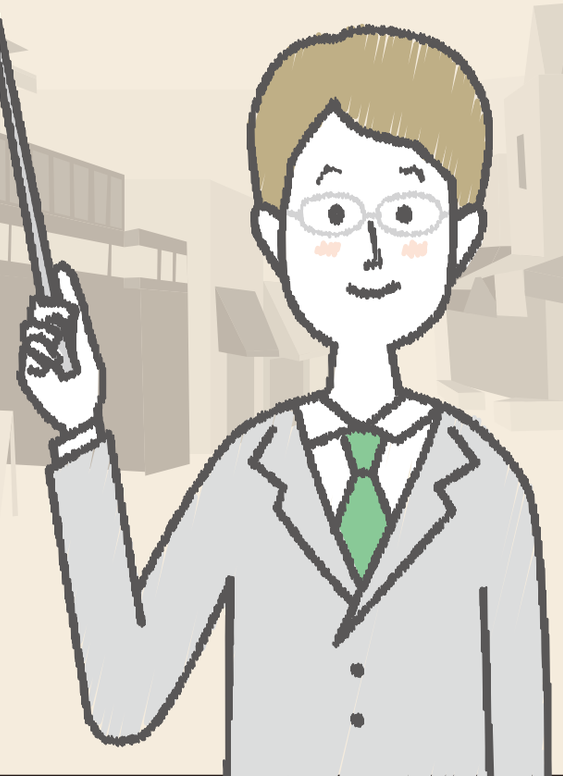
情報漏えい対策

○×クイズ

クイズに答えて理解度をチェック！



クレジットカード番号の非保持化を実施していれば、
クレジットカード番号等の漏えいは発生しない

答え：×

非保持化を実施している場合でも、OS の設定ファイルや管理サーバーの情報が不正に書き換えられ、偽の決済フォームに誘導することでクレジットカード番号等の個人情報を盗み取られる手口も発生しています。脆弱性の解消および恒常的な脆弱性の解消に関するセキュリティーアップデートを実施する必要があります。

クレジットカード番号を
保存・処理・送信している

答え：×

加盟店自身がクレジットカード番号の保存・処理・送信をするのではなく、適切な保護処理を行う決済代行事業者、決済センターへ委託するべきです。
(自社でクレジットカード番号を保存・処理・送信する場合は、PCIDSS※に準拠する必要がある)

※加盟店やサービスプロバイダにおいて、クレジットカード会員データを安全に取り扱う事を目的として策定されたクレジットカード業界のセキュリティー基準。Payment Card Industry Data Security Standard の頭文字をとったもの

EC サイトの運営とサーバー系機能を
同じパソコン管理していない

答え：○

同一パソコンで管理している場合、管理者権限を取得すると複数サーバーの管理者となるためリスクが高まります。リスク分散のため、Web サーバー系機能、AP サーバー系機能、DB サーバー系機能等は別のパソコンで管理することが望まれます。

公開領域に管理者向けのログイン画面のログイン履歴を
わかりやすいように保存している

答え：×

インターネット経由で管理者向けのログイン画面の機密情報やログイン情報を不正に取得される可能性があるため、インターネットでアクセスできない場所にデータログは保存すべきです。

管理者向けのログイン画面の
IP 制限を行っている

答え：〇

外部から不正にアクセスされる可能性があるため、加盟店が業務で使用する管理者向けのログイン画面はアクセスする企業の IP のみに制限を行うことが望ましいです。

管理者向けのログイン画面のログインパスワードは
初期設定のままで問題ない

答え：×

漏洩したパスワードもしくはパスワードの総当たり攻撃による不正ログインのリスクがあります。そのためログインパスワードは定期的に変更しましょう。（ワンタイムパスワード等の動的認証を設定した方がよりセキュリティは強化されます）

ユーザーに提供する「マイページ」に
クレジットカード番号、機密情報は表示している

答え：×

不正利用者がログインすればクレジットカード番号、機密情報が容易に取得できます。したがってクレジットカード番号は自社サイトでの入力を控え、機密情報は非表示に設定を変更します。


利用しているOS、ミドルウェア、
Webアプリケーションを
常にアップデートを心掛けている
○
×

答え：○

脆弱性を解消するため、OS、ミドルウェアは常に最新の状態にしましょう。Web アプリケーションについては、脆弱性対策を行ったセキュアコーティング済みのものを使いましょう。

サーバー内部にまで
監視ツールは導入していない

答え：×

不正ファイルのアップロードやペイメントアプリケーションの改ざん等を検知するため、サーバー内部に監視ツールを導入すべきです。

ウィルス対策ソフトを導入。
ソフトのセキュリティーも常に最新が安心だ

答え：○

ウィルスの侵入・動作を監視するため、最新版のウィルス対策ソフトを導入しましょう。（ウィルス対策ソフトは常駐型を推奨）

脆弱性診断は

導入時に一度だけ行えば良い

答え：×

自社サイトのリスクを検知するために、定期的に脆弱性診断（ベネトレーション診断）を行う必要があります。


ECサイトに関係のないサービスおよび
アプリケーションもインストールしている
○
×

答え：✕

サービスやアプリケーションに脆弱性が発覚しても管理が行き届かず、システム全体が脆弱性の影響を受ける可能性があるため、不要なサービスやアプリケーションはインストールしない。また、すでにインストールしている不要なサービスやアプリケーションはアンインストールしましょう。（特にレンタルサーバーを利用している場合は、不要なサービスやアプリケーションが多く入っている場合があるので注意が必要です）


系列サイト、委託先のセキュリティー体制まで
あえて構築していない
○
×

答え：×

系列サイト、委託先から自社サイトに関する情報が漏洩する可能性があります。そのため自社でセキュリティーポリシーを定め、定期的に管理可能な体制を構築する必要があります。


クラウド等のサービス利用において、
自社の責任範囲を把握している
○
×

答え：○

クラウド等のサービスから自社サイトに関する情報が漏洩する可能性があります。サービス側の作業範囲、セキュリティー対策を把握し、不足部分の対策は自社で行うようにします。

サイト利用者に対してまで
不正ログインに関する啓発活動は行っていない

答え：×

不正ログイン等を防止するため、利用者に対して「複雑で推測しにくいパスワードを設定する」「パスワードを使いまわさない」等の啓発を行いましょう。

情報漏洩対策チェックリスト

- [ ] クレジットカード番号を加盟店が保存・処理・送信しない
- [ ] サーバー系機能を同じパソコンで管理しない
- [ ] 公開領域に管理画面のログイン履歴を保存しない
- [ ] 管理画面の IP 制限を行う
- [ ] 管理画面のログインパスワードはワンタイムパスワードを設定する
- [ ] ユーザーに提供する「マイページ」にクレジットカード番号、機密情報は表示しない
- [ ] 利用している OS、ミドルウェア、Web アプリケーションを常にアップデートする
- [ ] サーバー内部に監視ツールは導入する
- [ ] ウィルス対策ソフトを導入し、ソフトのセキュリティーも常に最新化する
- [ ] 定期的に脆弱性診断を行う
- [ ] 不要なサービスおよびアプリケーションをインストールしない
- [ ] 系列サイト、委託先のセキュリティー体制を構築する
- [ ] クラウド等のサービス利用において、自社の責任範囲を把握する
- [ ] 利用者へ不正ログインに関する啓発を行う