附属文書20　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】）

クレジット取引セキュリティ対策協議会

2025年3月

# 〈本書の目的〉

- ✓ 不正利用被害額は高水準で推移しており、その大半がEC加盟店における「なりすまし」による不正利用が行われており、その対策が喫緊の課題となっております。
- ✓ クレジット取引セキュリティ対策協議会では、関係事業者が講じる対策を「クレジットカード・セキュリティガイドライン【6.0版】」に記載しています。
- ✓ EC加盟店の指針対策における必要な取組については、「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】」にて、「カード情報漏えい」や「不正利用」の手口からその防止に必要な対策について示しております。
- ✓ 本書は、「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】」記載の対策の内、重要な対策について、図表を用いて視覚的にわかりやすく説明しており、EC加盟店及び関係事業者の理解促進と意識の向上、対策の強化による不正利用被害の防止が図られることを目的としたものです。

# 第１部　EC加盟店における
# セキュリティ対策義務について

# 1. EC加盟店のセキュリティ対策義務の概要①

- EC加盟店は、割賦販売法において、「クレジットカード番号等の適切な管理」及び「クレジットカード番号等の不正な利用の防止」をするための措置を講じることが義務付けられている。
- EC加盟店の不正利用は、EC加盟店のシステムやWebサイトの脆弱性を原因とした情報の漏えい等により窃取されたカード情報にて行われてきたことから、「クレジット取引セキュリティ対策協議会（以下「協議会」という。）」では、「クレジットカード・セキュリティガイドライン（以下「セキュリティガイドライン」という。）」にて、カード情報保護対策の指針対策として「非保持化（非保持同等／相当）の実現又はPCI DSS準拠」を求めてきた。
- しかしながら、非保持化を達成した加盟店においても、ECサイト等の設定不備や既知の脆弱性を悪用した不正アクセス、大量かつ連続する不正アタックやフィッシング等の手段により窃取されたカード情報等が、コード決済やEC加盟店において不正利用される事案が顕著となっている。
- このような状況を踏まえ、「セキュリティガイドライン【6.0版】」からは、EC加盟店における「カード情報保護対策」「不正利用対策」において指針対策を追加した。
- 協議会では、EC加盟店のセキュリティ対策を強化するため検討や活動を進めており、より安全・安心なクレジットカードの取引環境が整備されることを目指している。

クレジットカード・セキュリティガイドライン（GL）対策経緯

| | 改正割賦販売法 2018年6月施行 | 2015年～2021年 | 2022年 | 2023年 | 2024年 | 2025年4月～ |
|---|---|---|---|---|---|---|
| | | 実行計画（16年～）、GL（20年～） | GL3.0版 | GL4.0版 | GL5.0版 | GL6.0版 |
| カード情報保護対策 | 第35条の16第1項 クレジットカード番号等の適切な管理 | クレジット取引セキュリティ対策協議会発足 | ①カード情報の非保持化　又は保持する場合はPCI DSS準拠 | | | ②EC加盟店のシステム及びWebサイトの「脆弱性対策」の実施 |
| 不正利用対策 | 第35条の17の15 同施行規則 第133条の14 クレジットカード番号等の不正な利用の防止 | | ①オーソリゼーション処理の体制整備<br>②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<br>③高リスク商材取扱加盟店：4方策のうち1方策<br>④不正顕在化加盟店：4方策のうち2方策 | | | ③EMV 3-Dセキュアの導入<br>④適切な不正ログイン対策の実施<br>⑤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、適切な対策の追加導入 |

# 1. EC加盟店のセキュリティ対策義務の概要②

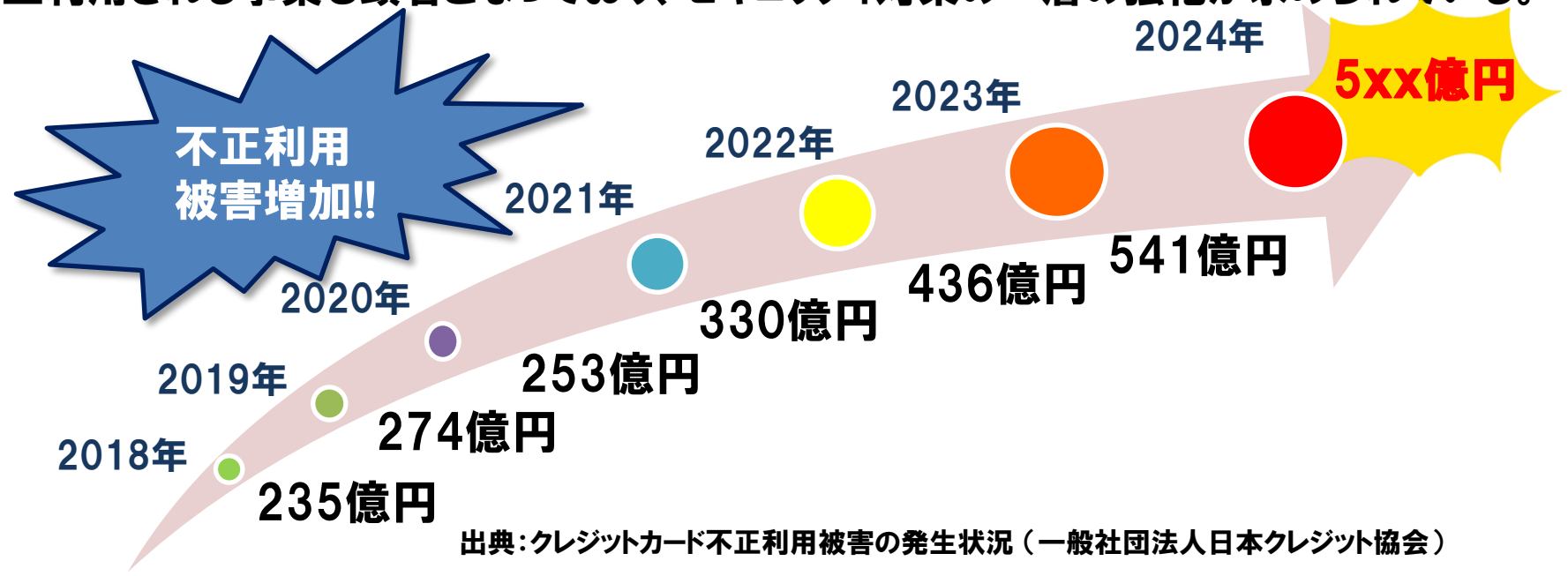
- ◆ 割賦販売法（法令上の義務）とセキュリティガイドライン（実務上の指針）で定める対策（指針対策）は以下の通り。
- ◆ 指針対策を講じれば、割賦販売法に規定する「必要かつ適切な措置」を講じていると見なされる。
- ◆ 対策の実施状況については、カード会社（アクワイアラー）、PSPより定期的に確認され、措置が講じられていない場合は、最終的にはクレジットカードの取引が停止されることもある。

| 割賦販売法 | | セキュリティガイドライン　6.0版 |
|---|---|---|
| 法令上の義務 | | 実務上の指針 |
| 加盟店の義務 | クレジットカード番号等の適切な管理<br>（第35条の16第1項） | ①　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<br>②　EC加盟店のシステム及びWebサイトの「脆弱性対策」の実施 ※ |
| | クレジットカード番号等の不正な利用の防止<br>（第35条の17の15） | ①　オーソリゼーション処理の体制整備<br>②　加盟店契約上の善良なる管理者の注意義務の履行<br>③　EMV 3-Dセキュアの導入 ※<br>④　適切な不正ログイン対策の実施 ※<br>⑤　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、適切な対策の追加導入（不正顕在化加盟店）※ |

※2025年4月指針対策追加・変更

# 2. 不正利用被害状況

- ◆ カード取引の不正利用被害額は、2023年に過去最高の541億円に達し、足元の2024年1月から9月の不正利用は393億円となり、高止まりの傾向にある。
- ◆ カード情報保護は、非保持化を中心に指針対策を実行して一定の効果があったが、最近は非保持化を達成したEC加盟店においてもシステム設定の不備（PW管理等）やWebサイトの脆弱性（ウイルス対策不備等）を利用し、外部からWebシステムの改ざん等が行われ、長期間に渡るカード情報の不正窃取が発生している。
- ◆ また、クレジットマスターで生成したカード情報やフィッシングの手口により窃取されたカード情報等にてコード決済やEC加盟店においてアカウント作成やログインがされ、不正利用される事案も顕著となっており、セキュリティ対策の一層の強化が求められている。




出典：クレジットカード不正利用被害の発生状況（一般社団法人日本クレジット協会）

# 3. ECサイト構築時の留意点

- ◆ EC加盟店がECサイトを構築する際に留意すべきは以下の通り。特にオープンソースソフトウェア（注）を利用しているEC加盟店（非保持対応済）での既知の脆弱性による情報漏えい事案が増加している。
- ◆ オープンソースソフトウェアを利用している場合は、バージョンアップ及びセキュリティパッチ適用等により、既知の脆弱性が無い状況を常に保つ様、EC加盟店の責任で対応する必要がある。

（注）オープンソースソフトウェア（open-source software）とは
- ✓ ソースコードが無償で公開されているソフトウェア
- ✓ いつでも無料でプログラムを利用でき、ソースコードのカスタマイズも自由

| | ショッピングモール ASP | オープンソースソフトウェア ・EC-CUBE ・WordPress 等 | パッケージ サービス |
|---|---|---|---|
| メリット | □ 安価で手軽 | □ 安価<br>□ 拡張性が高い | □ ECサイトの構築がし易い<br>□ 脆弱性情報は提供会社が発信 |
| デメリット | □ ランニングコストが発生<br>□ 独自性が打ち出しづらい<br>□ 拡張性が低い | □ サーバー管理が必要<br>□ カスタマイズにより最新バージョンにアップデートできない場合がある<br>□ 障害発生時は自社責任 | □ 導入費用が高い<br>□ 保守費用が発生 |

# 4. サイト構築、運用・保守の外部委託時の留意点

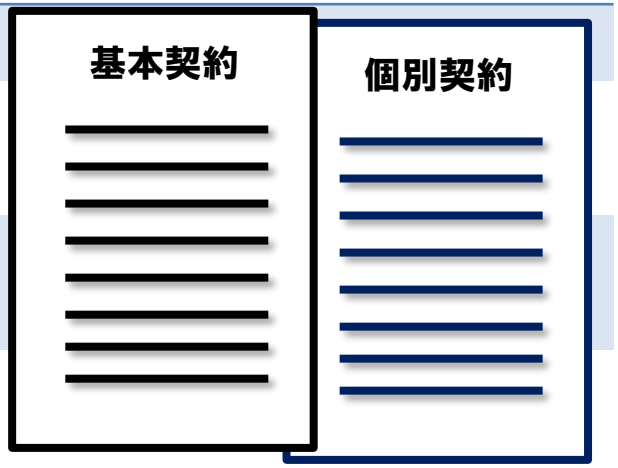
◆ ECサイトを構築し、運用・保守業務を外部に委託する場合は、委託先がEC加盟店が実施すべき「カード情報保護対策」「不正利用対策」を理解のもと構築・運用を行うことを求め、EC加盟店の責任において適切なセキュリティ対策を講じる必要がある。

## 〈ポイント①〉“契約内容を確認”しましょう！

### □ 運用・保守業務の委託範囲を確認

- ✓ 適切なセキュリティ対策を講じることの定めがあるか
- ✓ 情報漏えい時の対応について定めがあるか
- ✓ 委託元、委託先間の責任分界点について定めがあるか

全て網羅されているか？？



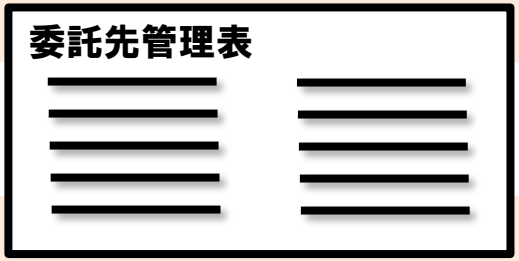

〈留意点〉一般的な基本契約には、パッチ適用などECシステム導入後の運用等について、上述の項目が盛り込まれておらず個別契約となるケースが多い。セキュリティ対策については自ら提案や説明を委託先へ依頼することが重要。

## 〈ポイント②〉EC加盟店は、“委託元として、委託先を適切に管理”しましょう！

### □ “外部委託先に任せていれば安心”は禁物

- ✓ 契約に基づく運用・保守業務の定期的な遂行状況の確認
- ✓ 上記が確認可能な社内管理体制の整備

委託先は遺漏なく対応できているか？？



# 5. 情報漏えいを発生させた場合の影響

◆ 割賦販売法では、EC加盟店がクレジットカード番号等の適切な管理を行うことが法的義務として求められている（割賦販売法第35条の16第1項）。

◆ EC加盟店で情報漏えいが発生した場合には、カード取引の停止に加えて、再開に至るまでにフォレンジック調査等に相応の期間を要し、また、フォレンジック調査費用、不正利用被害補償額、被害カードに関わる差替え費用等がEC加盟店に請求され、多大な費用負担が発生する点に留意が必要。

〈情報漏えいを発生させた場合の主な影響〉

- 漏えいの懸念が生じた場合は、被害防止のためにクレジットカード取引の即時停止が必要。
- 漏えいの懸念が生じてからフォレンジック調査実施、再発防止、アクワイアラーによる再開許可までおおよそ3か月から12か月の期間を要す。
- その間、ECビジネスの停止に追い込まれることとなり、逸失利益は大きくなることが想定され、加盟店の規模によるが、数百万円から数億円と言われる。
- その他、フォレンジック調査費用、コールセンター設置や書面の出状などユーザー（購入者）への対応費用等も要す。
- また、個人情報を取り扱う事業者が情報漏えい事案を発生させた場合、個人情報保護委員会に対する報告などカード会社と連携した対応が必要。
- 何よりもユーザー（購入者）からの信頼を失うことになる。
- 以上のことから、EC加盟店自身の責任において、情報漏えいを発生させないよう、予め必要なセキュリティ対策を実施しておくことが求められる。

# 第２部　EC加盟店における
# セキュリティ対策

# 0. EC加盟店におけるセキュリティ対策の概要

- ◆ EC加盟店はインターネットを通じて不正アクセスや、なりすましによる不正ログイン、不正利用等、様々な脅威にさらされている。また、それぞれのアクセス者が真正なユーザーであるか、攻撃者であるかの区別が難しい。
- ◆ よって、様々な攻撃や脅威から自社のECサイトを守るために、社内のシステム担当者、システム開発委託先等に確認の上、適切なセキュリティ対策を実施する必要がある。
- ◆ 想定される対策について以下の通り説明する。

| 不正の手口 | 対策 | 説明ページ |
|---|---|---|
| □ 設定の不備を突いた攻撃<br>□ 既知の脆弱性を悪用した攻撃<br>□ 連続したクレジットカードの有効性確認 | 1.クレジットカード番号等の適切な管理<br>−1.脆弱性対策 | P12～ |
| □ 不正アカウント作成<br>□ アカウント乗っ取り | 2.不正利用の防止<br>−1.不正ログイン対策<br>（決済前の対策） | P25～ |
| □ 真正なカード会員データによる「なりすまし」<br>□ 商品等転売 | 2.不正利用の防止<br>−2. 決済時・決済後の対策 | P32～ |

# 1-0. 脆弱性対策の概要

◆ カード会員データの漏えいの原因は以下が想定される。

- ロ オープンソースソフトウェア及びその他CMS(Contents Management System)を利用したサーバ設定の不備を突いた攻撃による漏えい
- ロ 既知の脆弱性などを悪用した攻撃による漏えい
- ロ カード会員データの有効性確認、クレジットマスター攻撃による漏えい

◆ 上記のセキュリティホールをついた漏えいへの対策箇所について、実際の事例等から以下を想定。

| 対策箇所 | 説明ページ |
|---|---|
| 1-1 ECサイトのシステム管理画面 | P13～ |
| 1-2 ECサイトの設定の不備 | P15～ |
| 1-3 既知の脆弱性 | P17～ |
| 1-4 マルウェア、ウィルスなどの不正ファイル | P23～ |
| 1-5 クレジットマスター、悪質な有効性確認への対策 | P24～ |

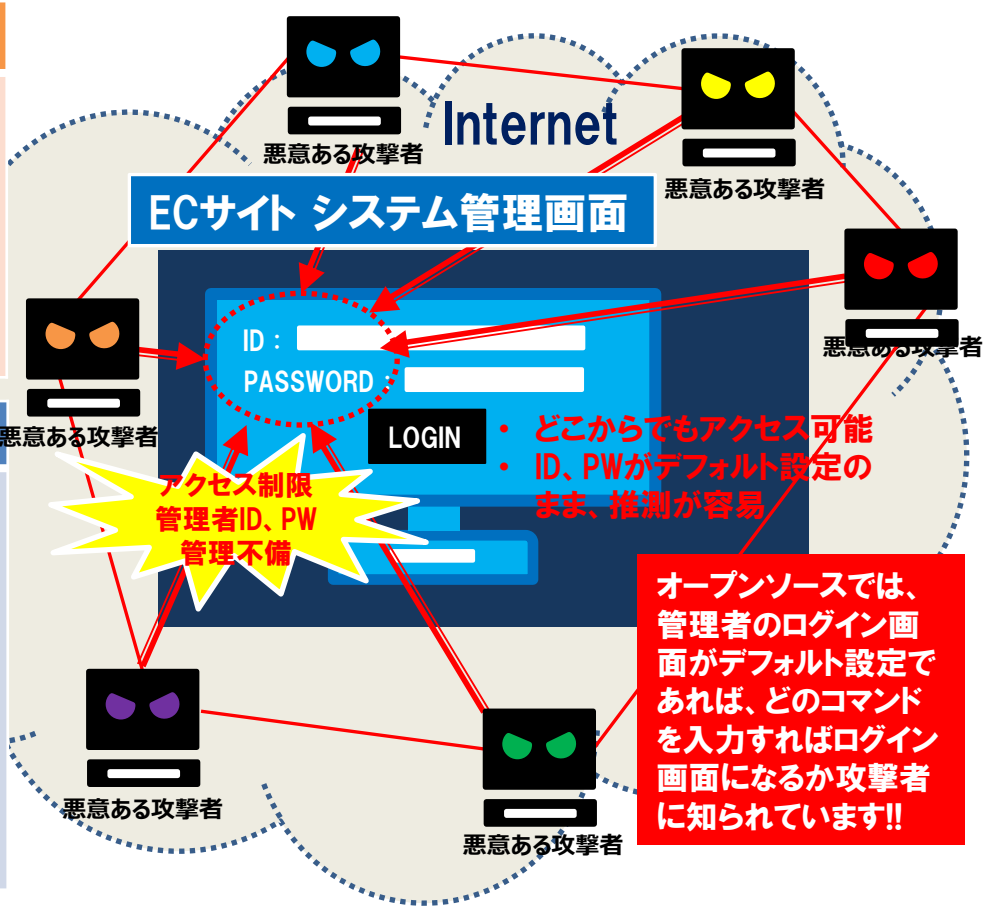
# 1-1-1. システム管理画面のアクセス制限不備と管理者のID/パスワード管理不足①

## 攻撃リスク

- ◆ 接続元を制限しないことにより、管理画面がインターネット上のどこからでもアクセスできてしまう。
- ◆ ID、パスワードが推測されやすい「管理者」「パスワード」等のデフォルト設定のままセットされており、変更されていない。
- ◆ その他「会社名」や「ドメイン名」も同様。

## 対策

- □ 管理画面にアクセス可能な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、管理画面にアクセスするためにベーシック認証を設ける。
- □ 取得されたアカウントを不正使用されないように2段階認証または多要素認証(2要素認証)を採用する。
- □ アカウントロック機能を有効にし 、10回以下のログイン失敗でアカウントをロックする。




!! 本対策は、**見直しの容易さや、目下の漏えい事案の全体の約7割をカバー**できることから、早急な措置が求められます(所要期間：設定変更とテスト対応でおおよそ数日程度)。

# 1-1-1. システム管理画面のアクセス制限不備と管理者のID/パスワード管理不足②

「EC-CUBE 2.x系 環境チェックリスト」における該当チェックポイント

| No. | 対応優先度 | カテゴリ | 項目 | 確認方法 | 対応方法 |
|---|---|---|---|---|---|
| 5 | 必須 | 意図しないディレクトリ・ファイルの露出 | 管理画面の URL を変更したにも関わらず、標準の admin フォルダが残存していないか | 管理画面の URL を標準の admin から変更した場合、admin フォルダが残っていないことをご確認ください。 | admin フォルダが残っている場合使用しなくなったプログラムが含まれています。 admin を削除してください。 |
| 10 | 必須 | ID/パスワード管理 | 管理画面のユーザーID/パスワードが推測されやすいものになっていないか | ユーザーIDとパスワードが同じ<br>ユーザーIDが admin など推測されやすいもの<br>パスワードが11文字以下<br>パスワードが数字のみ、英字のみなど、推測されやすいID/パスワードになっていないかご確認ください | システム設定＞メンバー管理より、適切なパスワードを設定ください。 |
| 11 | いずれか必須（※） | 管理画面のアクセス制限 | 管理画面が推測しやすい URL になっていないか | 管理画面の URL が admin など推測しやすい URL になっていないことをご確認ください。変更後にNo.5のadminフォルダが残存していないかも必ずご確認ください。 | システム設定＞セキュリティ設定より、admin 以外に変更してください。 |
| 12 | いずれか必須（※） | 管理画面のアクセス制限 | 管理画面のIP制限は実施しているか | 管理画面へのアクセスを制限しているかをご確認ください | システム設定＞セキュリティ設定より、IPアドレスを設定してください。 |

※ No. 11、No. 12の管理画面アクセス制御は、いずれか、もしくは両方の対応が必須となります。
出所：https://www.ec-cube.net/security/#securit_flow02　（セキュリティチェックシートを確認する）

!!

**本対策は、見直しの容易さや、目下の漏えい事案の全体の約7割をカバーできることから、早急な措置が求められます（所要期間：設定変更とテスト対応でおおよそ数日程度）。**

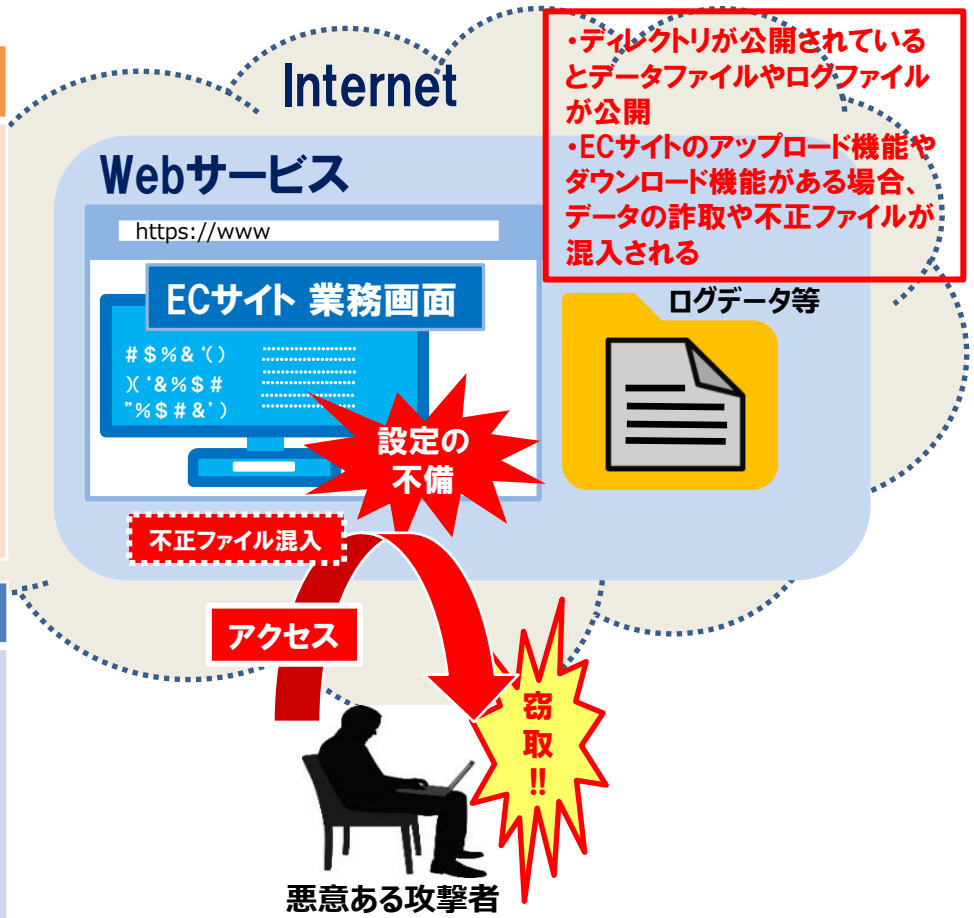
# 1-2-1. データディレクトリの露見に伴う設定の不備①

## 攻撃リスク

- ECサイトの初期構築時に、重要なファイルが配置された特定ディレクトリ以下全てのディレクトリが公開されてしまっている。
- また、パッケージログファイル等も併存しており、ログファイルのうち、IDやセッションIDが窃取されてしまう。
- パッケージのアップロード、ダウンロード機能が開放されており、データの窃取や不正ファイルが混入される。

## 対策

- 公開ディレクトリには顧客データや決済データ、アクセスログなどの、加盟店において重要なファイルを配置しない。
- Webサーバや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。




!! 本対策は、見直しの容易さや、目下の漏えい事案の全体の約7割をカバーできることから、早急な措置が求められます（所要期間：設定変更とテスト対応でおおよそ数日程度）。

# 1-2-1. データディレクトリの露見に伴う設定の不備②

「EC-CUBE 2.x系 環境チェックリスト」における該当チェックポイント

| No. | 対応優先度 | カテゴリ | 項目 | 確認方法 | 対応方法 |
|---|---|---|---|---|---|
| 1 | 必須 | 意図しないディレクトリ・ファイルの露出 | data以下のファイル、フォルダが公開されていないか | EC-CUBEのURL直下（例: https://example.com/path/to/ec-cube/data など）に data フォルダが公開されていないかご確認ください。<br>もしくは、EC-CUBEの URL と同階層（例:https://example.com/path/to/ec-cube の場合 https://example.com/path/to/data）に data フォルダが公開されていないかご確認ください。<br>https://example.com/path/to/ec-cube/data/Smarty/templates/default/site_frame.tpl などにアクセスし、ファイルの中身が表示されないことをご確認ください。 | data フォルダに .htaccess というファイル名で、以下の内容を保存してください。<br><br>order allow,deny<br>deny from all<br><br>保存した後、ファイルの中身が表示されないことをご確認ください。 |
| 5 | 必須 | 意図しないディレクトリ・ファイルの露出 | 管理画面の URL を変更したにも関わらず、標準の admin フォルダが残存していないか | 管理画面の URL を標準の admin から変更した場合、admin フォルダが残っていないことをご確認ください。 | admin フォルダが残っている場合<br>使用しなくなったプログラムが含まれています。admin を削除してください。 |

出所：https://www.ec-cube.net/security/#securit_flow02（セキュリティチェックシートを確認する）

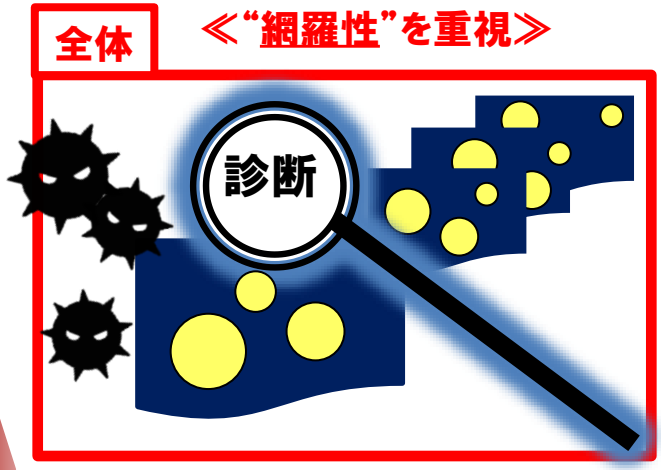
!!

**本対策は、見直しの容易さや、目下の漏えい事案の全体の約7割をカバーできることから、早急な措置が求められます（所要期間：設定変更とテスト対応でおおよそ数日程度）。**

# 1-3-1. 脆弱性診断またはペネトレーションテストの定期実施①

■ **脆弱性診断とは・・**

- ECサイトにある諸リスクの所在を明らかにするために実施する。
- 脆弱性診断を実施することにより、ECサイトにおける各リスクの所在を特定することができ、特定したリスクを修正することにより、ECサイトの機微なデータを外部に晒されるリスクの顕在化を回避することが期待できる。セキュリティ対策としては非常に有効である。
- 上記リスクの判定は、一般的には、米国発のCVSS（Common Vulnerability Scoring System：共通脆弱性評価システム）※によって管理されている。このCVSSでは、脆弱性の深刻度が10点満点中「4.0」点以上の脆弱性については修正することが推奨されている。（言い換えれば、未対処の脆弱性が4.0未満であること）*（カード情報保護対策の一方策であるPCI DSSでも規定されており、要件6や要件11などがこの項目に該当）*。

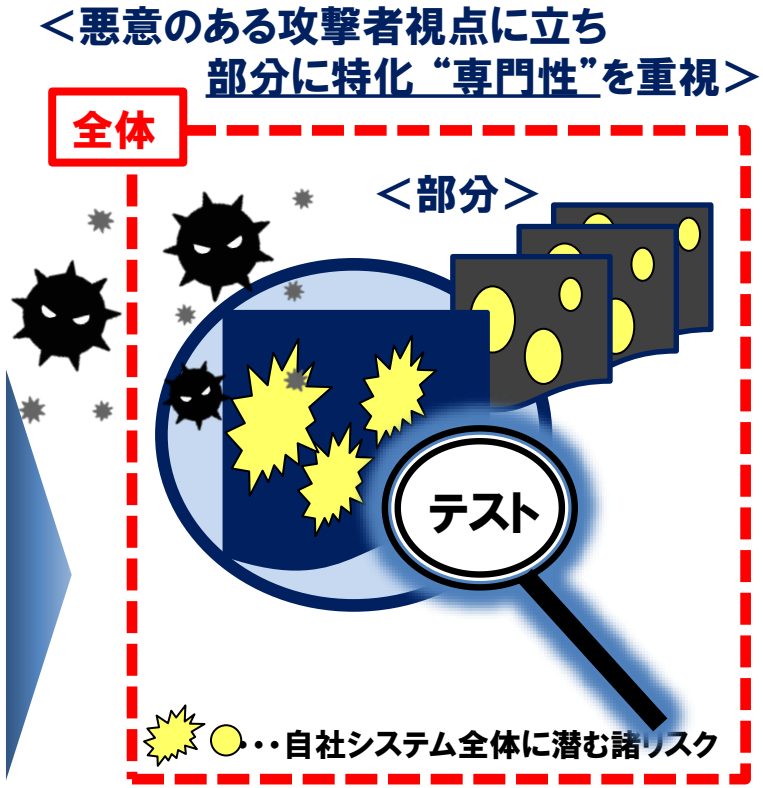



※（参考）詳しくは、
下記 IPA：独立行政法人情報処理推進機構も併せて参照。
https://www.ipa.go.jp/security/vuln/CVSS.html

# 1-3-1. 脆弱性診断またはペネトレーションテストの定期実施②

■ **ペネトレーションテストとは、脆弱性診断との相違点は・・**

- 前述の脆弱性診断とペネトレーションテストの共通点は、セキュリティ対策の一環として実施するという点。
- 脆弱性診断が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(“網羅性”を重視)する一方、本テストは、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。特定の脆弱性や問題点を発見することに主眼(高リスク資産を念頭に部分に特化、“専門性”を重視)が置かれる。




**対策**

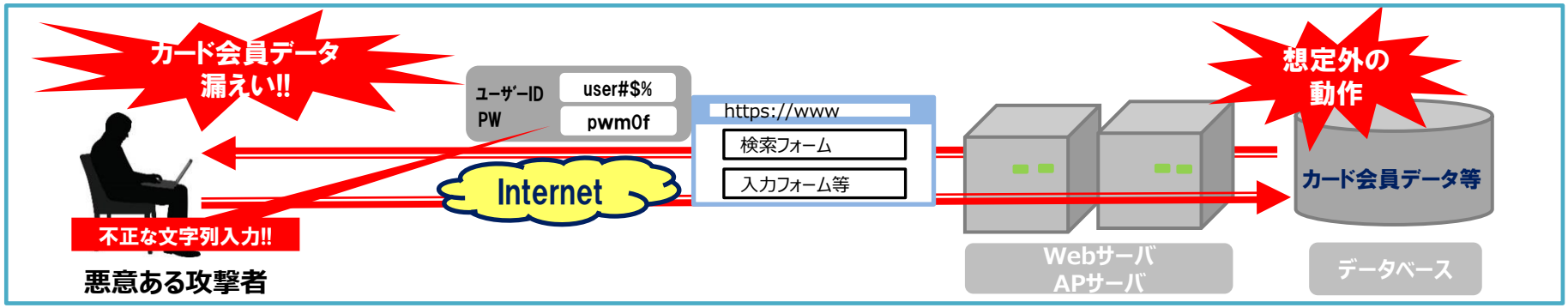
- □ 自社システムを構成する全体像を俯瞰して把握する。
- □ 脆弱性診断又はペネトレーションテストを定期的に実施し、必要な修正を行う。

# 1-3-2. SQLインジェクションの脆弱性①

## ■ SQLインジェクション攻撃とは・・・

- データベースと連携したWeb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、問題を悪用した攻撃を、「SQLインジェクション攻撃」という。

| 攻撃リスク | 対策 |
|---|---|
| ◆ パッケージをそのまま利用している場合において、セキュリティパッチを適用していない。<br>◆ カスタマイズして利用している場合において、開発部分の脆弱性に対する対処がなされていない（脆弱性診断も実施されていないことがほとんど）。 | □ 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。（バージョンアップには必要なセキュリティパッチの適用を含む。）<br>□ Webアプリケーションを開発また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。コーディングの脆弱性の対処にあたっては、「安全なウェブサイトの作り方」（IPA）を参考に対策を行う。 |



# 1-3-2. SQLインジェクションの脆弱性②

「EC-CUBE 2.x系 環境チェックリスト」における該当チェックポイント

| No. | 対応優先度 | カテゴリ | 項目 | 確認方法 | 対応方法 |
|---|---|---|---|---|---|
| 7 | 必須 | 過去の脆弱性への対応（危険度：高） | 公表された脆弱性のうち、危険度：高のものが修正されているか | https://www.ec-cube.net/info/weakness/index.php?level=3 にアクセスし、お使いのバージョンの危険度：高の脆弱性対応が済んでいるかご確認ください。 | 脆弱性に応じた修正を行ってください。<br>カスタマイズ等を行っている場合は、委託先の制作会社・開発会社へご相談ください。 |
| 13 | 推奨 | 過去の脆弱性への対応（危険度：中以下） | 公表された脆弱性のうち、危険度：中以下のものが修正されているか | https://www.ec-cube.net/info/weakness/ にアクセスし、お使いのバージョンの危険度：中以下の脆弱性対応が済んでいるかご確認ください。 | 脆弱性に応じた修正を行ってください。<br>カスタマイズ等を行っている場合は、委託先の制作会社・開発会社へご相談ください。 |

出所：https://www.ec-cube.net/security/#securit_flow02　（セキュリティチェックシートを確認する）

# 1-3-3. クロスサイト・スクリプティングの脆弱性①

■ **クロスサイト・スクリプティングとは・・・※**

- Web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、掲示板、Webのログ統計画面等、ユーザーからの入力内容やHTTPヘッダの情報を処理し、Webページとして出力するものがある。ここで、Webページへの出力処理に問題がある場合、そのWebページにスクリプト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」と呼ぶ。クロスサイト・スクリプティング攻撃の影響は、Webサイト自体に対してではなく、そのWebサイトのページを閲覧しているユーザーに及ぶ。
- Webアプリケーションにスクリプトを埋め込むことが可能な脆弱性がある場合、これを悪用した攻撃により、ユーザーのブラウザ上で不正なスクリプトが実行されてしまう可能性がある。

※（出所）IPA:独立行政法人情報処理推進機構
https://www.ipa.go.jp/security/vuln/websecurity/cross-site-scripting.html

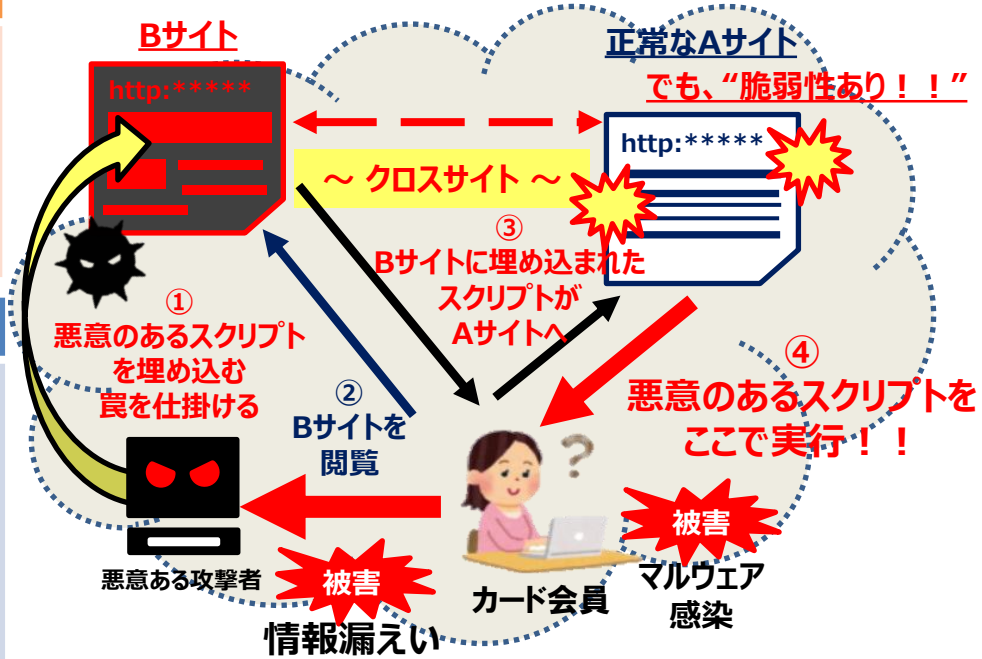
# 1-3-3. クロスサイト・スクリプティングの脆弱性②

## 攻撃リスク

- ◆ パッケージをそのまま利用している場合において、セキュリティパッチを適用していない。
- ◆ カスタマイズして利用している場合において、開発部分の脆弱性に対する対処がなされていない（脆弱性診断も実施されていないことがほとんど）。

## 対策

- □ 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。（バージョンアップには必要なセキュリティパッチの適用を含む。）
- □ Webアプリケーションを開発また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。コーディングの脆弱性の対処にあたっては、「安全なウェブサイトの作り方」（IPA）を参考に対策を行う。




※（対策の詳細）IPA：独立行政法人情報処理推進機構
https://www.ipa.go.jp/security/vuln/websecurity/cross-site-scripting.html

# 1-4-1. 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

■ **マルウェアとは・・**

- 「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、アドウェア、フィッシング、ファーミング、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、マルウェアの種類は様々。

■ **ウイルス対策ソフトとは・・**

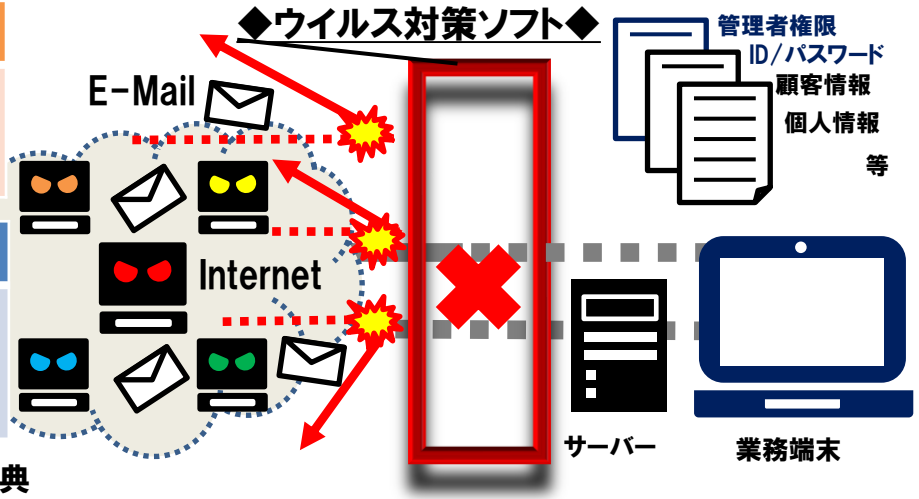
- ウイルスを検出・削除し、ウイルスに感染するのを未然に防ぐためのソフトウェア。ワクチンソフトと同義語。ウイルス対策ソフトウェア会社から市販されている。パソコンにプレインストールされているものもあるが、その場合は3ヶ月等の有効期限があるため、継続して使用するには更新手続が必要※1。

**攻撃リスク**

◆ 昨今の漏えい事案では、業務端末へのウイルスの侵入からサーバーへの感染なども考えられる。

**対策**

□ サーバー、業務端末に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。




ウイルス、スパイウェア等各種マルウェアから
サーバー、業務端末を防御！！

※1（出所）IPA：独立行政法人情報処理推進機構 ウイルス用語辞典
https://warp.da.ndl.go.jp/info:ndljp/pid/11440710/www.ipa.go.jp/security/virus/beginner/dic/dic_sub.html

# 1-5-1. クレジットマスター及び悪質な有効性確認への対策

## ■ クレジットマスター及び悪質な有効性確認とは・・

- クレジットマスター（以下、「クレマス」という。）とは、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手口である。
- また、悪質な有効性確認とは、クレマスで生成したカード情報やフィッシングで窃取したカード情報が、EC加盟店での利用等を通じて実際に使用できるカード番号かを確認する手口をいう。

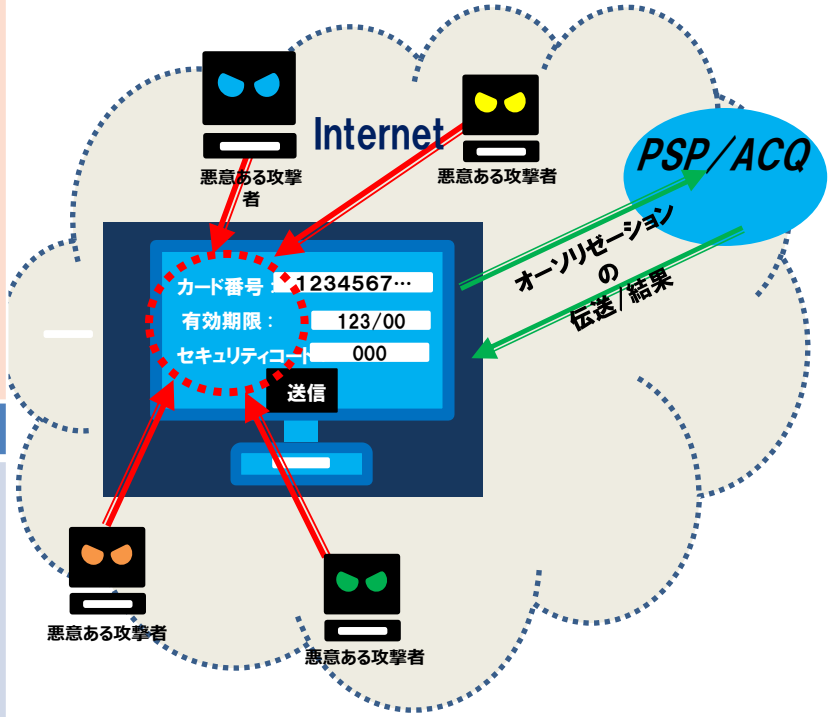
### 攻撃リスク

- ◆ 「なりすまし」による会員登録時、又は会員のログインフォームへの不正ログイン後に、クレジットカード決済の登録/変更の機能を悪用されると、有効なカード会員データを窃取される恐れがある。また、会員登録をしない場合のゲスト購入時にもクレジットカード決済の機能を悪用されると、クレマスで生成したカード番号やフィッシング等で窃取したカード番号等をもとに悪質な有効性確認を行われ、有効なカード会員データを窃取される恐れがある。
- ◆ 攻撃者は、日本国内のIPアドレスからよりも、海外のIPアドレスから悪質な有効性確認を実施することが多い。

### 対策

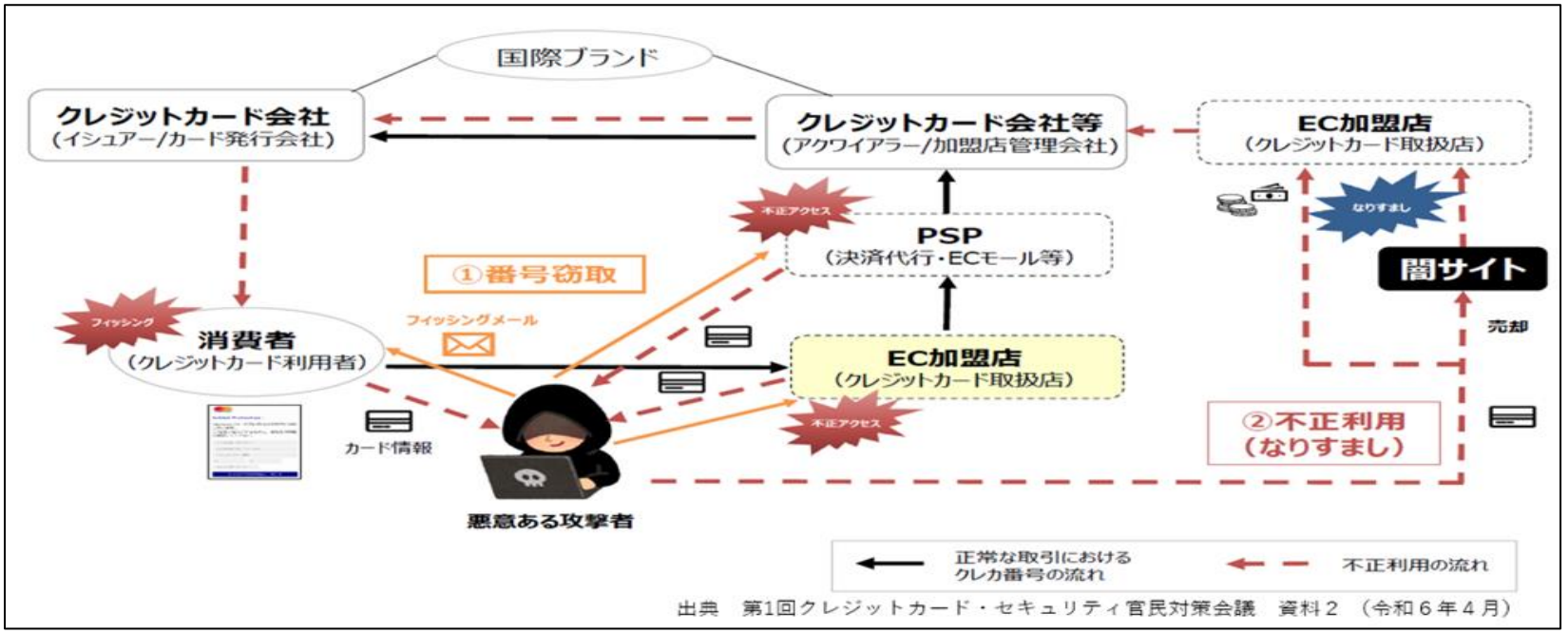
- □ 「不審なIPアドレスからのアクセス制限」を行う。特に海外からの攻撃が非常に多いため、海外からのアクセスが不要な場合は遮断を行う。
- □ 「同一アカウントからの入力制限」「オーソリ拒否時に、エラー内容が分からないようにエラー内容を非表示」にする。
- □ EMV 3-DセキュアやSMS通知など本人認証ができる対策を行う。
- □ 有効性確認の回数制限を設けるなどの対策を行う。

### ECサイト 登録会員のクレジットカード決済画面



# 2-0. 不正利用対策の概要①

- EC加盟店等の脆弱性への攻撃や不正アクセス等、クレマスによるカード情報の大量窃取の他、最近ではカード情報のみならず顧客属性情報を丸ごと窃取するEC加盟店・カード会社等を模したフィッシングが主流となっている。
- この窃取したカード情報や属性情報、アカウント(ID)等を利用し、以下の不正が行われている。
  - ・カード情報等を利用し、不正なアカウントの登録を行う「不正アカウント作成」
  - ・アカウント(ID)や類推したパスワード等を利用して不正にログインし、会員属性情報の変更等を行う「アカウント乗っ取り」
  - ・Webサイトの「ゲスト購入」の決済機能を利用した不正利用や悪質な有効性確認

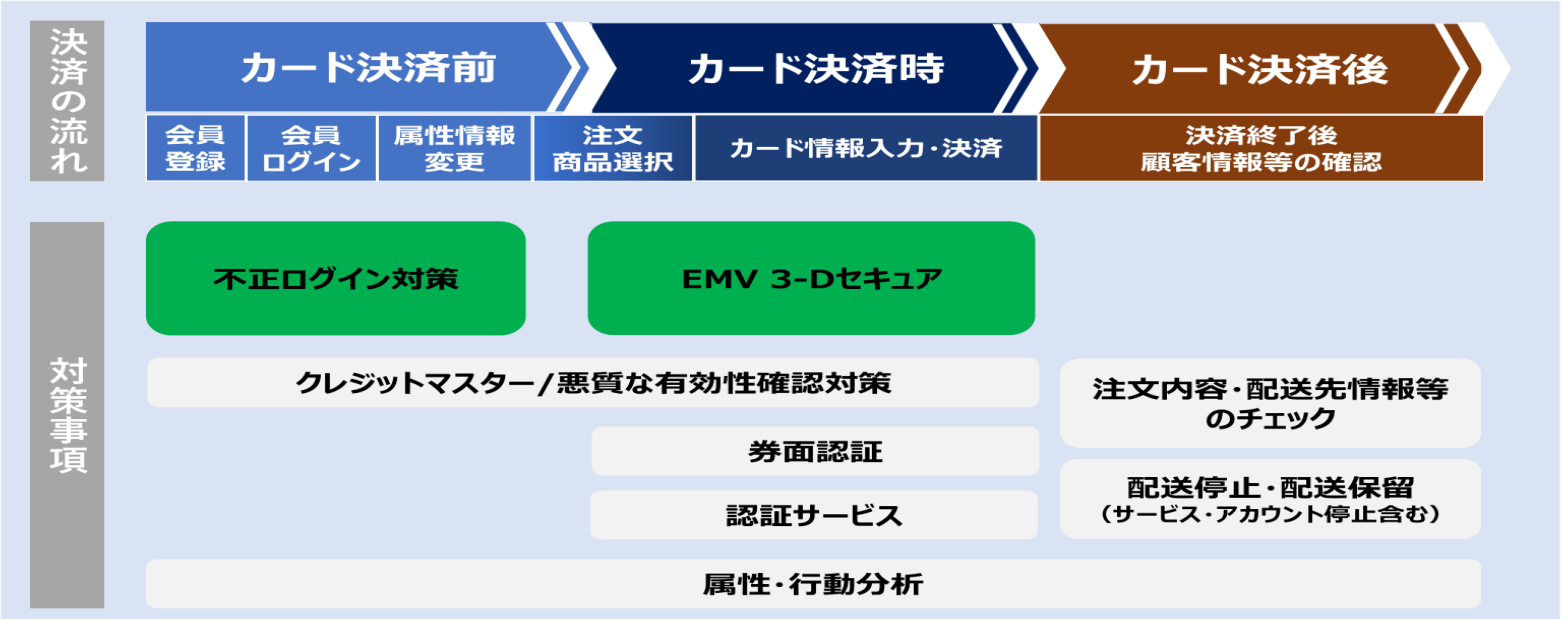



出典　第1回クレジットカード・セキュリティ官民対策会議　資料2　(令和6年4月)

# 2-0. 不正利用対策の概要②

- EC加盟店における不正利用は、Webサイトにおける購入・決済の前から行われており、不正利用を防止するには、Webサイトの利用を開始する「カード決済前」、商品を購入する「カード決済時」、商品の受け渡しが行われる「カード決済後」の場面まで、取引の流れを考慮した場面ごとに対策を行い、不正利用対策の実効性を高めることが重要であり、これが「線の考え方」に基づく対策の導入である。

- 指針対策である「カード決済時」の「EMV 3-Dセキュアの導入」及び「カード決済前」の「適切な不正ログイン対策の実施」を中心として、「カード決済後」の場面まで、「線の考え方」に基づく適切な対策の導入により、不正利用の防止を図る。



# 2-1-1. 不正ログイン対策（決済前の対策）の概要①

◆ 不正ログイン対策とは

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・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クレジットカード情報や会員属性情報、アカウント（ID）・パスワード等を利用して不正にログインし、不正利用されることがある。これらの対策を総じて不正ログイン対策とする。

◆ 不正ログインを起点とした不正利用の原因として以下が想定される。

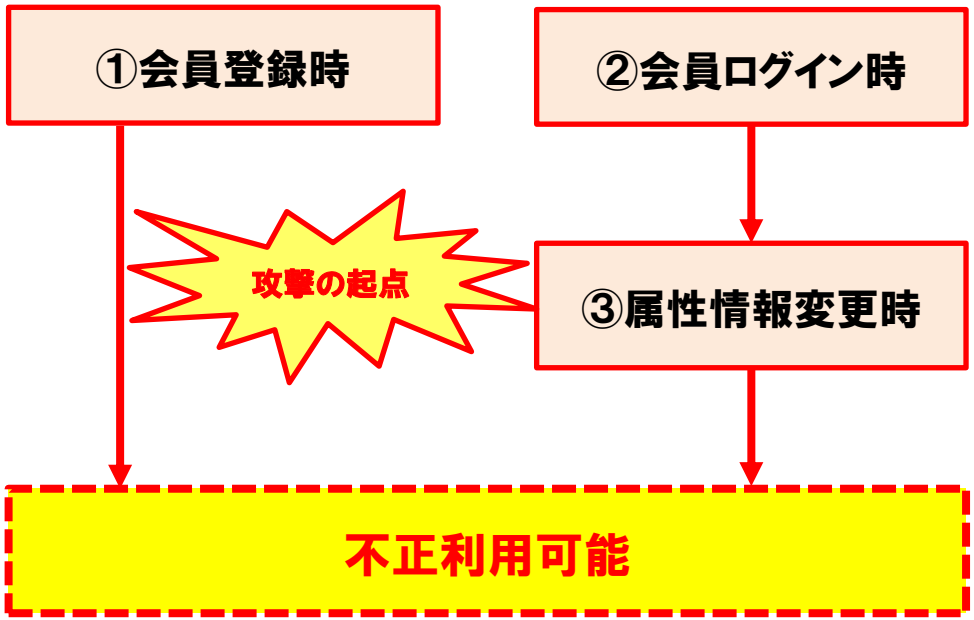
- 不正なアカウントが作成される。
- フィッシングメール等で不正取得されたアカウント情報及びアカウント/パスワードクラッキングにより、不正ログインをされる。
- 不正ログインによりカード番号や属性情報の変更が可能となり不正利用される。

◆ 不正ログインの場面について、実際の事例等から以下を想定。

| 対策箇所 | 説明ページ |
|---|---|
| 2-1-2 会員登録時の対策 | P29 |
| 2-1-3 会員ログイン時の対策 | P30 |
| 2-1-4 属性情報変更時の対策 | P31 |

# 2-1-1. 不正ログイン対策（決済前の対策）の概要②

## ■ 攻撃の起点として狙われる3つの場面




・①会員登録時や②会員ログイン時、③属性情報変更時において、不正ログイン対策が重要となる。

・特にEC加盟店の登録会員の会員ログインフォームは、インターネット経由でアクセスが可能であり、攻撃者の攻撃の起点となり得るので注意が必要である。これは、複数のEC加盟店へ機能を提供する大手ECモールにも同様のことが言える。

### 各場面における想定リスク

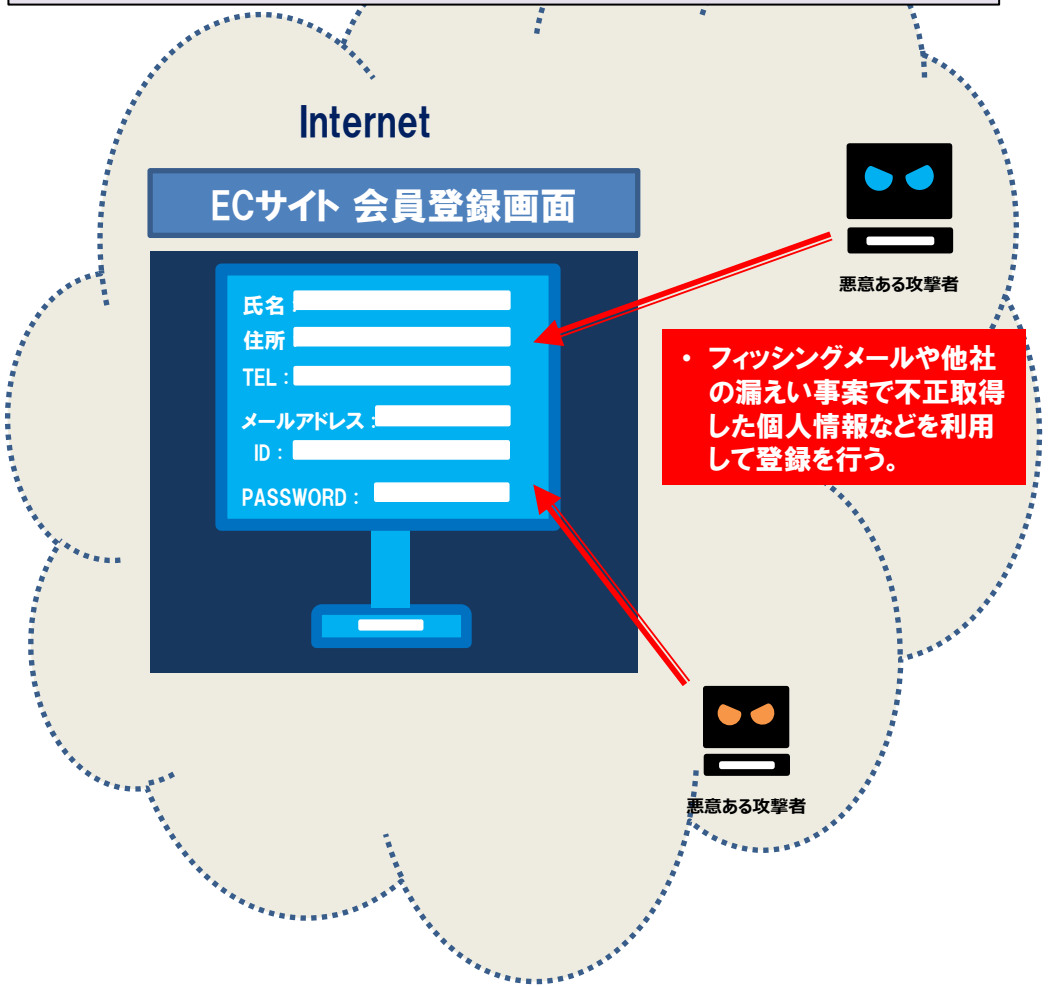
**①会員登録時**
- 不正なアカウントが作成されるリスクがある。

**②会員ログイン時**
- フィッシングメール等で不正取得されたアカウント情報及びアカウント/パスワードクラッキングにより、不正ログインをされるリスクがある。
- 不正ログインによりカード番号や属性情報の変更が可能となり、不正利用されるリスクがある。

**③属性情報変更時**
- フィッシングメールや漏えい事案などで窃取した個人情報を悪用して、配送先の変更や登録情報の変更を行うことができ、不正利用やWalletチャージも可能となるリスクがある。

# 2-1-2. 会員登録時の対策

※会員登録時だけではなく、商品配送等のため、個人情報の入力を促す場面も含まれる



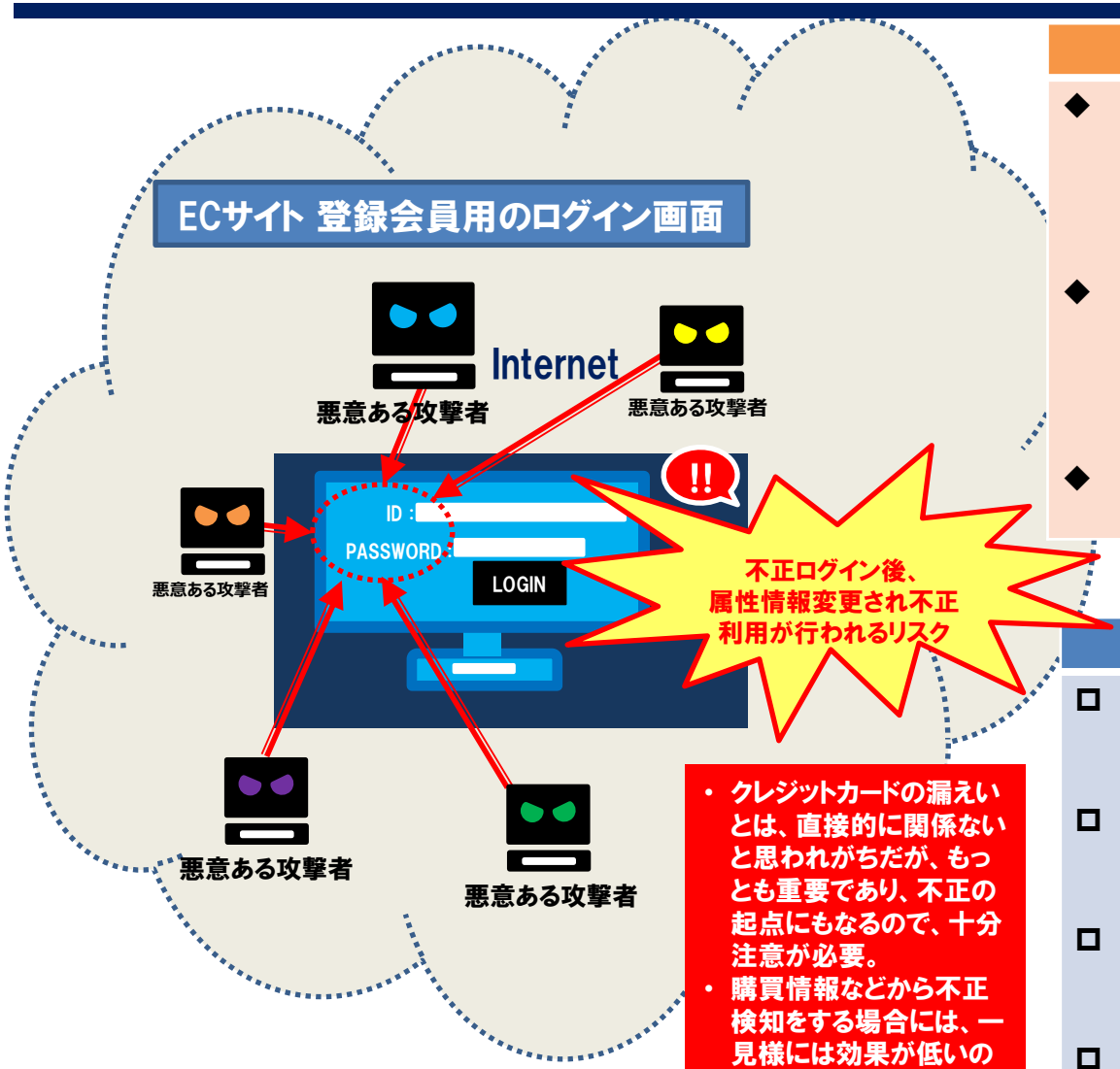

## 攻撃リスク

- ◆ フィッシングメールによる個人情報の不正取得や他社の漏えい事案などからの漏えいされたデータを用いて、「なりすまし」することが可能である。
- ◆ 海外の攻撃者が、日本の攻撃者に指示を行う手口もあり、当該手口に対しては、IPアドレスによって不正利用と見分けることが困難である。

## 対策

- □ 会員登録時の個人情報（氏名・住所・電話番号・メールアドレス等）が不自然な表示ではないか、また不自然な組み合わせではないかを確認する。攻撃者が海外である場合には、漢字やカナなどの入力されている個人情報が間違っている場合が多く、確認を行う。
- □ 「不審なIPアドレスからのアクセス制限」を行う。特に海外からの攻撃が非常に多いため、海外からのアクセスが不要な場合は遮断を行う。
- □ 不正ログインをされた場合でも、会員本人に気づきを与えられるように、2段階認証などによる本人認証を行う。
- □ 属性・行動分析を利用する。

# 2-1-3. 会員ログイン時の対策




- クレジットカードの漏えいとは、直接的に関係ないと思われがちだが、もっとも重要であり、不正の起点にもなるので、十分注意が必要。
- 購買情報などから不正検知をする場合には、一見様には効果が低いので注意!!

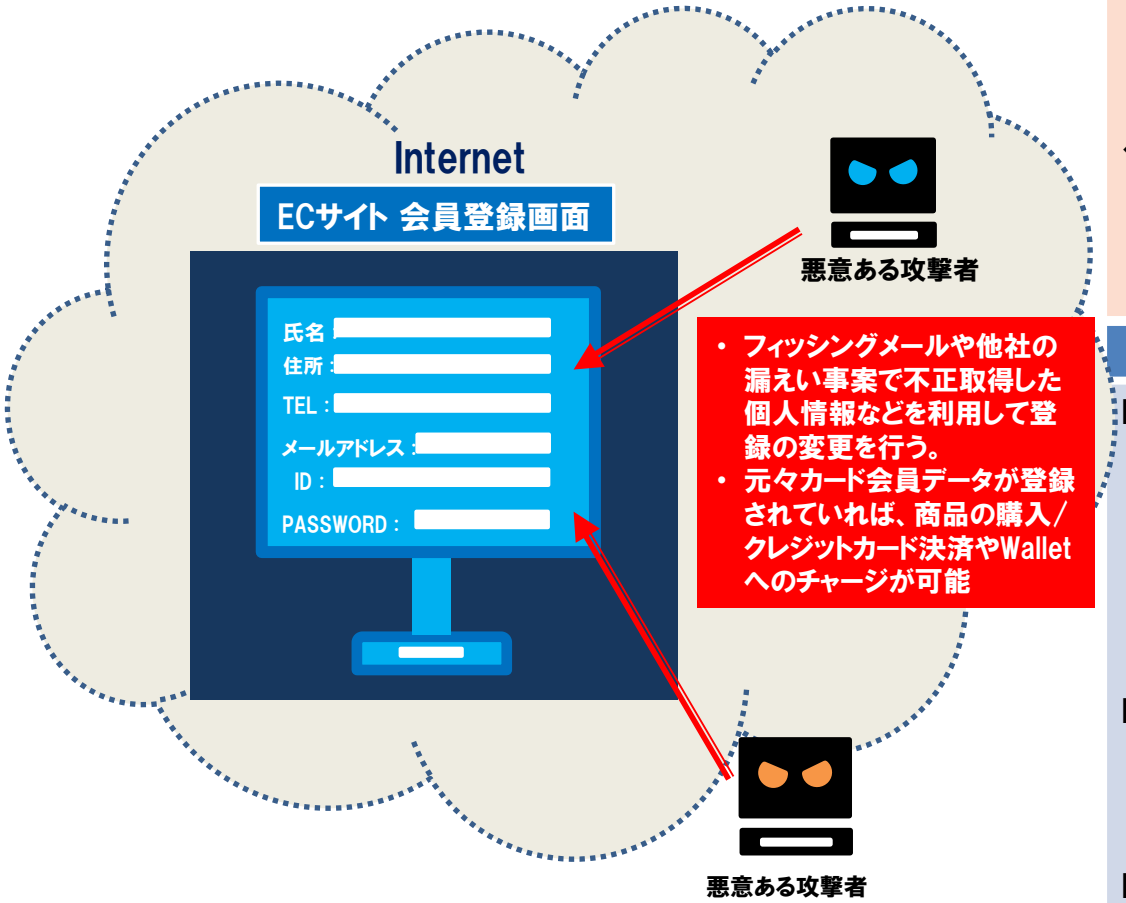
## 攻撃リスク

- ◆ 会員用のログイン画面は、公開する必要があり、アクセス制限が難しく、このような状況を悪用し、フィッシングメールや他社の漏えい事案などで不正取得した「ID/パスワード」を利用した、アカウント/パスワードクラッキングが頻繁に行われている。
- ◆ IDはメールアドレスであることが多く、更に静的パスワードはパスワードクラッキング等により推測されやすい。また、「なりすまし」による不正ログインが実行されても、正常なログインであるため、EC加盟店は不正ログインに気づきにくい。
- ◆ 攻撃者は海外からクラッキングを実施することが多い。

## 対策

- □ 「不審なIPアドレスからのアクセス制限」を行う。特に海外からの攻撃が非常に多いため、海外からのアクセスが不要な場合は遮断を行う。
- □ アカウント/パスワードクラッキングの対応として、ログイン試行回数の制限強化、スロットリングを行う。
- □ 不正ログインをされた場合でも、会員本人に気づきを与えられるように、2段階認証などによる本人認証を行う。
- □ 会員ログイン時のメールやSMS通知などを行う。
- □ その他、「デバイスフィンガープリント」等を利用する。

# 2-1-4. 属性情報変更時の対策




## 攻撃リスク

- ◆ 不正ログインにより、攻撃者が不正に窃取した真正なカード会員の属性情報を変更し、当該アカウントによるWallet チャージ等の不正利用が発生する恐れがある。
- ◆ 海外の攻撃者が、日本の攻撃者に指示を行う手口もあり、当該手口に対しては、IPアドレスによって不正利用と見分けることが困難である。

## 対策

- □ 属性情報変更時の個人情報（氏名・住所・電話番号・メールアドレス等）が不自然な表記ではないか、また不自然な組み合わせではないかを確認する。攻撃者が海外である場合には、漢字やカナなどの入力されている個人情報が間違っている場合が多く、確認を行う。
- □ 「不審なIPアドレスからのアクセス制限」を行う。特に海外からの攻撃が非常に多いため、海外からのアクセスが不要な場合は遮断を行う。
- □ 属性情報などの変更時には、元々登録されていた本人に対して気づきを与えられるように2段階認証などによる本人認証を行う。
- □ 属性・行動分析やデバイスフィンガープリント等を利用する。

# 2-2. 決済時の対策

## ■ 決済時の観点

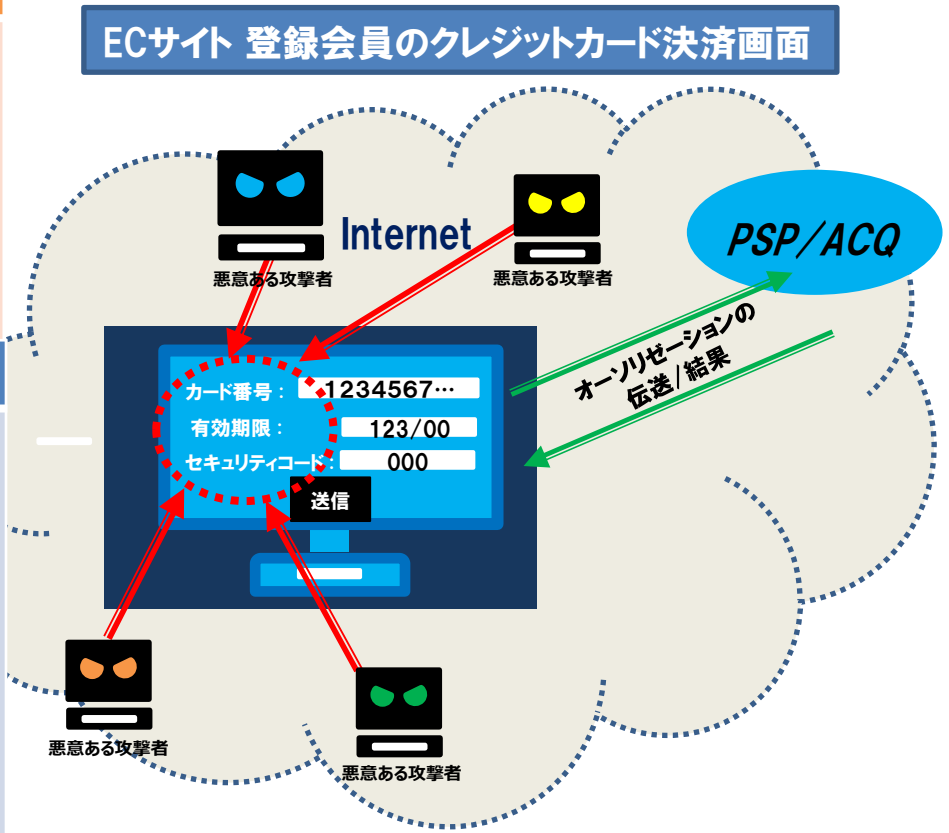
- インターネットを通じてクレジットカード決済が可能なECサイトでは、決済画面を通じて、窃取された真正なカード情報等を利用して決済が可能である。これらの利便性を悪用して他人に「なりすまし」をして、様々な商品を購入されるリスクが一般的である。

### 攻撃リスク

- ◆ 他社ECサイトの漏えい事案やクレマス、悪質な有効性確認、フィッシングメールなどにより窃取された真正なカード情報等を利用して、決済時に「なりすまし」による商品購入が行われる。
- ◆ 不正なアカウント登録、あるいは正規のアカウントに不正ログインをして商品を購入される。

### 対策

- □ 真正なカード会員データによる「なりすまし」の対策として「EMV 3-Dセキュア」を導入し、カード会社（イシュアー）側の本人認証を経てオーソリを行う。
- □ オーソリ時にセキュリティコードを利用した券面認証を行いイシュアー側の確認を行う。
- □ 決済時に属性・行動分析を活用し、真正なカード会員の利用であるかのリスク判断を行う。
- □ PSPまたはサービス提供事業者が提供する固有の認証サービスを用いて、真正なカード会員本人であることを確認する。



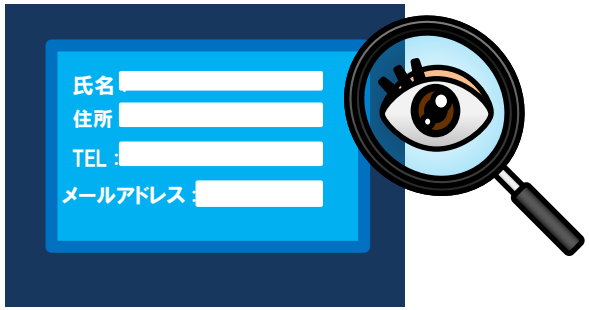
# 2-3. 決済後の対策

## ■ 被害防止対策の観点

- 不正購入された商品の配送を未然に防ぐために、加盟店自ら配送情報を確認し、被害防止に努める必要がある。

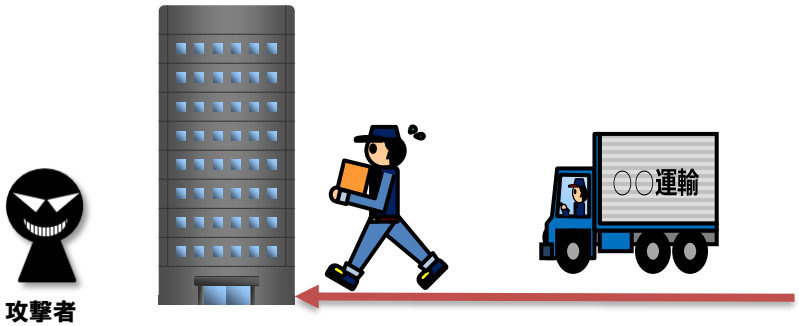
### 攻撃リスク

- ◆ 攻撃者は、決済時に他人の真正なカード会員データを利用して購入した商品を現金化するために、空き家、受け子、置き配、配送事業所、不正な配送先等で商品を受け取る。
- ◆ デジタルコンテンツやオンラインチケットなどの配送を伴わない商品については、決済後即時又は比較的短期間に利用される。




### 対策

- □ 不正に購入された商品等が攻撃者などに渡らないように、商品の配送時に「氏名表記」「姓名カナ表記」「住所」「電話番号」等の規則性や組合せを担当者による目視などで確認または照合し、配送停止や配送保留を行う。
- □ カード会社によるモニタリングにて不正利用の懸念がある場合、カード会社からのEC加盟店に対する配送停止・配送保留の要請に協力する。
- □ 属性・行動分析を活用し、上記の属性情報を確認の上、配送停止・配送保留を行うよう努める。
- □ 配送を伴わない商品については、同じ攻撃者によるアクセスを防ぐため、決済前の不正ログイン対策や決済時の不正利用対策の強化に努める。
- □ 配送を伴わない商品については、アカウントの停止などを行うよう努める。



# 3. 最後に・・・

- 技術の進歩に伴い、不正利用の手口とそれに対するセキュリティ対策は変化するものであり、セキュリティ対策の取組に終わりはありません。
- EC加盟店においては非保持化の実現に加えて、それ以前に自社のシステム、Webサイトの「脆弱性対策」を徹底し、自社で構築したシステムに対し、不断の対策を講じ続ける姿勢が求められます。
- オープンソースを利用している場合は、開発元からの注意喚起や開発元へ積極的な情報提供を求め、常にセキュリティパッチ等「脆弱性対策」の追加的な対策を講じる必要があります。
- またECサイトを構築、運用・保守業務を外部に委託する場合は、EC加盟店が行うべき「脆弱性対策」「不正利用対策」の理解のもと構築・運用を行うことを求め、EC加盟店の責任において適切な対策を講じる必要があります。
- 漏えい事案を発生させてしまった場合や、不正利用が発生した場合は、速やかに契約しているカード会社（アクワイアラー）やPSPにご連絡をお願いいたします。

# 【参考資料】

- **経済産業省 ： 2019年12月20日**

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

  https://warp.da.ndl.go.jp/info:ndljp/pid/11433651/www.meti.go.jp/press/2019/12/20191220013/20191220013.html

- **株式会社イーシーキューブ**

  01_ご利用のEC-CUBEのバージョンを確認する

  EC-CUBEのバージョンにより対応・対策が異なりますので、まずはEC-CUBEのバージョンをご確認ください。

  https://www.ec-cube.net/security/#securit_flow02

- **IPA（Information-technology Promotion Agency, Japan 独立行政法人情報処理推進機構）**

  安全なウェブサイトの作り方

  https://www.ipa.go.jp/security/vuln/websecurity/index.html

  「EC サイト構築・運用セキュリティガイドライン」

  https://www.ipa.go.jp/security/guide/vuln/guideforecsite.html

- **個人情報保護委員会（PPC：Personal Information Protection Commission）**

  漏えい等の対応（個人情報）：https://www.ppc.go.jp/personalinfo/legal/leakAction/

  個人情報の研修資料・ヒヤリハットコーナー：https://www.ppc.go.jp/personalinfo/hiyarihatto/

  注意情報一覧：https://www.ppc.go.jp/news/careful_information/#tab01_anchor01

# 【改訂履歴】

| | 版数 | 改訂日 | 改訂概要 |
|---|---|---|---|
| 試行運用資料 | セキュリティ・チェックリスト第1版 | 2021年3月 | • 試行運用資料として策定 |
| | セキュリティ・チェックリスト第2版 | 2022年3月 | • 既知の脆弱性対策として脆弱性診断（またはペネトレーションテスト）を追加<br>• 判明した脆弱性への対応策の一つととしてクロスサイト・スクリプティングを追加<br>• ウィルス、マルウェア対策ソフトの導入、運用を追加 |
| | セキュリティ・チェックリスト第3版 | 2023年6月 | • 「不正ログイン対策」として決済前の3つの場面における対策を追加 |
| 附属文書21 | | 2024年3月 | • 附属文書21として附属文書化 |
| 附属文書20<br>別紙b | EC加盟店におけるセキュリティ対策導入ｶﾞｲﾄﾞ補足資料 | 2025年3月 | • 「脆弱性対策」「不正ログイン対策」の指針対策化に伴う関連文書の整理・統合により、附属文書20の補足資料に位置付けを変更するとともに資料名を変更<br>• 「不正利用対策の概要」「カード決済時」「カード決済後」の対策を追加 |