経済産業省

安全・安心

資料４－１

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1.1版

2022年8月4日

経済産業省　商務・サービスグループ
商取引監督課

改定履歴

経済産業省HPより引用

版数	発行日	主な改訂内容
第１版	2022年6月2日	初版発行
第1.1版	2022年6月20日	各論編における以下のページを追加 P.20：（追補）重要インフラのサイバーセキュリティに係る行動計画の改定 P.21：（参考）サイバーセキュリティ体制構築・人材確保の手引き

目次（総論編）

経済産業省HPより引用

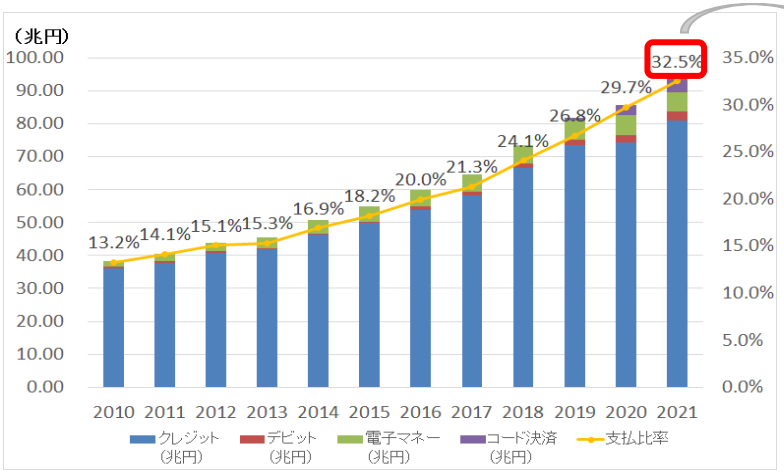
1．背景

経済産業省HPより引用

キャッシュレス決済の伸長

国内キャッシュレス決済額・比率は順調に増加（うちクレジットカード取引は約９割）

キャッシュレス支払額及び決済比率の推移



2025年6月まで
40%
※目標値

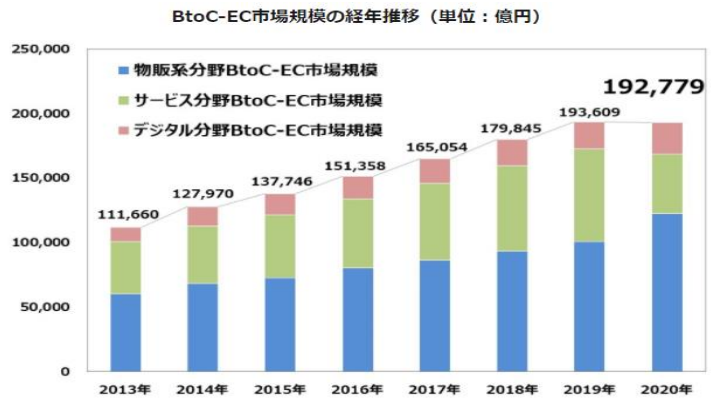
うちクレジット：
約100兆円
※見込み

出典：経済産業省HP

参考：民間(矢野経済研究所)の試算によると、キャッシュレス決済額全体は2025年に約**150**兆円まで拡大するとされている

EC決済サービスの伸長

EC取引の伸長に伴って、消費者のクレジットカード番号の入力機会が増加



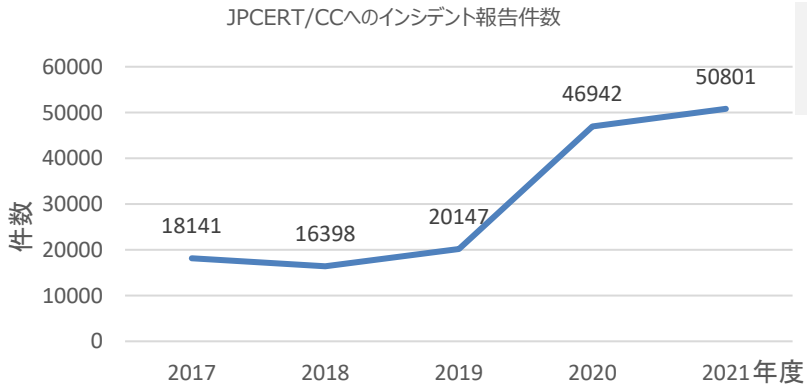
2021年
EC市場規模
約19兆円

出典：令和2年度産業経済研究委託事業（電子商取引に関する市場調査）経済産業省

参考：民間(SBペイメント)の試算によると、EC決済のうち約 **8** 割はクレジットカードを使った決済が行われている

サイバーセキュリティインシデントの発生

全業種的にサイバーセキュリティインシデントへの脅威が高まっている

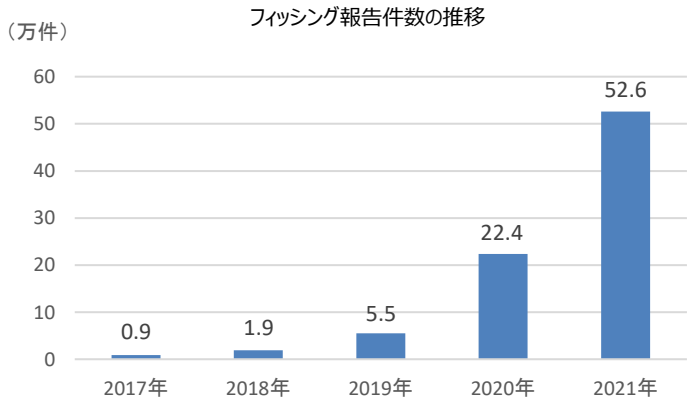


2021年度
報告件数
約 5 万件

出典：JPCERT/CCインシデント報告対応レポート（2022年４月14日）

フィッシング被害の増加

近年、消費者を狙ったフィッシングの報告件数も急増



2021年
フィッシング報告件数
約53万件

フィッシングとは：
メールやSMSを通じて、個人情報等（クレジットカード番号等を含む）をだまし取ること

出典：JC3HP（フィッシングターゲットの変遷）

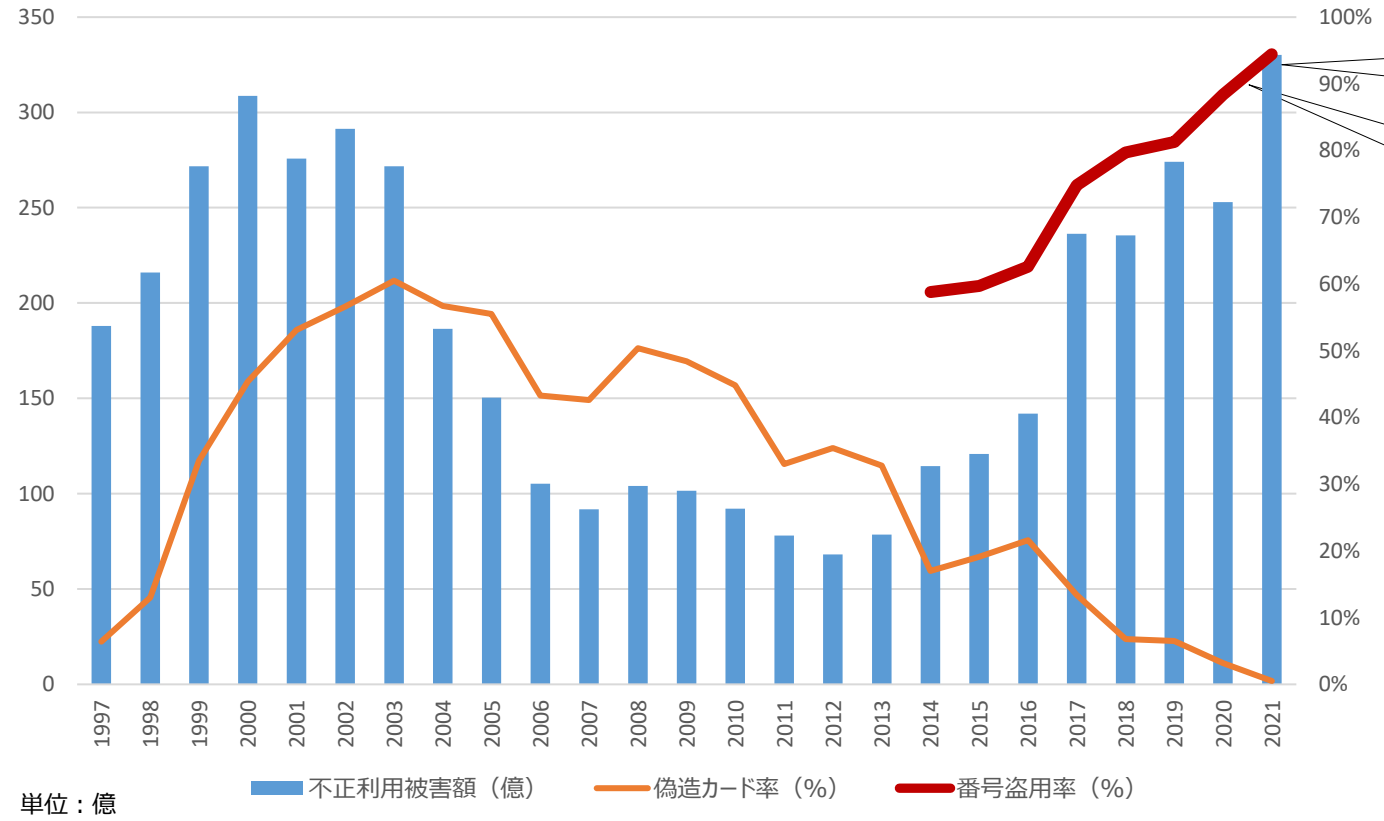
1．背景

経済産業省HPより引用

結果として、不正利用被害額は過去最高に、そのうち番号盗用被害額も過去最高に

※　サイバー攻撃やフィッシング等によって漏えい・割り出されたクレジットカード情報を用いて、クレジットカードによる不正利用に使われている

国内発行クレジットカードにおける年間不正利用被害額推移



単位：億

2021年における不正利用被害**総額**
330億円

2021年の不正利用被害総額に対する**番号盗用**の被害割合
94%

想定される番号盗用の原因

- クレジットマスター
  （クレジットカード番号自体は盗まず、他人のクレジットカード番号から確率的に割り出す手法）
- 加盟店等、事業者からの漏えい
- フィッシング
  （メールやSMS等を通じて、利用者からクレジット情報等をだまし取る）

出典：日本クレジット協会（令和４年３月）

補足：ダークウェブでのクレジットカード番号等の取得による不正利用

※　盗まれたクレジットカード情報は、ダークウェブ等において売買され、不正利用に使われることもある

事案１）クレジットカードの情報をダークウェブで入手し、高級腕時計を購入し売却したとして逮捕
事案２）クレジットカードの情報をダークウェブで購入し悪質事業者に売りさばいたとして学生を逮捕

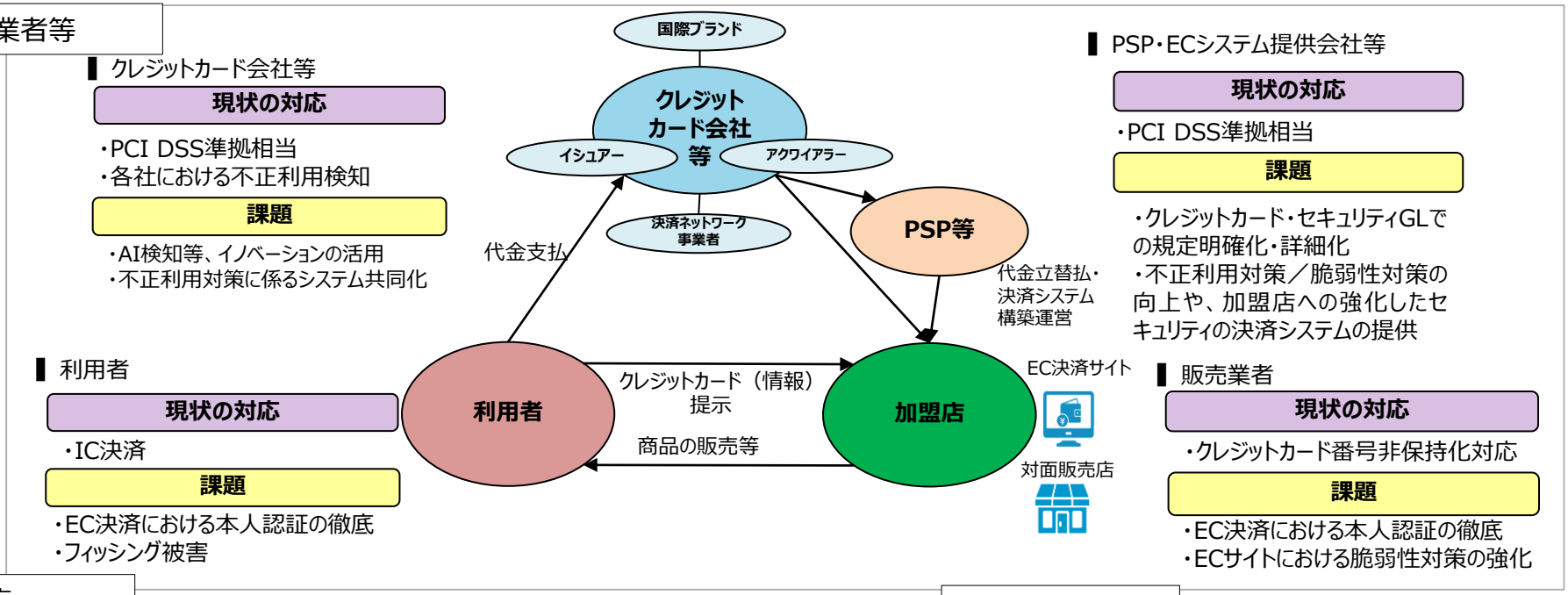
参考：民間セキュリティ会社の調査によると、日本のクレジットカード情報は闇サイトで平均約5200円で販売されているとの情報も（2022/4/4　共同通信社）

2．クレジットカードシステムのセキュリティ対策の現状と課題

経済産業省HPより引用

- 加盟店と利用者との決済サービスをクレジットカード会社が提供するという基本的関係をもとに様々な事業者が参画。
- クレジットカードシステムに対するセキュリティは、
  ① 当初は、**クレジットカード会社**によるPCI DSS準拠等の漏えい防止対策。
  ② 一方、キャッシュレス決済の広まりに伴い、**利用者**や**加盟店**といったフロントでの対策も重要。
  ③ 最近では、**決済代行業者（PSP）等**の、クレジットカード会社と加盟店の間にいる事業者が決済情報を集積している場合も多く、これらの事業者におけるさらなるセキュリティ対策強化が課題と認識。
- 今後は、関係事業者・関係省庁・関係団体等の連携がより一層重要になる。

関係事業者等



クレジットカード会社等

現状の対応

・PCI DSS準拠相当
・各社における不正利用検知

課題

・AI検知等、イノベーションの活用
・不正利用対策に係るシステム共同化

PSP・ECシステム提供会社等

現状の対応

・PCI DSS準拠相当

課題

・クレジットカード・セキュリティGLでの規定明確化・詳細化
・不正利用対策／脆弱性対策の向上や、加盟店への強化したセキュリティの決済システムの提供

利用者

現状の対応

・IC決済

課題

・EC決済における本人認証の徹底
・フィッシング被害

販売業者

現状の対応

・クレジットカード番号非保持化対応

課題

・EC決済における本人認証の徹底
・ECサイトにおける脆弱性対策の強化

関係省庁

経済産業省

・割賦販売法に基づく監督・検査
・消費者からの相談受付・相談事例の収集
・消費者被害防止に向けた注意喚起

警察庁

・各種罰則に基づく検挙活動
・サイバーインシデント対応／フィッシング対策
ーサイバー警察局

内閣サイバーセキュリティセンター（NISC）

・重要インフラ事業者（クレジット分野で約50社指定）のサイバーセキュリティ対策

消費者庁

・消費者被害防止に向けた注意喚起

関係団体等

日本クレジット協会（JCA）

・認定割賦販売協会
・クレジット取引セキュリティ対策協議会事務局

フィッシング対策協議会

・フィッシングに関する情報収集／提供／動向分析

日本サイバー犯罪対策センター（JC3）

・サイバー犯罪等のサイバー空間の脅威に対し、情報共有や手口分析等

3．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

クレジットカード会社等　加盟店　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）		経済産業省HPより引用
▌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 （クレジットカード番号等の適切管理規定） － PCI DSS準拠相当 － 非保持化	✓ さらなる制度的措置の検討 －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 ✓ 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 － 対面取引におけるIC決済の推進 － 非対面取引における本人認証の導入 （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 ✓ 本人認証方法の高度化 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 ⇒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 ✓ 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 ✓ 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） ✓ 周知啓発の強化 ✓ 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

4．安全・安心なクレジットカード決済環境の進展と今後のロードマップ（イメージ）

経済産業省HPより引用

（追補）今後の取組：セキュリティ対策についての更なる詳細な検討

経済産業省HPより引用

- 今後「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」を踏まえて、技術的な観点も含めより詳細に議論していくことを検討。
- 産業構造審議会割賦販売小委員会のメンバーとも連動しながら議論を進め、年明けから来春までに同小委員会に報告することを目指す。

趣旨：昨今のクレジットカード番号等の漏えい事案への対応も含め、安全・安心なクレジットカード決済を確保するため、具体的な対応の方策等について、学識者、業界、実務家等で議論。

方向性（案）

・クレジットカード番号を安全に管理する（漏えい防止）

・クレジットカード番号を不正利用させない（不正利用防止）

・クレジットの安心・安全な利用に関する周知・犯罪の抑止

→

国の検討会
（今夏～今冬（年末目途））

・実施するべきセキュリティ対策の検討
　例：決済代行業者のセキュリティ対策のあり方
　　本人認証の進め方
・具体の工程、プレーヤー
・監督の強化

→

小委員会での報告
（年明け～来春）

・対策の提示
・GL改訂ほか

目次（各論編）

経済産業省HPより引用

経済産業省HPより引用

1．制度

クレジットカード会社のセキュリティに関する主な関係法令（法律・ガイドライン等）

経済産業省HPより引用

- クレジットカード会社のセキュリティへの対応は、クレジットカード番号等の観点から、主に割賦販売法・個人情報保護法、重要インフラの観点からサイバーセキュリティ基本法によって、規律されている。

法令	割賦販売法 ・クレジットカード番号等の適切な管理 ・クレジットカード番号等の不正な利用の防止	個人情報の保護に関する法律 ・個人情報の不正利用や不適切な取扱いを防ぐため、個人情報を取り扱う事業者が遵守すべき義務等	サイバーセキュリティ基本法 ・サイバーセキュリティに関する施策の基本理念の策定 ・重要インフラ事業者の努力義務に関する規定等
方針等	割賦販売法（後払分野）における監督の基本方針	個人情報の保護に関する基本方針	サイバーセキュリティ戦略
	信用購入あっせん業者等に対する検査基本方針及び検査基本計画		重要インフラの情報セキュリティ対策に係る第4次行動計画（改定中）
ガイドライン	クレジットカード・セキュリティガイドライン（クレジット取引セキュリティ対策協議会） 割賦販売法におけるセキュリティ規定、実務上の指針	個人情報の保護に関する法律についてのガイドライン（通則編）等 対個人情報取扱事業者 信用分野における個人情報保護に関するガイドライン 対与信事業者	クレジットCEPTOARにおける情報セキュリティガイドライン
ガイドライン関連文書	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（日本クレジット協会）　等		

割賦販売法におけるセキュリティ対策

経済産業省HPより引用

- 割賦販売法では、以下の改正により、クレジットカード番号等についてのセキュリティ対策を**義務付け、適切な履行**を確保するため、監督を実施してきたところ。
  - ・平成20年改正：クレジットカード会社に対する**クレジットカード番号漏えい対策の義務化、クレジットカード番号不正取得の禁止**
  - ・平成28年改正：加盟店への**クレジットカード番号漏えい防止・不正利用防止対策の義務化、**アクワイアラー等への**加盟店調査義務化**
  - ・令和２年改正：**決済代行業者、QRコード決済事業者・ECプラットフォーム事業者等**について、クレジットカード番号漏えい対策の**義務主体に追加**

1．クレジットカード番号等の適切な管理（法第35条の16）

- クレジットカード番号等取扱業者（イシュアー、加盟店等）は、**クレジットカード番号等の漏えい防止**の適切な管理のために必要な措置を講じなければならない。
- クレジットカード番号等取扱業者は、**クレジットカード番号等の取扱いを委託した者**に対してクレジットカード番号等の適切な管理のために必要な**指導その他の措置**を講じなければならない。

2．クレジットカード番号等の不正な利用の防止（法第35条の17）

- **加盟店**は、クレジットカード番号等の**不正利用を防止**するために必要な措置を講じなければならない。

3．加盟店調査等の義務（法第35条の17の8）

- クレジットカード番号等取扱契約締結事業者に対し、**加盟店調査**（悪質加盟店の排除、クレジットカード番号等の漏えい防止、不正利用の防止の措置状況）及び**調査結果に基づいた必要な措置を義務付け**。

4．クレジットカード番号等の不正取得（法第49条の２第２項）

- 不正な手段（人への欺罔、不正アクセス等）によるクレジットカード番号等の取得行為の禁止。罰則の対象。

クレジットカード情報の漏えい防止措置（クレジットカード番号等取扱業者）、不正利用防止措置（加盟店）、クレジットカード番号等取扱契約締結事業者による加盟店調査及び必要な措置等により、安全・安心なクレジットカード利用環境の実現を図る。

（追補）令和２年割賦販売法改正について

経済産業省HPより引用

- **決済代行業者の役割の増大や、スマートフォン決済等の新たな後払い決済サービス提供主体の登場により、クレジットカード番号の情報漏えいリスク**に対する懸念が高まっていることを踏まえ、「割賦販売法の一部を改正する法律」を令和３年４月１日に施行し、**クレジットカード番号等の適切管理の義務主体の拡充**を行った。

クレジットカード番号等の適切管理の義務主体の拡充

クレジットカード番号等取扱事業者(※)	対象事業者	セキュリティ対策	違反に対する措置等
１号　・・・ イシュアー 「クレジットカード等購入あっせん業者」（二月払含む）	・クレジットカード会社等	**PCI DSS準拠 同等以上**	改善命令・罰金 報告徴収・立入検査等
２号　・・・ 加盟店　（旧法３号） 「クレジットカード等購入あっせん関係販売業者」 「クレジットカード等購入あっせん関係役務提供事業者」	**令和２年改正で追加**	**非保持** または、PCI DSS準拠	改善命令・罰金なし 報告徴収・立入検査
３号　・・・ アクワイアラー　（旧法２号） 「立替払取次業者」	・クレジットカード会社等	**PCI DSS準拠 同等以上**	改善命令・罰金 報告徴収・立入検査等
４号　・・・決済代行業者 「立替払取次業者（３号）のために、加盟店に対して、立替金の交付を行う事業者」	・**決済代行業者**（ネット取引、対面取引双方） ・EC モール事業者	**PCI DSS準拠 同等以上** ※対面は、非保持可	改善命令・罰金 報告徴収・立入検査
５号　・・・利用者向け決済サービス 「利用者から提供を受けたクレジットカード番号等を用いて、次回以降、当該クレジットカード番号等を入力することなく、商品購入等を行うことができるサービスを提供する事業者」	・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 その他名称の如何にかかわらず、クレジットカード情報と紐づけた他の決済用番号で決済を行う事業者	**PCI DSS準拠 同等以上**	改善命令・罰金 報告徴収・立入検査
６号　・・・利用者向け決済サービス委託先 「第５号の事業者が提供する決済サービスについてクレジットカード番号等の管理を受託する事業者」	・第5号事業者からクレジットカード情報の管理を受託している事業者	**PCI DSS準拠 同等以上**	改善命令・罰金 報告徴収・立入検査
７号　・・・加盟店向け決済システム提供事業者 「後払い決済において、立替払取次業者にクレジットカード番号等を提供する事業者」（２号に対し提供）	・決済代行業者（ネット取引、リアル取引双方） ・EC システム提供会社 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	**PCI DSS準拠 同等以上**	改善命令・罰金 報告徴収・立入検査

割賦販売法（後払分野）に基づく監督の基本方針

経済産業省HPより引用

- 監督の基本方針は、信用購入あっせん業者（イシュアー）、クレジットカード番号等取扱業者（クレジットカード会社・PSP等・加盟店）及びクレジットカード番号等取扱契約締結事業者（アクワイアラー等）が、割賦販売法に基づき実施するべき取組を明示し、これら事業者による適切な業務運営を促進することを目的として策定したもの。
- 「クレジットカード番号等の適切な管理」について、技術的な指針として「クレジットカード・セキュリティガイドライン」を引用する他、漏えい等の事故発生時の体制整備を求めている。

監督の基本方針の構成

第１章　信用購入あっせん業者等の監督に関する基本的考え方

第２章　信用購入あっせん業者等に対する監督
〇クレジットカード番号等の適切な管理等
・クレジットカード番号等取扱業者対応項目
（クレジットカード会社・PSP等・加盟店）
・クレジットカード番号等取扱契約締結事業者対象項目
⇒ 加盟店調査及び措置
・委託先の管理

第３章　検査

「クレジットカード番号等の適切な管理」の実現手段・方法

- 最新の技術動向等を踏まえて毎年見直しが行われる**「クレジットカード・セキュリティガイドライン」**に掲げられる措置が実務上の指針となっている
- **同ガイドラインに掲げる措置又はそれと同等以上の措置**を講じている場合には「必要かつ適切な措置」が講じられているものと認められる（性能規定）

「クレジットカード番号等の適切な管理」のための体制の整備規程

クレジットカード番号等の適切な管理に係る体制整備（加盟店以外）

（１）社内規則等の整備
（２）責任部署及び責任者の設定
（３）クレジットカード番号等の漏えい等の事故が発生した場合等における対応
対応部署を決定
事故の状況の把握
当該事故の発生状況に応じた事故の拡大防止措置の実施
事故の対象となるクレジットカード番号等の速やかな特定
事故の原因を究明するための調査の速やかな実施のための体制の整備
デジタルフォレンジック調査等の調査を実施する体制の整備
（４）不正利用検知モニタリングの実施やクレジットカード番号等の差し替え等の必要な措置
（５）類似の漏えい等の事故を再発防止するための措置の検討
（６）関係事業者への連絡体制の整備
事故発生時に迅速かつ適切な対応を実施するよう役職員に周知
（７）クレジットカード番号等の取扱いを外部委託する場合の委託先への指導及び監督
（８）委託先における漏えい等の事故等の場合の対応部署の明確化　等

クレジットカード番号等の適切な管理に係る措置事項（加盟店）

- クレジットカード番号等の管理者を限定する等、自社の役職員によるクレジットカード番号等の不正な取扱いを防止するための措置を講じる

クレジットカード・セキュリティガイドライン

経済産業省HPより引用

- **割賦販売法に規定するセキュリティ対策の「実務上の指針」**として位置づけられる「クレジットカード・セキュリティガイドライン」は、クレジット取引セキュリティ対策協議会において毎年度改定（令和４年３月８日　3.0版改定）。漏えい対策を担う**クレジットカード番号等取扱業者**の定義を明確化するほか、ECサイトでの本人認証として、EMV 3-Dセキュアを推奨。
- 新たな取組として、新規の加盟店契約時にアクワイアラーやPSPが、契約主体によるクレジットカード・セキュリティガイドラインに定める対策の実施状況を確認するといった取組の実施を検討中。

１．クレジットカード情報保護対策分野

〇対加盟店
クレジットカード情報の「非保持化」
脆弱性対策、ウイルス対策、管理者権限の管理、デバイス管理等の漏えい防止対策の実施

〇対クレジットカード会社、決済代行会社・ECシステム提供会社等
PCI DSS準拠

２．不正利用対策分野

１）クレジットカード・決済端末のIC化
⇒ 加盟店でのPIN（暗証番号）入力のスキップ機能の廃止（2025年3月までに実施）

２）EC取引におけるクレジットカード情報の不正利用対策

〇対EC加盟店
不正利用リスクに応じたEMV3-Dセキュア等の本人認証、券面認証（セキュリティコード）、不正検知システム、不正配送先データベースの照合等の不正利用対策の多面的・重層的な実施

〇対決済代行会社等
EMV3-Dセキュア等の本人認証、券面認証（セキュリティコード）、不正検知システム、不正配送先データベースの照合等の不正利用対策のEC加盟店への提供体制の構築及び導入の推進

〇対クレジットカード会社（イシュアー）
EMV3-Dセキュアの導入、固定パスワードからワンタイムパスワードへの移行、生体認証等のデバイス認証の導入、不正利用検知システムの精度向上・強化、クレジットカード利用時のクレジットカード会員へのメールやアプリ等による通知の実施

〇対クレジットカード会社（アクワイアラー）
EC加盟店への不正利用対策（EMV3-Dセキュアを含む）の導入に関する指導、情報共有

３．消費者及び事業者等への周知・啓発について

〇フィッシングの被害に遭わないための取組　等

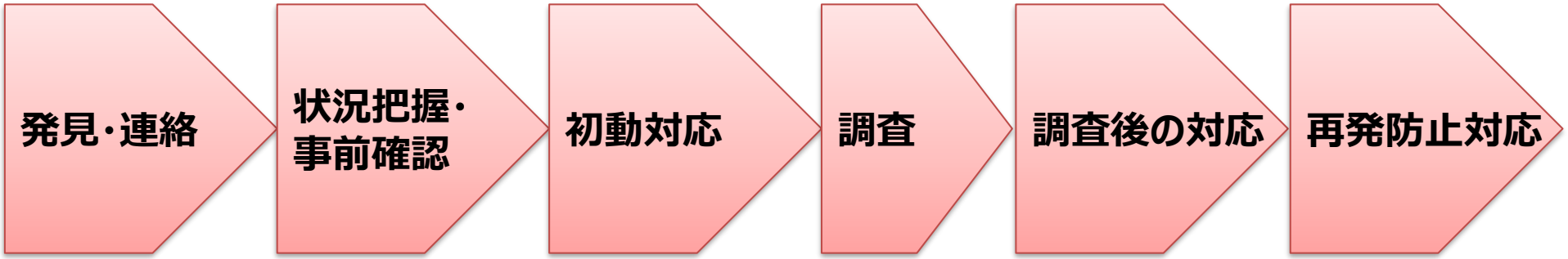
経済産業省HPより引用

（追補）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

- 「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。

個人情報保護法：信用分野ガイドライン

経済産業省HPより引用

- クレジットカード会社（イシュアー）は要保護性の高い個人信用情報を保有していることから、個人情報保護法に基づく通則ガイドラインに加え、格別の措置として信用分野ガイドラインに基づく措置が求められている。

信用分野ガイドラインの概要

根拠	信用分野（物品又は役務の取引に係る信用供与に関する分野）における事業者の取り扱う信用情報が「**個人の権利利益の一層の保護を図るため特にその適正な取扱いの厳格な実施を確保する必要がある個人情報**」であることから、ガイドラインで特別な措置を行う必要性があるため（個人情報保護法第６条）
対象	与信事業者（自社割賦業者、ローン提携販売業者、包括信用購入あつせん業者、個別信用購入あつせん業者等）
成立	平成28年（令和４年４月１日に改正）
所管	個人情報保護委員会・経済産業大臣連名告示（官報掲載）

個人情報保護委員会から経済産業省への権限委任措置の概要

権限委任内容	報告徴収、立入検査等。加えて、令和２年改正個情法により**個人データの漏えい等の報告**も追加。
対象	包括信用購入あつせん業者・個別信用購入あつせん業者・認定割賦販売協会・指定信用情報機関

信用分野ガイドラインにおける措置内容

信用分野ガイドラインにおける措置内容	令和２年改正に関する記載事項
• 機微（センシティブ）情報を取得・利用・第三者提供できる場合を限定 • 利用目的の通知、第三者提供において本人の同意を得る場合等には、原則として書面による • 個人の支払能力に関する情報を個人信用情報機関へ提供する場合はオプトアウト※を用いない（いずれも努力義務）等	• 外国にある第三者への提供を本人同意に基づいて行う場合、書面によるものとする（努力義務） • 法律で定める報告が必要な場合における個人データの漏えい等は、経済産業省に対して報告を行う　等

※ 機微（センシティブ）情報 ・・・ 労働組合への加盟、門地及び本籍地等
※ オプトアウト ・・・ 本人の求めがあれば事後的に停止すること等を前提に、本人の同意なく個人データを提供すること

サイバーセキュリティ基本法：重要インフラ事業者／クレジットCEPTOARの取組

経済産業省HPより引用

- **「サイバーセキュリティ基本法」**に基づく「第3次行動計画（平成26年5月）」で、「情報システムが障害に至った場合、**国民生活・社会経済活動に多大な影響を及ぼすおそれがある**」として、**クレジット分野**は**「重要インフラ」に指定。**
- クレジット分野における重要インフラ事業者（クレジットCEPTOAR）に対するガイドライン**「情報セキュリティガイドライン」**では、クレジット決済サービスの遅延・停止やクレジットカード情報の大規模漏えい発生防止を目的として、**安全基準等の整備や障害発生時の対応・行政への報告**を規定。

クレジットCEPTOAR ※ 情報セキュリティガイドラインにより、サイバー攻撃を想定した訓練等取組を実施

- クレジットカード会社(39社)、決済代行会社(9社)、決済ネットワーク事業者(2社)の**合計50社**で構成（令和４年6月現在）
- 活動目標：サイバー攻撃により、クレジットカード決済システムが機能不全となり、クレジットカード決済サービスの遅延・停止、クレジットカード情報の大規模漏えいが発生しないこと。

情報セキュリティガイドラインに基づく取組のポイント

Ⅰ　安全基準等の整備

①**セキュリティ管理態勢の整備**（サイバー攻撃への監視・対応体制、報告・広報体制、情報収集・共有体制等）

②**サイバー攻撃に備えた多層防御策**

- **入口対策**（ファイアウォール設置、抗ウィルスソフトの導入等）
- **内部対策**（特権ID・パスワードの適切な管理、不要なIDの削除等）
- **出口対策**（通信ログ等の取得・分析、不適切な通信の検知・遮断等）

③ネットワークへの**脆弱性診断**とセキュリティ水準の定期的評価等の実施

④サイバー攻撃を想定した**訓練**の実施

⑤サイバーセキュリティに係る**人材の育成・拡充**等に関する計画策定と実施

Ⅱ　障害発生時の対応

- クレジットカード決済システムにおいて**「サイバーセキュリティ事案」が発生**した場合、重要インフラ事業者は、**被害の拡大を防止**するため、発生したサイバーセキュリティ事案に応じた**適切な対応を迅速に講じること**。
- 発生した**システム障害の内容・発生原因、復旧見込等を公表**し、顧客からの問合せ対応のため、必要に応じ、**コールセンター等の体制**を迅速に整備。
- システム障害の**原因究明**、**復旧までの影響調査**、**改善措置**、**再発防止策**等を講ずること。

Ⅲ　行政への報告

- **サイバーセキュリティ事案が発生**した場合には、**経済産業省に報告**（緊急を要する場合には、NISCに報告）。
- 平日夜間・休日時にも経済産業省担当者、日本クレジット協会担当者、関係事業者等が緊急連絡をとれる体制を整備。

（注）サイバーセキュリティ事案とは、情報通信ネットワークや情報システム等の悪用により、サイバー空間を経由して行われる不正侵入、情報の窃取、改ざんや破壊、情報システムの作動停止や誤作動、不正プログラムの実行やDDoS攻撃等の、いわゆる「サイバー攻撃」により、サイバーセキュリティが脅かされる事案をいう。

※CEPTOAR(セプター)：重要インフラ事業者等の情報共有・分析機能及び当該機能を担う組織を、英語名称（Capability for Engineering of Protection, Technical Operation, Analysis and Response）の略称。
クレジットCEPTOAR運営会議の事務局は日本クレジット協会（2014年４月～）。

（追補）重要インフラのサイバーセキュリティに係る行動計画の改定

経済産業省HPより引用

- **「重要インフラのサイバーセキュリティに係る行動計画」**が令和４年６月１７日に改定（改定前は「重要インフラの情報セキュリティ対策に係る第４次行動計画」）。
- 割賦販売法上の指定信用情報機関である指定信用情報機関（CIC）が重要インフラ事業者に追加。

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 サイバーセキュリティ戦略本部決定）の概要

1. 第４次行動計画における有効な取組は継続

2. サイバーセキュリティ基本法が公布・施行されたことを踏まえて対応

- ✓題名を「重要インフラのサイバーセキュリティに係る行動計画」へ
  - 「情報セキュリティ対策」から「サイバーセキュリティ」へ
- ✓行動計画はサイバーセキュリティ基本法に基づき策定することを明示
- ✓「サイバーセキュリティ」の定義を明確化
  - サイバーセキュリティ基本法第２条に規定する「サイバーセキュリティ」をいう
    電磁的方式による情報の安全管理のために必要な措置並びに情報システム及び情報通信ネットワークの
    安全性及び信頼性の確保のために必要な措置が講じられ、その状態が適切に維持管理されていること
- ✓関係主体の責務を明確化
  - 「国」、「地方公共団体」、「重要インフラ事業者」、「サイバー関連事業者その他の事業者」

3. 障害対応体制の強化の在り方を抜本的に見直し

- ✓現在の「経営層への働きかけ」から、組織統治にサイバーセキュリティを組み入れる方針を具体的に記載

経営層、CISO、戦略マネジメント層、システム担当者を含めた組織全体での対応の促進

サイバーセキュリティ体制が適切でなく情報漏えい等の損害が生じた際、経営層は損害賠償責任を問われ得る

4. 将来の環境変化を先取り

- ✓サプライチェーン等を含め包括的に対応

別紙１ 対象となる重要インフラ事業者等と重要システム例（抜粋）

重要インフラ分野	対象となる重要インフラ事業者等	対象となる重要システム例
クレジット	・主要なクレジットカード会社 ・主要な決済代行業者 ・指定信用情報機関 等	・クレジット(包括信用購入あっせん及び二月払購入あっせん)に係る決済システム ・信用情報提供・収集システム

（参考）サイバーセキュリティ体制構築・人材確保の手引き

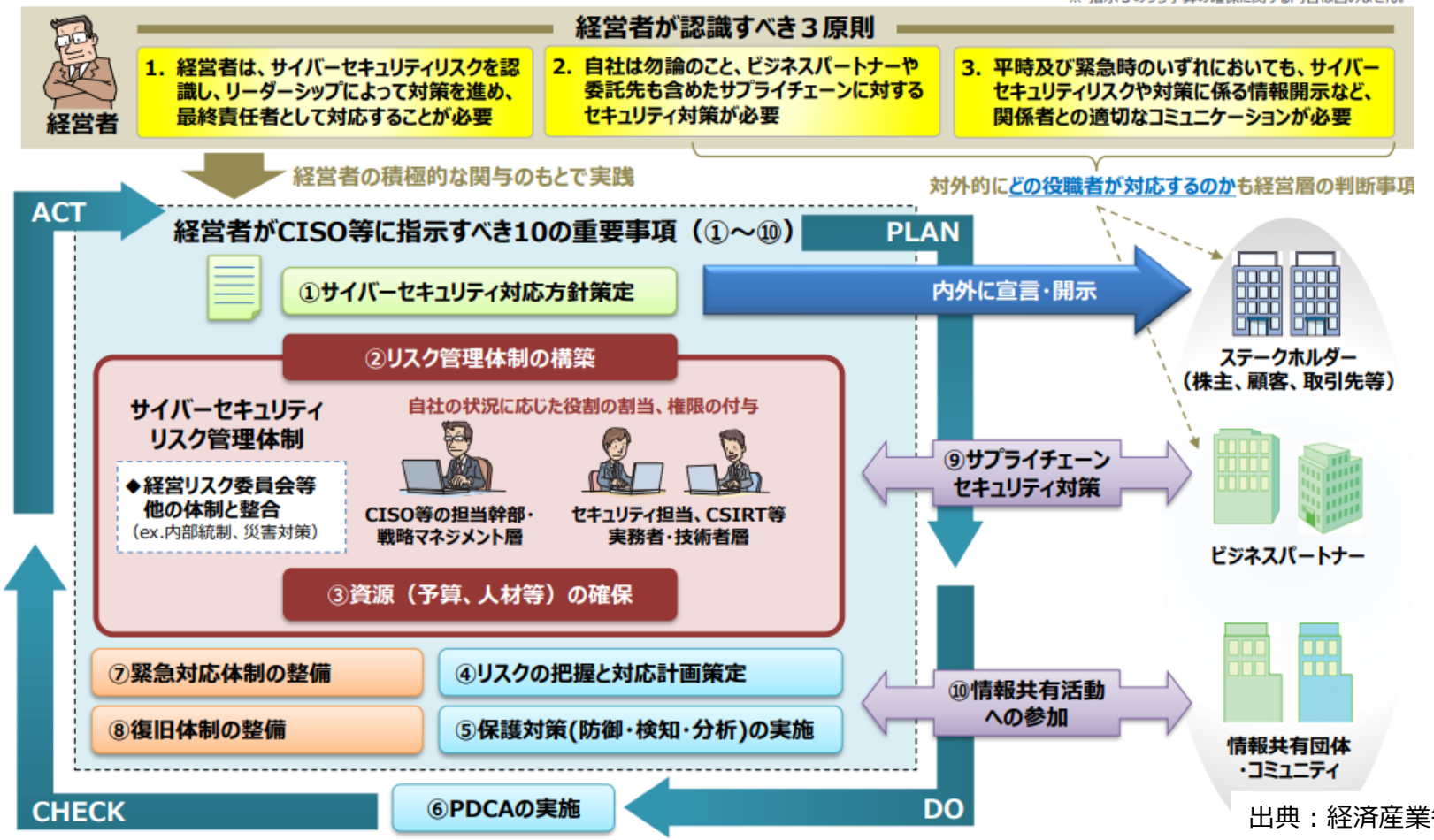
経済産業省HPより引用

- 「サイバーセキュリティ経営ガイドライン」（経済産業省・情報処理推進機構策定）において示されている重要１０項目のうち、**「サイバーセキュリティリスク管理体制の構築」、「サイバーセキュリティ対策のための資源（予算、人材等）確保」**についての参考文書。**令和４年６月１５日に改定。**

サイバーセキュリティ経営ガイドラインの全体像における手引きの位置付け

企業におけるサイバーセキュリティ対策の推進において、その基盤となる下図の赤枠部分（「リスク管理体制の構築」と「資源（予算、人材等）の確保」）は経営者が積極的に関わって実践すべき取組。『サイバーセキュリティ体制構築・人材確保の手引き』はその具体的検討のための参考文書。※

※ 指示３のうち予算の確保に関する内容は含みません。



出典：経済産業省HP

（追補）経済安全保障への対応

経済産業省HPより引用

- 経済活動に関して行われる国家及び国民の安全を害する行為を未然に防止する重要性が増大していることに鑑み、経済安全保障推進法が成立（令和４年５月11日）。
- クレジットカード業は基幹インフラとして、指定された事業者は、サービスの安定的な提供の確保のため、重要設備の導入・維持管理等の委託をする際は、国の事前審査が必要となる。

1．基本方針の策定 等（第１章）

・経済施策を一体的に講ずることによる安全保障の確保の推進に関する基本方針を策定。
・規制措置は、経済活動に与える影響を考慮し、安全保障を確保するため合理的に必要と認められる限度において行わなければならない。

2．重要物資の安定的な供給の確保に関する制度（第２章）

国民の生存や、国民生活・経済活動に甚大な影響のある物資の安定供給の確保を図るため、特定重要物資の指定、民間事業者の計画の認定・支援措置、特別の対策としての政府による取組 等を措置。

特定重要物資の指定	事業者の計画認定・支援措置	政府による取組	その他
・国民の生存に必要不可欠又は国民生活・経済活動が依拠している物資で、安定供給確保が特に必要な物資を指定	・民間事業者は、特定重要物資等の供給確保計画を作成し、所管大臣が認定 ・認定事業者に対し、安定供給確保支援法人等による助成やツーステップローン等の支援	・特別の対策を講ずる必要がある場合に、所管大臣による備蓄等の必要な措置	・所管大臣による事業者への調査

3．基幹インフラ役務の安定的な提供の確保に関する制度（第３章）

基幹インフラの重要設備が我が国の外部から行われる役務の安定的な提供を妨害する行為の手段として使用されることを防止するため、重要設備の導入・維持管理等の委託の事前審査、勧告・命令 等を措置。

審査対象	事前届出・審査	勧告・命令
・対象事業：法律で対象事業の外縁（例：電気事業）を示した上で、政令で絞り込み ・対象事業者：対象事業を行う者のうち、主務省令で定める基準に該当する者を指定	・重要設備の導入・維持管理等の委託に関する計画書の事前届出 ・事前審査期間：原則30日（場合により、短縮・延長が可能）	・審査の結果に基づき、妨害行為を防止するため必要な措置（重要設備の導入・維持管理等の内容の変更・中止等）を勧告・命令

4．先端的な重要技術の開発支援に関する制度（第４章）

先端的な重要技術の研究開発の促進とその成果の適切な活用のため、資金支援、官民伴走支援のための協議会設置、調査研究業務の委託（シンクタンク） 等を措置。

国による支援	官民パートナーシップ（協議会）	調査研究業務の委託（シンクタンク）
・重要技術の研究開発等に対する必要な情報提供・資金支援等	・個別プロジェクトごとに、研究代表者の同意を得て設置 ・構成員：関係行政機関の長、研究代表者/従事者 等 ・相互了解の下で共有される機微情報は構成員に守秘義務	・重要技術の調査研究を一定の能力を有する者に委託、守秘義務を求める

5．特許出願の非公開に関する制度（第５章）

安全保障上機微な発明の特許出願につき、公開や流出を防止するとともに、安全保障を損なわずに特許法上の権利を得られるようにするため、保全指定をして公開を留保する仕組みや、外国出願制限 等を措置。

技術分野等によるスクリーニング（第一次審査）	保全審査（第二次審査）	保全指定	外国出願制限
・特許庁は、特定の技術分野に属する発明の特許出願を内閣府に送付	①国家及び国民の安全を損なう事態を生ずるおそれの程度 ②発明を非公開とした場合に産業の発達に及ぼす影響 等 を考慮	・指定の効果：出願の取下げ禁止、実施の許可制、開示の禁止、情報の適正管理 等	補償

施行期日

・①審査対象 公布後１年６月以内 ②審査・勧告・命令 公布後１年９月以内
（対象事業者の指定から６月間は経過措置として適用を開始しない）

経済産業省HPより引用

2．共通対策

クレジットカード番号保護のための国際基準（PCI DSS）

漏えい防止

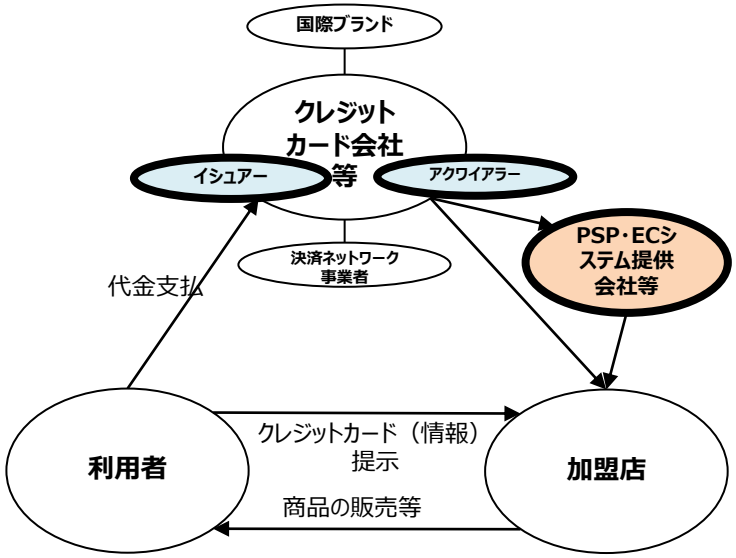
経済産業省HPより引用

- PCI DSSは、国際ブランドが策定するクレジットカードの取扱いにおけるセキュリティ基準。割賦販売法「クレジットカード番号等の適切な管理」規定の実務上の指針となっているクレジットカード・セキュリティガイドラインにおいて、技術的基準として規定している。

PCI DSSとは

- クレジット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
  (Payment Card Industry Data Security Standard の略)
- 安全なネットワークの構築やクレジット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

準拠が必要な者（太枠）



参考：PCI DSSの改訂について

- 2022年3月に、9年ぶりのメジャーバージョンアップとなる「PCI DSS v4.0」が公開。
- 現時点版であるPCI DSSv3.2.1の有効期限は2024年３月31日であり、それまでは移行期間としてどちらでも準拠可能。（**移行期間は2025年３月31日まで**）
- 以下のような内容が追加されている。
  - オンラインスキミングやフィッシングなどへの新しい攻撃手法への対応
  - クラウドサービスを利用した準拠に関する考え方の整理　等

EC決済における本人認証手法（EMV 3-Dセキュア）

経済産業省HPより引用

不正利用防止

- ３Ｄセキュアとは、**EC加盟店における**不正利用防止のため、**クレジットカード利用者の本人認証**を行う手法であり、あらかじめ登録した**パスワードによって**本人認証を行う。
- 2022年10月よりサービスが終了し、**EMV 3-Dセキュア**に代替される。

３Ｄセキュアとは

- EC加盟店でのクレジットカード決済の際に、**利用者があらかじめイシュアーに登録したパスワードにより本人認証を行う**方法
- 1999年にVISAがインターネット取引での本人認証の強化を目的とし3Dセキュアを発表
- VISAが2002年に3Dセキュアの仕様公開・ライセンス提供(無償)を行い、他ブランド（MasterCard、JCB、AMERICAN EXPRESS、DISCOVER・Diners、UnionPay）も3Dセキュアを採用
  ※「３-D」は、イシュアードメイン（利用者、イシュアー）、アクワイアラードメイン(加盟店、PSP、アクワイアラー)、相互運用ドメイン（国際ブランド）の３つのドメインを表す
- 3Dセキュアは2022年10月でサービスが終了し、**EMV 3-Dセキュアに代替**
- 欧州等では、すでにPSD2（欧州決済サービス指令第2版）における強力な本人認証としてSCA(Strong Customer Authentication)が義務化されており、SCAの対応策としての3Dセキュア導入が進展

各ブランドの3DSのサービス名称

VISA SECURE / mastercard ID Check / AMERICAN EXPRESS SafeKey / JCB J/Secure / DISCOVER / Diners Club INTERNATIONAL / ProtectBuy / UnionPay 銀联 UnionPay 3D Secure 2.0

参考： EMVCo EMV 3-D Secure https://www.emvco.com/emv-technologies/3d-secure/

経済産業省HPより引用

不正利用防止

EC決済における本人認証手法（EMV 3-Dセキュア）

- EMV 3-Dセキュアは、従来の３Dセキュアの更新版。パスワードの入力負荷の軽減やユーザビリティーの改善により、クレジットカード決済時の離脱（カゴ落ち）リスクの改善が見込まれる。

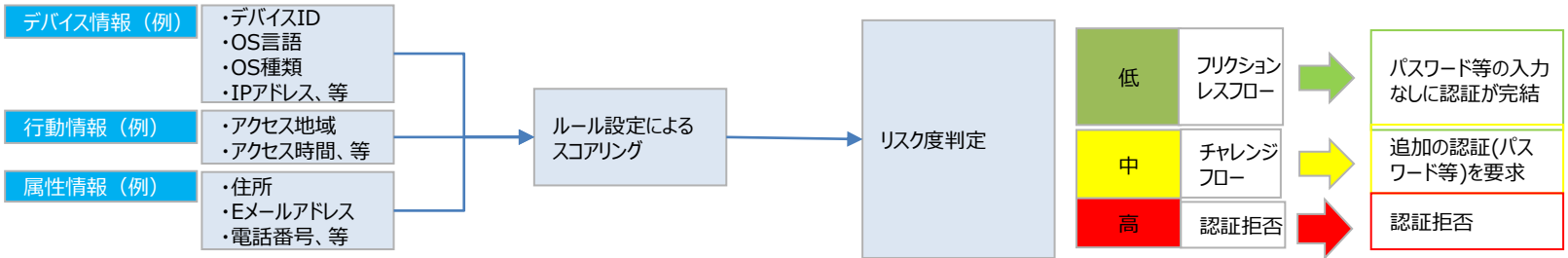
旧３DセキュアとEMV ３-Dセキュアの比較

旧3Dセキュア（2022年10月サービス終了）
全取引にパスワードを毎回入力
固定パスワードで一律認証
ブラウザ取引のみ

EMV 3-Dセキュア			
特長	内容	メリット	
		会員	加盟店
パスワード入力負荷を低減	・原則リスクベース認証※のみとなり、会員へのパスワード要求が不要（フリクションレス）	入力負担軽減	取引離脱リスクの減少（カゴ落ちリスクの減少）
ワンタイムパスワードによる本人認証	・中リスク判定時のみワンタイムパスワードなどによる追加認証を実施	パスワード漏洩による不正リスクの軽減	会員のパスワード忘れによる機会損失の軽減
スマホアプリへの対応	・ブラウザに加え、スマートフォンやタブレットのアプリ内決済に対応	利便性向上	認証ツールの拡大

※参考：リスクベース認証

ネット通販で使用されるパソコンやスマートフォンにおける機器やネットワークの情報から不正使用を判定する手法。
認証（スコアリング）によるリスク度判定によって、認証処理が異なる。

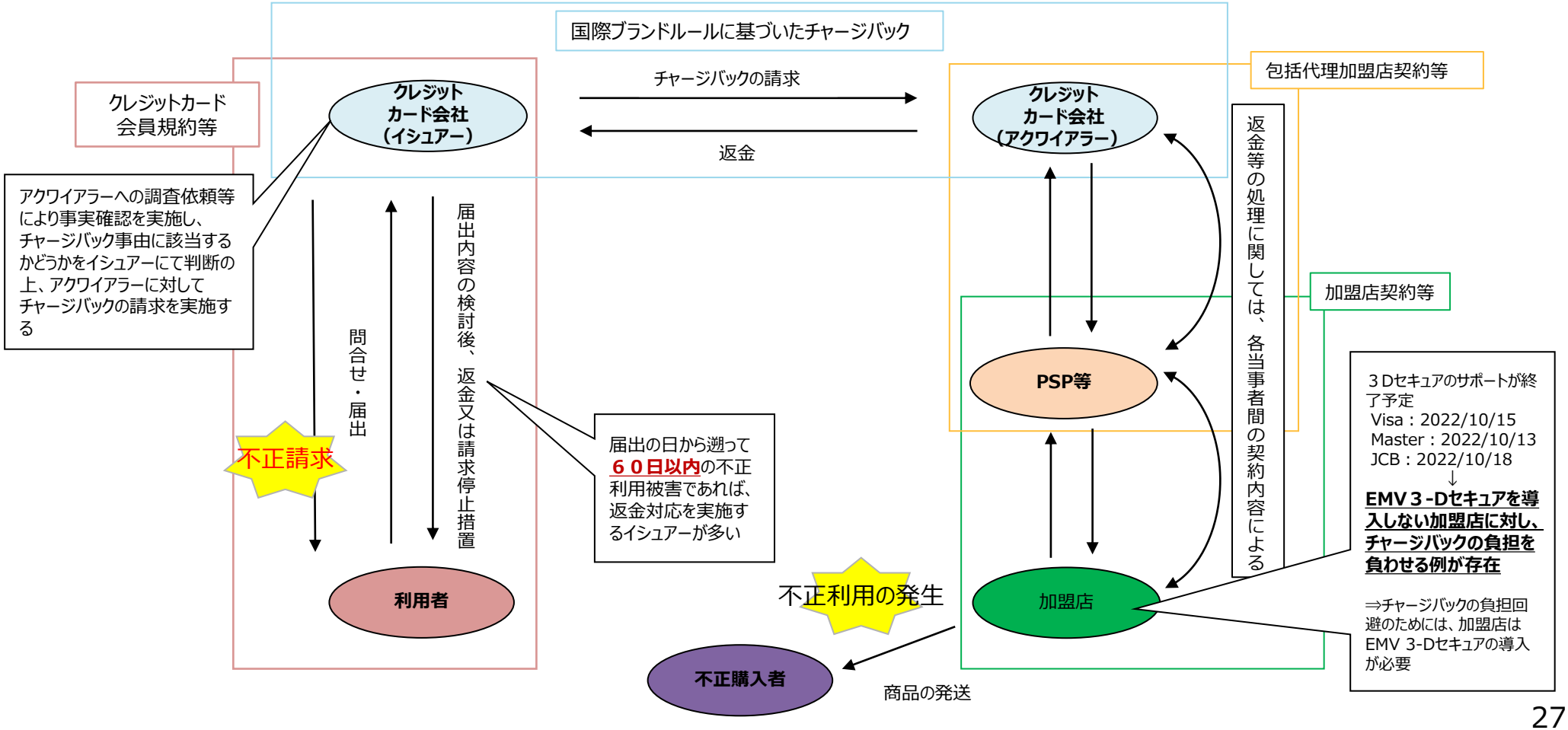


出典：クレジット取引セキュリティ対策協議会
「EMV 3-Dセキュア導入ガイド」

（参考）不正利用発生時の加盟店負担（EMV 3-Dセキュアの導入必要性の例）

経済産業省HPより引用

- クレジットカードの不正利用が発生した場合における決済額の補償処理は、①イシュアー・利用者間での返金等の処理、②イシュアー・アクワイアラー間でのチャージバック（代金返還）の処理、③アクワイアラー側（アクワイアラー・PSP等・加盟店）での返金等の処理に分けられる
- 加盟店が負担するかどうかは各当事者間の契約内容による。ただし、セキュリティ対策としてEMV 3-Dセキュアを導入しない加盟店に対しては、チャージバックの負担を負わせる規約としているアクワイアラーも存在。**<u>加盟店においては、セキュリティ対策を強化（EMV ３-Dセキュアの導入）することで、負担を回避することが出来る。</u>**



フィッシング被害防止対策

周知・犯罪防止

経済産業省HPより引用

- フィッシング被害防止対策としては、①なりすましをされる側であるクレジットカード会社等・加盟店における取組②利用者における自衛の取組③関係省庁・団体等における周知啓発や情報収集等を通し、総合的に取り組むべき。

▌クレジットカード会社等

クレジットカード会社等においては、**クレジットカード会員サイト等**を模したフィッシング対策を防止することが必要
⇒**利用者とのやりとりの工夫やフィッシング対策サービスの利用、関係者への情報連携**

- メールドメイン認証
- SMS等に添付するURLの連携から専用アプリへ
- フィッシング対策サービスを提供する事業者の利用
- フィッシング事案を受領したら、警察や業界団体・利用者に通知

⇒P.34

▌加盟店

加盟店においては、**商品販売サイトや会員サイト等**を模したフィッシング被害を防止することが必要
⇒（クレジットカード会社と対策は類似）**利用者とのやりとりの工夫やフィッシング対策サービスの利用、関係者への情報連携**

- メールドメイン認証
- SMS等に張り付けるURLからの連携防止
- フィッシング対策サービスを提供する事業者の利用
- フィッシング事案を受領したら、警察や業界団体・利用者に通知

⇒P.41

▌利用者

利用者においては、自衛策として**クレジットカード情報を安易に入力しない**ことが大切
信頼出来るサイトやアプリからのみクレジットカード情報を取り扱う意識を持つ

- パソコンやモバイル端末は、安全に保つ
- 不審なメールに注意する
- 電子メールに記載されたリンクはクリックしない
- 不審なメールやサイトは報告する
- クレジットカード会社・加盟店の連絡先リストを作る

⇒P.50

▌関係省庁・関係団体等

関係省庁・関係団体では、フィッシング被害の分析等と同時に、周知啓発・広報等にも取り組んできている
今後は、**より一層の協力関係の構築**が必要

経済産業省商取引監督課

警察庁サイバー警察局

日本クレジット協会（JCA）

フィッシング対策協議会

日本サイバー犯罪対策センター（JC3）

⇒P.59

（参考）フィッシングにおけるクレジットカード番号の被害

周知・犯罪防止
経済産業省HPより引用

- フィッシングとは、メールやSMS等を通じて、利用者から個人情報等（クレジットカード番号等を含む）をだまし取ること。不正利用に用いるクレジットカード番号の詐取が主な目的。

近年のクレジットカードの不正利用は、番号盗用が主な被害要因
番号盗用は、フィッシングによる被害がその原因の一つ

2021年クレジットにおける不正利用被害額に占める
番号盗用の割合は、94%である。

想定される番号盗用の原因

- クレジットマスター
  （クレジットカードを盗まず、他人のクレジットカード番号を割り出す）
- 加盟店等、事業者からの漏えい
- フィッシング
  （メールやSMSを通じて、利用者からクレジット情報等をだまし取る）

最終的にクレジットカード番号を詐取することを狙ったフィッシングが多い

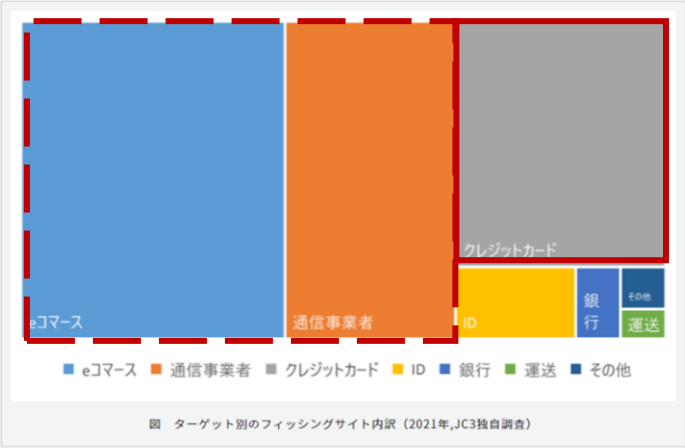


図　ターゲット別のフィッシングサイト内訳（2021年,JC3独自調査）

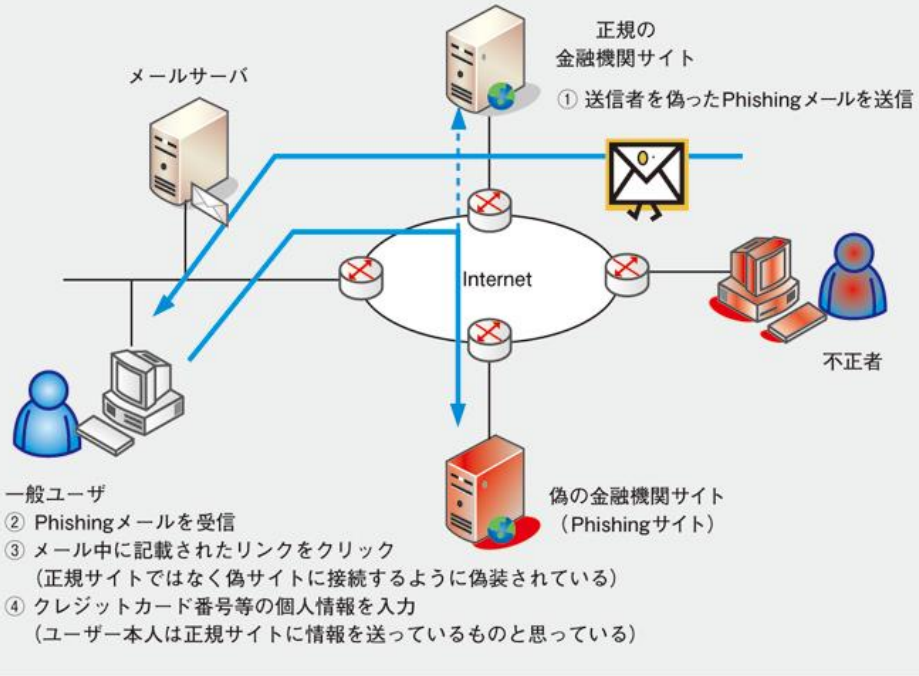
クレジットカード会社を装い、クレジットカード番号等を入力させる事例

クレジットカード番号を入力させることを目的の一つとしている、他事業種のフィッシング事例

出典：JC3「フィッシングターゲットの変遷」

メールやSMSを通じてクレジットカード番号等の情報をだまし取られ、最終的に不正利用に用いられる

フィッシングによる漏えいの構造



出典：フィッシング対策協議会HP

経済産業省HPより引用

３．個別対策

（１）クレジットカード会社

クレジットカード会社(イシュアー／アクワイアラー)におけるセキュリティに関する規定

漏えい防止
不正利用防止
経済産業省HPより引用

- クレジットカード会社におけるセキュリティ関係規制として、漏えい防止としてPCI DSSの準拠／不正利用防止としてモニタリング等が求められている

規定	漏えい等防止	不正利用防止
割賦販売法	クレジットカード番号等の漏えい、滅失又は毀損の防止その他のクレジットカード番号等の適切な管理のために必要な措置	
施行令・施行規則	• 漏えい等の事故の発生を防止するための措置 • 漏えい等の事故が発生した時等、状況把握、拡大防止、原因究明調査 • 類似の漏えい等の事故の再発防止策 • クレジットカードを消費者の利益の保護に欠ける方法で取り扱わない	• 漏えい等の事故が発生した時等において、利用者以外による漏えい等したクレジットカード番号での利用を防止するための措置
監督の基本方針	• 漏えい防止のための基準（クレジットカード・セキュリティガイドラインが実務上の指針）を満たす • 漏えい時における、情報連携や行政への報告体制の整備 • **ガイドラインに掲げる措置又はそれと同等以上の措置**を講じている場合には「必要かつ適切な措置」が講じられているものと認められる	• 漏えい等発生時に、**不正利用検知モニタリングの実施やクレジットカード番号等の差し替え等の必要な措置を実施**
クレジットカード・セキュリティガイドライン（実務指針）における記載	• **PCI DSS** に準拠し、これを維持・運用する	

クレジットカード会社におけるセキュリティに関する規定(加盟店調査)

漏えい防止
不正利用防止
経済産業省HPより引用

- クレジットカード会社のうち、**加盟店契約**を結ぶアクワイアラー等の事業者は「**クレジットカード番号等取扱契約締結事業者」として、**加盟店が講じる**セキュリティ対策の実施状況の確認**、加盟店への指導等**適切な対策の実施**の指導が求められる。

「クレジットカード番号等取扱契約締結事業者」に課される加盟店調査義務等

①初期調査（加盟店契約時）

- 加盟店の所在地・代表者、商材・役務内容、販売方法等
- **セキュリティ対策（クレジットカード番号等の適切な管理及び不正利用の防止）の実施内容**
- 苦情の発生状況、苦情処理のための体制　等

②途上調査（加盟店契約締結後）

- **セキュリティ対策の実施状況（情報漏えい、不正使用の発生状況等）**
- 悪質取引の有無（消費者トラブルの発生状況等）

③加盟店調査の結果に基づく必要な措置

- **法令で定める基準に適合しない加盟店に対する必要な措置**
  - ◇合理的な期間内に基準に適合するよう**指導すること**
  - ◇指導に従わないとき又は適合することが見込まれない場合、**加盟店契約を解除すること**

➡セキュリティ対策については、「クレジットカード・セキュリティガイドライン」に基づく取組を進めていくことが必要

不正利用防止のための取組事例（クレジットカード会社）

経済産業省HPより引用

不正利用防止

- クレジットカード会社における不正利用防止対策としてリアルタイムでのモニタリングが実施されている。大量のデータをAIにより処理し、不正検知の粒度を高めようとしている会社も存在。
- 不正利用検知システム等を基に、適正な取引であるか確認を行い、不正である場合にはクレジットカードの取引停止・交換等の対応を行う。

不正利用検知システムの利用

各クレジットカード会社は、オーソリゼーション（取引承認）において、独自で**不正利用モニタリングシステムを利用**しており、24時間・365日のモニタリングを通して、**不正検知**に努めている

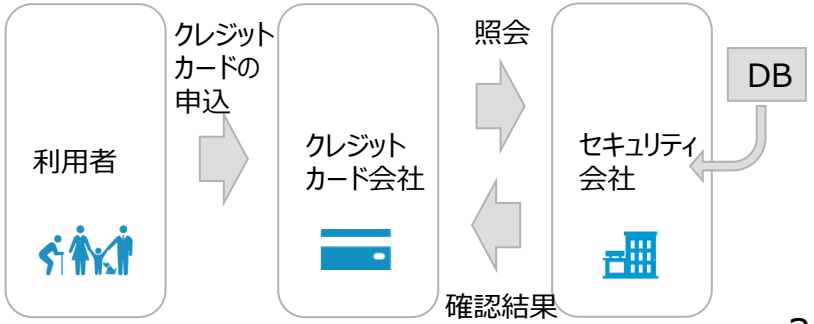
不正利用検知後の対応

不正利用モニタリングシステムを通した検知の結果、不正利用の可能性があると判明した取引におけるフローは一般的に以下の通り。

実際に利用を行ったか クレジットカード保有者に確認 → クレジットカード取引の停止処理 → クレジットカード交換等の対応

参考：クレジットカード購入時等における不正アクセス防止（本人確認）のためのサービス

- あるセキュリティ会社では、本人確認の方法の一つの要素として「電力設備情報」のデータベースを活用し、それをもとになりすまし検知サービスを提供。
- クレジットカード会社では、外部データ等も利用しながら、日々本人確認の精度向上となりすまし防止に努めている。



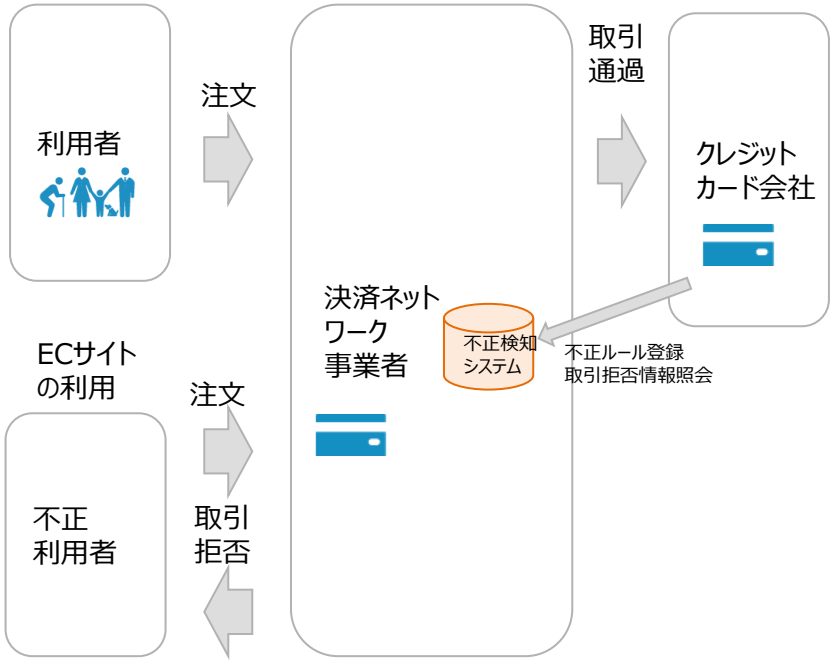
不正利用防止のための取組事例（決済ネットワーク事業者）

経済産業省HPより引用

不正利用防止

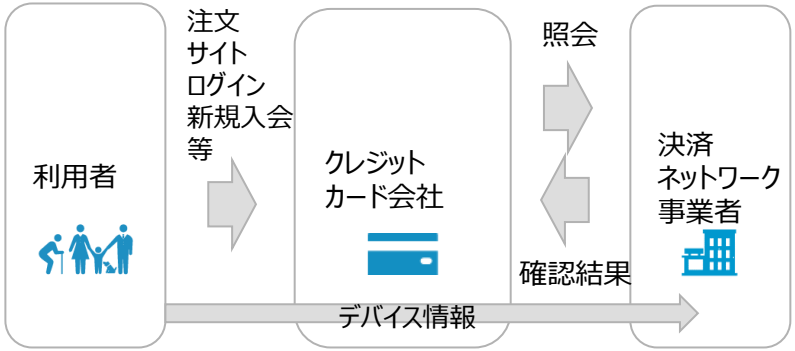
決済情報をもとにクレジットカード会社の代わりに不正取引検知

- クレジットカード取引における決済ネットワーク事業者は、利用者の加盟店での決済情報を、クレジットカード会社に向けて伝送する役割を果たす。
- ある大手決済ネットワーク事業者では、決済情報をシステムによって不正利用か判定するサービスを提供している。
- クレジットカード会社が、不正判定に当たってのルールを決済ネットワーク事業者に登録を行い、それをもとに判断を行う。また、不正取引として拒否となった取引については、クレジットカード会社が決済ネットワーク事業者に照会を行い、情報を得ることができる。これにより、不正検知のルールの向上につなげることができる。



クレジットカード会社等に届く注文情報やサイトログイン情報等もとに不正取引を検知

- 不正取引を精度高く検知するクラウドサービスを、クレジットカード会社等に提供している。
- 利用者自身からの操作であることを確認するため、操作する端末（パソコン、スマートフォン等）の情報と、取引情報と突合させることによって、属性・行動分析を実施している。



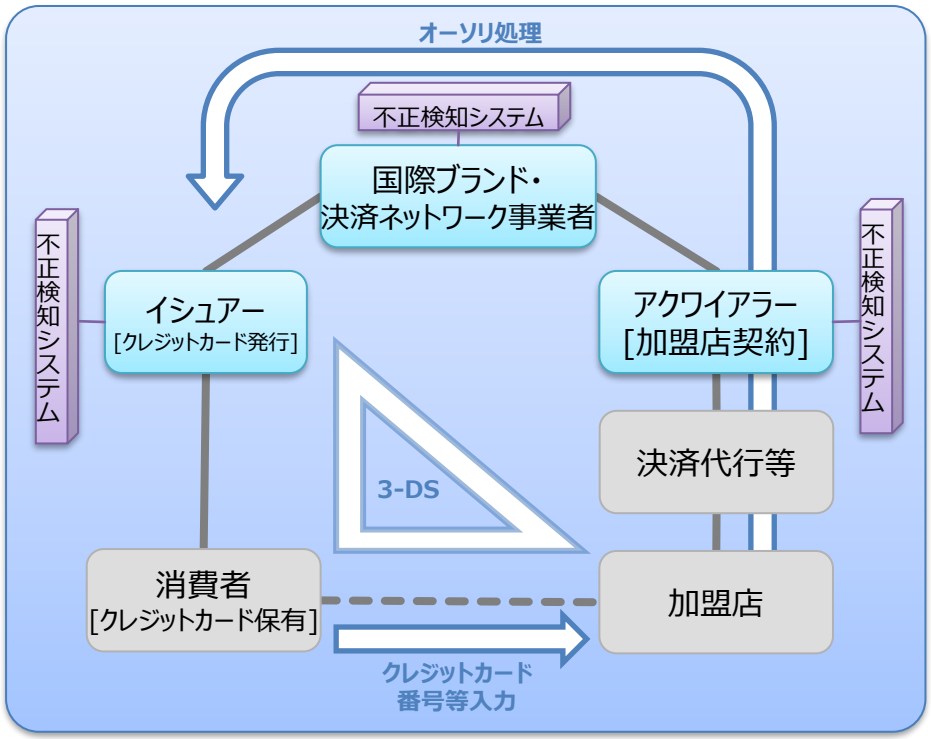
共同システムによる不正検知の可能性

経済産業省HPより引用

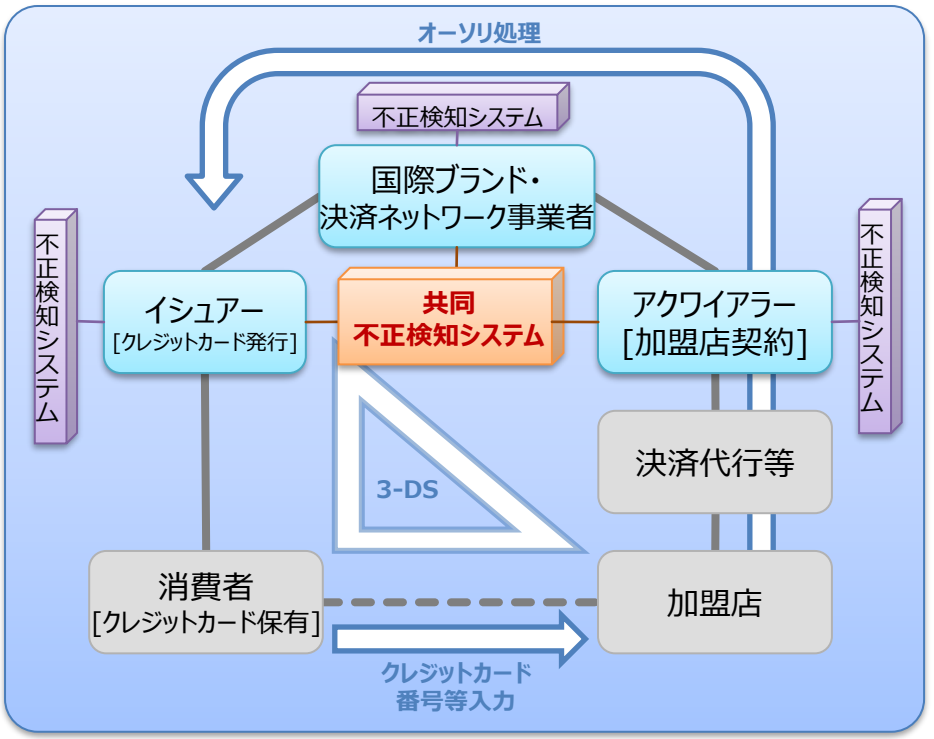
不正利用防止

- クレジット決済システム全体での不正検知能力の向上に向けて、個社で実施していた不正検知システムを共同化していくことが有効との考えがある。
- これまで各社が取り組んでいたノウハウやデータ等を共有することで、より高度な不正検知の実現を目指すことが期待される。

共同化前



共同化のイメージ



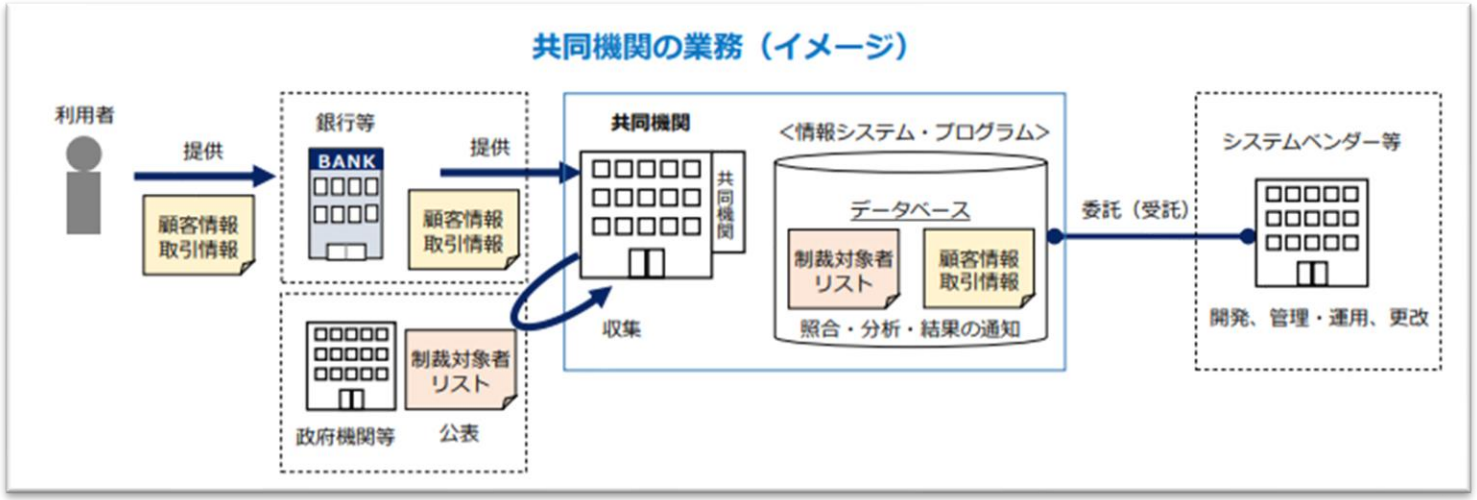
（参考）金融分野における共同システムの取組の参考例

経済産業省HPより引用

- 金融分野では、「為替取引分析業」の創設により、マネー・ローンダリング対策として共同システムの創設が検討されている。

為替取引分析業の創設

- 銀行等によるマネー・ローンダリング対策として、「取引フィルタリング」「取引モニタリング」について、システムを用いた高度化・効率化を図っていく必要がある。
- これらの業務の中核的な部分を共同化して実施する主体を為替取引分析業として、銀行等の委託を受けて、為替取引に関して業務を行うことを議論（令和４年通常国会）



出典：
金融審議会「資金決済ワーキング・グループ」（第２回）　（2021年11月11日）　金融庁説明資料

フィッシング対策のための取組事例（クレジットカード会社）

周知・犯罪防止
経済産業省HPより引用

- フィッシング対策のため、クレジットカード会社においては以下の取組がある。
  ①利用者とのコミュニケーション手段を工夫する
  ・メールドメイン認証を行い、受信者がフィッシングメールとのドメインの違いを区別できるようにする
  ・ウェブブラウザに遷移させるSMSの利用から、専用アプリにおけるやりとりへの移行を行う
  ②フィッシング対策サービスを提供する事業者を利用する
  ・フィッシングサイトの捜索やテイクダウン（サイトの取下げ依頼等）を委託する
- そのほか、クレジットカード会社を模したフィッシング事案等を発見した際は、警察・フィッシング対策協議会・JC3といった団体に報告するとともに、利用者に対して注意喚起を行うことも大切。

フィッシング対策としての具体的な取組事例

メールドメイン認証

- メール送信において、送信側（クレジットカード会社・加盟店）が**送信ドメイン認証技術**（例：SPF、DKIM及びDMARC等）の導入を行うことにより、認証されていないドメインからのメールに対して受信側が警告や受領拒否を行うことができるようになる。

SMS等に添付するURLの連携から専用アプリへ

- 日々のコミュニケーション手段として、SMSに事業者のURLリンクを利用者に送信し、URLを通して会員情報を入力させるやり方を続けると、類似のSMSを用意され、フィッシングの被害を誘発してしまう。
- 専用アプリ等を用いることで、利用者が安心して会員サイト等を利用することが出来る。

フィッシング対策サービスを提供する事業者の利用

- フィッシング対策サービスとして提供されているものの例
  - ✓ フィッシング検知
  - ✓ テイクダウン
    ホスティング・レジストラ事業者への削除依頼
    ブラウザ事業者への警告表示依頼（セーフブラウジング）　等
- クレジットカード会社は、フィッシング対策サービスを提供する事業者を利用することにより、効率的かつ実効的な対応ができる。

※ホスティング事業者・・・Webサーバやメールサーバの貸し付けを行う事業者
※レジストラ事業者・・・ドメインの取得を請け負う事業者

フィッシング事案を受領したら、警察や業界団体・利用者に通知

- フィッシング事案を認知した際に、テイクダウン（フィッシングサイトの削除申請）等につなげるためにも、警察・フィッシング対策協議会・JC３といった関係団体への通報を行う。
- また、利用者に対しても周知を行う。

出典：フィッシング対策協議会

経済産業省HPより引用

3．個別主体
（２）加盟店

加盟店におけるセキュリティに関する規定

経済産業省HPより引用

漏えい防止

不正利用防止

- 漏えい防止として非保持化、不正利用防止として対面でのIC対応・非対面での不正利用対策等が求められている。

規定	漏えい等防止	不正利用防止
割賦販売法	クレジットカード番号等の漏えい、滅失又は毀損の防止その他のクレジットカード番号等の適切な管理のために必要な措置	利用者による不正な利用を防止するために必要な措置
施行令・施行規則	• 漏えい等の事故の発生を防止するための措置 • 漏えい等の事故が発生した時等、状況把握、拡大防止、原因究明調査 • 類似の漏えい等の事故の再発防止策 • クレジットカードを消費者の利益の保護に欠ける方法で取り扱わない	• クレジットカード番号等の通知を受けたとき、当該通知が利用者によるものであるかの適切な確認 • 加盟店において不正利用されたとき、その発生状況を踏まえ、類似の不正利用を防止するための措置
監督の基本方針	• 漏えい防止のための基準（クレジットカード・セキュリティガイドラインが実務上の指針）を満たす	• 不正利用防止のための基準（クレジットカード・セキュリティガイドラインが実務上の指針）を満たす
クレジットカード・セキュリティガイドライン（実務指針）における記載	**・クレジットカード番号等の非保持化措置** ※ 保持等する場合は、非保持と同等/相当又はPCI DSS 準拠 （補足） ※４つの方策 １）本人認証　２）券面認証　３）属性・行動分析　４）配送先情報 ※高リスク商材取扱加盟店 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 ※不正顕在化加盟店 クレジットカード会社（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 EC 加盟店	**＜対面取引＞決済端末の全てを IC 対応** **＜非対面取引＞** • 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リスクや被害状況に応じた**非対面不正利用対策の導入**。 • 「高リスク商材取扱加盟店」での本ガイドラインが掲げる**４つの方策**の内1方策以上、「不正顕在化加盟店」は 2 方策以上の導入。

中小EC加盟店等におけるセキュリティ対策

漏えい防止

経済産業省HPより引用

- 加盟店のECサイトの構築（クラウド上での構築や、OSS（オープンソースソフトウェア）の利用等）にあたり、セキュリティ意識が低く十分なメンテナンスが行われないことによって、EC加盟店のサイトの脆弱性を狙った不正アクセスの対象となっている。
- 当省においてもOSSの一つであるEC-CUBEに脆弱性が存在するとして、加盟店に対する**注意喚起を実施**(令和元年12月）しているが、サイバー漏えい事案は、**約２割増加**。※（EC-CUBE関連は、**約４割増加**※）

※契約締結事業者からの商取引監督課への報告内容を基に、同一事案の重複を除外し、令和元年と令和2年を比較

- OSSの構築環境を随時検証し、的確な安全対策を行うよう呼びかけ。

EC-CUBEに関する注意喚起の掲載

経済産業省
Ministry of Economy, Trade and Industry

株式会社イーシーキューブが提供するサイト構築パッケージ「EC-CUBE」の脆弱性等について（注意喚起）

2019年12月20日

▶安全・安心

「EC-CUBE」の一部のバージョンには、クレジットカード番号等の漏えいの原因となる脆弱性等があることから、「EC-CUBE」を利用されているインターネットショップの皆様におかれましては、以下の点にご注意いただきますようお願いいたします。

本件概要

- 株式会社イーシーキューブが開発・提供するインターネットサイト構築パッケージ「EC-CUBE」の脆弱性等を突いたインターネットショップのサイトの改ざん等により、クレジットカード番号等が窃取されるといった被害が多発しております。
- 2019年現在までにインターネットショップが公表した漏えい事案において、約14万件のクレジットカード番号等が漏えいしていることが確認されております。
- このような甚大な被害が発生している状況に鑑み、インターネットショップの皆様におかれましては、「EC-CUBE」のご利用状況について再度検証を行い、ご利用を継続する場合には、的確な安全対策を行ってください。
- ご対応についてご不明な点がありましたら、下記の問い合わせ窓口までご連絡ください。

【本件に関するお問い合わせ窓口】

株式会社イーシーキューブ

電話：06-4795-7506

受付時間：10時～12時、13時～17時 土曜日、日曜日・祝日及び年末年始を除く

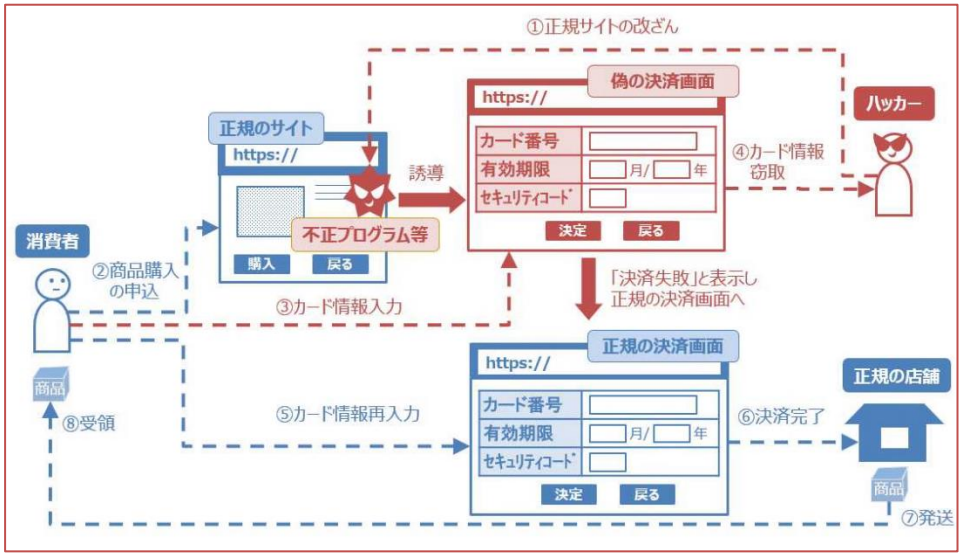
イーシーキューブ ホームページ

※本件に関する詳細は以下をご覧ください

- イーシーキューブ：サイト改ざんによるクレジットカード流出被害が増加しています

出典：経済産業省HP

ECサイトの脆弱性を狙った番号漏えい（搾取）イメージ



出典：
消費者庁・経済産業省「インターネットショップでのクレジットカード番号の漏えい・不正利用に注意しましょう」（令和２年２月13日）

（追補）ECサイトセキュリティ対策促進事業（令和３年度補正）

漏えい防止

経済産業省HPより引用

- 中小企業者等が運営するECサイトについて、システムベンダー等との契約・運営保守状況や脆弱性に関する調査を実施予定。
- サイト運営事業者が特に陥りやすいセキュリティの誤解や対策を明らかにし、ECサイト構築時・運営時に留意すべき事項をまとめたガイドラインやモデル契約の策定・普及を予定。

①実際に被害を受けた企業へのヒアリング
- 被害の原因、事業への影響、被害後の対応、教訓等を把握

②ECサイト関係ベンダーへのヒアリング
- 各ベンダーのセキュリティ対策状況、保守契約のメニュー等を確認

③中小企業の自社構築ECサイトの脆弱性診断
- 募集対象は、自社でECサイトを構築・運用している中小企業
- 診断対象は、事業規模、構築方式、使用パッケージ、業種等を勘案し選定
- 脆弱性診断、ヒアリングによりECサイトのセキュリティ対策状況を確認・把握

来春を目処

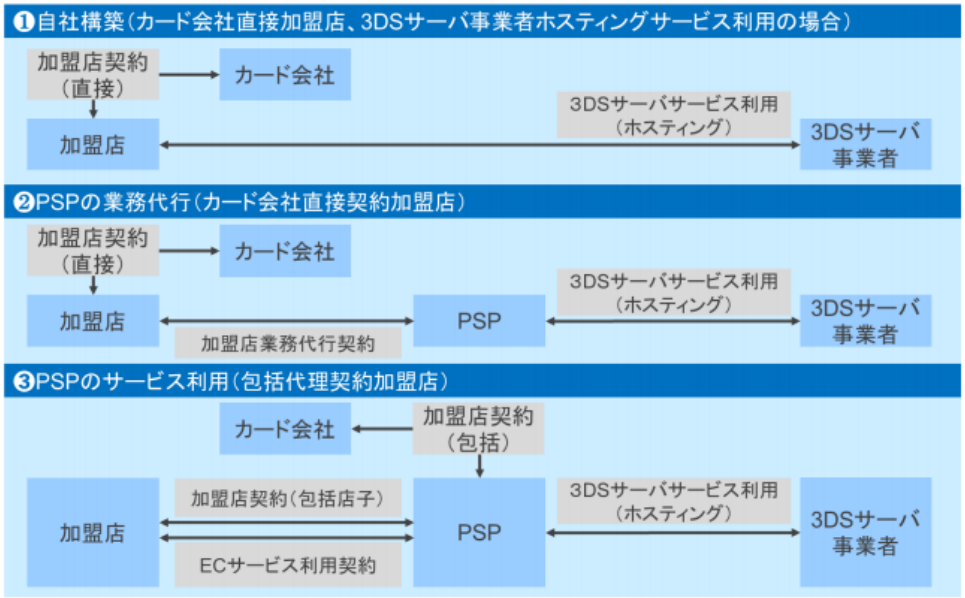
ECサイト向けセキュリティ対策ガイドラインの作成
- ①～③の成果を元にガイドラインを策定、普及

加盟店における新たなEC決済の本人認証手法（EMV 3-Dセキュア）

経済産業省HPより引用

- EMV 3-Dセキュア導入には、一般的に加盟店システムの改修が必要となる。
- EMV 3-Dセキュア導入により、チャージバック発生時の負担が、加盟店からクレジットカード会社の負担に変更となる。

加盟店におけるEMV 3-Dセキュア導入方法



出典：クレジット取引セキュリティ対策協議会「EMV 3-Dセキュア導入ガイド」

EMV 3-Dセキュアを導入していない場合のチャージバック事例

表：各本人認証を導入している場合において、不正利用が発生した場合の加盟店負担の有無（一例）

	2021年10月まで	2021年10月～2022年10月まで	2022年10月以降
旧３Dセキュア	なし	一部あり	あり
EMV 3-Dセキュア	なし	なし	なし
導入なし	あり	あり	あり

不正利用防止のための取組事例（加盟店）

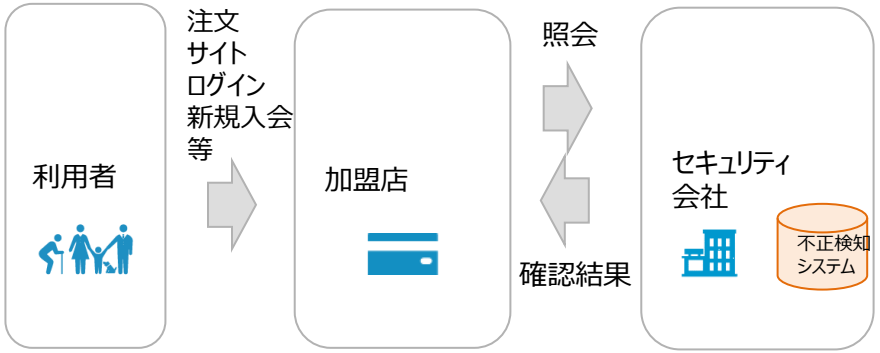
経済産業省HPより引用

不正利用防止

- 加盟店に対して提供される不正利用検知サービス（不正取引検知システム等）を利用することによって、加盟店における不正利用対策を実現。

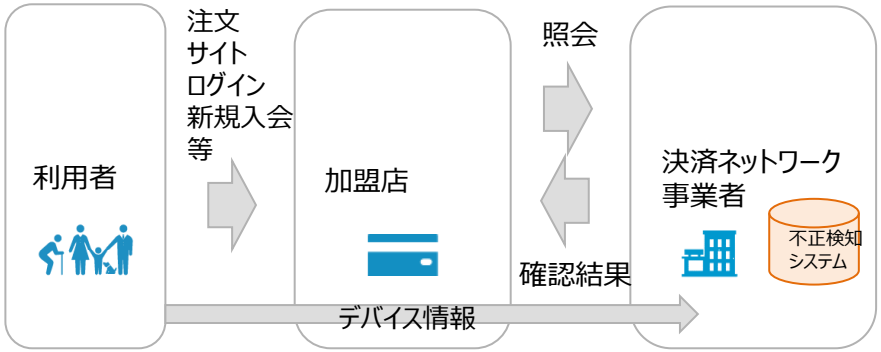
ECサイトでの注文時における不正利用検知サービスの提供（セキュリティ会社）

- ECサイトでのクレジットカード不正利用防止のため、加盟店が受領した注文のうち不正利用を検知して防ぐサービスを加盟店に対して提供
- サービス内部では、外部データベースとの突合やデバイス情報との照合、独自アルゴリズムによる不正行動分析等によって不正利用を判定している



加盟店に届く注文情報やサイトログイン情報等をもとに不正取引を検知

- ある決済ネットワーク事業者では、不正取引等を精度高く検知するクラウドサービスを、加盟店に提供している
- 利用者自身からの操作であることを確認するため、操作する端末（パソコン、スマートフォン等）の情報と、取引情報とを突合させることによって、属性・行動分析を実施している



フィッシング対策のための取組事例（加盟店）

周知・犯罪防止
経済産業省HPより引用

- フィッシング対策のため、加盟店においては以下の取組がある。
  ①利用者とのやりとりを工夫する
  ・メールドメイン認証を行い、受信者がフィッシングメールとのドメインの違いを区別できるようにする
  ・ SMS等に添付されるURLから、自社サイト等に連携しないようにする
  ②フィッシング対策サービスを提供する事業者を利用する
  ・フィッシングサイトの捜索やテイクダウン（サイトの取下げ依頼等）を委託する
- そのほか、加盟店を模したフィッシング事案等を発見した際は、警察・フィッシング対策協議会・JC3といった団体に報告するとともに、利用者に対して注意喚起を行うことも大切。

フィッシング対策としての具体的な取組事例

メールドメイン認証

- メール送信において、送信側（クレジットカード会社・加盟店）が**送信ドメイン認証技術**（例：SPF、DKIM及びDMARC等）の導入を行うことにより、認証されていないドメインからのメールに対して受信側が警告や受領拒否を行うことができるようになる。

SMS等に張り付けるURLからの連携防止

- 日々のコミュニケーション手段として、SMSに事業者のURLリンクを利用者に送信し、URLを通して会員情報を入力させるやり方を続けると、類似のSMSを用意され、フィッシングの被害を誘発してしまう。
- SMS等に添付されるURLから自社サイトへの連携を行わないよう利用者とのやりとりの方法を変える、といった対応策を検討する必要がある。

フィッシング対策サービスを提供する事業者の利用

- フィッシング対策サービスとして提供されているものの例
  - ✓ フィッシング検知
  - ✓ テイクダウン
    ホスティング・レジストラ事業者への削除依頼
    ブラウザ事業者への警告表示依頼（セーフブラウジング） 等
- 加盟店は、フィッシング対策サービスを提供する事業者を利用することにより、効率的かつ実効的な対応ができる。

※ホスティング事業者・・・Webサーバやメールサーバの貸し付けを行う事業者
※レジストラ事業者・・・ドメインの取得を請け負う事業者

フィッシング事案を受領したら、警察や業界団体・利用者に通知

- フィッシング事案を認知した際に、テイクダウン（フィッシングサイトの削除申請）等につなげるためにも、警察・フィッシング対策協議会・JC３といった関係団体への通報を行う。
- また、利用者に対しても周知を行う。

出典：フィッシング対策協議会

経済産業省HPより引用

３．個別主体
（３）PSP・ECシステム提供会社等

漏えい防止

PSP等におけるセキュリティに関する規定

経済産業省HPより引用

- 割賦販売法に基づく漏えい防止対策として、クレジット・セキュリティガイドラインにてPCI DSSの取得を求めている。

「決済代行業者等」の定義（クレジット・セキュリティガイドラインより）

(1)決済代行業者等（法35条の16 第1項第4号又は第7号該当事業者）
以下のいずれかの業務を行う決済代行業者（PSP 含む）※1、ECモール、ECシステム提供会社※2等の事業者の総称。
① 特定のアクワイアラーのために加盟店に立替払いをする業務
② 加盟店のためにクレジットカード情報（以下「カード情報」という。）をアクワイアラーに提供（当該アクワイアラー以外の者を通じた提供を含む。）する業務。

※1 ここでいう決済代行業者は、インターネット上の取引においてEC加盟店にクレジットカードスキームを提供し、カード情報を処理する事業者であるPSP と、インターネット以外の取引において加盟店にクレジットカードスキームを提供し、カード情報を処理する事業者をいう。
※2 ここでいうECシステム提供会社は、アクワイアラーとの契約有無にかかわらず、決済システムを運営しEC加盟店にサービスとして提供する事業者をいう。ASP/SaaSとしてEC加盟店にサービス提供する形式や、EC加盟店に購入プラットフォームを提供する形式等がある。

「決済代行業者等」における割賦販売法上の規制内容

規定	漏えい等防止
割賦販売法	・クレジットカード番号等の漏えい、滅失又は毀損の防止その他のクレジットカード番号等の適切な管理のために必要な措置を講じる
監督の基本方針	・漏えい防止のための基準（クレジットカード・セキュリティガイドラインが実務上の指針）を満たす
クレジットカード・セキュリティガイドライン（実務指針）における記載	・**PCI DSS** に準拠し、これを維持・運用する

漏えい防止

不正利用防止

経済産業省HPより引用

PSP等におけるセキュリティに関する規定（加盟店調査）

- PSP等であっても「**クレジットカード番号等取扱契約締結事業者**」として登録が必要となり、加盟店が講じるセキュリティ対策の**実施状況の確認**、**適切な対策の実施**の指導が求められる場合が存在。
- その場合には、**初期調査、途上調査**にて**セキュリティ対策の実施状況を確認**し、**調査の結果に基づく必要な措置**が、**行われるよう適切な指導**を行うことが求められる。

●「クレジットカード番号等取扱契約締結事業者」に課される加盟店調査義務等

①初期調査（加盟店契約時）

- 加盟店の所在地・代表者、商材・役務内容、販売方法等
- **セキュリティ対策（クレジットカード番号等の適切な管理及び不正利用の防止）の実施内容**
- 苦情の発生状況、苦情処理のための体制　等

②途上調査（加盟店契約締結後）

- **セキュリティ対策の実施状況（情報漏えい、不正使用の発生状況等）**
- 悪質取引の有無（消費者トラブルの発生状況等）

③加盟店調査の結果に基づく必要な措置

- **法令で定める基準に適合しない加盟店に対する必要な措置**
  - ◇合理的な期間内に基準に適合するよう**指導すること**
  - ◇指導に従わないとき又は適合することが見込まれない場合、**加盟店契約を解除すること**

➡セキュリティ対策については、「クレジットカード・セキュリティガイドライン」に基づく取組を進めていくことが必要

PSP等に必要な不正利用対策のための取組全体像

経済産業省HPより引用

不正利用防止

- PSP等は、**EC加盟店の不正利用対策をサポート**することが必要。具体的には、加盟店やイシュアーとの連携を図ることがセキュリティ・ガイドラインに記載

加盟店に対する不正利用対策の適切な助言

- EC加盟店に対して、非対面不正利用対策の具体的な方策の導入について、適切な助言・協力ができるよう体制の整備をするとともに、リスク・被害発生状況に応じた方策導入の確実な実施のためEC加盟店に対する指導及び状況に応じた適切な提案。

イシュアーとの不正情報についての連携

- オフアス取引において、EC加盟店における非対面不正利用対策の更なる向上のため、クレジットカード会社（イシュアー）から提供された不正情報についてできるだけ多くのEC加盟店と迅速な情報共有に努める。各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ため、各加盟店との間で迅速な情報共有に努める。

EMV ３-Dセキュア等の不正検知システムの導入サポート

- EC加盟店の不正の発生状況を注視し、取扱い商材や取引状況等を踏まえ、EMV 3-Dセキュアや属性・行動分析（不正検知システム）の導入の促進に向けたサポートを行うなど、必要な対策を講じる。

不正利用対策の各方策を提供できる体制の構築

- ガイドラインに掲げる「本人認証」「券面認証」「属性・行動分析（不正検知システム）」「配送先情報」の各方策を提供できる体制を構築し、契約先の EC加盟店における導入の推進に努める。

加盟店からの真正利用確認照会等

- EC加盟店からの真正利用確認照会や情報連携に取組む

経済産業省HPより引用

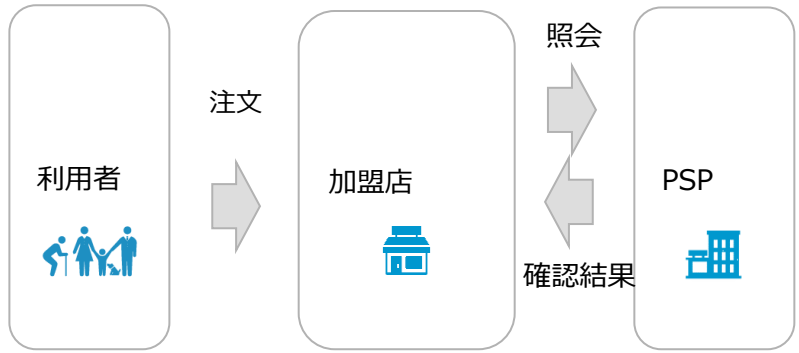
不正利用防止

PSP・ECシステム提供会社等におけるセキュリティ対策の取組事例

- PSPは、加盟店に対して不正利用検知システムの提供を行っている。
- また、クラウド等におけるEC決済システムを提供している事業者においても、加盟店へのセキュリティ対策向上のための説明会・バージョンの更新・パッケージの紹介等を行っている。

加盟店に送られた注文が不正取引かを検知（PSP）

- PSPは、加盟店に代わってクレジットカード情報を保有し、利用者情報・加盟店の注文情報を把握することが出来る
- あるサービスにおいては、利用者の決済に対して、加盟店が保持する利用者についての情報と、実際の注文内容を精査し、不正取引を検知
- AIの技術を活用しながら、スコアリング、ルール判定等の工程を行い、不正利用検知につなげている



加盟店に提供するシステムの安全性向上のための取組（ECシステム提供会社）

ECシステム提供会社のセキュリティ対策の例として、以下の取組を実施

自社サービスのバージョン更新
（PCI DSSのアップデート含む）

漏えい防止対策の実施
（サイバー攻撃への防御等）

不正利用防止対策の実施
（AI不正検知等）

加盟店に対するセキュリティ対策
（セキュリティ強化機能導入）
のための周知（勉強会開催等）

経済産業省HPより引用

3．個別主体
（４）　利用者

クレジットカード決済における媒体の変化（対面決済）

漏えい防止

不正利用防止

経済産業省HPより引用

- 決済端末・クレジットカードの形態は、利便性やセキュリティ技術の向上とともに変遷。

クレジットカード等

磁気

ICカード

タッチ決済（非接触）

・VISA／Master／JCB等
各国際ブランドのクレジットカードにおいて
タッチ決済機能が追加されてきている

カードレス

読取端末

こする（磁気リーダー）

挿す（接触IC）

かざす（非接触IC）

明細通知

紙における領収書の確認（基本的には月ごと）

アプリ等における確認

月ごとの確認 → 取引ごとの確認（アプリ等）

画像出典：パナソニックコネクトHP：https://connect.panasonic.com/jp-ja/products-services/mobile/lineup/jt-r600

クレジットカード決済における媒体の変化（非対面決済）

漏えい防止

不正利用防止

経済産業省HPより引用

- EC決済時における必要な情報やインターフェースも利便性やセキュリティ技術の向上とともに変遷。

	クレジットカード情報	クレジットカード情報 ＋静的パスワード	クレジットカード情報 ＋ワンタイムパスワード	生体認証
決済時に必要な情報	・クレジットカード情報 クレジットカード番号 有効期限 氏名 ＋ セキュリティコード	・クレジットカード情報 クレジットカード番号 有効期限 氏名 ＋ セキュリティコード ＋ ・静的パスワード （利用者における事前設定）	・クレジットカード情報 クレジットカード番号 有効期限 氏名 ＋ セキュリティコード ＋ ・動的パスワード （SMS等に送信されるパスワードを決済画面に入力）	・表情等の生体情報をもとに端末にログインすることで決済
決済インターフェース	インターネット取引			
	スマートフォン			

リスクベースアプローチによるパスワードの入力回数の減少

・EMV 3-Dセキュアによって認証を行うことにより

⇒ リスクベース認証により、会員は ID・パスワード等の入力をすることなく認証が完了する場合が出てくる（利便性と安全性の両立）

フィッシング対策のための取組事例（利用者）

周知・犯罪防止

経済産業省HPより引用

- フィッシング対策のためには、利用者自身の自衛策として「クレジットカード情報を安易に入力しない」ことが大切。信頼出来るサイトやアプリからのみ、クレジットカード情報を取り扱う意識を持つことが必要。

利用者におけるフィッシング対策の５つのポイント（フィッシング対策協議会HPより）

1	2	3	4	5
パソコンやモバイル端末は、安全に保つ	**不審なメールに注意する**	**電子メールに記載されたリンクはクリックしない**	**不審なメールやサイトは報告する**	**クレジットカード会社・加盟店の連絡先リストを作る**
パソコンやモバイル端末は安全に保つ	銀行やクレジットカード会社はメールで個人情報を確認しないことに注意する	電子メールに記載されたリンクは偽装可能なことに注意する	フィッシング対策協議会に報告を行う	挙動に違和感を感じたらすぐに問い合わせる
インターネットブラウザを最新のものにする	メール等における違和感に注意			サービス事業者や警察等の連絡先は控える
ウイルス対策ソフトを導入する	電子署名が付いていれば安全			

出典：フィッシング対策協議会HP

（参考）フィッシング対策協議会HPにおける消費者への注意喚起

周知・犯罪防止

経済産業省HPより引用

- フィッシング対策協議会HPにて、近時発生しているフィッシング事例を紹介し、注意を促す取組を行っている。

出典：フィッシング対策協議会HP

経済産業省HPより引用

４．関係行政機関･団体

日本クレジット協会（JCA）

経済産業省HPより引用

- 一般社団法人日本クレジット協会（Japan Consumer Credit Association：JCA）は、割賦販売法に基づく「認定割賦販売協会」の認定及び個人情報保護法に基づく「認定個人情報保護団体」の認定を受け、自主規制機関として活動を実施。
- クレジット業界の団体としての活動や消費者向けの広報活動等も行っている。

活動内容

- 会員が割賦販売法及び関係法令を遵守し、クレジット取引の秩序を保持するための規則の制定（自主ルール作成等）
- 会員に法令遵守等の体制を整備させるための指導及びその遵守状況の調査
- クレジット取引に係る知識の普及及び啓発　等

自主規制団体としての活動

セキュリティ基準に関する自主規制規則の制定

•法令、クレジットカード・セキュリティガイドラインを基に、クレジットカード番号等取扱業者(加盟店を除く。)におけるクレジットカード番号等の適切な管理のための必要な措置を規定した自主規制規則を制定

遵守状況等の確認

•包括信用購入あっせん業者及びクレジットカード番号等取扱契約締結事業者への法令・自主規制規則の遵守状況調査において、当該事業者のクレジットカード番号等の適切な管理の状況を調査

•クレジットカード番号等取扱契約締結事業者への遵守状況調査において、加盟店調査及び調査結果に基づいた措置の実施状況を調査

フィッシング被害防止における注意喚起

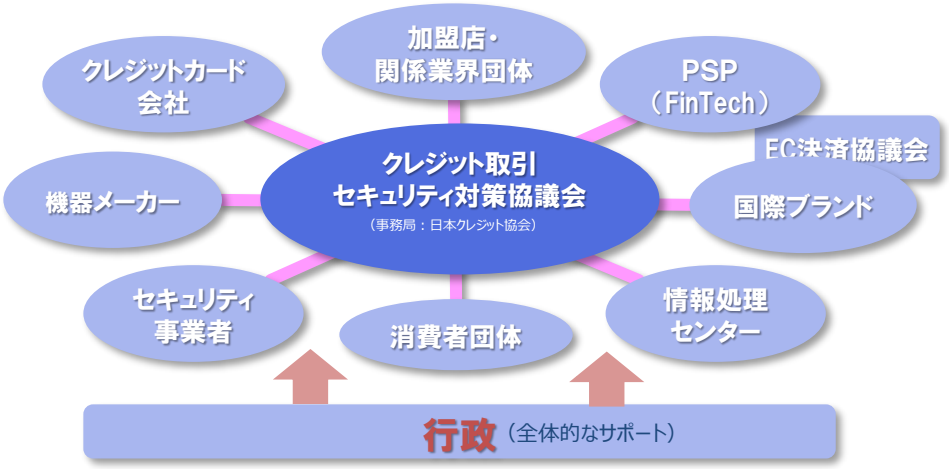
出典：日本クレジット協会HP

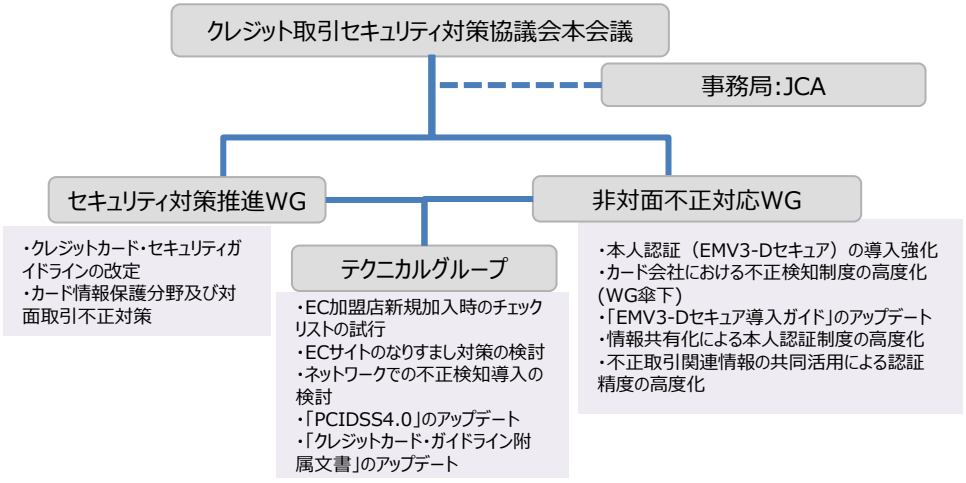
クレジット取引セキュリティ対策協議会

経済産業省HPより引用

- 平成28年より、**クレジット取引セキュリティ対策協議会**にて**「実行計画」**を策定。
- 令和２年からは、**「クレジットカード・セキュリティガイドライン」**を策定。（毎年度改訂）

クレジット取引セキュリティ対策協議会の体制





クレジットカード・セキュリティガイドラインの概要

1．クレジットカード情報保護対策分野

○加盟店におけるクレジットカード情報の**「非保持化」**

○クレジットカード会社、決済代行業者等、コード決済事業者等の**「PCI DSS準拠」**

2．不正利用対策分野

○対面取引におけるクレジットカード取引のIC化

○クレジットカード会社による**EMV3-Dセキュアの早期導入**

○クレジットカードとコード決済事業者等が提供する**決済サービスと連携する際のオーソリモニタリング、セキュリティコードの照合、3-Dセキュアによりパスワード照合等の多面的重層的な対策**

○加盟店における不正利用のリスクに応じた多面的・重層的な不正利用防止対策　等

3．消費者及び事業者等への周知・啓発について

○フィッシングの被害に遭わないための取組　等

警察庁サイバー警察局

経済産業省HPより引用

- 令和４年４月より、警察庁内の新組織としてサイバー警察局を設置。

背景

- コロナ渦を契機とした社会のデジタル化
- サイバー空間の公共空間化
- 悪質なマルウェアを用いた攻撃手法の拡大など、サイバー空間の脅威の拡大

組織構造

サイバー警察局

サイバー企画課

サイバー捜査課　情報技術解析課

- 対策・情報集約・分析
- 捜査指導・調整
- 解析
- 人材育成・教養
- 技術的支援

サイバー特別捜査隊

特別捜査隊には捜査権が付与

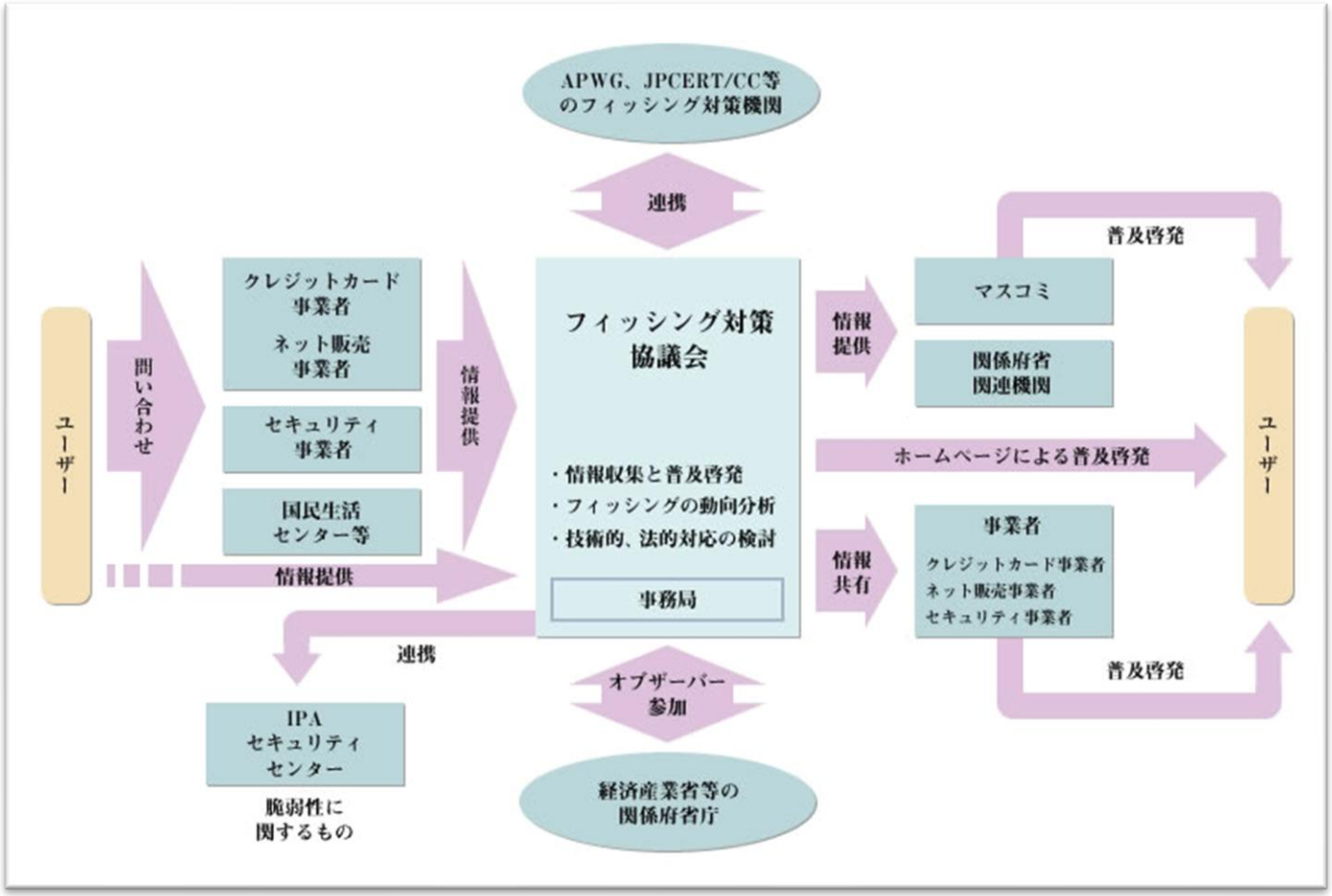
- 重大サイバー事案の捜査
- 国際共同捜査等への積極的な参画

警察庁情報提供をもとに事務局作成

フィッシング対策協議会

経済産業省HPより引用

- フィッシング対策協議会は、フィッシングに関する情報収集・提供、注意喚起等の活動を中心とした対策の促進を目的として設立された団体。（事務局をJPCERT/CCが担当）
- フィッシングに対する情報収集と普及啓発・動向分析とともに、技術的・法的対応の検討を行っている。



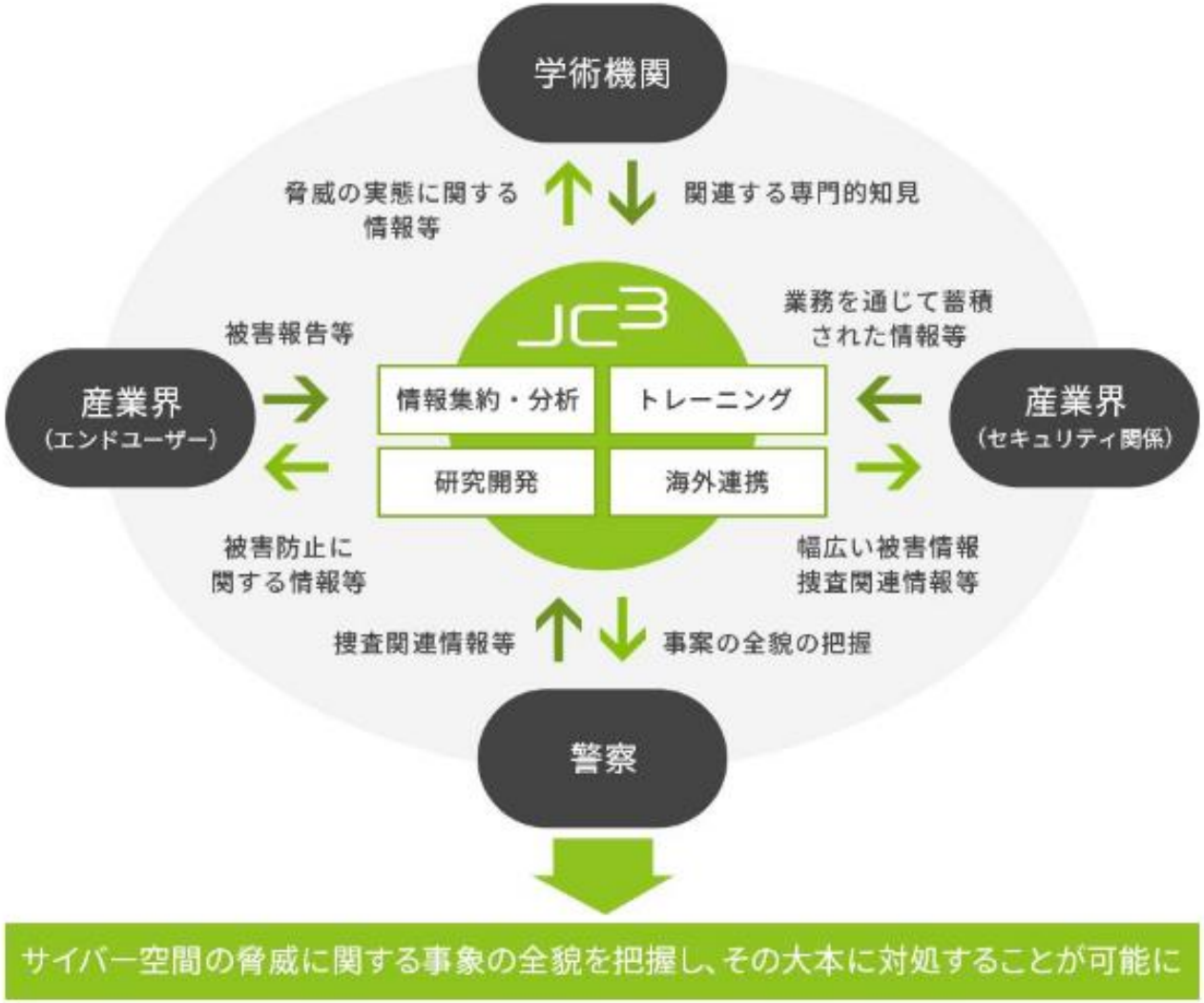
※　JPCERT/CCとは
インターネットを介して発生する侵入やサービス妨害等のコンピュータセキュリティインシデント(インシデント) について、
日本国内に関する報告の受け付け、対応の支援、発生状況の把握、手口の分析、再発防止のための対策の検討や助言などを、技術的な立場から行う。
特定の政府機関や企業からは独立した中立の組織として、日本における情報セキュリティ対策活動の向上に取組む。

出典：フィッシング対策協議会HP

日本サイバー犯罪対策センター（JC3）

経済産業省HPより引用

- JC3は、産業界、学術機関、法執行機関等、それぞれが持つサイバー空間の脅威への対処経験を集約・分析し、その結果を共有することで、サイバー空間全体を俯瞰し、サイバー犯罪等のサイバー空間の脅威の大本を特定・軽減・無効化することを目指す非営利団体。

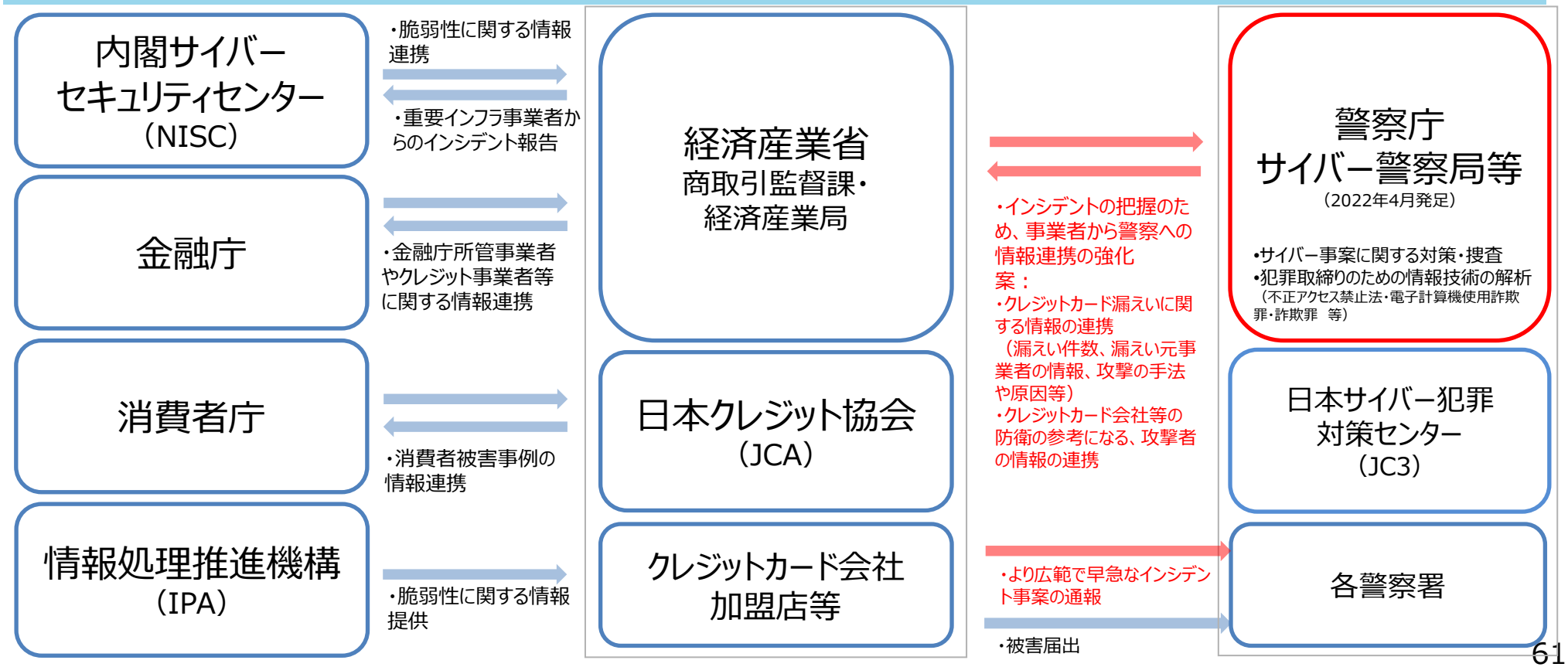


出典：JC3HP

関係行政機関・団体との連携強化（サイバーセキュリティ対策関係）

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
経済産業省HPより引用

- 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。



関係行政機関・団体との連携強化（フィッシング対策関係）

経済産業省HPより引用

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。