資料４－４

経済産業省

経済産業省におけるサイバーセキュリティ施策の取組状況について

令和５年３月２２日

経済産業省

１．クレジットカード業界でのサイバーセキュリティ施策

クレジットカード決済システムの更なるセキュリティ対策強化に向けた主な取組のポイント

キャッシュレス決済及びEC取引の普及に伴い、クレジットカード決済市場の規模が増加する一方、サイバー攻撃やフィッシング詐欺の増加等を背景に、クレジットカードの不正利用被害額が増加傾向。こうした中で、非対面取引におけるクレジットカード決済の更なるセキュリティ対策強化を図るため、クレジットカード決済網に関わる多様なプレーヤーによる多面的・重層的なセキュリティ対策の取組を整理。

Ⅰ．漏えい防止（クレジットカード番号等の適切管理の強化）

（１）EC加盟店・アクワイアラー等

◆EC加盟店

- 従前の**非保持化**等の対策に加え、クレジットカード番号等の適切管理義務の水準を引き上げるべく、**ECサイト自体の脆弱性対策**を必須化（システム上の設定不備改善、脆弱性診断、ウイルス対策等）【セキュリティ対策GL改定】
  ※引き続き、漏えい事案が多発しているOSS（オープン・ソース・ソフトウェア）を利用したサイトの運用の対策（2019年国から注意喚起）も継続強化
- アクワイアラー等からの調査に基づき、ECサイトの脆弱性対策の実施状況を申告
  ※昨年10月～試行的運用開始
- **「ECサイト構築・運用セキュリティガイドライン」**（IPA：今年度末策定）等を踏まえた自主的取組の充実 ※対策の例：WAF（Webアプリケーションファイアウォール）の導入等

◆アクワイアラー等

- 加盟店管理（セキュリティチェック）における**EC加盟店調査事項の対象拡大**【セキュリティ対策GL】
  ※昨年10月～試行的運用開始(再掲)　→　2025年度～法的義務化
  ←調査の頻度やシステム整備等、実務的に運用可能な加盟店管理手法となるよう要検討

＜継続的検討事項（更なる制度的措置の必要性）＞

- 加盟店管理の実効性担保に向けた国の監督の関与の在り方
  ※他、トークナイゼーションの技術の利用等、将来的な課題も存在

（２）決済代行業者等

＜継続的検討事項（更なる制度的措置の必要性）＞

- PSPの実態整理を踏まえた監督の在り方、EC決済システム提供者の範囲の明確化

（３）クレジットカード番号等取扱業者

◆イシュアー等

- 最新の国際セキュリティ基準「**PCI DSS v4.0**」準拠への移行（～2024年３月末）

＜継続的検討事項（更なる制度的措置の必要性）＞

- EC加盟店を含む、クレジットカード番号等取扱業者でのセキュリティ対策の表示等

（４）漏えい時のインシデント対応の強化

◆EC加盟店・決済代行業者等

- 漏えい時の**利用者への連絡・公表の早期化**等【業界マニュアル改定】
  ※「サイバー攻撃被害に係る情報の共有・公表ガイダンス検討会」（NISC等）でのガイダンスも参

◆日本クレジット協会（認定割賦販売協会）

- 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**（セキュリティ問題の原因・分析等）

＜継続的検討事項（更なる制度的措置の必要性）＞

- 漏えい時の国への報告、被害拡大防止・利用者保護に向けたクレジットカード決済サービスの即時停止・再開の判断の明確化

Ⅱ．不正利用防止

（１）利用者本人の適切な確認の強化

◆イシュアー・EC加盟店

- 不正利用防止措置として、利用者本人しか知り得ない・持ち得ない情報（ワンタイムパスワード・生体認証等）による利用者の適切な確認**（本人認証）**の仕組みを順次導入（～2024年度末）【セキュリティ対策GL改定】
  ※アカウントの紐付け時の確認等、運用については更なる検討が必要
- 原則全てのEC加盟店で、国際的な本人認証手法「**EMV 3DS**」の**導入**【セキュリティ対策GL改定】
- 利用者の適切な確認の実効性を担保するため、イシュアーの**リスクベース認証**の精度の向上（利用者の行動分析、AI等を活用した利用者の行動分析等）
  ※リスクや取引規模が大きい加盟店での更なる不正利用防止措置の運用検討

＜継続的検討事項（更なる制度的措置の必要性）＞

- 不正利用防止措置の主体の整理、利用者本人の適切な確認の実効性担保に向けたモニタリング等

（２）不正利用情報の共有化と活用

◆業界横断的な取組

- **イシュアー間の不正利用情報の共有**に向けた枠組みの検討・連携の促進

Ⅲ．犯罪抑止・広報周知

（１）フィッシング対策

◆イシュアー

- サイトのテイクダウンや送信メールのドメイン管理**（DMARC）**等によるフィッシング詐欺への自衛・推奨

（２）警察等との連携による犯罪抑止

◆国・イシュアー・EC加盟店

- **警察庁サイバー警察局や都道府県警等の連携強化**による犯罪抑止【業界マニュアルへの反映等】
  ※「サイバー事案の被害の潜在化防止に向けた検討会」（警察庁）を踏まえて今後具体化（今年度末）

（３）利用者への広報周知

◆日本クレジット協会・イシュアー・国

- クレジットの安全・安心な利用に関する利用者への被害防止のための措置の**広報・周知**（利用明細の確認、EMV3DSのワンタイムパスワード設定等）

※「世界一安全な日本」創造戦略（2022年12月改定）においても、クレジットカード等の決済の本人認証や不正検知の強化、フィッシング対策の推進等が必要とされている。
※セキュリティ対策GL：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）

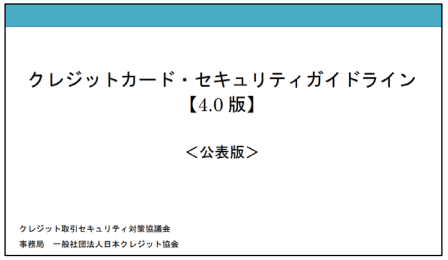
クレジットカード･セキュリティガイドライン４.０

- 2023年３月14日、クレジット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）にてクレジットカード取引に関わる事業者が実施するべきセキュリティ対策を定めた**「クレジットカード･セキュリティガイドライン」**を改訂。（クレジットカード･セキュリティガイドライン【4.0版】）

１．クレジットカード･セキュリティガイドラインについて

●「クレジットカード・セキュリティガイドライン」とは、安全・安心なクレジットカード利用環境を整備するため、**クレジットカード取引に関わるカード会社、加盟店、決済代行業者等の関係事業者**が実施するべきクレジットカード情報漏えい及び不正利用の防止のための**セキュリティ対策の取組を取りまとめたもの**。

● 同ガイドラインは、**割賦販売法に規定するセキュリティ対策義務の「実務上の指針」**として位置づけられており、同ガイドラインに「指針対策」として掲げられてい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、**同法で定めるセキュリティ対策の基準を満たしていると認められる。**



クレジットカード･セキュリティガイドラインのウェブページはこちら↑
https://www.j-credit.or.jp/security/document/index.html

２．主な改訂内容

（１）クレジットカード情報保護対策

・EC加盟店は、新規の加盟店契約の申込前に自らECサイトにセキュリティ対策を実施し、契約申込みの際にアクワイアラー※2又はPSP ※3に**脆弱性対策等のセキュリティ対策の実施状況**を記載した**申告書を提出する。（試行）**
・アクワイアラー及びPSPは、EC加盟店に対して、新規の加盟店契約の申込みに際してEC加盟店自らのセキュリティ対策の実施とその申告を求めるとともに、**申告内容をもとにセキュリティ対策の実施状況を確認する。（試行）**
（なお、「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」（経済産業省 2023年1月20日）において、EC加盟店のECシステムやECサイト自体の**脆弱性対策等の基本的なセキュリティ対策を必須とすることを**2024年度末までに**本ガイドラインに追記する**ことが求められている。）

（２）不正利用対策

・原則、全てのEC加盟店は、2025年3月末までに**EMV3-Dセキュアの導入**を求める。
・イシュアー※4は、EMV 3-Dセキュアの本人認証方法として「静的（固定）パスワード」から「動的（ワンタイム）パスワード」等の認証方法への移行環境を整え、2025年3月末までに自社カード会員が**「動的（ワンタイム）パスワード」等の認証方法へ登録・移行する**よう取組む。
・アクワイアラー及びPSPは、2025年3月末までに、原則、全てのEC加盟店がEMV3-Dセキュアの導入を計画的に進められるようサポートを行う。
また、「不正顕在化加盟店」※5に対して**早期にEMV 3-Dセキュアを導入**するよう働きかける。

（３）消費者及び事業者等への周知・啓発

イシュアーは、カード会員によるEMV3-Dセキュアの登録、「動的（ワンタイム）パスワード」等の認証方法の登録・移行を促進するためのカード会員への周知、啓発を行う。
イシュアーは、カード会員に対して、不正利用被害の防止のために、利用明細の確認、身に覚えのない取引があった場合のイシュアーへの連絡等の重要性についての周知、啓発活動に取組む。
イシュアーは、カード会員のフィッシングによる不正利用被害の防止のために、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は行わないなどの注意事項等の周知、啓発活動に取組む。
アクワイアラー又はPSPは、**EC加盟店に対して、2025年3月末までに原則、全てのEC加盟店においてEMV3-Dセキュアの導入が求められる旨、周知する。**

※1　Payment Card Industry Data Security Standard 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。
※2　クレジットカード加盟店を開拓、加盟店契約を締結する事業者。
※3　Payment Service Providerの略。インターネット上の取引においてEC加盟店にクレジットカード決済スキームを提供し、カード情報を処理する事業者。
※4　クレジットカードを発行する事業者。
※5　アクワイアラー各社が把握する不正利用金額が3ヵ月連続で50万円を超えているEC加盟店。

クレジットカード会社等におけるフィッシング対策の強化

2023年２月１日、クレジットカード会社等に対し、送信ドメイン認証技術（DMARC*）の導入をはじめとするフィッシング対策の強化を要請。

*DMARC: Domain-based Message Authentication, Reporting, and Conformanceの略称。

- **<u>DMARCの導入によるなりすましメール対策</u>**

  ・利用者向けに**公開する全てのドメイン名（メールの送信を行わないドメイン名を含む）**について、**DMARCを導入すること。**
  ・DMARC導入にあたっては、受信者側でなりすましメールの**受信拒否を行うポリシー(reject)**での運用を行うこと。

- **<u>全般的なフィッシング対策</u>**

  ・フィッシング対策協議会が策定した**「フィッシング対策ガイドライン」**において、
  フィッシングに対して**有効とされている対策（即時通知、BIMI等を含む）**を実施すること。

経済産業省
Ministry of Economy, Trade and Industry

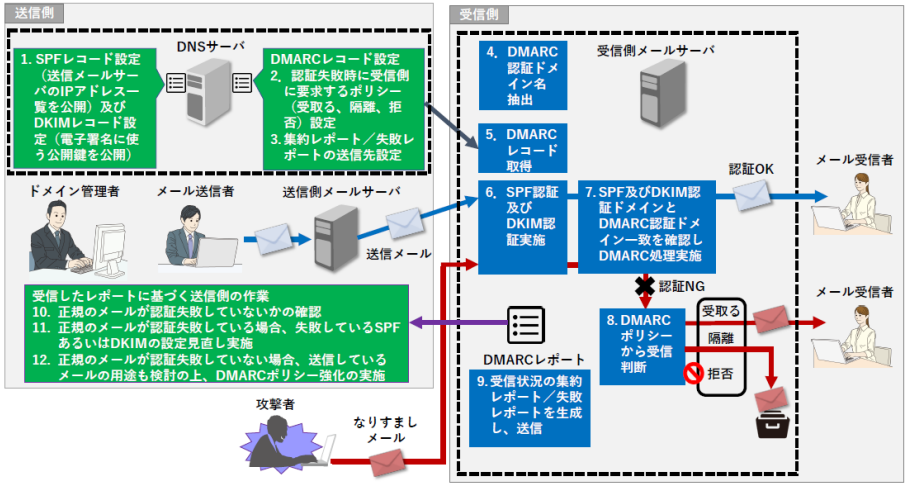
クレジットカード会社等に対するフィッシング対策の強化を要請しました

2023年2月1日　同時発表：警察庁・総務省

▶安全・安心

経済産業省、警察庁及び総務省は、クレジットカード番号等の不正利用の原因となるフィッシング被害が増加していることに鑑み、クレジットカード会社等に対し、送信ドメイン認証技術（DMARC*）の導入をはじめとするフィッシング対策の強化を要請しました。

昨今、悪意のある第三者が、クレジットカード会社等を騙った電子メール等を利用者に送信し、利用者を当該電子メール等のリンクから偽サイトに誘導したうえで、利用者のクレジットカード番号等を詐取する攻撃（いわゆるフィッシング）が多発しています。



図：DMARCの仕組み
出典：迷惑メール対策推進協議会「送信ドメイン認証技術導入マニュアル」

【参考】「世界一安全な日本」創造戦略2022（抜粋）

2022年12月20日閣議決定

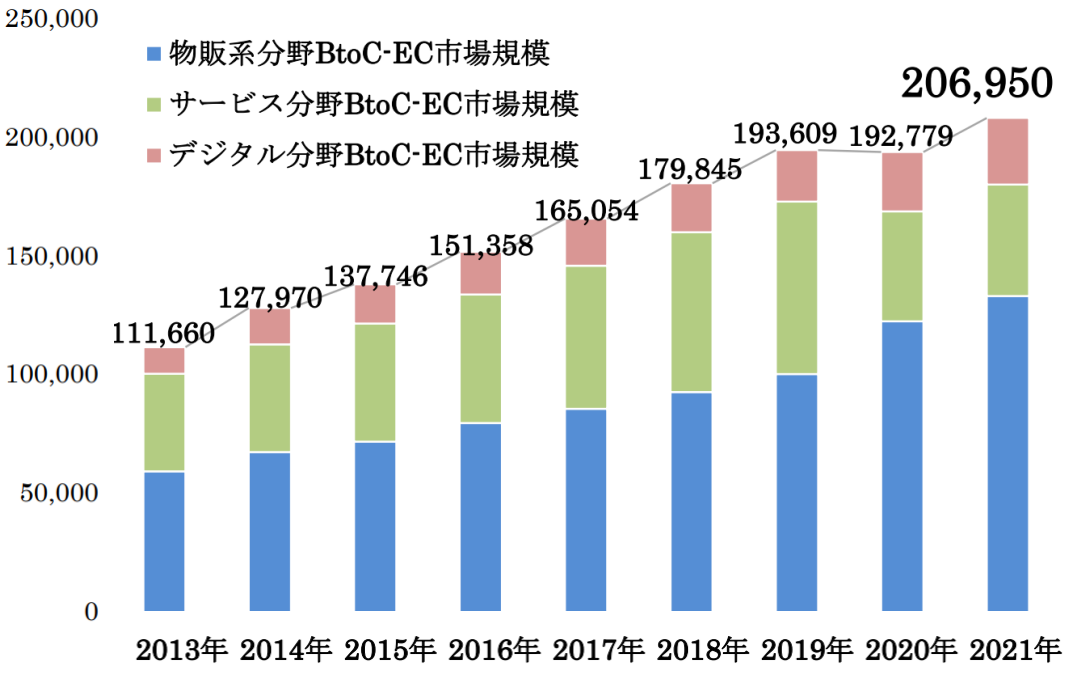
１　デジタル社会に対応した世界最高水準の安全なサイバー空間の確保
（４）民間事業者、関係機関等と連携したサイバーセキュリティ強化
③　<u>フィッシング対策の推進</u>
警察が把握したフィッシングサイト等に関する情報をウイルス対策ソフト事業者等に提供するほか、<u>関係団体等と連携し、民間事業者に対して、</u>
<u>送信ドメイン認証技術（DMARC、SPF、DKIM等）の導入等のなりすましメール対策</u><u>を講じるよう働き掛ける</u>。

２．ECサイト業界でのサイバーセキュリティ施策

ECサイトにおけるサイバー攻撃等の被害

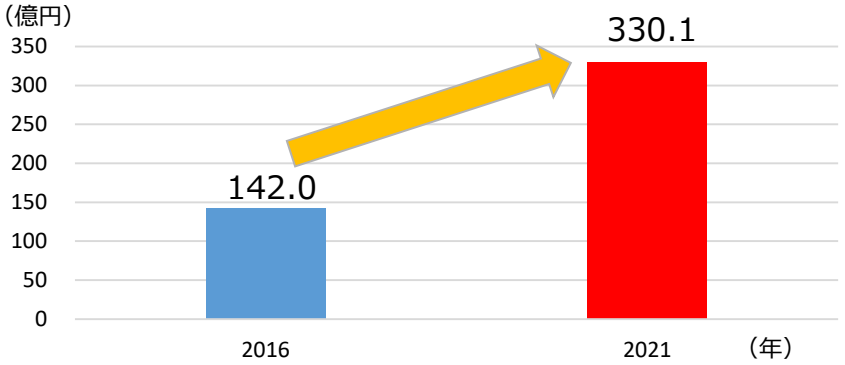
- EC取引の拡大等に伴い、ECサイトにおいて、**個人情報やクレジットカード情報を入力する機会が増加**。
- ECサイトへのサイバー攻撃等により、クレジットカード情報が漏洩する事案が多数発生。2021年の国内発行クレジットカードの**年間不正利用被害額**は、**約330億円**であり、**2016年と比較すると、2倍以上**。
- 被害にあったECサイトの**閉鎖期間**は、**１社平均で約9ヶ月**。従業員規模300名以下の企業で、**売上高の損失額が1,000万円以上**と回答した企業は**6割超**。

BtoC-EC市場規模の経年推移



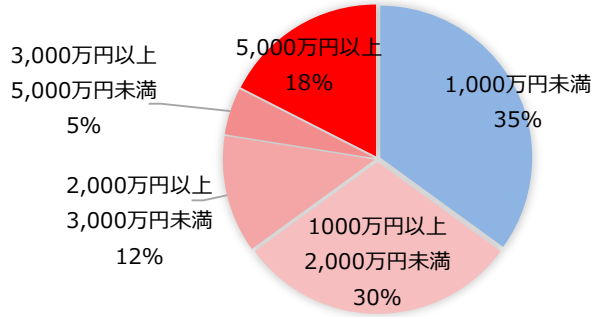
出典：令和3年度デジタル取引環境整備事業（電子商取引に関する市場調査）（経済産業省）

年間不正利用被害総額の比較



日本のクレジット統計（日本クレジット協会）を基に経済産業省が作成

ECサイト閉鎖期間における売上高の損失額



ECサイト構築・運用セキュリティガイドライン（IPA）を基に経済産業省が作成

ECサイト構築・運用セキュリティガイドライン

- 中小企業が構築・運営するECサイトのセキュリティ対策に課題が多くみられることから、IPAは、**中小企業が運営するECサイトの脆弱性診断**を実施するとともに、ECサイトの構築・運用に必要な**セキュリティ対策と実践方法を解説したガイドラインを策定**。
- ガイドラインでは、経営者にセキュリティ対策の基本を認識いただけるよう、**サイバー被害による影響や対策の重要性**をデータとともに解説。
- また、実務者に構築時・運用時に必要なセキュリティ対策要件を確認いただけるよう、**チェックリスト形式**で解説。

経営者編

サイバー被害の状況を紹介

- ✓ サイバー被害を受けたECサイト運営事業者の**9割以上が、自社構築サイト**
- ✓ 中小企業50社を対象に実施した、脆弱性診断（①Webアプリケーション診断、②プラットフォーム診断）の結果、**危険度「高」と判定された事業者は5割**

サイバー攻撃を受けたECサイト運営の問題点を指摘

- ✓ 調査をした社の7割以上が、ECサイト構築プログラムやCMS等の脆弱性を放置または最新版へのアップデートを未実施。
- ✓ 調査をした社の9割が保守など運用時のセキュリティ対策を未実施

経営者が認識すべき7つの重要項目を提示

① 組織全体の方針の策定
② 予算や人材の確保
③ セキュリティ対策の検討指示
④ セキュリティ対策の見直し指示
⑤ 緊急時（インシデント発生時）の体制整備
⑥ 責任の明確化
⑦ 最新動向の収集

実践編

ECサイトの運用時におけるセキュリティ対策要件

要件No	セキュリティ対策要件（構築時）	区分
1	「安全なウェブサイトの作り方」及び「セキュリティ実装チェックリスト」に準拠して、ECサイトを構築する。	必須
2	サーバ及び管理端末等で利用しているソフトウェアをセキュリティパッチ等により最新の状態にする。	必須
⋮	⋮	⋮
13	保管したログやバックアップデータを保護する。	推奨
14	サーバ及び管理端末において、セキュリティ対策を実施する。	推奨

ECサイトの構築時におけるセキュリティ対策要件

要件No	セキュリティ対策要件（運用時）	区分
1	サーバ及び管理端末等で利用しているソフトウェアをセキュリティパッチ等により最新の状態にする。	必須
2	ECサイトへの脆弱性診断を定期的及びカスタマイズを行った際に行い、見つかった脆弱性を対策する。	必須
⋮	⋮	⋮
6	WAFを導入する。	推奨
7	サイバー保険に加入する。	推奨

ECサイト構築・運用セキュリティガイドラインのウェブページはこちら⇒
https://www.ipa.go.jp/security/guide/vuln/guideforecsite.html