資料６

# クレジットの安全・安心な利用に関する周知・犯罪の抑止等

## （公表版）

令和４年11月15日

経済産業省　商務・サービスグループ

商取引監督課

# 目次

# クレジットカード番号セキュリティ対策の３つの方向性

クレジットカード加盟店会社等　利用者　PSP等

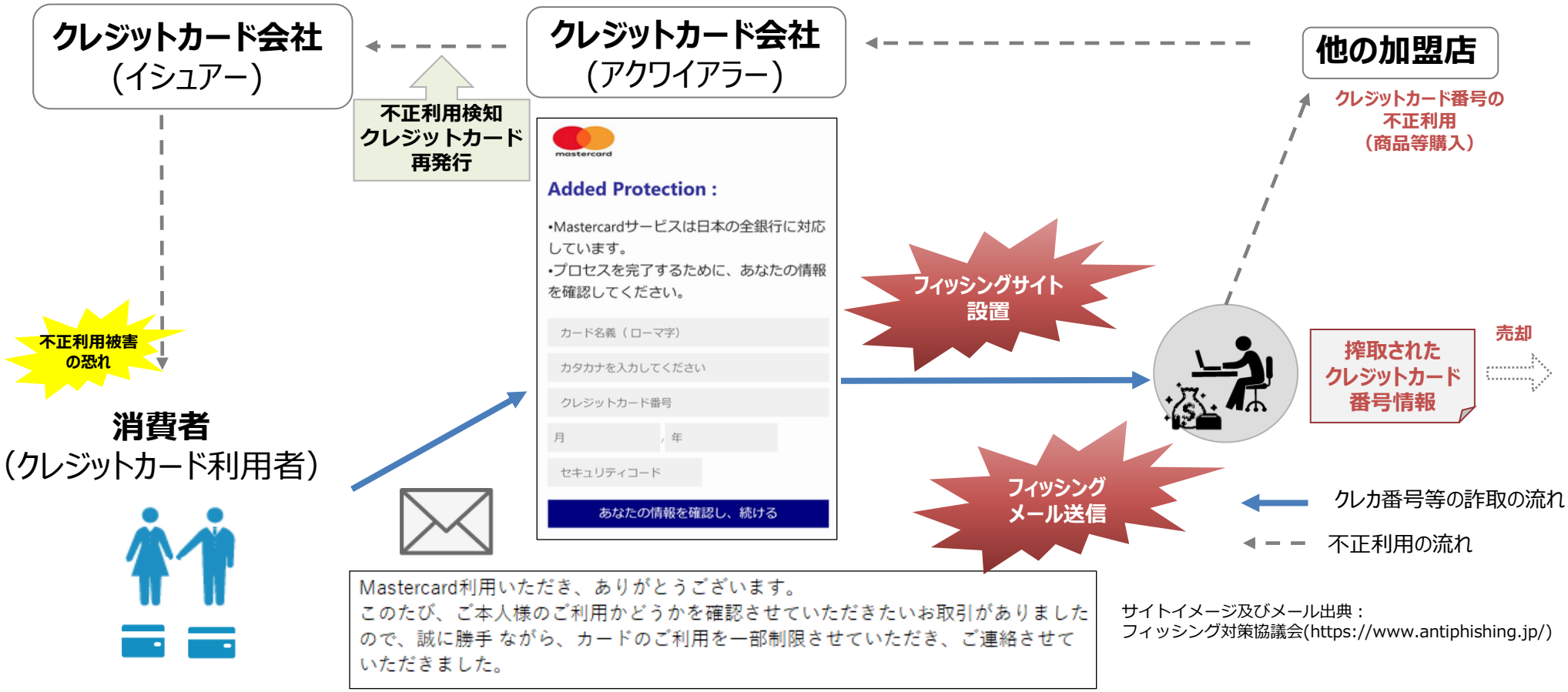
| 目的意識 | これまでの取組 | 今後の方向性 |
|---|---|---|
| **クレジットカード番号を安全に管理する（漏えい防止）** | | |
| ▌クレジット決済に関与するプレイヤーは、クレジットカード番号を取り扱う上でシステム等の安全性を確保する | ✓ 割賦販売法に基づく対応<br>（クレジットカード番号等の適切管理規定）<br>－ PCI DSS準拠相当<br>－ 非保持化 | ✓ さらなる制度的措置の検討<br>－クレジットカード・セキュリティガイドラインでのアップデート<br>✓ 加盟店やPSP等のECサイト、システムの脆弱性対策の強化 |
| **クレジットカード番号を不正利用させない（不正利用防止）** | | |
| ▌決済を承認する際には本人認証を行い、なりすましをさせない | ✓ 割賦販売法に基づく対応<br>－ 対面取引におけるIC決済の推進<br>－ 非対面取引における本人認証の導入<br>（セキュリティコード・静的パスワード等における認証） | ✓ 特に非対面取引における本人認証の原則化<br>✓ 本人認証方法の高度化<br>生体認証・ワンタイムパスワード等といった強力な本人認証方法を推進<br>⇒EMV-3Dセキュアの普及 |
| ▌決済取引をモニタリングし、不正利用を検知する | ✓ クレジットカード会社等における個社での不正検知の取組<br>✓ 明細、利用履歴の確認（クレジットカード会社等における明細通知・利用者における確認） | ✓ 共同システムの構築・新しい技術や方法に基づく不正利用検知のイノベーション<br>✓ 明細による確認強化（リアルタイム通知等、利用者へのアラート機能の充実） |
| **クレジットの安全・安心な利用に関する周知・犯罪の抑止** | | |
| ▌利用者は、悪意を持った第三者からのフィッシング被害に遭わないよう対策を行う | ✓ フィッシング対策協議会や日本クレジット協会等における周知啓発 | ✓ フィッシング対策に向けた多層的な取組（送信ドメイン認証（DMARC）等）<br>✓ 周知啓発の強化<br>✓ 事業者と行政機関等における連携強化 |
| ▌漏えい防止・不正利用防止で行き届かない部分については、執行で対応 | ✓ 割賦販売法第49条の２（クレジットカード番号等の不正利用・取得）／不正アクセス禁止法等に基づく執行対応 | ✓ 経済産業省と警察庁（サイバー警察局等）との連携強化 |

（資料）クレジットカードシステムのセキュリティ対策の更なる強化に向けた方向性（クレジット・セキュリティ対策ビジョン2025）（第30回産構審割販小委（令和４年６月）

# １－１．クレジットの安全・安心な利用に関する犯罪の抑止（フィッシング対策）

# 漏えい事案：消費者（フィッシング被害）

- サイバー攻撃によるクレジットカード番号盗用以外にも、**消費者自身が偽サイトにクレジットカード番号やID・パスワード等を入力する**フィッシングによるクレジットカード番号等の漏えい事案も存在。

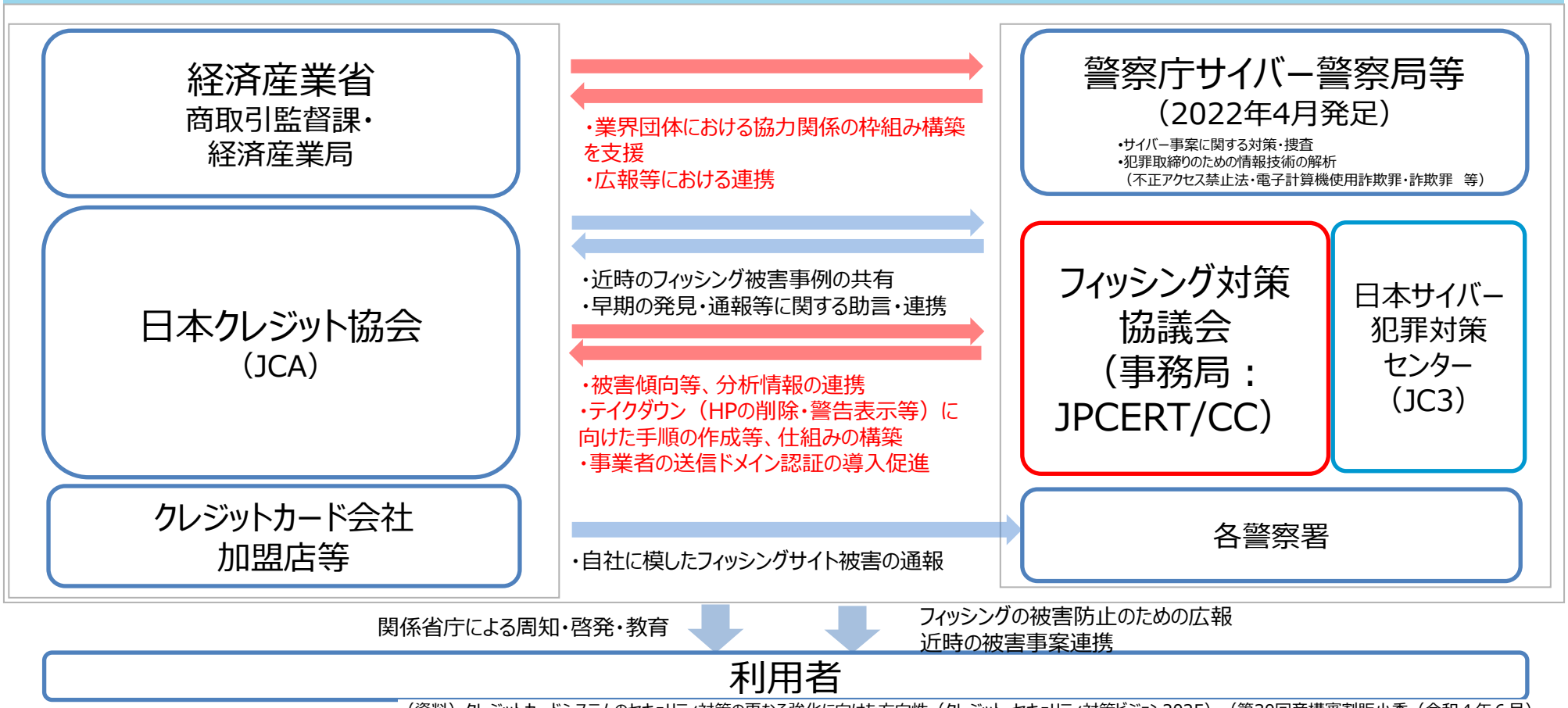



サイトイメージ及びメール出典：
フィッシング対策協議会(https://www.antiphishing.jp/)

# 関係行政機関・団体との連携強化（フィッシング対策関係）

赤枠・・・取組を強化している主体
赤矢印・赤字・・・新たな取組案
青矢印・黒字・・・これまでの取組

- 従来より、クレジットカード会社等はフィッシングサイトを作成されるなどの被害を認識すると、関係行政機関・団体への報告・相談を行うとともに、所管の警察署にも通報を行ってきた。
- 一方、昨今のEC決済の伸長に伴い、フィッシング報告件数・それに伴う被害が急増。
- 今後は、より効果的な情報連携のため関係省庁間・業界団体間での連携強化のほか、事業者自身の送信ドメイン認証（DMARC）促進等や消費者啓発・広報を行っていくことも考えられる。



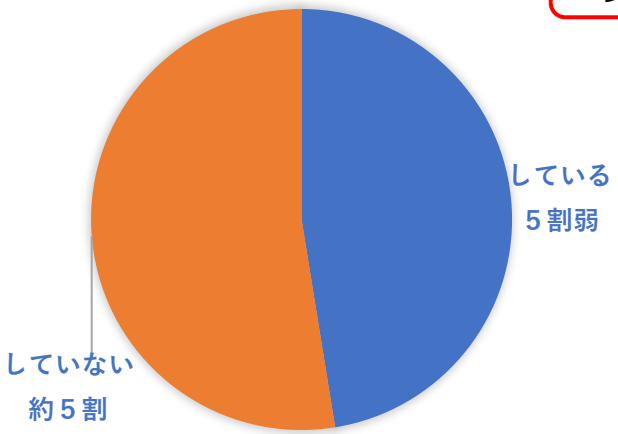

（資料）クレジットカードシステムのセキュリティ対策の更なる強化に向けた方向性（クレジット・セキュリティ対策ビジョン2025）（第30回産構審割販小委（令和４年６月）

# 消費者のフィッシング対策への取組の現状

- フィッシング被害に遭わないように意識・対策している消費者はまだ半数弱。
- うち、実効的な対策を実施できている消費者は一定程度に留まる。

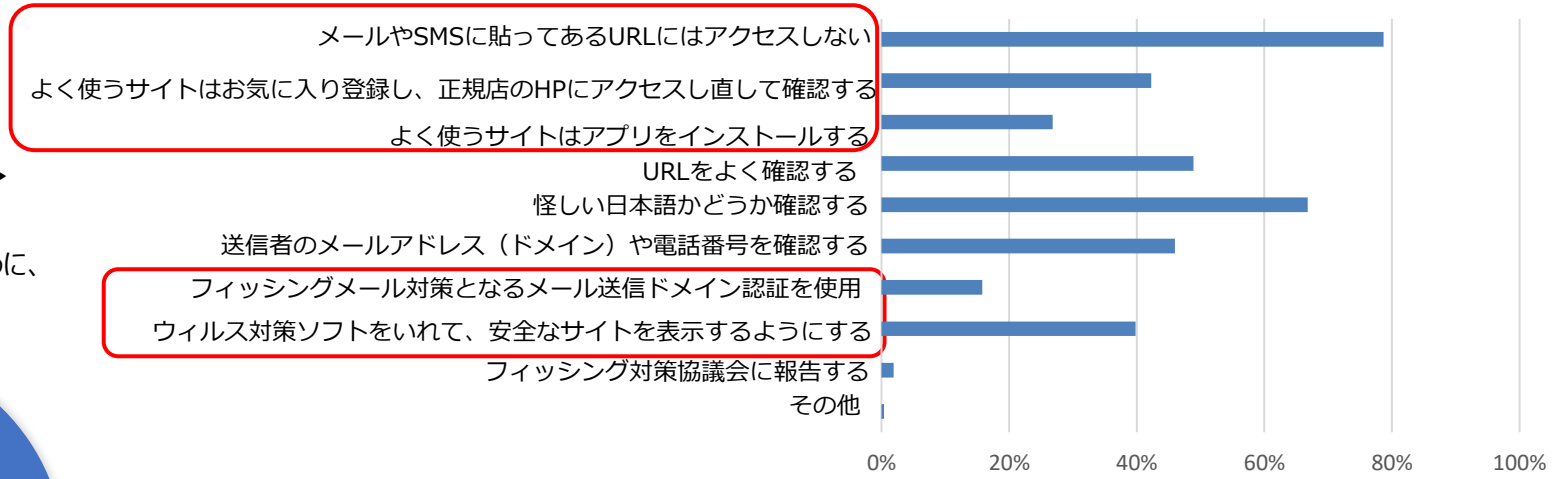
**<利用者のフィッシング対策>**

問：フィッシングの被害に遭わないように、
自分で何か対策をしていますか。



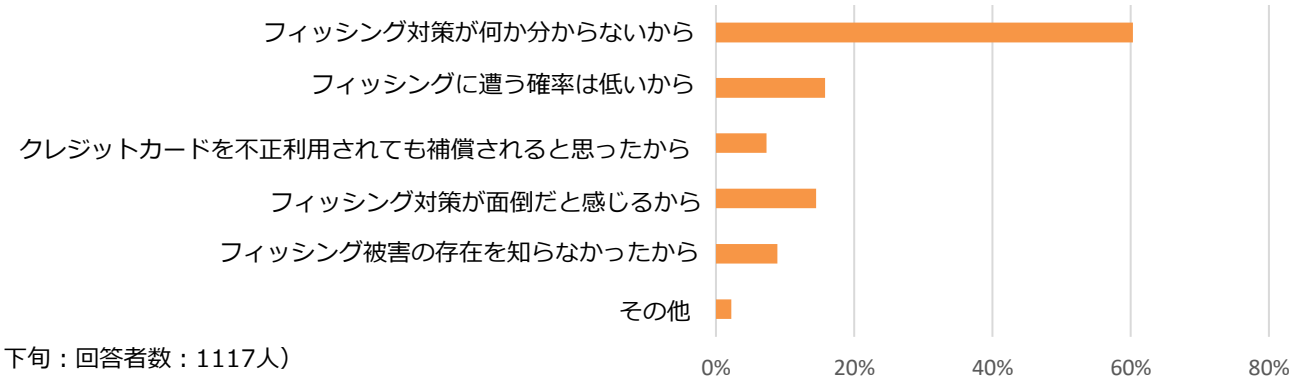

**<利用者のフィッシング対策の内容>**

問：フィッシングの被害に遭わないためにどんな対策をしていますか。
※対策をしていると回答した者（複数回答）




**<利用者がフィッシング対策をしていない理由>**

問：フィッシングの被害に遭わないように対策をしないのは、なぜですか。
※対策をしていないと回答した者（複数回答）




「クレジットカード利用に関するアンケート」　（2022年9月下旬：回答者数：1117人）

# （参考）JCAの利用者向け広報活動

- JCAでは、ウェブサイトにて利用者への注意を呼びかける動画等を公開。


日本クレジット協会「フィッシング詐欺被害に遭わないための注意事項」
https://www.j-credit.or.jp/customer/attention/attention_02.html

# フィッシング対策の強化に向けて

- フィッシング技術が巧妙化し、クレジットカード情報を取得しようとするサイトが大半を占めるなか、クレジットカード情報を保護するため、利用者への注意喚起による利用者の対応だけでなく、サイトを持つ事業者自らも対応することが必要。
- クレジットカード業界全体をあげて、まずは、クレジットカード会社をかたるフィッシングサイトのテイクダウンやクレジットカード会社のドメイン管理等による未然防止による多面的・重層的な自衛が必要ではないか。

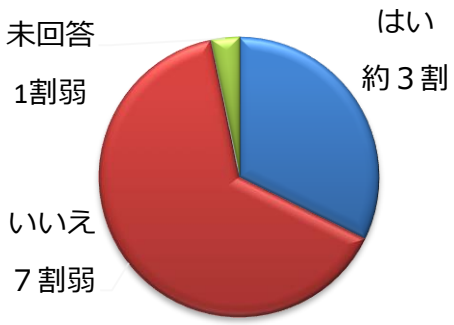
| | これまでの対策 | 考えられる対策（案） |
|---|---|---|
| **JCA** | 利用者への注意喚起 | |
| **イシュアー** | 利用者への注意喚起 | ●フィッシングサイトの監視<br>・フィッシングサイトの検知・テイクダウン<br>●消費者の誤認防止<br>・送信ドメイン認証技術（DMARC等）の導入、ドメインの適切な管理<br>・カード情報を入力させるURLを貼らない |
| **EC加盟店** | | ●フィッシングサイトの監視<br>・フィッシングサイトの検知・テイクダウン<br>●消費者の誤認防止<br>・送信ドメイン認証技術（DMARC等）の導入、ドメインの適切な管理<br>・カード情報を入力させるURLを貼らない |
| **利用者** | 自発的な注意 | ●リテラシー<br>・正規のURLのお気に入り登録やアプリからログインする<br>・フィッシング対策を講じているカード発行会社、EC加盟店を選択<br>・個人情報の漏えい事案の多発に伴い、自分の情報が既に漏えいしているかもしれない意識をもつ<br>・フィッシングメールがあること・被害の状況を認知する<br>・正規メールの見分け方・見分けることの困難さを理解する<br>●設定<br>・メールフィルターの設定 |

# （参考）クレジットカード会社のDMARC等の対策への取組状況

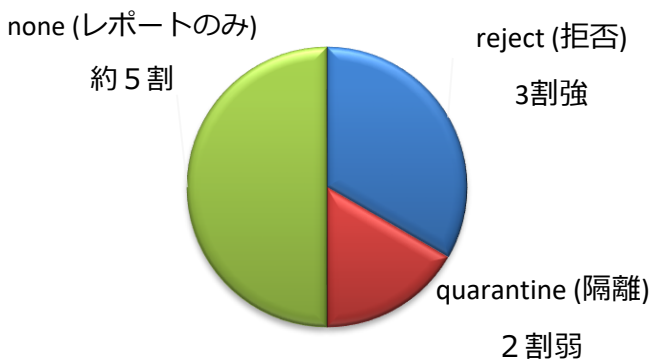
- 主要なクレジットカード会社※の約３割がDMARCを導入。
  うち、受信者に効果のある正式運用(DMARC Policy Enforcement)は、約半数。
  ※事務局で把握している30社程度のイシュアー
- フィッシングメールや偽サイトを確認した場合、約半数が、テイクダウンや関係機関に連絡。

## 主要なクレジットカード会社での取組状況

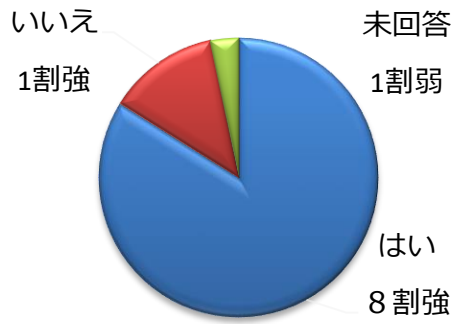
**<全てのドメインでのDMARC導入>**



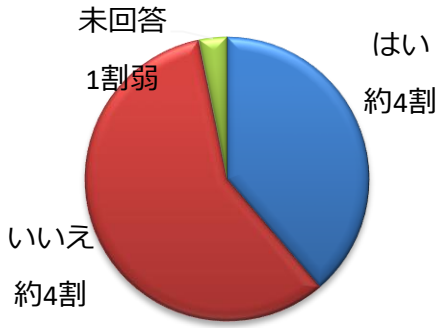

**<全てのドメインでのDMARC導入事業者におけるポリシー設定>**
**※複数回答あり**



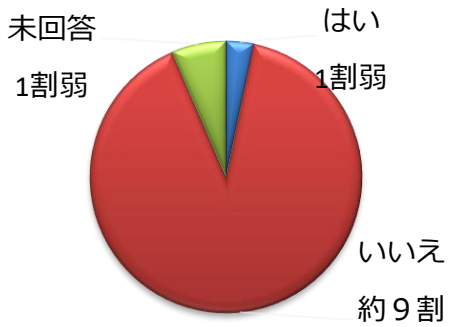

**<SPF (Sender Policy Framework)の導入>**



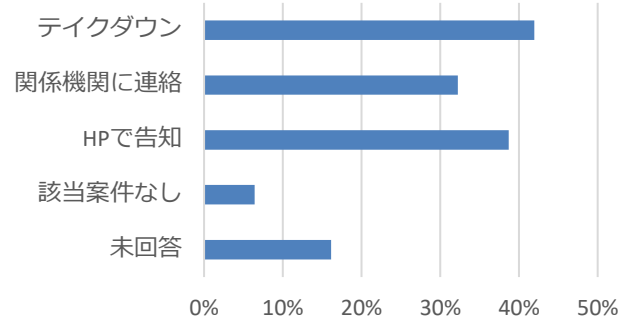

**< DKIM(DomainKeys Identified Mail) の導入>**




**< BIMI の導入>**




**< フィッシングメールや偽サイトを見つけた場合の対応>**
**※複数回答あり**



# （参考）フィッシングに関する罰則について

- フィッシングについては、そのプロセスごとに不正アクセス禁止法や割賦販売法で違法行為を問える場合がある。割賦販売法では、フィッシングのプロセスに着目しておらず、人を欺いてクレジットカード番号等を提供させている場面のみを捉えている。

**■フィッシングサイトの構築**

- 不正アクセス禁止法は、フィッシングサイトを構築すること等により、アクセス制御に係る他人の識別符号の入力を不正に要求する行為を禁止し、罰則を措置（第７条、第１２条第４号）。
- 構成要件として、フィッシングサイトが、①**アクセス管理者**になりすました上で、②**識別符号**の入力を要求するものでなければならない。

※①カード会社を装うもの以外の詐欺サイトは「アクセス管理者」になりすましていない点で、②クレジットカード番号のみを入力させるサイトは「識別符号」の入力を要求していない点で本罪の対象とならない。

不正アクセス禁止法第７条の適用関係

| サイトの形式 | 窃取しようとする情報 | | | |
|---|---|---|---|---|
| | ID・パスワード | 3DSの認証パスワード | セキュリティコード | クレジットカード番号 |
| カード会社を装う形式のサイト（偽サイト） | ○ | △*1 | ×*2 | × |
| カード会社を装わない形式の詐欺サイト | × | × | × | × |

*1 クレカ番号と併せて入力させた場合。 *2個別事例に応じて検討する必要がある。

**■クレジットカード番号等の窃取**

- 割賦販売法は、人を欺いてクレジットカード番号等を提供させる行為について禁止し、罰則を措置（第４９条の２第２項柱書き）。

※本罪の成立には、クレジットカード番号等を実際に「提供させる」ことが必要であり、単にフィッシングサイト・偽サイトを開設する行為やフィッシングメールを送信する行為自体は本罪に当たらない。

**■窃取した情報の保管**

- 不正アクセス禁止法は、不正アクセス行為の用に供する目的で、不正に取得されたアクセス制御機能に係る他人の識別符号を保管する行為を禁止し、罰則を措置（第６条、第１２条第３号）。
- フィッシングサイト構築に係る罰則の論点と同様、本罪の成立には保管されている情報が「識別符号」である必要がある。

※保管情報がクレジットカード番号のみでは本罪は不成立。

# （参考）「世界一安全な日本」創造戦略2022

- 2020年東京オリンピック・パラリンピック大会の開催を見据え、犯罪を更に減少させ、国民の治安に対する信頼感を醸成することを目的として、政府が講ずべき施策を「「世界一安全な日本」創造戦略」としてとりまとめ（平成25年12月10日犯罪対策閣僚会議・閣議決定）。
- 人口構成の変化、科学技術の進展等による社会情勢の変化や国際情勢の変化、サイバー空間の脅威を始めとした様々な治安課題が生じていること等も踏まえ、今般、現行戦略を改定予定。
  ※現在パブコメ実施中(https://public-comment.e-gov.go.jp/servlet/Public?CLASSNAME=PCMMSTDETAIL&id=060221111&Mode=0)

■新戦略の骨子

**1.デジタル社会に対応した世界最高水準の安全なサイバー空間の確保**
2.国内外の情勢に応じたテロ対策、カウンターインテリジェンス機能の強化等の推進
3.犯罪の繰り返しを食い止める再犯防止対策の推進
4.組織的・常習的に行われる悪質な犯罪への対処
5.子供・女性・高齢者等全ての人が安心して暮らすことのできる社会環境の実現
6.外国人との共生社会の実現に向けた取組の推進
7.「世界一安全な日本」創造のための治安基盤の強化

■クレジットセキュリティ関係施策（現時点版）

1　デジタル社会に対応した世界最高水準の安全なサイバー空間の確保
（４）民間事業者、関係機関等と連携したサイバーセキュリティ強化

② **キャッシュレス決済、インターネットバンキング等の不正利用対策の推進**
（警察庁・金融庁・経済産業省）
クレジットカード等のキャッシュレス決済サービスや、インターネットバンキング等を不正に利用するサイバー犯罪に関し、関係団体、民間事業者等と連携し、**本人認証や不正検知の強化**など、被害実態を踏まえた有効な対策を推進する。

③ **フィッシング対策の推進**
（警察庁・総務省・経済産業省）
警察が把握したフィッシングサイト等に関する情報をウイルス対策ソフト事業者等に提供するほか、関係団体等と連携し、民間事業者に対して、**送信ドメイン認証技術（DMARC等）の導入等のなりすましメール対策**を講じるよう働き掛ける。

# １－２．クレジットの安全･安心な利用に関する犯罪の抑止（警察等との連携）

# クレジットカード決済に関する罰則について（概要）

- 偽造クレジットカードによる被害が拡大する中、平成１３年、刑法に支払用カード電磁的記録に関する罪（第１８章の２）を追加。
- カード番号の不正使用被害が相次いだことを踏まえ、平成２０年、割賦販売法にクレジットカード番号等の不正取得、提供、盗用等に係る罰則規定を新設（第４９条の２）。

## 1. スキミング等による偽造カードの作成・使用

・支払用カード電磁的記録不正作出・同供用（刑法第１６３条の２）

（背景）クレジットカード等の普及に伴い、カード偽造が社会問題化

## 2. クレジットカード番号等の窃取

・クレジットカード番号等の不正取得・提供（割賦販売法第４９条の２）

（背景）カード会社の従業員等からのクレジットカード番号等の漏えい事件や不正利用事案の発生

・不正アクセス行為の禁止（不正アクセス禁止法第３条・１１条）

※カード番号等窃取のための会員サイトへの不正ログイン等

・他人の識別符号を不正に取得する行為、識別符号の入力を不正に要求する行為の禁止（不正アクセス禁止法第４条・１２条）

## 3. クレジットマスター

・偽計業務妨害（刑法第２３３条）等

## 4. 窃取したクレジットカード番号等の使用（不正利用）

・ECサイト等：電子計算機使用詐欺（刑法第２４６条の２）、私電磁的記録不正作出・同供用（第１６１条の２第１項、第３項）＋窃盗（第２３５条）
・リアル店舗 ：詐欺（第２４６条）、私電磁的記録不正作出・同供用（第１６１条の２第１項、第３項）＋窃盗（第２３５条）

# （参考）クレジットカード決済に関する罰則

## 1．スキミング等による偽造カードの作成･使用

**刑法**

（支払用カード電磁的記録不正作出等）
第百六十三条の二　人の財産上の事務処理を誤らせる目的で、その事務処理の用に供する電磁的記録であって、クレジットカードその他の代金又は料金の支払用のカードを構成するものを不正に作った者は、十年以下の懲役又は百万円以下の罰金に処する。預貯金の引出用のカードを構成する電磁的記録を不正に作った者も、同様とする。
２　不正に作られた前項の電磁的記録を、同項の目的で、人の財産上の事務処理の用に供した者も、同項と同様とする。
３　不正に作られた第一項の電磁的記録をその構成部分とするカードを、同項の目的で、譲り渡し、貸し渡し、又は輸入した者も、同項と同様とする。
（不正電磁的記録カード所持）
第百六十三条の三　前条第一項の目的で、同条第三項のカードを所持した者は、五年以下の懲役又は五十万円以下の罰金に処する。
（支払用カード電磁的記録不正作出準備）
第百六十三条の四　第百六十三条の二第一項の犯罪行為の用に供する目的で、同項の電磁的記録の情報を取得した者は、三年以下の懲役又は五十万円以下の罰金に処する。情を知って、その情報を提供した者も、同様とする。
２　不正に取得された第百六十三条の二第一項の電磁的記録の情報を、前項の目的で保管した者も、同項と同様とする。
３　第一項の目的で、器械又は原料を準備した者も、同項と同様とする。
（未遂罪）
第百六十三条の五　第百六十三条の二及び前条第一項の罪の未遂は、罰する。

## 2．クレジットカード番号等の窃取

**割賦販売法**

第四十九条の二　クレジットカード番号等取扱業者若しくはクレジットカード番号等取扱受託業者又はこれらの役員若しくは職員若しくはこれらの職にあつた者が、その業務に関して知り得たクレジットカード番号等を自己若しくは第三者の不正な利益を図る目的で、提供し、又は盗用したときは、三年以下の懲役又は五十万円以下の罰金に処する。
２　**人を欺いてクレジットカード番号等を提供させた者**も、前項と同様とする。クレジットカード番号等を次の各号のいずれかに掲げる方法で取得した者も、同様とする。
一　クレジットカード番号等が記載され、又は記録された人の管理に係る書面又は記録媒体の記載又は記録について、その承諾を得ずにその複製を作成すること。
二　**不正アクセス行為（不正アクセス行為の禁止等に関する法律（平成十一年法律第百二十八号）第二条第四項に規定する不正アクセス行為をいう。）を行う**こと。
３　**正当な理由がないのに、有償で、クレジットカード番号等を提供し、又はその提供を受けた者も、第一項と同様とする。**正当な理由がないのに、有償で提供する目的で、クレジットカード番号等を保管した者も、同様とする。
４　前三項の規定は、刑法その他の罰則の適用を妨げない。

# （参考）クレジットカード決済に関する罰則

**不正アクセス禁止法**

（定義）
第二条　この法律において「アクセス管理者」とは、電気通信回線に接続している電子計算機（以下「特定電子計算機」という。）の利用（当該電気通信回線を通じて行うものに限る。以下「特定利用」という。）につき当該特定電子計算機の動作を管理する者をいう。
２　この法律において「識別符号」とは、特定電子計算機の特定利用をすることについて当該特定利用に係るアクセス管理者の許諾を得た者（以下「利用権者」という。）及び当該アクセス管理者（以下この項において「利用権者等」という。）に、当該アクセス管理者において当該利用権者等を他の利用権者等と区別して識別することができるように付される符号であって、次のいずれかに該当するもの又は次のいずれかに該当する符号とその他の符号を組み合わせたものをいう。
一　当該アクセス管理者によってその内容をみだりに第三者に知らせてはならないものとされている符号
二　当該利用権者等の身体の全部若しくは一部の影像又は音声を用いて当該アクセス管理者が定める方法により作成される符号
三　当該利用権者等の署名を用いて当該アクセス管理者が定める方法により作成される符号
３　この法律において「アクセス制御機能」とは、特定電子計算機の特定利用を自動的に制御するために当該特定利用に係るアクセス管理者によって当該特定電子計算機又は当該特定電子計算機に電気通信回線を介して接続された他の特定電子計算機に付加されている機能であって、当該特定利用をしようとする者により当該機能を有する特定電子計算機に入力された符号が当該特定利用に係る識別符号（識別符号を用いて当該アクセス管理者の定める方法により作成される符号と当該識別符号の一部を組み合わせた符号を含む。次項第一号及び第二号において同じ。）であることを確認して、当該特定利用の制限の全部又は一部を解除するものをいう。
４　この法律において**「不正アクセス行為」とは、次の各号のいずれかに該当する行為**をいう。
**一　アクセス制御機能を有する特定電子計算機に電気通信回線を通じて当該アクセス制御機能に係る他人の識別符号を入力して当該特定電子計算機を作動させ、当該アクセス制御機能により制限されている特定利用をし得る状態にさせる行為（当該アクセス制御機能を付加したアクセス管理者がするもの及び当該アクセス管理者又は当該識別符号に係る利用権者の承諾を得てするものを除く。）**

**二　アクセス制御機能を有する特定電子計算機に電気通信回線を通じて当該アクセス制御機能による特定利用の制限を免れることができる情報（識別符号であるものを除く。）又は指令を入力して当該特定電子計算機を作動させ、その制限されている特定利用をし得る状態にさせる行為（当該アクセス制御機能を付加したアクセス管理者がするもの及び当該アクセス管理者の承諾を得てするものを除く。次号において同じ。）**

**三　電気通信回線を介して接続された他の特定電子計算機が有するアクセス制御機能によりその特定利用を制限されている特定電子計算機に電気通信回線を通じてその制限を免れることができる情報又は指令を入力して当該特定電子計算機を作動させ、その制限されている特定利用をし得る状態にさせる行為**

# （参考）クレジットカード決済に関する罰則

**不正アクセス禁止法（続き）**

**（不正アクセス行為の禁止）**
第三条　何人も、**不正アクセス行為をしてはならない。**
**（他人の識別符号を不正に取得する行為の禁止）**
第四条　何人も、**不正アクセス行為（第二条第四項第一号に該当するものに限る。第六条及び第十二条第二号において同じ。）の用に供する目的で、アクセス制御機能に係る他人の識別符号を取得してはならない。**
**（他人の識別符号を不正に保管する行為の禁止）**
第六条　**何人も、不正アクセス行為の用に供する目的で、不正に取得されたアクセス制御機能に係る他人の識別符号を保管してはならない。**
（識別符号の入力を不正に要求する行為の禁止）
第七条　何人も、アクセス制御機能を特定電子計算機に付加したアクセス管理者になりすまし、その他当該アクセス管理者であると誤認させて、次に掲げる行為をしてはならない。ただし、当該アクセス管理者の承諾を得てする場合は、この限りでない。
一　当該アクセス管理者が当該アクセス制御機能に係る識別符号を付された利用権者に対し当該識別符号を特定電子計算機に入力することを求める旨の情報を、電気通信回線に接続して行う自動公衆送信（公衆によって直接受信されることを目的として公衆からの求めに応じ自動的に送信を行うことをいい、放送又は有線放送に該当するものを除く。）を利用して公衆が閲覧することができる状態に置く行為
二　当該アクセス管理者が当該アクセス制御機能に係る識別符号を付された利用権者に対し当該識別符号を特定電子計算機に入力することを求める旨の情報を、電子メール（特定電子メールの送信の適正化等に関する法律（平成十四年法律第二十六号）第二条第一号に規定する電子メールをいう。）により当該利用権者に送信する行為
（罰則）
第十一条　第三条の規定に違反した者は、三年以下の懲役又は百万円以下の罰金に処する。
第十二条　次の各号のいずれかに該当する者は、一年以下の懲役又は五十万円以下の罰金に処する。
一　第四条の規定に違反した者
三　第六条の規定に違反した者
四　第七条の規定に違反した者

# （参考）クレジットカード決済に関する罰則

## 3．クレジットマスター

**刑法**

（信用毀損及び業務妨害）
第二百三十三条　虚偽の風説を流布し、又は**偽計を用いて、人の信用を毀損し、又はその業務を妨害した者**は、三年以下の懲役又は五十万円以下の罰金に処する。

## 4．窃取したクレジットカード番号等の利用（不正利用）

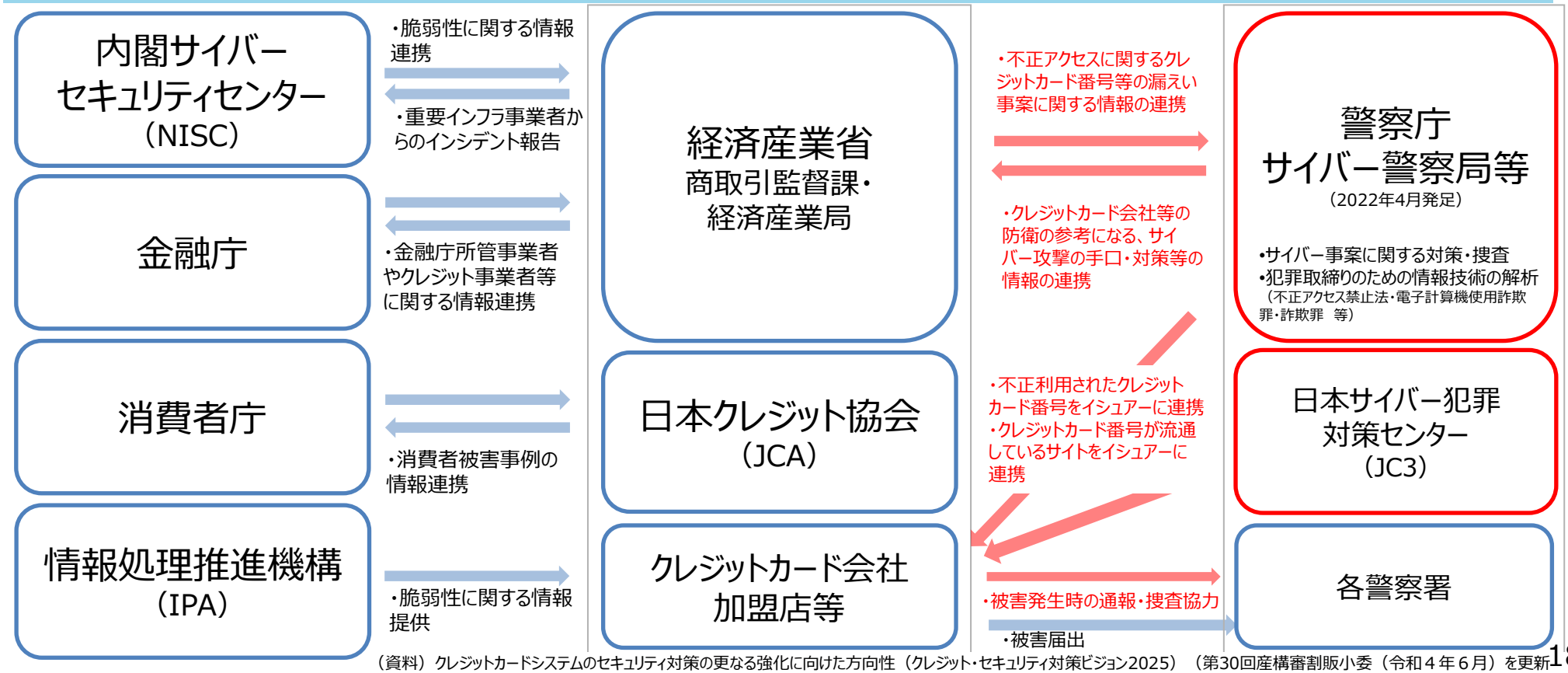
**刑法**

（電磁的記録不正作出及び供用）
第百六十一条の二　**人の事務処理を誤らせる目的で、その事務処理の用に供する権利、義務又は事実証明に関する電磁的記録を不正に作った**者は、五年以下の懲役又は五十万円以下の罰金に処する。
２　（略）
３　**不正に作られた権利、義務又は事実証明に関する電磁的記録を、第一項の目的で、人の事務処理の用に供した**者は、その電磁的記録を不正に作った者と同一の刑に処する。
４　前項の罪の未遂は、罰する。
（窃盗）
第二百三十五条　**他人の財物を窃取した者**は、窃盗の罪とし、十年以下の懲役又は五十万円以下の罰金に処する。
（未遂罪）
第二百四十三条　第二百三十五条から第二百三十六条まで、第二百三十八条から第二百四十条まで及び第二百四十一条第三項の罪の未遂は、罰する。
（詐欺）
第二百四十六条　**人を欺いて財物を交付させた者**は、十年以下の懲役に処する。
２　前項の方法により、財産上不法の利益を得、又は他人にこれを得させた者も、同項と同様とする。
（電子計算機使用詐欺）
第二百四十六条の二　前条に規定するもののほか、**人の事務処理に使用する電子計算機に虚偽の情報若しくは不正な指令を与えて財産権の得喪若しくは変更に係る不実の電磁的記録を作り**、又は**財産権の得喪若しくは変更に係る虚偽の電磁的記録を人の事務処理の用に供して、財産上不法の利益を得、又は他人にこれを得させた者**は、十年以下の懲役に処する。
（未遂罪）
第二百五十条　この章の罪の未遂は、罰する。

# 犯罪抑止に向けた関係行政機関等との連携強化（サイバー犯罪）

赤枠・・・取組を強化している主体
赤矢印・赤字・・・新たな取組案
青矢印・黒字・・・これまでの取組

- 従来より、クレジットカード会社等はサイバー攻撃によるインシデント時に関係行政機関・団体への報告・相談を行うとともに、所管の警察署にも通報を行ってきた。
- 一方、昨今は、サイバー攻撃によるクレジットカード番号等の漏えいや不正利用等のサイバー犯罪が急増。
- 今後は、更に犯罪防止に資するべく、より詳細かつ実効的な情報共有を行うため、関係省庁・業界団体間での連携強化の構築も、対策として考えられる。




（資料）クレジットカードシステムのセキュリティ対策の更なる強化に向けた方向性（クレジット・セキュリティ対策ビジョン2025）（第30回産構審割販小委（令和４年６月）を更新

# ご議論いただきたい事項

**１－１．クレジットの安全･安心な利用に関する犯罪の抑止（フィッシング対策）**
**総論：巧妙化していくフィッシングへの対策について、どのように取り組むべきか。**

**①イシュアーでの対応**
これまで、クレジットカード業界の対応は、利用者への注意喚起という対策が主であったところ。
（１）クレジットカード関連のフィッシングが増加するなか、利用者での対策だけでは十分ではないのではないか。クレジットカード業界・イシュアーとしても、フィッシングを未然に防止するため、自衛していくことが必要ではないか。
（２）カード会社がフィッシングから自衛する対策として、他に考えられる対策はないか。
**②利用者での対応** **（３と併せて議論）**
（１）利用者はフィッシングに対し、どのような点を優先して注意・対応すべきか。

**１－２．クレジットの安全･安心な利用に関する犯罪の抑止（警察等との連携）**
**総論：クレジットカード決済の安全・安心な利用を確保するため、クレジットカード決済に関する犯罪を抑止するため、どのような対応が求められるか。**

現在、経産省・警察庁間でサイバー犯罪事案の迅速な連携・これらを踏まえた手口・対策の共有等について検討されているところである。
（１）クレジットカード決済に関する犯罪を抑止していくうえで、今後、注力していくべき方向性は何か。

# ２．クレジットカード番号等の漏えい対策
# （インシデント対応・漏えい防止にかかる利用者保護）

# クレジットカード番号等の漏えい対策の位置づけ

- クレジットカード番号等の不正利用は、クレジットカード決済網の事業者からの漏えい、フィッシング、クレジットマスター等による手法が原因と考えられている。
- サイバー攻撃や利用者へのオンラインツールでの接触の増加、機械学習の進展により、どの手法も、従前より高度化してきていると考えられる。
- クレジットカード番号等の漏えい対策は、クレジットカード決済システムの信頼性を確保するため、同システムに携わるすべての事業者の責務であり、クレジットカード番号等の不正利用の未然防止に直接寄与するもの。今回の議論は、特にサイバー攻撃により、事業者からクレジットカード番号等が漏えいするものを焦点とする。

**事業者からの漏えい**
**（サイバー攻撃によるクレジットカード番号等の窃取）**

**クレジットカード番号等の**
**漏えい防止対策**

**消費者からの漏えい**
**（フィッシング）**

**クレジットカード番号等の**
**不正利用対策**

**クレジットカード番号等の有効性確認による割り出し**
**（クレジットマスター）**

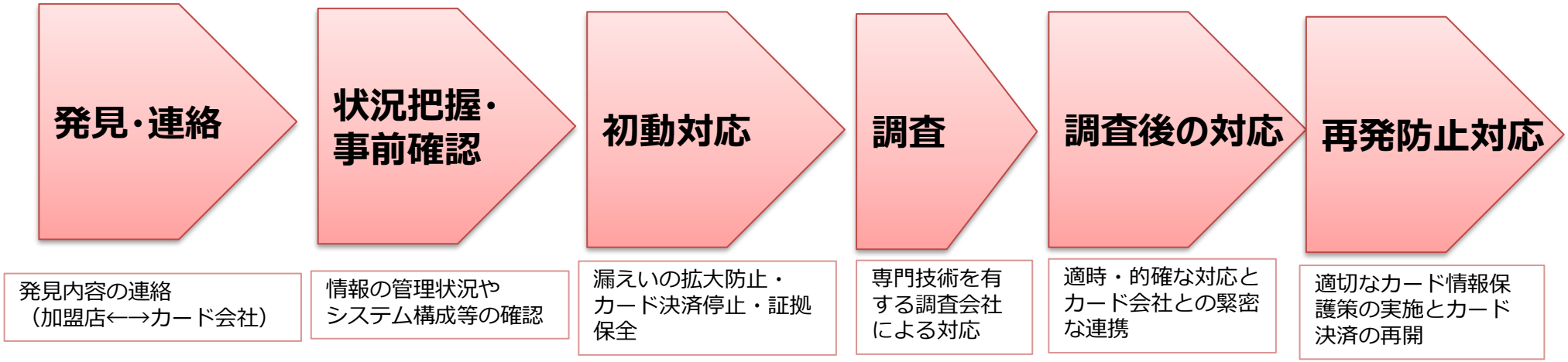
**クレジットの安全・安心な利用**
**に関する周知・犯罪抑止**

# 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

- 「クレジットカード・セキュリティガイドライン」の関連文書として、加盟店向けに、クレジットカード情報が漏えい（懸念含む）した際の対応ポイントを、日本クレジット協会で策定。
- 情報漏えいの被害を最小限に抑え、顧客を保護するため、状況把握等と関係団体への報告が求められている。

## 概要

基本的な対応の流れは、以下の通り



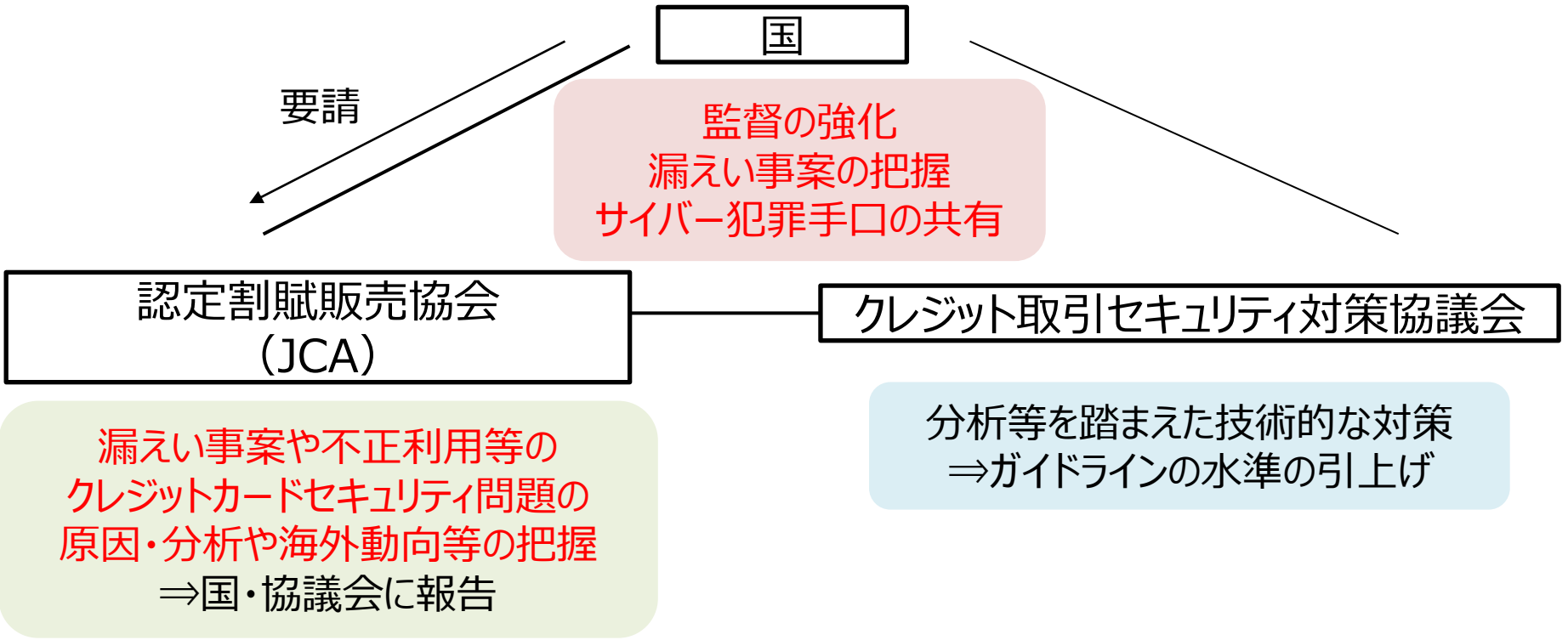

初動対応として、**「個人情報保護委員会等への報告（速報）」**について、
調査後の対応として、**「個人情報保護委員会等への報告（追完）」**や**「警察への被害届出」**について、対応することが記載されている。

これらは、付録の「対応チェックシート」にも記載され、対応漏れの防止が図られている。

（資料）クレジットカードシステムのセキュリティ対策の更なる強化に向けた方向性（クレジット・セキュリティ対策ビジョン2025）（第30回産構審割販小委（令和４年６月））を更新

# クレジットカード業界のセキュリティ対策に関する体制強化に向けて

- 業界として、次の漏えいや不正利用を防止するため、国としても監督を強化するほか、業界内でクレジットカード番号等の漏えい事案や不正利用の原因・分析を把握するための仕組み、これを踏まえたクレジットカード業界内への周知や再発防止の対策強化をはかっていくことが考えられる。



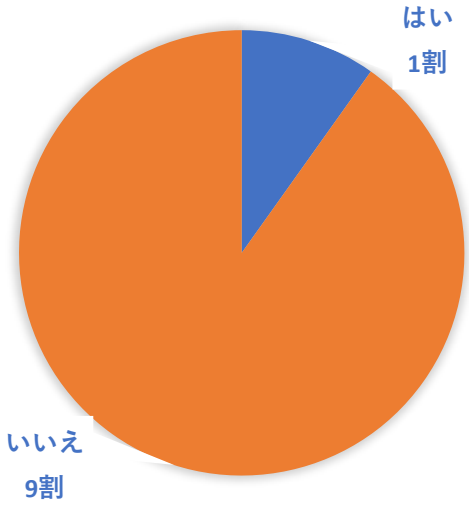
# 3. 利用者への周知

# 安全・安心な利用に向けた利用者への周知

- クレジットカード決済における安全・安心な利用には、利用者自身の対応も必要不可欠。
- 怪しいECサイトでも、安い、そこでしか買えない等の理由で購入してしまう利用者は、約１割。
- 一方、ECサイトでのセキュリティ対策を事前に把握したいと思っている利用者が大半。

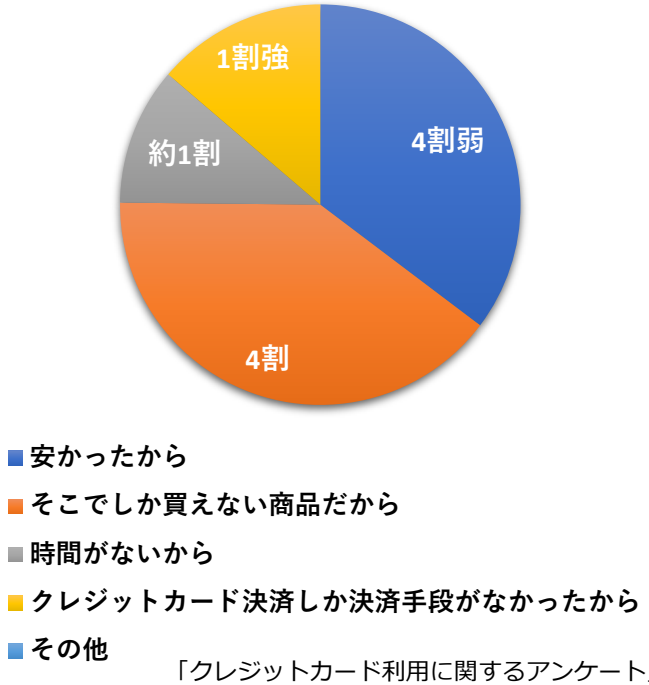
**＜怪しいサイトでの購入経験＞**

問：インターネットショッピングで、Webサイト画面を怪しいと思っても、クレジットカード決済で購入したことがありますか。



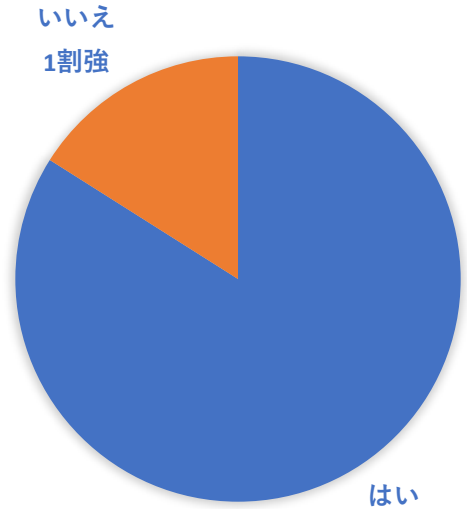

**＜怪しいサイトで購入した理由＞**

問：Webサイト画面が怪しいと思ったにも関わらず、購入した理由を教えてください。
（複数回答可 ）




**＜EC加盟店のセキュリティ対策を把握したい利用者ニーズ＞**

問：インターネットショッピングでの購入決済の前に、そのショッピングサイトでどんなクレジットカード決済のセキュリティ対策がとられているか把握したいと思いますか。




「クレジットカード利用に関するアンケート」　（2022年9月下旬：回答者数：1117人）

# 安全・安心な利用に向けた利用者への周知

- 不正利用を防止するため、利用明細の確認やEMV 3-Dセキュアの認証用パスワードの設定、クレジットカード番号等の漏えいを防止するため、利用者側でのフィッシング対策について周知。

**消費者への周知事項の骨子**

※下線は今後新たに呼びかけていくもの

□ 前提

- 個人情報等の漏えい実態

□ 不正利用被害の防止対策

- 利用明細・利用通知の確認
- EMV 3-Dセキュアの認証用パスワードの設定

□ 漏えい防止対策

- 利用者側でのフィッシング対策
  - ー迷惑メールフィルターの設定
  - ー正規メールとフィッシングメールの見分け方を理解
  - ーフィッシングメール、偽サイトを発見した場合の対応（協議会への報告等）
  - ー送信認証技術（DMARC等）、フィルタリング等の対策を取っている事業者の選択

# ご議論いただきたい事項

**２．クレジットカード情報保護対策・漏えい防止（インシデント対応・漏えい防止にかかる利用者保護）**
**総論：クレジットカード番号等の漏えいのインシデント時に、利用者を保護していくため、どのような対応が求められるか。**

**３．クレジットの安全・安心な利用に関する周知**
**総論：クレジットカード決済網の一員として、利用者もクレジットカード決済の利用にかかる対応が必要。これまでの議論を踏まえ、利用者にどのように周知すべきか。**

（１）当面の間、力点を置いて周知すべき内容は何か。
（２）どのような手法での周知が有効か。