確保等についての周知・啓発に取り組む。また、フィッシング対策として、カード会社等がカード情報等の入力を求めるメールや SMS を送ることはないこ

と、不審なメールや SMS のリンク先にカード情報等を送信しないこと、不正利用被害の自衛として利用履歴や利用明細を確認することなどについて周知・啓発を行う。

5-7-5 業界団体

①各事業者へのサポート

以下のサポートを行う。

- ・加盟店におけるセキュリティ対策については、多額の投資や業務の変更等を要することもあり、適切な情報の収集と分析等が必要となるが、個社の取組のみでは限界もある。こうした事情を踏まえ、本ガイドラインの内容を広く周知するとともに、セキュリティ対策について必要な助言や情報提供を行い、その取組を支援する。
- ・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、「重要インフラのサイバーセキュリティに係る行動計画」（2022年6月17日策定・2024年3月8日改定 https://www.nisc.go.jp/pdf/policy/infra/cip_policy_2024.pdf）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。
- ・最新の不正利用発生状況を踏まえた「不正顕在化加盟店」の基準や「相対的にリスクの高い商材」の継続的な検討、不正利用被害が継続的に発生する EC 加盟店の不正利用の発生状況の分析・評価、加盟店が取り扱う商材に応じた各対策の有効性の検証等を継続して行う。

②周知・啓発

以下の周知・啓発を行う。

- ・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及び不正利用対策の必要性や各対策の有効性等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、消費者団体及び関係団体（一般社団法人キャッシュレス推進協議会、EC 決済協議会、一般社団法人 Fintech 協会）等との連携を強化し、事業者向けの情報発信に取り組む。
- ・不正利用による被害の実態や最新の犯罪手口、不正利用対策に対する取組の成功事例等について、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宜情報発信を行う。
- ・カード会員が利用覚えのない取引を発見し、カード会社（イシューア）に連絡することで、不正利用を認知し、より早くカードの無効手配・処理を行うことにより不正利用被害を防止するために、利用明細を確認することの重要性について周知・啓発に取り組む。
- ・引き続き IC 取引では本人確認のため「PIN の入力」が必要になることの周知・啓発に取り組む。
- ・カード会社（イシューア）や行政等と連携し、カード会員に対し EMV 3-D セキュア利用の必要性や動的（ワンタイム）パスワード等の認証方法による安全性の確保等についての周知・啓発に取り組む。
- ・カード会社（イシューア）や行政、フィッシング対策協議会等の関係団体等と連携し、カード会員がフィッシングによる不正利用被害に遭わないために、フィッシングの手口や不

審と思われるサイトにはカード情報等の入力を行わないなどの注意事項等について周知・啓発に取り組む。

- ・引き続きカード会社（イシューアー）と連携し、ECサイト利用者のログインID・パスワードの使い回しの危険性等について周知・啓発に取り組む。
- ・カード会社（イシューアー・アクワイアラー）と連携し、「本人確認としてのサイン取得」及び「PINバイパスの廃止」については、引き続き周知・啓発に取り組む。

第6章 その他関係事項

6-1 消費者及び事業者等への周知・啓発

クレジットカード取引のセキュリティ対策に関する消費者及び事業者への周知・啓発については、カード会社（イシューア・アクワイアラー）、PSP、加盟店、国際ブランド、業界団体等の各関係事業者は、それぞれの立場で様々な機会を捉えて積極的かつ継続的に行うことが必要である。

6-1-1 消費者及び事業者等への周知・啓発

消費者への周知・啓発では、クレジットカード取引のセキュリティ対策を強化することが、消費者の安全・安心な消費生活による快適な環境づくりに資するものとなることから、消費者のクレジットカード取引におけるセキュリティ対策への理解と協力が得られるよう取り組むことが重要である。

これまで取り組んできた消費者への周知・啓発に加え、新たな決済ルールや仕組みに応じた取引ルールの見直しと、それに伴う消費者への周知・啓発という新たな決済ルール等への円滑な移行への取組も重要である。

特に、フィッシング等を起因とするカード会員からのカード情報窃取等による不正利用被害も増加しており、カード会社をはじめとする関係事業者においてはDMARCその他のフィッシング対策を講じているものの、事業者における対策だけでは限界もあることから、消費者であるカード会員自らがフィッシングの被害に遭わないための取組が強く求められるところである。

6-1-2 事業者等への周知・啓発

クレジットカード取引における不正を企図する攻撃者の手口は日々巧妙化していくため、関係事業者は最新の手口やセキュリティ技術等に関する情報を常に収集することが求められる。

また、行政及び日本クレジット協会は、関係事業者に対して、本ガイドラインの内容を広く周知し、セキュリティ対策について必要な助言や情報提供を行うなどにより、関係事業者の取組を支援することが必要である。

【履歴】

2020年3月19日	新規制定	1.0版
2021年3月10日	改訂	2.0版
2022年3月8日	改訂	3.0版
2023年3月14日	改訂	4.0版
2024年3月14日	改訂	5.0版
2025年3月4日	改訂	6.0版