セキュリティ・チェックリスト

― EC加盟店における基本的なセキュリティ対策 ―

第3版

クレジット取引セキュリティ対策協議会

【改訂履歴】

版数	改訂日	概要
第1版	2021年3月	策定
第2版	2022年3月	• P9 EC加盟店のビジネス上のリスクにおけるコスト負担について、例示を追記。 • P13-23、いま必要なセキュリティ対策【重点対策】に関し、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)を追加すると共に、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への対策を追加、併せて、ウィルス、マルウェア対策ソフトの導入、運用を追加し、従来【3つの重点対策】としていたものを【4つの重点対策】とし、これに伴いレイアウトを再構成。 • P26最後に・・について、情報漏えい発生時の対処について追記。
第3版	2023年6月	• P12-24 従前【4つの重点対策】としていたものを「カード会員データの漏えい等の対策」と5つの対策とし、レイアウトを再構成。 • P25-29 新たに「不正ログイン対策」として3つの場面における対策を追加。 • P30 3.追加的な対策の参照情報としてIPAが取りまとめた「EC サイト構築・運用セキュリティガイドラインのURLを記載。

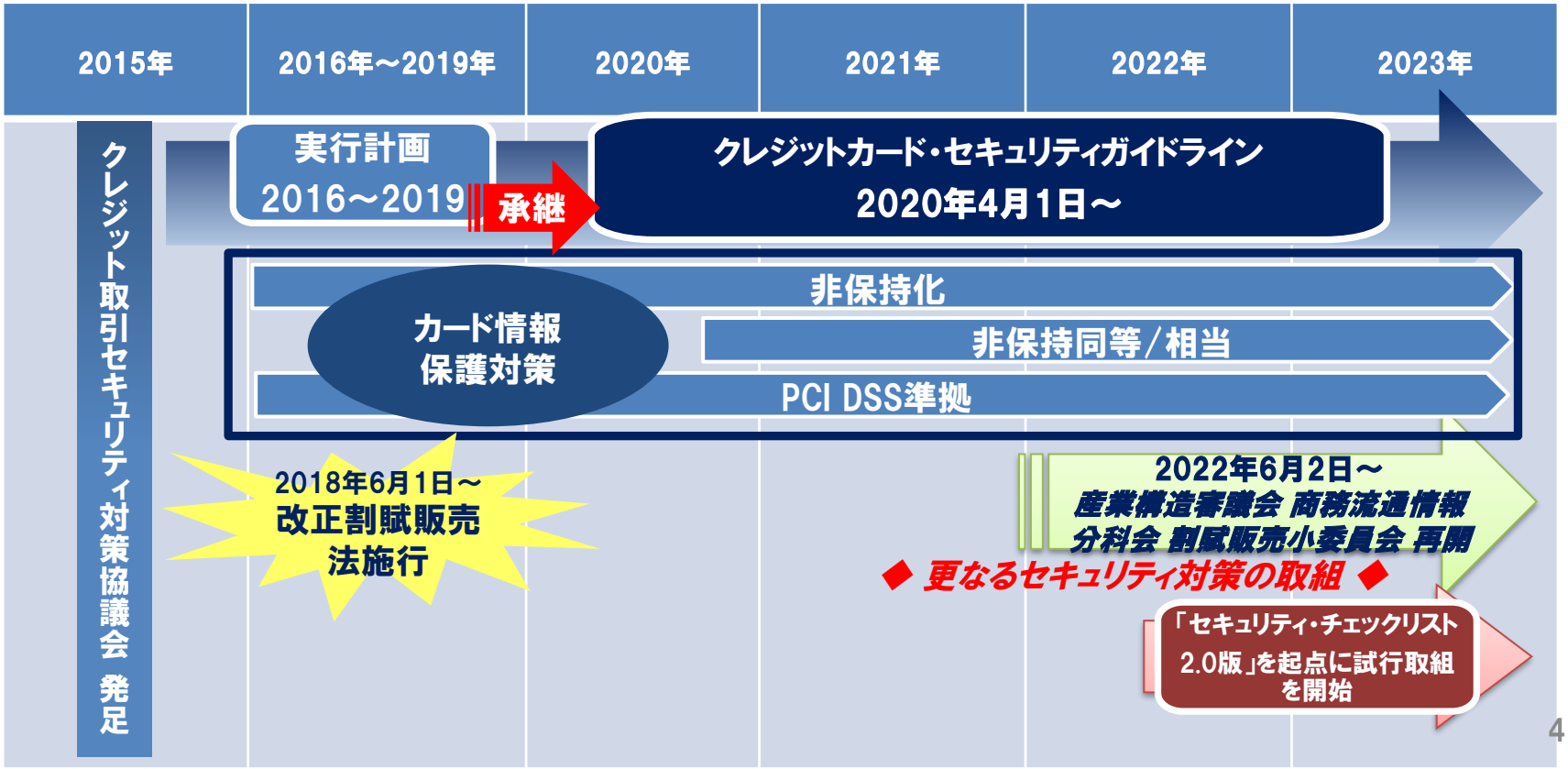
〈本書の目的〉

- ✓ クレジットカード取引に関わる全てのステークホルダーは、「クレジットカード・セキュリティガイドライン」に基づき、各々に求められるセキュリティ対策を講じております。
- ✓ EC加盟店においては、2018年6月より施行の改正割賦販売法により、同対策の措置が義務化され、PCI DSSに準拠しない加盟店については非保持化の実現により求められるセキュリティ対策を措置しているところ、カード漏えいの手口の変化もあり、一層のセキュリティ対策強化の取組が喫緊の課題となっております。
- ✓ 本書は、このような状況を踏まえ、今後の必要な取り組みを示し、EC加盟店におけるセキュリティ意識の向上と基本的なセキュリティ対策の強化、これによるカード会員データの漏えい及び不正利用の防止を目的として取りまとめております。
- ✓ なお、EC加盟店のみなさまにとっての理解促進に資するよう、第１部でEC加盟店におけるセキュリティ対策義務について解説した上で、第２部でEC加盟店における対策について解説する構成となっております。

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

- 加盟店におけるセキュリティ対策は改正割賦販売法により義務化されることとなり、非保持化（非保持同等／相当）の実現もしくはPCI DSS準拠が求められている。
- しかし、最近の傾向では「非通過型」により非保持化を達成したEC加盟店における漏えい事故が主流となりつつあり、脆弱性対策、ウイルス対策、管理者権限の管理、デバイス管理等の基本的なセキュリティ対策が実施されていないため、外部からの不正アクセスやウイルスの侵入、システムの改ざんや機器の脆弱性により、カード会員データを不正に窃取される事案が発生している。
- 上記を踏まえ、クレジット取引セキュリティ対策協議会では、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。



2. 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）とクレジットカード・セキュリティガイドライン（実務指針）で定める対策の他に求められる対策を本セキュリティ・チェックリストで定める。

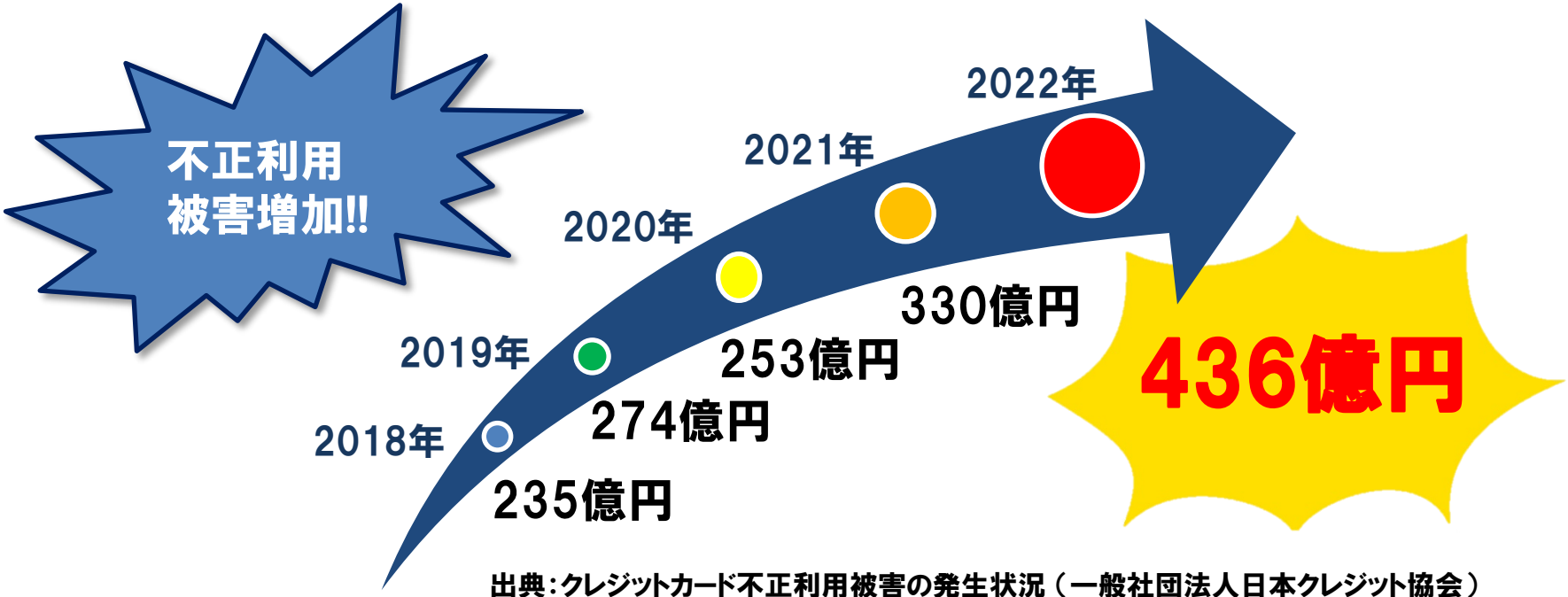
	割賦販売法	クレジットカード・セキュリティガイドライン
	法令上の義務	実務指針
加盟店の義務	① クレジットカード番号等の適切な管理 （同法 第35条の16第1項） ② 同 不正利用の防止 （同法 第35条の17の15）	① 非保持化（非保持同等/相当）もしくはPCI DSS準拠 （同ガイドライン P13～P27） ② オーソリゼーション処理の体制整備と加盟店契約上の善良なる管理者の注意をもって不正利用を防止/リスクや被害状況に応じた不正利用対策の導入 （同ガイドライン P38～P45）

〈上記以外に2025年4月より求められる対策〉

	セキュリティ・チェックリスト
今後必要となる対策	■ 非保持化を達成したEC加盟店からカード情報が窃取されており、最近の漏えい事故の傾向等を踏まえ、自社システムの定期的な点検を行い、この点検結果に基づき、必要あれば追加的な対策を導入するなどの適切な対応をとることが求められる。 （ガイドライン P13）

3. 情報漏えい事案の状況

- 非保持化が進捗する一方で、不正利用被害額は、依然、増加傾向にある。
- 最近は非保持化を達成したEC加盟店における漏えいが主流となりつつあり、脆弱性対策、ウイルス対策、管理者権限の管理、デバイス管理等の基本的なセキュリティ対策が実施されていないため、外部からの不正アクセスやウイルスの侵入、システムの改ざんや機器の脆弱性により、カード会員データを不正に取得される事案が発生している。
- 非保持化実現したEC加盟店であっても、法令で義務化されている方策の実現に加え、ECサイト構築上のリスクとその顕在化により情報漏えいに繋がり得ることを十分認識した上で、基本的な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）

4. ECサイト構築時の留意点

◆ 加盟店自らにおいて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加盟店での情報漏えい事案が増加傾向にある。オープンソースソフトウェアを利用している場合は、導入から時間が経ち、セキュリティパッチ更新の不備や脆弱性対策の不備が無いようにEC加盟店の責任で対策する必要がある。

(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 □ 拡張性が高い	□ ECサイトの構築がし易い □ 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 □ 独自性が打ち出しづらい □ 拡張性が低い	□ サーバー管理が必要 □ 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 □ 障害発生時は自社責任	□ 導入費用が高い □ 保守費用が発生

5. サイト構築、運用・保守の外部委託時の留意点

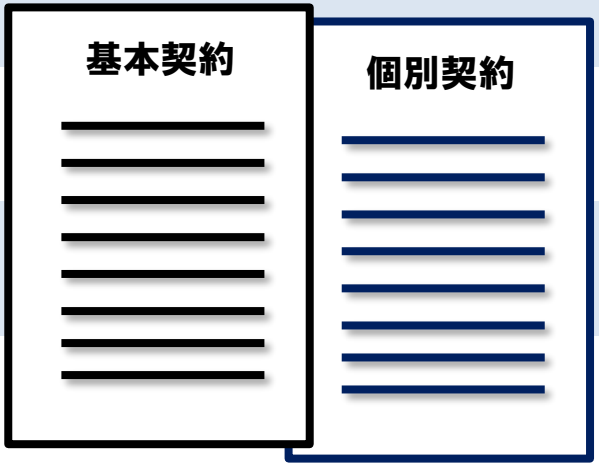
◆ ECサイトを構築し、運用・保守業務を外部に委託する場合もEC加盟店の責任において適切なセキュリティ対策を講じる必要がある。

〈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が措置され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？？



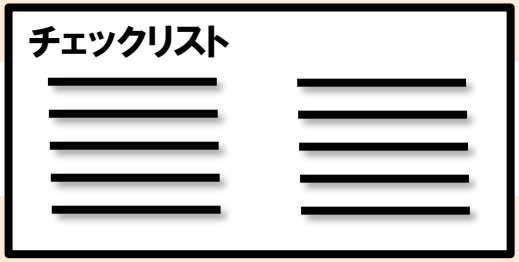
<留意点> 一般的な基本契約には、脆弱性対策やパッチ適用などのセキュリティ対策等、上述の項目が盛り込まれておらず個別契約となるケースが多い。セキュリティ対策については自ら提案や説明を委託先へ依頼することが重要。

〈ポイント②〉“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？？



6. 情報漏えいを発生させた場合の影響

◆ 割賦販売法では、加盟店においても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加盟店における対策

0. EC加盟店における対策の概要

- ◆ 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。
- ◆ 想定されるセキュリティ対策について以下の通り説明する。

攻撃手法例	対策	説明ページ
□ 管理者のアカウント/パスワードクラッキングによる不正アクセス □ 既知の脆弱性/設定の不備を利用した不正アクセス □ 有効性確認・クレジットマスター	【重点対策】 1. カード会員データの漏えい等の対策	P12～
□ 他人のカード会員データの悪用 □ 他人の登録ID/パスワードの悪用 □ ユーザのアカウント/パスワードクラッキングによる不正アクセス	2. 不正ログイン対策	P25～
-	3. 追加的な対策	P30～

1. カード会員データの漏えい等の対策の概要

◆ 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 悪質な有効性確認、クレジットマスターへの対策	P24～

1-1-1 管理者画面のアクセス制限不備と管理者のID/PW管理不足①

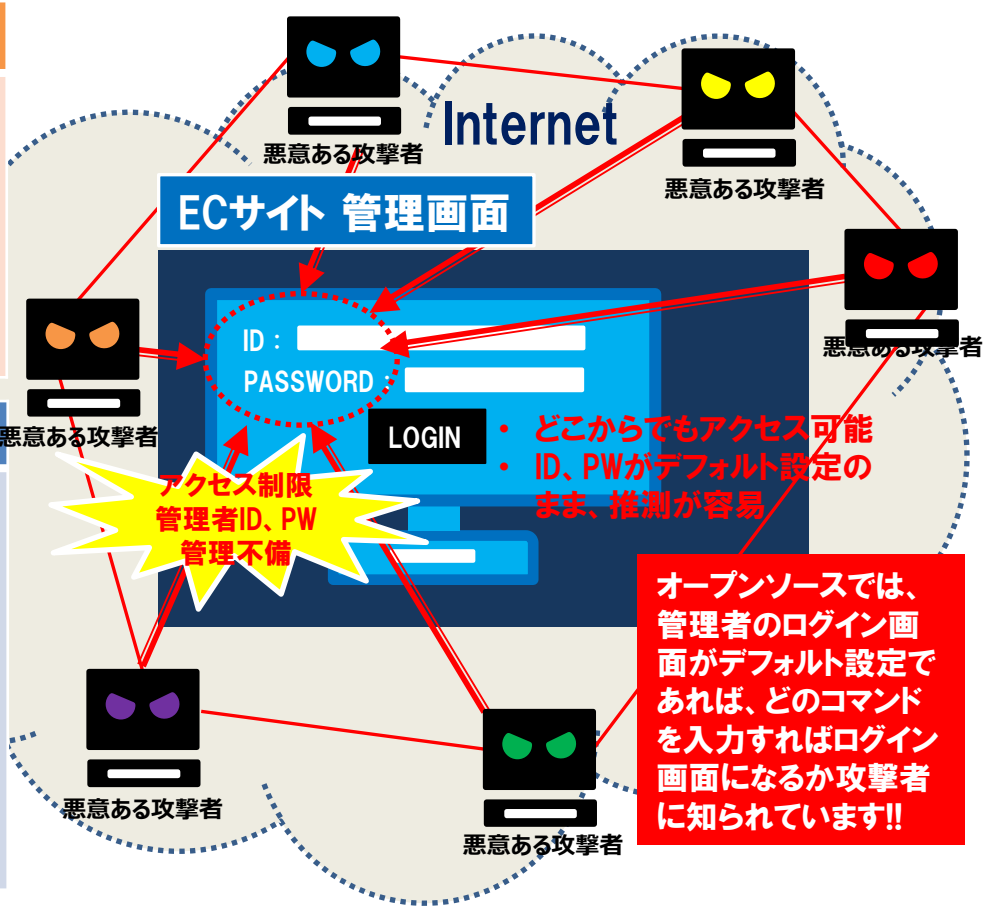
攻撃リスク

- ◆ 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二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。

※ PCI DSS ver4.0では、「10回」以下とされています。



!! 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 管理者画面のアクセス制限不備と管理者のID/PW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ユーザーIDが admin など推測されやすいもの パスワードが8文字以下 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/news/detail.php?news_id=349

!! 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）。

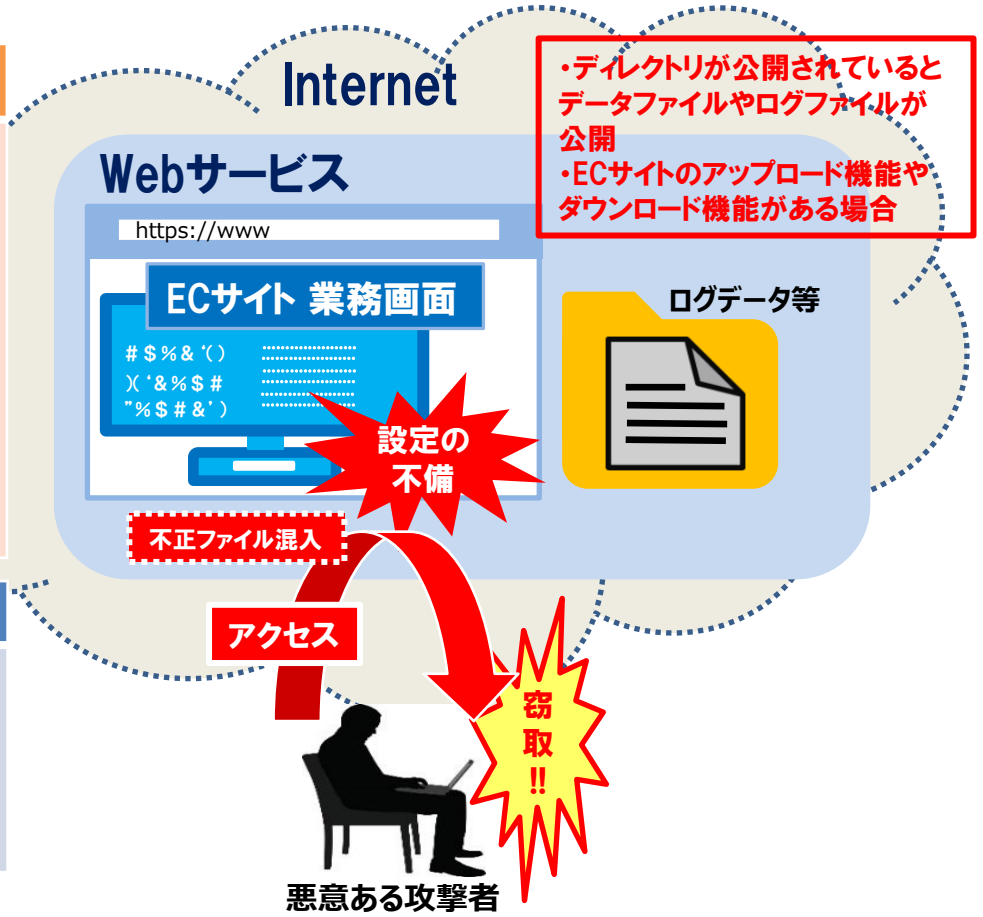
1-2-1 データディレクトリの露見に伴う設定の不備①

攻撃リスク

- ECサイトの初期構築時に、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が詐取されてしまう。
- 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、データの詐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）。

【重点対策】

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。 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。 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。 order allow,deny deny from all 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 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/news/detail.php?news_id=349

!!

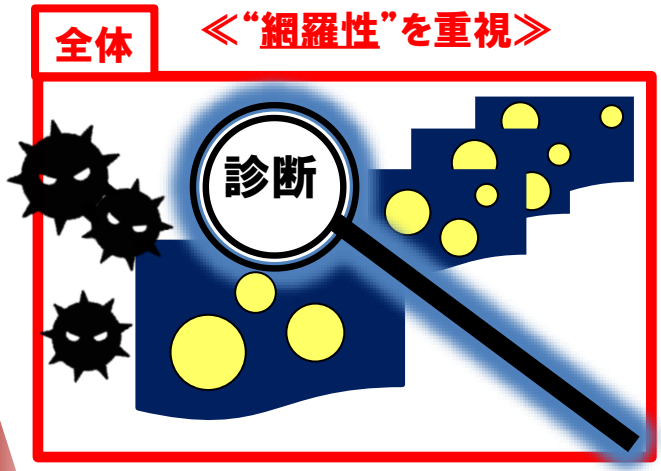
本対策は、見直しの容易さや、目下の漏えい事案の全体の約7割をカバーできることから、早急な措置が求められます（所要期間：設定変更とテスト対応でおおよそ数日程度）。

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

【前提の確認】 ロ 自社システムを構成する全体像を俯瞰し、把握できていますか？

■ **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。人間に例えると健康診断のようなもの。
- 年次で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ます。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。
- 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）*。



“既知の脆弱性”
（世の中に既に広く知れ渡っている脆弱性）
を把握！！

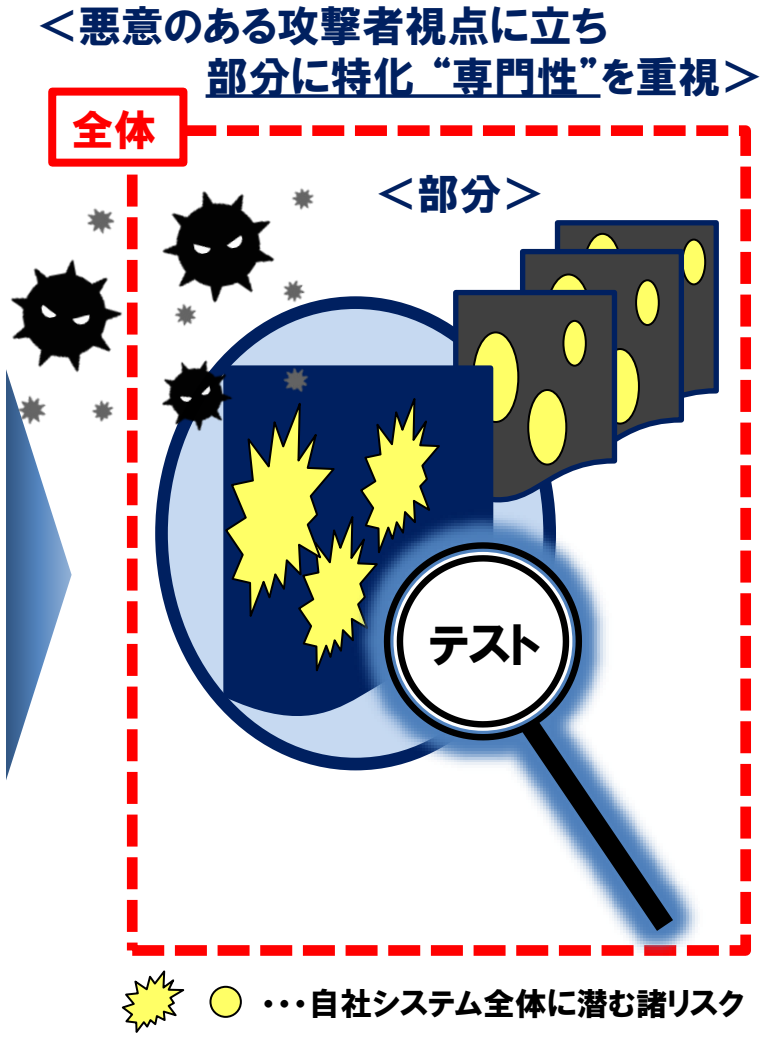
※（参考）詳しくは、
下記 IPA：独立行政法人情報処理推進機構も併せて参照。
https://www.ipa.go.jp/security/vuln/CVSS.html

【重点対策】

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。



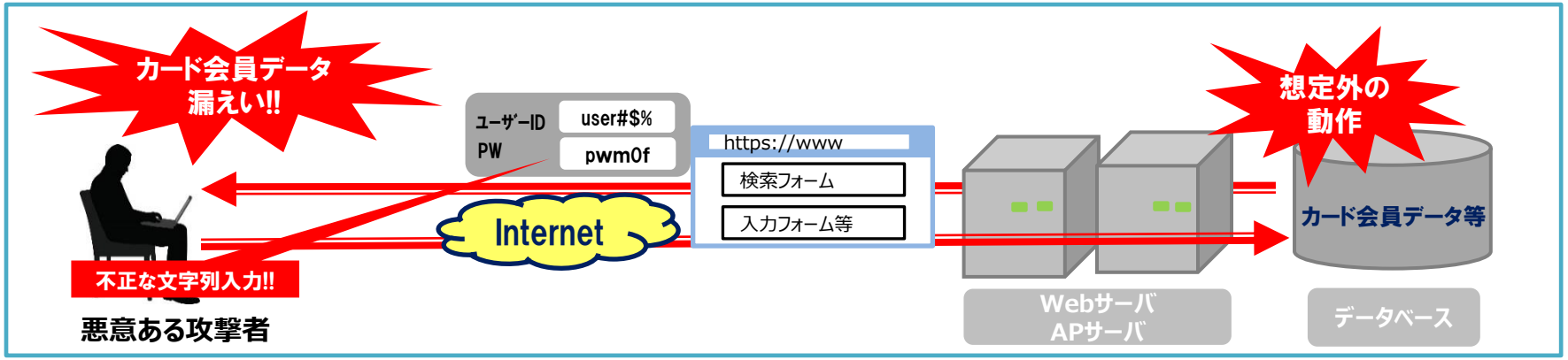
【重点対策】

1-3-2 Webアプリケーションの脆弱性対策 SQLインジェクション①

■ SQLインジェクション攻撃とは・・・

- Webアプリケーション上での対策に不足があると、攻撃者が入力した不正な命令を含む文字列がデータベースにそのまま受け渡される。これを悪用し、データベースの想定外の動作を引き起こし、データベースに保存されていたデータの取り出しや、不正なデータの書き込みを行う攻撃のこと。

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。 ◆ 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(当該脆弱性が無いものが望ましい)やソフトウェアのバージョンアップを行う。 □ Webアプリケーションを開発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。その際には、入力フォームの入力値のチェックも行う。



【重点対策】

1-3-2 Webアプリケーションの脆弱性対策 SQLインジェクション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。 2020年01月30日現在 2.13.1 ~ 2.17.0 は確認されたすべての危険度高の脆弱性対応が完了しているバージョンとなります。	脆弱性に応じた修正をおこなってください。 カスタマイズ等をおこなっている場合は、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。 2020年01月31日現在 2.13.5、2.17.0 は確認されたすべての脆弱性対応が完了しているバージョンとなります。	脆弱性に応じた修正をおこなってください。 カスタマイズ等をおこなっている場合は、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/news/detail.php?news_id=349

【重点対策】

1-3-3 Webアプリケーションの脆弱性対策 クロスサイト・スクリプティング①

■ **クロスサイト・スクリプティングとは・・・※**

- ウェブアプリケーションの中には、検索のキーワードの表示画面や個人情報登録時の確認画面、掲示板、ウェブのログ統計画面等、ユーザーからの入力内容やHTTPヘッダの情報を処理し、ウェブページとして出力するものがある。ここで、ウェブページへの出力処理に問題がある場合、そのウェブページにスクリプト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、ウェブサイト自体に対してではなく、そのウェブサイトのページを閲覧しているユーザーに及ぶ。
- ウェブ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-HTML-1_5.html

【重点対策】

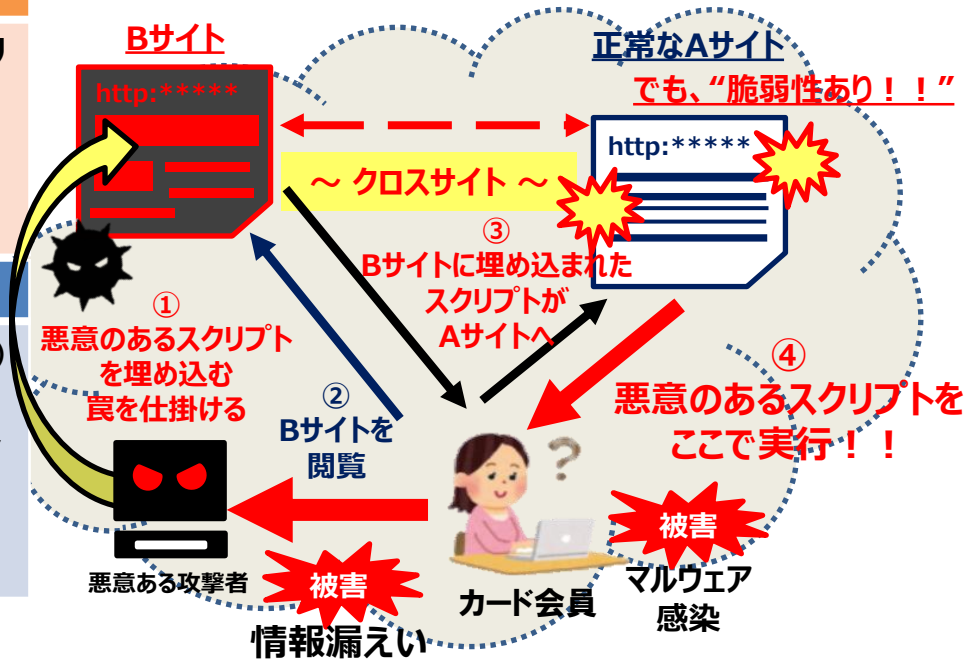
1-3-3 Webアプリケーションの脆弱性対策 クロスサイト・スクリプティング②

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（次頁で解説の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（当該脆弱性が無いものが望ましい）やソフトウェアのバージョンアップを行う。
- □ Webアプリケーションを開発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。その際には、入力フォームの入力値のチェックも行う。



※（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-HTML-1_5.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・・**

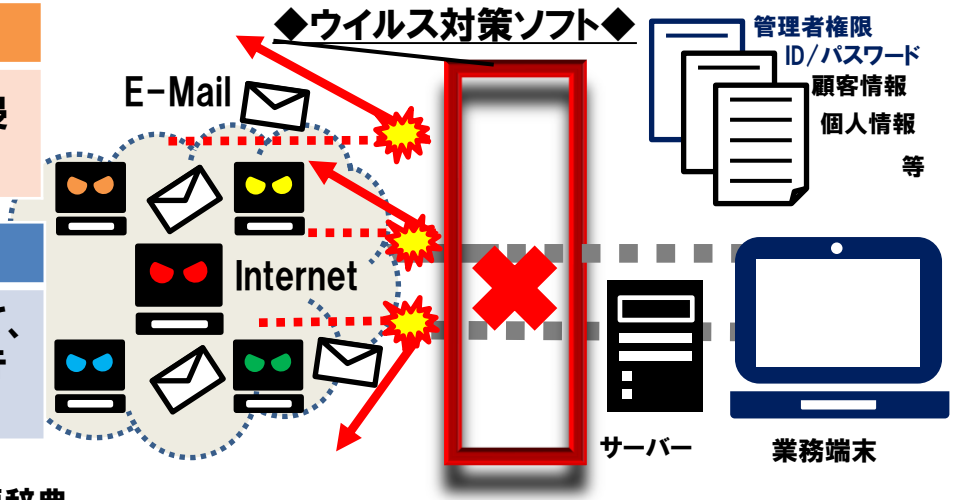
- ウイルスを検出・削除し、ウイルスに感染するのを未然に防ぐためのソフトウェア。ワクチンソフトと同義語。ウイルス対策ソフトウェア会社から市販されている。パソコンにプレインストールされているものもあるが、その場合は3ヶ月等の有効期限があるため、継続して使用するには更新手続が必要※1。

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。



※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://www.ipa.go.jp/security/virus/beginner/dic/dic_sub.html

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！！

【重点対策】

1-5-1 悪質な有効性確認、クレジットマスターへの対策

■ **クレジットマスターとは・・**

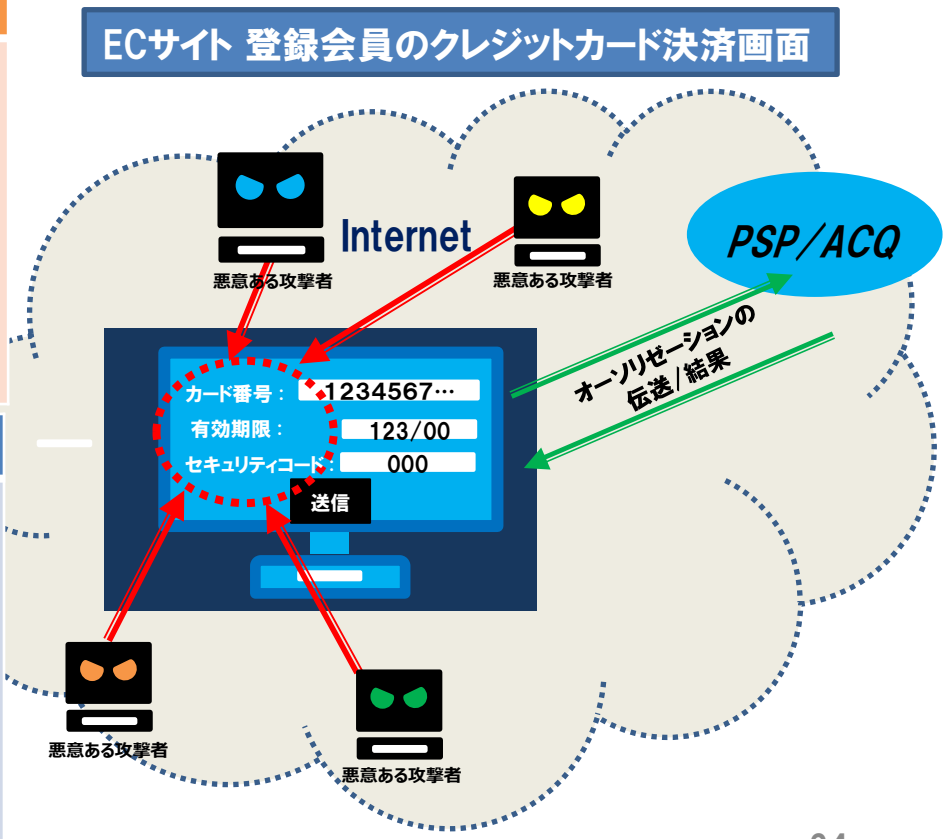
- クレジットマスター(略称:クレマス)とは、カード会員データの登録/変更時およびクレジットカード決済時において、カード番号の採番の規則性を悪用して機械的に生成した大量のカード番号等の有効性を、ECサイトを介して確認し、有効なクレジットカード番号等を不正取得する手口。

攻撃リスク

- ◆ 会員登録時の「なりすまし」による登録時、また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、カード会員データの有効性確認、クレジットマスターを行われる恐れがあり、有効なカード会員データを不正取得される。
- ◆ 攻撃者は特に日本国内のIPよりも海外IPから悪質な有効性確認/クレジットマスターを実施することが多い。

対策

- □ 海外からの攻撃が非常に多いため「不審なIPアドレスからのアクセス制限」を行う。
- □ 有効なカード会員データの漏えい対策として「同一アカウントからの入力制限」「エラー時に、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
- □ EMV3-DセキュアやSMS通知など本人確認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。



2-1 不正ログイン対策の概要

◆ 不正ログイン対策とは

カード会員（ユーザ）が加盟店の機能を利用する際に、加盟店サイトの会員となりカード会員データ及び属性情報などを登録する為、これらのデータを利用して不正利用が行われる。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。

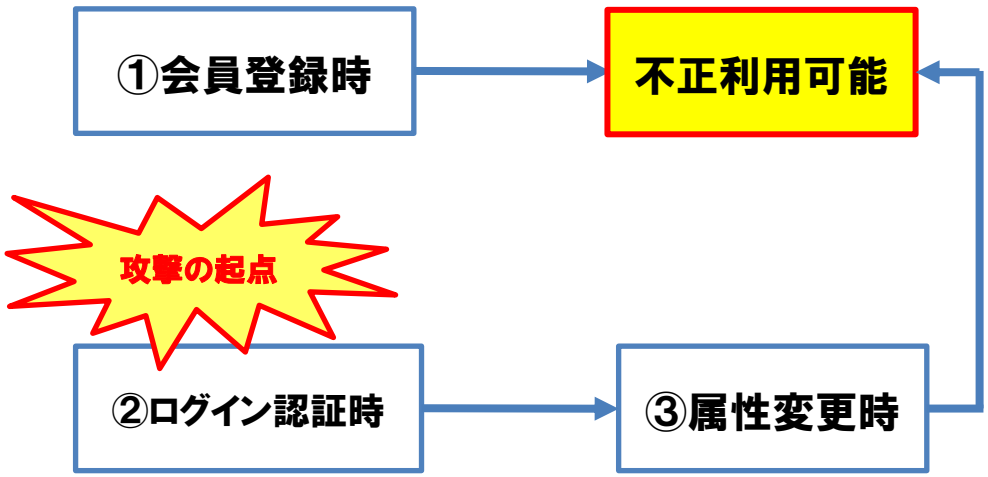
- 不正なアカウントが作成され、カード会員データを登録される。
- 不正に取得したカード会員データを利用し、不正ログインによりクレジットカード番号の変更や属性変更が可能となり、不正利用される。
- フィッシングメール等で不正取得されたアカウント情報及びアカウント/パスワードクラッキングにより、不正ログインをされる。

◆ 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
1-1 会員登録時	P27
1-2 ログイン認証時	P28
1-3 属性情報変更時	P29

2-2 何故、3つの場面で対策が必要なのか

■ 攻撃の起点として狙われる場面



・①会員登録時や②ログイン認証時においても<u>不正利用対策</u>が重要となる。

・特にEC加盟店の登録会員のログイン認証フォームは、インターネット経由でアクセスが可能であり、攻撃者の攻撃の起因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

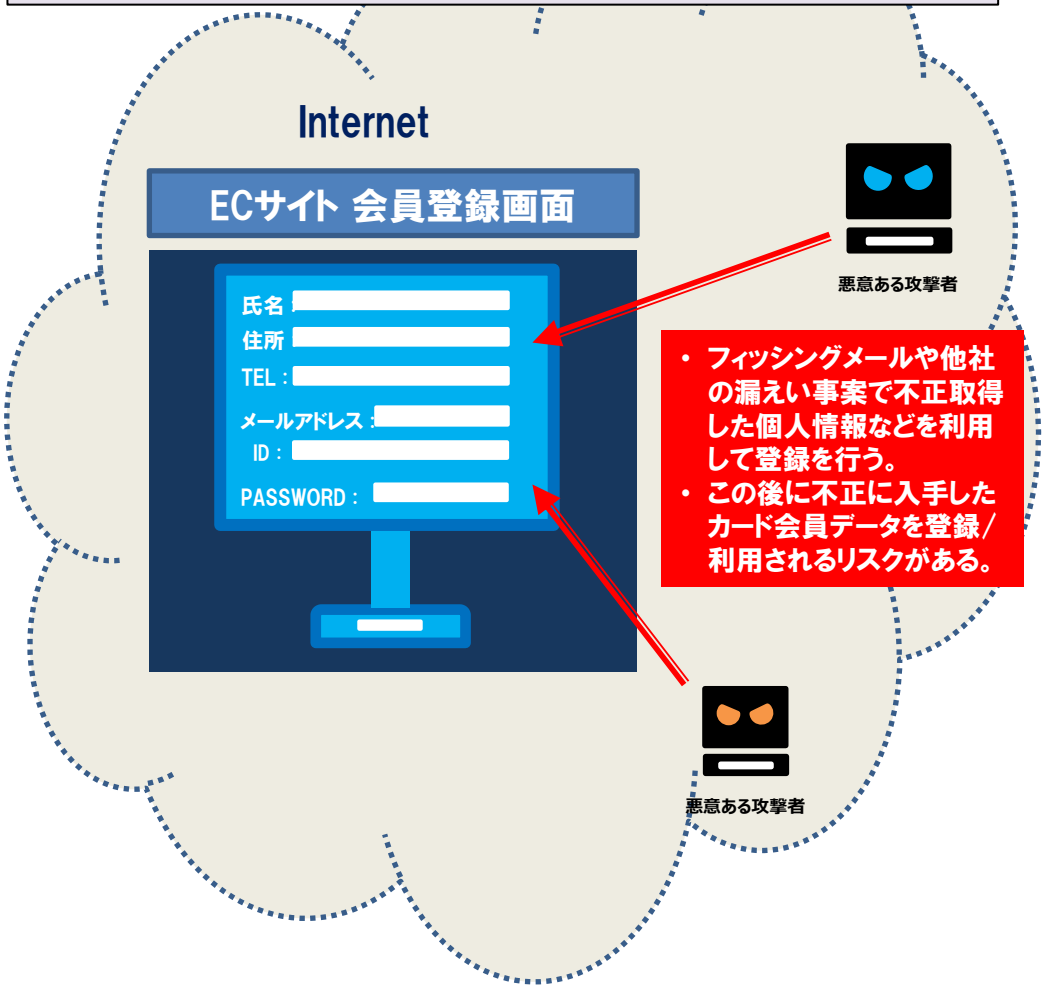
①会員登録時
- 不正なアカウントが作成され、カード会員データを登録されるリスクがある。

②ログイン認証時
- 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の変更や属性変更が可能となり、不正利用が実施されるリスクがある。

③属性変更時
- フィッシングメールや漏えい事案などで不正取得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。

2-3 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



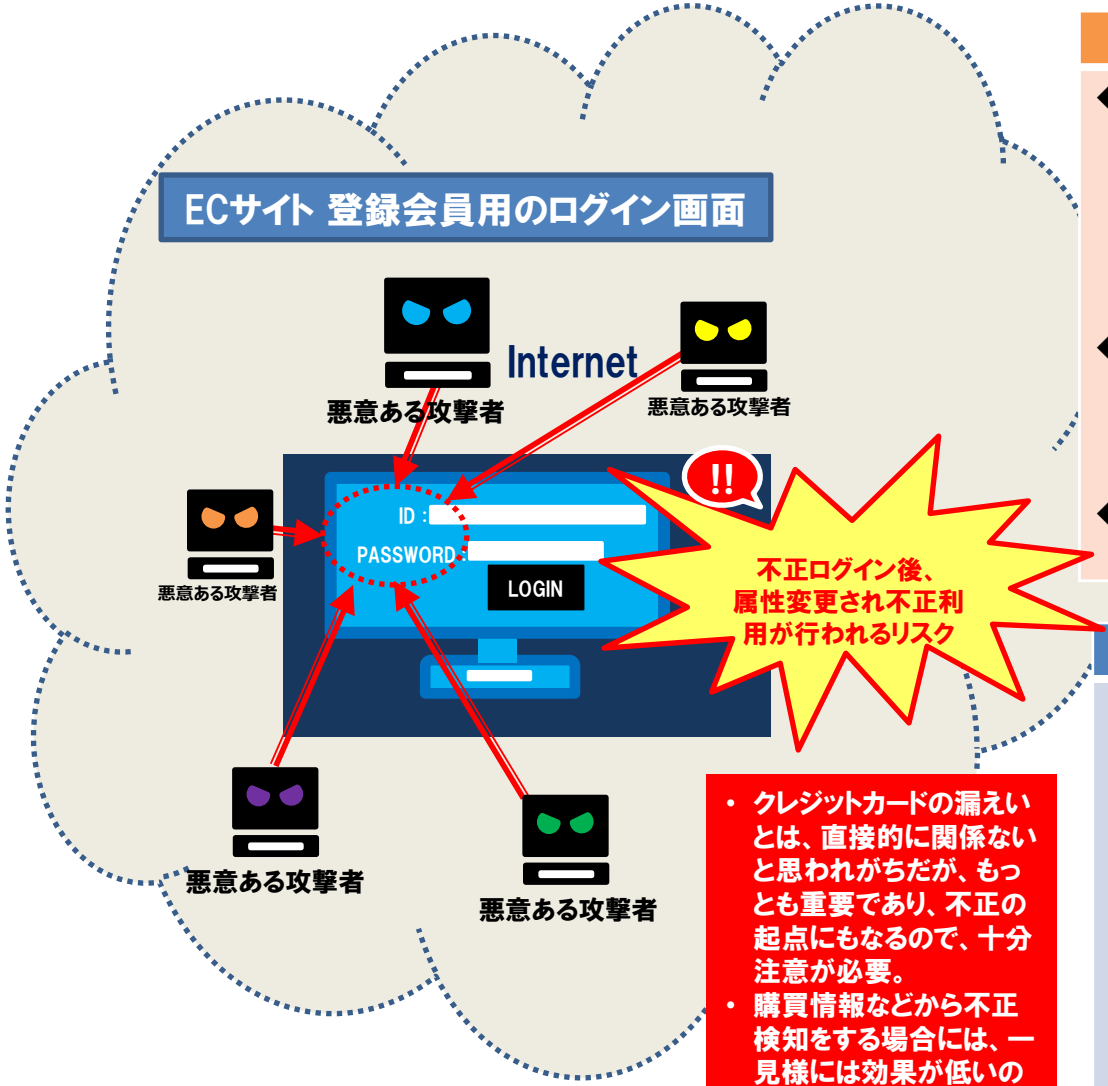
攻撃リスク

- ◆ フィッシングメールによる個人情報及びカード会員データ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」の登録することが可能であり、不正に入手したカード会員データを登録/利用されるリスクがある。（Walletへのチャージなどに悪用される。）
- ◆ 海外の不正利用主導者が、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。
- □ 海外からの攻撃も非常に多く「不審なIPアドレスからのアクセス制限」を行う。
- □ 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、本人確認を行う。
- □ 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、二要素認証などによる本人確認を行う。
- □ 不正検知システムを利用する。

2-4 ログイン認証時の対策



- 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!!

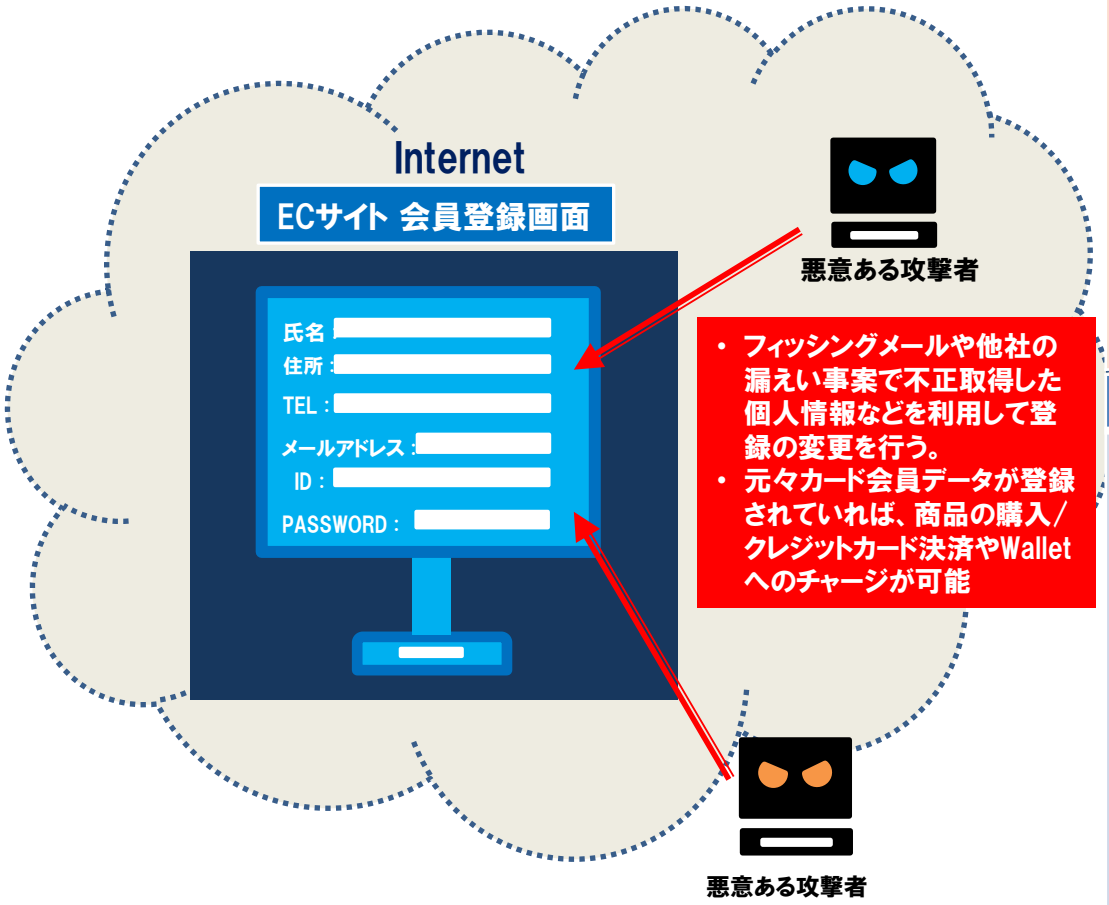
攻撃リスク

- ◆ 会員用のログイン画面は、インターネットに公開する必要があるので、アクセス制限ができず、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、また静的パスワードは推測されやすい為、「なりすまし」による、不正ログインを実行されても、会員本人及びEC加盟店は気づきにくい。
- ◆ 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

- □ 海外からの攻撃が非常に多い為「不審なIPアドレスからのアクセス制限」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」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、二要素認証などによる本人確認を行う。
- □ ログイン時のメールやSMS通知、スロットリングなどを行う。
- □ その他、「デバイスフィンガープリント」等を利用する。

2-5 属性情報変更時の対策



攻撃リスク

- ◆ 不正ログイン後に、フィッシングメールや漏えい事案などで不正取得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チャージも可能になる。
- ◆ 海外の不正利用主導者が、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

- □ 攻撃者が海外である場合には、入力されている個人情報が間違っている場合が多く、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の本人確認が重要になる。その為、個人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「二要素認証」や、SMS認証等の「二段階認証」により本人確認を行う。
- □ 海外からの攻撃が非常に多いため「不審なIPアドレスからのアクセス制限」を行う。
- □ その他「不正検知システム(Fraudサービス)/デバイスフィンガープリント」等を利用する。

3. 追加的な対策

◆ 前述の対策の他に追加的な対策として以下の対策も有効である

- ロ インフラ／サーバーに対してデフォルト設定のパスワード等を利用しないこと
- ロ 常にオープンソースなどのソフトウェアを最新のバージョンに保つこと
- ロ ファイル整合性監視の導入、運用
- ロ IPS(Intrusion Prevention System)の導入
- ロ WAF(Web Application Firewall)の導入

※ IPSとWAFについては予防策としての脆弱性の検知と防御になります。正常な通信を不正であると誤って検知してしまう“誤検知”を回避するため、攻撃を識別するルールであるシグネチャー(Signature)の随時更新が必要です。

※また、上記のセキュリティ対策を実施する際に、IPAが取りまとめた「EC サイト構築・運用セキュリティガイドライン」も参考にしてください。
https://www.ipa.go.jp/security/guide/vuln/guideforecsite.html

4. 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、**それ以前に基本的なセキュリティ対策を徹底し、**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EC加盟店は、**開発元からの注意喚起を元に、あるいは開発元に積極的に情報提供を求め、早急に追加的なセキュリティ対策を講じてください。**
- 一つのEC加盟店で漏えい事案が発生すると、すぐさま他の加盟店での不正利用被害へと波及し、業界全体に相当額の損失を招くこととなります。自社のECサイトを適切に保護するためにも、本資料を参考にすると共に、各オープンソースの開発元が公表しているセキュリティチェックリストをご活用ください。
- **万が一、漏えい事案を発生させてしまった場合は、速やかに契約しているカード会社や決済代行会社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 ： 2019年12月23日**

  【重要】クレジットカード流出被害が増加しています。EC-CUBEご利用店舗のセキュリティチェックをお願いいたします。

  https://www.ec-cube.net/news/detail.php?news_id=348

- **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 - 1.1 SQLインジェクション

  https://www.ipa.go.jp/security/vuln/websecurity/sql.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

◎ 本件に関するお問合せ先

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
セキュリティ対策推進センター

E-mail　gykikaku2@jcredit.jp