ECサイトに必要なセキュリティ対策とは｜運営タイプ別対策や注意点

「ECサイトを始めたいけど、セキュリティについてはどんなことに気を付ければいいの？
「対策って本当に必要なの？どのようなことをすればいいの？」

ECサイトを立ち上げようとしている人の中には、セキュリティについて一体何をすればいいのか、また、小規模なビジネスでも本当にセキュリティ対策が必要なのか、疑問に思う人も多いのではないでしょうか。

結論を先に言うと、**ECサイトを運営する際に、セキュリティ対策は絶対に必要です。**

というのも、ECサイトの運営者がセキュリティ対策を怠ると、下記のような被害にあう恐れがあるからです。

ECサイトのセキュリティ上の不備を狙った攻撃による被害
個人情報が漏えいする
顧客のクレジットカードを悪用される
Webサイトが改ざんされる

上記のような被害が起きると、数千万～数億円規模の多額の賠償金が発生したり、会社の社会的信用を失ったりと、運営会社にとっての損害は大変大きなものとなります。

セキュリティの不備による被害にあわないためにも、ECサイトを運営する際には、しっかりとセキュリティ対策を行うようにしましょう。

具体的なセキュリティ対策としては、次のような対策が必要となります。

ECサイトを運営する際に必要なセキュリティ対策6つ
不正アクセスを防ぐ
バグ・セキュリティホールを防ぐ
ワーム・ウイルス感染を防ぐ
ユーザーデータを適切に保護管理する
ユーザー認証システムを強化する
社員へのセキュリティ教育を徹底する

ただし、モール型、ASP型などといった**EC**サイトの運営タイプによっては、全ての対策を自社で行う必要がないケースもあるため、自社の運営タイプに合わせて必要な対策を取るようにしましょう。

▼この記事で分かること

- ECサイトでセキュリティ対策をしないと起こる被害事例3つ
- ECサイトのセキュリティ対策6つ
- 運営タイプ別に見たセキュリティ対策の担当範囲
- セキュリティ対策を失敗せずに行うポイント

最後まで読むことで、**EC**サイトのセキュリティ対策の詳細や、運営タイプ別（モール型、**ASP**型など）のセキュリティ対策が分かります。

また、セキュリティ対策を行う上での注意点も紹介するため、ぜひ最後まで目を通し、効果的なセキュリティ対策を行なうために役立ててください。

1. ECサイトのセキュリティは強固な対策が必要！

冒頭でも触れましたが、**ECサイトを運営する際には、しっかりとセキュリティ対策を取ることが必要です。**

なぜならセキュリティ対策をしないでいると、悪意ある第三者から不正アクセス攻撃などを受け、次のような被害が起こる可能性が高くなるからです。

ECサイトのセキュリティ上の不備を狙った攻撃による被害
個人情報が漏えいする
顧客のクレジットカードを不正利用される
Webサイトが改ざんされる

これらの被害により、企業は多額の賠償金を支払うことになったり、社会的信用を失ったり、業務が停止したりと、運営会社は大きな損害を受けることになります。

ここでは、セキュリティ対策を怠ると実際にどのような被害を受けるか、実例とともに紹介します。

自社のサービス上でも起こりかねないような実例については十分に注意し、同様の被害を起こさないように、「2. ECサイトのセキュリティ対策6つ」で紹介する対策を取るようにしましょう。今すぐに対策を知りたいという方は上記を見てください。

1-1. セキュリティ対策を怠ると起こる被害のパターン3つ

ECサイトに必要なセキュリティ対策を怠ってしまうと、その部分がセキュリティ上の弱点となり、ハッカーなどの攻撃者に狙われやすい状態となります。

具体的には、下記のような被害にあう恐れがあるため注意しましょう。

ECサイトのセキュリティ上の不備を狙った攻撃による被害
個人情報が漏えいする
顧客のクレジットカードを不正利用される
Webサイトが改ざんされる

一つずつ内容を具体的に見ていきましょう。

1-1-1. 個人情報が漏えいする

不正アクセスを防ぐ対策をしていなかったり、ユーザー情報を適切に保護管理する対策を取っていないと、個人情報を盗み出され、流出してしまうケースが多く見られます。

不正アクセスで個人情報が漏えいしたケースとして、例えば、下記のようなケースがありました。

【個人情報漏えいの事例】

企業名	内容と原因	賠償額など

ベネッセ	2014年約3500万件の顧客情報が流出。 顧客情報データベースの運用や保守管理を委託していたシステム会社の社員が情報を不正に転売したことが原因。	顧客3500万人に対し1人当たり500円の金券をお詫びで配布。 顧客への補償に200億円、事後処理に60億円の費用が発生。

ベネッセのケースでは、顧客データが適切に保護管理されていなかったため、関係会社の社員によって不正に持ち出され、大規模な個人情報の流出となりました。

損害額としては、その年のベネッセの決算情報によると、顧客への補償に**200**億円、おわび文書の発送や事件の調査などに**60**億円かかり、合計**260**億円の特別損失が発生したとされています。

また、JNSA（NPO法人日本ネットワークセキュリティ協会）の調査によると、個人情報が流出した場合、一人当たりの損害賠償額の平均は**28,308**円と言われています。（出典：JNSA「インシデント損害額レポート2021」）。数千件の個人情報が流出しただけでも損害賠償額は、数千万～1億円もの金額になります。個人情報が流出すると経済的ダメージが大きいと言えます。

1-1-2. 顧客の クレジットカードを不正利用される

バグやセキュリティホールを防ぐ対策をしていない、ユーザー認証を厳格化していないなどセキュリティ対策を行なっていないと、不正アクセスをされ、クレジットカードを不正利用されることがあります。

クレジットカードの不正利用については、例えば下記のような被害例があります。

【クレジットカードの不正利用の事例】

企業名	内容と原因	賠償額など
A社	ECサイトのシステム上の脆弱性を狙って、WEBサイトを改ざんし偽の入力フォームを作成。顧客が偽入力フォームに入力したクレジットカード情報を使って合計2500万円の不正使用。	合計9,490万円の被害。内訳はお詫び品送付費用650万円、事故原因調査費300万円、コールセンター設置費1050万円など。

参考：JNSA（NPO法人日本ネットワークセキュリティ協会）「インシデント損害額調査レポート　2021年版」

一般的に、ユーザーのクレジットカードを攻撃者に不正利用されてしまうと、ECサイト側には下記のような費用の負担が発生します。

- フォレンジック調査の費用
- チャージバックの費用負担

フォレンジック調査の費用とは、クレジットカード情報の漏えいについての原因を特定するための調査費用のことです。カード会社との加盟店契約があり、漏えい事故を起こした場合には、フォレンジック調査をすることが義務付けられています。調査費用は数百万円程度かかるうえ、調査中は**EC**サイトを休止することになります。

チャージバックの費用負担とは、クレジットカードの持ち主が不正使用についての支払いに同意しない場合、クレジットカード会社が売上を取り消しますが、その取り消しにした売上について、ECサイトが支払うことを指しています。不正利用をされた分だけ、**EC**サイトのチャージバックの費用負担が増えます。

これらの費用負担があるため、クレジットカードの不正利用をされた場合のECサイトの被害額はとても大きいと言えます。

1-1-3. Webサイトを改ざんされる

ECサイトがセキュリティ対策を怠っている場合、攻撃者が不正アクセスをし**Web**サイトを改ざんして偽サイトを作り、ユーザーが入力した**ID**・パスワード、クレジットカード情報などを搾取し、悪用するという手口もあります。

Webスキミングと言われ、近年増加している手口です。

【Webサイトの改ざんの事例】

企業名	内容と原因	賠償額など
航空会社**British Airways**	2019年9月、Webスキミングでクレジットカード情報などの個人情報38万件の流出	2000万ポンド（約27億円）の制裁金

Webスキミングの事例としてよく知られているのはイギリスの航空会社British　Airwaysの例です。Webサイトが不正アクセスにより改ざんされ、38万人の顧客が入力したクレジットカード情報などが盗み取られました。

これは、当時対応可能であったセキュリティ対策を実施していれば防げた事故として、英国のプライバシー規制機関の情報コミッショナー事務局（ICO）は航空会社British　Airwaysに対し、**2000**万ポンド（約**27**億円）の制裁金を科しました。

Webサイトの改ざんによる被害は、個人情報の流出やクレジットカードの不正利用などにもつながるため、注意したい被害と言えます。

2. ECサイトのセキュリティ対策6つ

ECサイトについてセキュリティ対策の必要性を把握して頂けたことと思います。

実際にセキュリティ事故の被害を抑えるためには、次のようなセキュリティ対策が必要です。

ECサイトを運営する際に必要なセキュリティ対策6つ	
1	不正アクセスを防ぐ
2	バグ・セキュリティホールを防ぐ

3	ワーム・ウイルス感染を防ぐ
4	ユーザーデータを適切に保護管理する
5	ユーザー認証システムを強化する
6	社員へのセキュリティ教育を徹底する

「1.不正アクセスを防ぐ」から「5.ユーザー認証システムを強化する」まではシステム上の対策となり、「6.社員へのセキュリティ教育を徹底する」は、社員向けの対策となります。

以下では、それぞれの具体的な対策の内容について紹介しますので参考にしてみてください。

ただし、これらの対策を実際に行なう実施者は、**EC**サイトの運営タイプごとに異なります。

【運営タイプ別セキュリティ対策の担当範囲】

運営タイプ	社員向けの対策	システム上のセキュリティ対策
モール型 （楽天、**amazon**のようなショッピングモール形態）	自社で行う	ベンダーが対応
ASP型 （**BASE**や**STORES**のような**ASP**サービス）	自社で行う	ベンダーが対応
オープンソース型 （公開されているソースコードを使って自社開発）	自社で行う	自社で行う
パッケージ型 （**EC-CUBE**、**Commerce21**のような必要機能のパッケージ利用）	自社で行う	ベンダーが対応
フルスクラッチ型 （完全自社開発）	自社で行う	自社で行う

上の表にあるように、**EC**サイトの運営タイプによってはシステム上のセキュリティ対策は、自社でなくシステムやソフトウエアを提供するベンダー（販売会社）が対応することになります。

したがってシステム上のセキュリティ対策を自社で行わない、「モール型」「ASP型」「パッケージ型」でECサイトを運営している場合は、6つの対策のうち「2-6.　社員へのセキュリティ教育の徹底」について確認し重点的に対応するようにしましょう。他の対策は参考程度に確認し、ベンダー会社を選ぶ際などに役立てるとよいでしょう。

それでは、詳しく見ていきましょう。

2-1. 不正アクセスを防ぐ

ECサイトに対しての不正アクセスを防ぐ対策を取っておくことが大切です。

ハッカー・攻撃者は、常にECサイトのシステムに不正アクセスをしようと狙っています。目的は大量の個人情報を盗み取ったり、ユーザーになりすまして勝手に商品を購入したりするためです。

これらの不正アクセスを防ぐために、下記のような対策を取りましょう。

＜不正アクセスを防ぐ具体策＞
- セキュリティ製品の導入
- ソフトウエアのアップデート
- **ASP**のショッピングカートの利用

各対策の具体的な内容は下記の通りです。

2-1-1. セキュリティ製品の導入

不正アクセスを検知・遮断するためのセキュリティ製品を取り入れるようにしましょう。

具体的には、下記**3**種類のセキュリティ機能を取り入れる必要があります。

＜サーバー・ネットワーク用セキュリティ製品＞
- **FW**（**Firewall**）：社内ネットワークとインターネットとの境界に設置し、不正アクセスをブロックするシステム
- **IDS**（**Intrusion Detection System**）**/IPS**（**Intrusion Prevention System**）：不正侵入検知システム。外部からの不正な侵入を検知し、管理者に通知します。IPSは検知・通知だけでなく、不正侵入を遮断するところまで対応するシステムです。
- **WAF**（**Web Application Firewall**）：Webアプリケーションに特化したファイアウォール。Webアプリケーションに不正な構文を送りつけて侵入する攻撃を防ぎます。

「FW（Firewall）」は社内ネットワークと社外インターネットとの境界点、「IDS/IPS」は社内ネットワーク、「WAF」はWebアプリケーションと、それぞれ保護する対象が異なるため、まんべんなく揃えましょう。揃えない場合には隙のあるところを攻撃されかねません。

実際にセキュリティ製品を導入する際には、上記機能を持つ製品を個別に導入するケースと、**UTM**（統合脅威管理**(Unified Threat Management)**という3機能をワンセットにしたセキュリティ製品を導入するケースとがあります。

例えば下記のような商品があるため、参考にしてください。

【セキュリティ製品おすすめ事例】

種類	製品名（開発会社名）	特徴	参考価格
UTM	Check Point700シリーズ（株式会社ピーエスアイ）	中小企業におすすめ。コストを抑えて包括的なセキュリティ対策が可能。	初年度導入価格：366,000円～ 次年度価格（ライセンス1年）：90,000円～など
次世代	Untangle（ウェアポータル株式	導入機器をリモート環境で一元管理。	年額180,000円～/12ラ

型FW	会社）	既存のファイアウォールに追加導入可。	イセンス～
IDS / IPS	**L2Blocker**（株式会社ソフトクリエイト）	既存のネットワーク構成を変えずに導入可能。無線LAN環境にも対応可。	380,000円 ～
WAF	**Scutum**（株式会社セキュアスカイ・テクノロジー）	11年連続国内シェアNo.1のクラウド型WAF。Webアプリの脆弱性を狙う攻撃を防御し、情報漏えいや改ざんのリスクからサイトを保護。	29,800円/月～

2-1-2. ソフトウエアのアップデート

ソフトウエアには、開発メーカーや利用者が気づいていないセキュリティ上の欠陥を抱えている場合があります。通常、そうしたシステム上の欠陥は見つかり次第、開発メーカーが修正プログラムをリリースするため、利用者は早急に修正プログラムを更新するようにしましょう。

中には、開発メーカーがソフトウエアの欠陥を公表してから、修正プログラムをリリースするまでの間にその欠陥を狙って不正アクセスが行われる場合もあります。

このためソフトウエアのアップデートを速やかに行うことはもちろん、ソフトウエアの欠陥が公表されれば、不正アクセスがないかどうか監視に気を配るなどの対応も合わせて行うようにしましょう。

2-1-3. ASPのショッピングカートを利用する

ショッピングカートについて、自社で開発するよりも、**ASP**のショッピングカートを利用することもおすすめです。

ECサイトにおいて、ショッピングカートがセキュリティ上、最も注意が必要な部分と言えます。ショッピングカートでは、決済を行うため銀行口座やクレジットカードなどの支払情報を扱うからです。

この部分については、セキュリティの専門性の高い既存のASPサービスを利用することも不正アクセス対策としておすすめです。

ASPのショッピングカートには下記のようなメリット・デメリットがあります。初期費用が無料、ランニングコスト月額数千円といったものもあるため、気軽に試してみることも可能です。

ASPショッピングカートのメリットデメリット	
メリット	デメリット
● 初期費用やランニングコストが、自作のショッピングカートなどと比べて安くすむ ● 必要な機能がそろっている ● 最新機能を使うことができる ● セキュリティ対策はベンダーが対応	● カスタマイズができない ● 独自のサービスや売り方を実施しにくい

2-2. バグ・セキュリティホールを防ぐ

ECサイトで使用しているソフトウエアなどのバグ・セキュリティホールを防ぐ対策をしておくことも大切です。

バグやセキュリティホールとは、プログラム上の誤り・欠陥のことで、バグやセキュリティホールをそのままにしておくと、ECサイトのシステムやアプリケーションが想定していない動き方をすることがあります。

そうした不具合があると不正アクセスが可能になることがあるため、バグ・セキュリティホールを放置しておくことは厳禁です。

ソフトウエアの開発メーカーでは通常、ソフトウエアの欠陥が発見されるとすぐに修正プログラムを開発し、利用者に配布します。利用者は開発メーカーから修正プログラムや最新版のソフトウエアがリリースされればすぐに更新するようにしましょう。

リリースの通知は、ソフトウエア上で通知されたり、開発メーカーからメールなどの手段で通知されたりします。通知を見落とさないように気を付けましょう。

また自社で使用しているすべてのソフトウェアについて、ソフトウェアの更新情報を早めに入手できるように、週に1回以上開発メーカーのWEBサイトでリリースをチェックするなどの体制を整えておきましょう。

2-3. ワーム・ウイルス感染を防ぐ方法

ワーム・ウイルス感染を防ぐためには、セキュリティ製品を導入するようにしましょう。

特に社員が使用する個別のパソコン端末にウイルス対策ソフトを入れるといった対策が大切です。

攻撃者は、狙った企業のシステムに侵入するために、その企業の社員に対してウイルスに感染させるためのファイルを添付したメールを送るなどといった攻撃をすることがあります。

社員がうっかり添付ファイルを開封してしまうとパソコンがウイルス感染してしまい、そこから個人情報などの企業内の重要情報が漏えいすることがあります。

ウイルス対策ソフトをパソコン端末に入れることで、不審なメールをブロックしたり、ウイルス感染を招く危険なWebサイトへのアクセスをブロックしたりすることができます。

■パソコン用セキュリティ製品の選び方

パソコン用セキュリティ製品を選ぶ際には、下記のメリットとデメリットを踏まえて、よく検討するようにして下さい。

パソコン端末用セキュリティ製品のメリット・デメリット	
メリット	デメリット
● 最新のウイルス対策が可能 ● 集中管理がしやすい	● 費用がかかる ● 業務上の動作に影響する場合がある

パソコン用セキュリティ製品のメリットとして、最新のウイルス対策が可能となる点のほか、集中管理がしやすいということが挙げられます。管理者側でソフトウエアを更新できるため、ソフトウエアの更新もれによるウイルス感染被害を防ぐことができます。社員数が多い企業の場合など、集中管理で多くのパソコン環境を一気に整えられるため、管理が楽になります。

デメリットとしては、費用がかかりますが、1ユーザー当たり年間3,500～5,000円程度です。また、ソフトウエアによっては、業務上の動作が遅くなることもあります。

無料で試せるセキュリティ製品も多くあるため、実際に使用し「管理はしやすいか」「業務上の動作に支障はないか」「サポート体制は整っているか」などといった点を確認しつつ、選ぶようにしましょう。

2-4. ユーザーデータを適切に保護管理する

ユーザーデータを適切に保護管理する対策としては、次の2つの方法があります。

- ユーザーデータへのアクセス権限を制限する
- ユーザーデータを第三者が閲覧できない場所に保管する

2-4-1. ユーザーデータへのアクセス権限を制限する

ユーザーデータなど重要なデータベースへのアクセス権限について適切に設定するようにしましょう。

全てのユーザーに全ての権限を与えるのでなく、最低限必要な利用者に必要最低限のアクセスを許可することが大切です。アカウント権限を適切に設定することで、なりすましによる不正アクセスがあった場合に被害を少なくすることができます。

2-4-2. ユーザーデータを第三者が閲覧できない場所に保管する

ユーザーデータなどの重要データを、セキュリティの強固な場所に保管するなど、第三者が閲覧できない場所に保管するようにしましょう。

サーバー上の公開フォルダなど、URLを知っていれば誰でも閲覧可能な場所などには決して保存しないようにしましょう。

2-5. ユーザー認証システムを強化する

ユーザー認証システムの強化には、下記のような対策がおすすめです。

- 「多要素認証」の導入
- 第三者に推察されにくいパスワードを使う

2-5-1. 「多要素認証」の導入

複数の認証方式を組み合わせることを「多要素認証」と言います。サイトにログインする際のユーザーの認証方法については、ユーザーの利便性も考えて要素を多くしすぎず、**2**つの認証方式を組み合わせた「二要素認証」を導入するとよいでしょう。

例えば、ログイン時にID・パスワードに加えて、携帯電話あてにそのときのみ利用可能なパスワードをSNS送信して入力させたり、顔認証、指紋認証などを行ってログインするといった方法があります。

2-5-2. 第三者に推察されにくいパスワードを使う

ユーザーがパスワードを設定する際には、第三者に推察されにくい複雑なパスワードの設定を促すようにしましょう。

例えば、下記のようなルールを設けることをおすすめします。

＜パスワード設定ルール＞
- パスワード設定には、英字（大文字・小文字）、数字・記号のすべてを含み12文字以上とする
- パスワードに生年月日や電話番号を含めない
- パスワードに有効期間を設け、利用者に定期的に変更させる

例えば英数記号を含めた12桁のパスワードにした場合、パスワードをランダムに作り上げ総当たり攻撃で不正アクセスを行なおうとしても40万年かかると言われています。推察されにくいパスワード設定にすることは不正アクセス防止に役立ちます。

※多要素認証に画像認証を導入することもおすすめです。

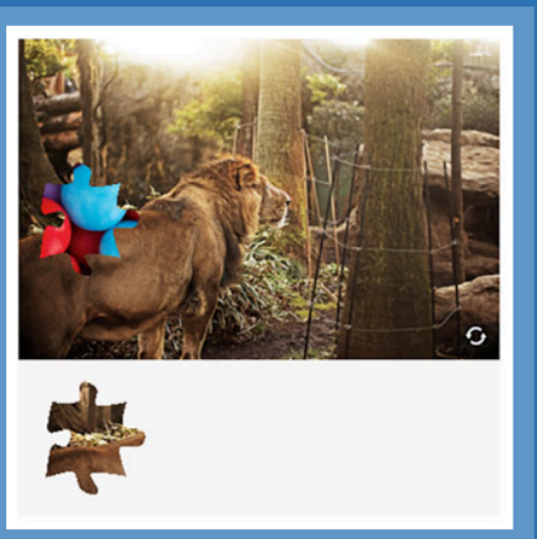
画像認証とは、ログイン実行時に、英数字などの文字列をコンピューターが認識しにくい画像で表示し、ユーザーに入力をさせる機能のことです。機械化された攻撃では突破しにくい認証機能であるため、リスト型攻撃に限らず機械的な不正ログインに対して抑制効果が見込めます。

＼画像認証にはCapy CAPTCHAがおすすめ！／

「リスト攻撃」完全対応！スパムボット（コンピューターによる自動プログラム）による攻撃をしっかり防ぎます。

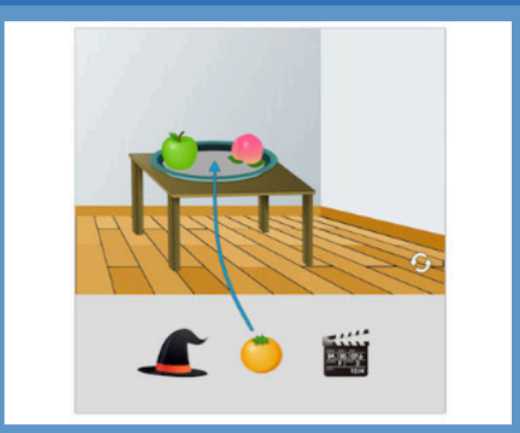
画像認証は、「パズルキャプチャ」「アバターキャプチャ」と豊富なラインナップをそろえています。

パズルキャプチャ



パズルピースを空いているパズル穴にはめることで人間を認証。

アバターキャプチャ



パズルキャプチャよりさらにBOTに厳しいCAPTCHA。
お題通りにアイテムを所定の位置に置くことで人間を認証。
UIとしてもポップでかわいいデザイン。

詳しくはこちら

2-6. 社員へのセキュリティ教育の徹底

不正アクセスを防ぐには、社員にセキュリティ教育を徹底することも大切です。

社員のセキュリティ教育が必要な理由と具体的な対策は下記の通りです。

2-6-1. 情報漏えい事故の原因の約8割が人為的ミスによるもの

実は、セキュリティの不備による情報漏えい事故について、原因の約8割が「人為的ミス」によるものです。

下記は、JNSA（NPO法人日本ネットワークセキュリティ協会）調査による情報漏洩の原因です。

【2018年情報漏洩の原因】

	原因		件数	割合
1位	紛失・置忘れ	人為的ミス	116件	26.2%
2位	誤操作	人為的ミス	109件	24.6%
3位	不正アクセス	システムの問題	90件	20.3%
4位	管理ミス	人為的ミス	54件	12.2%
5位	盗難	人為的ミス	17件	3.8%
6位	設定ミス	人為的ミス	16件	3.6%
7位	内部犯罪・内部不正行為	人為的ミス	13件	2.9%
8位	不正な情報持ち出し	人為的ミス	10件	2.3%
9位	バグ・セキュリティホール	システムの問題	8件	1.8%
10位	その他	人為的ミス	6件	1.4%
11位	目的外使用	人為的ミス	3件	0.7%
12位	ワーム・ウイルス	システムの問題	1件	0.2%
合計			443件	100%

参考：JNSA「2018年 情報セキュリティインシデントに関する調査報告書【速報版】」

上の表によると、社員や関係者などが個人情報を紛失したり置き忘れたりするケース（26.4%）や、システムを誤って操作して情報を流出させたりするケース（24.6%）など、人為的なミスが事故原因全体の**77.7%**を占めます。

ECサイトのセキュリティについては、システム上のセキュリティ対策だけでなく、人為的なミスを起こさないためのセキュリティ対策がとても重要と言えます。

2-6-2. 社内のセキュリティルールを設定し、遵守させる

「紛失・置き忘れ」「誤操作」「管理ミス」などといった人為的ミスを防ぐため、情報セキュリティポリシーなどのセキュリティ方針・ルールを設定し、社員に共有し遵守させるようにしましょう。

社員が守る具体的なルールとしては、下記のような内容を盛り込むようにしましょう。

<セキュリティのための社内ルール>
- 勝手にパソコンにソフトウェアをインストールしない
- 不審なメールを開かない
- 不審なホームページにアクセスしない
- 社員が外部に持ち出すモバイル端末には、ユーザー名・パスワードを記憶させない
- 外部に端末を持ち出す場合は、申請を義務付け、持ち出し専用端末を持ち出す
- 社員の私用機器は持ち込まない
- 機器・資料の廃棄ルールを遵守する

ルールを設けるだけでなく、ルールに違反したときの罰則を定めたり、時々セキュリティテストを行ったりするなどして、社内にルールを浸透させる工夫も必要です。

社員にセキュリティルールをしっかりと認識させ、実行させるようにしましょう。

3. 常に最新情報を確認し、迅速に対応することが大切！

最後に、ECサイトのセキュリティ対策を失敗せずに行うポイントをお伝えします。

ECサイトのセキュリティ対策で失敗しないための重要なポイントは、

- 常に最新情報・ニュースを確認する
- ニュースに対して必要な対策を迅速に行う

ことです。

具体的には次のような内容となります。

3-1. 常に最新のセキュリティ関連のニュース情報などを確認する

セキュリティ対策のためには、最新のセキュリティ関連の情報を入手しておくことが大切です。

例えば、使用しているソフトウエアについて、開発メーカーから欠陥が発見されたことが発表されてから、1週間も経たないうちに、その欠陥を狙って不正アクセス攻撃を受けることもあります。修正プログラムの提供を受ける前に攻撃にあうこともあるため、セキュリティ関連の情報を早めに入手し、対策を取ることが必要です。

セキュリティ関連の情報やニュースはセキュリティ製品の会社が運営している専門の情報サイトやメールマガジンを利用するなどして、情報収集をするようにしましょう。

3-2. ニュースに対して必要な対策を迅速に行う

セキュリティに関するニュースで、自社にも影響のありそうなニュースを確認した場合は、迅速にセキュリティ対策を取るようにしましょう。

例えば、メールにウイルス感染用のファイルを添付して送付するという攻撃手口について、最近は取引先からの返信メールを装って送る手口が増えているというニュースをキャッチしたとします。その場合、自社でもそうした攻撃を受けたときに被害を受けないように、社員に取引先からのメールだからといって油断して添付ファイルを開封することのないよう指導するといった対策が必要となります。

最新のセキュリティ情報に沿って、迅速にできる対応を取ることがセキュリティ被害を抑えるために役立ちます。

まとめ

ECサイトの運営者がセキュリティ対策を怠ると、下記のような被害にあう恐れがあることを紹介しました。

ECサイトのセキュリティ上の欠陥を狙った攻撃による被害
個人情報が漏えいする
顧客のクレジットカードを悪用される
Webサイトが改ざんされる

上記のような被害が起きると、多額の賠償金が発生したり、企業の社会的信用を失ったりと、企業にとっての損害は大変大きなものとなります。

このため、しっかりとセキュリティ対策を取ることをおすすめします。

ECサイトを運営する際に必要なセキュリティ対策は下記の通りです。

ECサイトを運営する際に必要なセキュリティ対策5つ
不正アクセスを防ぐ
バグ・セキュリティホールを防ぐ
ワーム・ウイルス感染を防ぐ
ユーザーデータを適切に保護管理する
ユーザー認証システムを強化する
社員にセキュリティ教育を行う

ECサイトの場合、運営タイプによって、セキュリティ対策の担当範囲が下記の通り異なります。

【運営タイプ別セキュリティ対策の担当範囲】

運営タイプ	社員向けの対策	システム上のセキュリティ対策
モール型 （楽天、**amazon**のようなショッピングモール形態）	自社で行う	ベンダーが対応
ASP型 （**BASE**や**STORES**のような**ASP**サービス）	自社で行う	ベンダーが対応
オープンソース型 （公開されているソースコードを使って自社開発）	自社で行う	自社で行う
パッケージ型 （**EC-CUBE**、**Commerce21**のような必要機能のパッケージ利用）	自社で行う	ベンダーが対応

フルスクラッチ型 （完全自社開発）	自社で行う	自社で行う

自社の運営タイプに合うものを参照して対策を取るようにしましょう。

ECサイトのセキュリティ対策で失敗しないためには、最新の情報をチェックしながら、継続して対策を行なうことが大切です。

これらの情報を踏まえて、効果的なセキュリティ対策を行うようにしてください。