資料１－５

2022年度EC加盟店サイトセキュリティガイドライン検討委員会

ガイドライン作成のための論点（案）

2022年９月２日

独立行政法人情報処理推進機構
セキュリティセンター

ECサイト向けセキュリティ対策ガイドラインの構成イメージ

■ 第一部　ECサイトにおけるセキュリティ対策

① はじめに
② ECサイトが狙われている（ECサイト攻撃からの被害事例、調査結果を踏まえて）
③ なにが問題なのか（ECサイトの脆弱な点、調査結果を踏まえて）
④ 攻撃に対しどのように向き合うべきか（対策に対する指針）
⑤ 対策をしないと何が起きるのか？（サイトおよび事業停止、お客様への迷惑）

■ 第二部　ECサイト構築の各フェーズにおける対策

① 具体的な対策
   a. 組織的な対策
   b. サイト計画時における対策
   c. サイト構築時における対策
   d. サイト公開時における対策
   e. サイト運用時における対策
   ※自社によるECサイト構築と、ショッピングASPカートによるECサイト構築の両方式におけるのメリット・デメリットを定量的に記載
② ECサイト開発時・運用時における外部発注契約上の注意事項
   • 契約に係る問題点、契約のあり方、注意事項
③ その他
   • 実際に被害にあった際の対応、対策
   • 現在の自組織のセキュリティ状況確認のチェックリスト

■ 参考資料

ECサイト向けセキュリティ対策ガイドラインのスコープ

議論・取りまとめの前提

- 中小企業の自社構築のECサイトを対象とし、ECサイトからのクレジットカード情報および個人情報漏えい対策をスコープとする
- 制度面（割賦販売法含む）の議論はスコープ外とする
- ECサイトの脆弱性対策を技術面、契約面から議論する

※割賦販売法の義務を履行しているか否か、そして義務の範囲が適当であるかは、今回の事業のテーマからは外しております。

議論していただきたい内容

- ECサイト向けセキュリティ対策ガイドラインにおいて、技術面、契約面からみた、EC脆弱性対策の推奨事項について、どのような内容を記載するべきか

ガイドライン作成のための論点（案）

1．サイト開設計画時における対策

★は重点項目案

★①ECサイトオーナに対し、セキュリティの重要性をどのように認識してもらうか？

・今回入手した被害事例を心に刺さるように匿名でうまく活用したい。

★②セキュリティ被害・保守コストの把握、サービス利用の検討をどのように実施してもらうか？

・自社構築の場合には、脆弱性診断・アップデート・改修等の保守コストと被害コストを正しく把握してもらい、あわせて、ECサイトのシステムのアップデートやWebサーバーのメンテナンス等の保守管理をすべて任せられるショッピングモール型やASPショッピングカート型のサービスの利用について検討してもらうべきではないか？

・その為にどういう情報を提供し、どうプロモーションをすれば有効であるか？

・現在、自社構築時の保守コスト(目安)算定(初期構築の何％を保守コストとして見込めばいいかの試算)資料を作成中。自社構築とモール・ASPのコスト比較表を、第２回会合にて提示予定。

★③年商が小さく(年商1,000万円未満等)、十分なセキュリティ対策がとれないサイトオーナをどう誘導するか？

・自社構築を実施させないよう誘導すべきか？どう誘導するか？

ガイドライン作成のための論点（案）

2．サイト自社構築・運用時における対策（前ページからの続き）　★は重点項目案

【構築・運用を外部委託する場合】

★①構築・運用事業者の選定条件

・サイト構築時点で、運用時に必要なセキュリティ対策（脆弱性情報・注意喚起情報のモニタリング、セキュリティパッチの適用、定期的な脆弱性診断、コスト含む）をサイトオーナに認識してもらう必要がある。どのように推奨するのが効果的か？

・セキュリティ面で問題のないサイトを構築でき、運用時の必要なセキュリティ対策（脆弱性情報のモニタリング、セキュリティパッチ、定期的な脆弱性診断）ができる外部委託事業者を選定してもらうことが必要

・例えば、構築・運用事業者選定チェックリストの作成等は効果はあるか？

★②構築・運用契約に盛り込むべき項目

・構築契約：セキュリティ設計、納品前脆弱性診断、計画不適合期間におけるセキュリティ運用項目など

・運用契約：脆弱性情報・注意喚起情報のモニタリング、セキュリティパッチの適用、定期的な脆弱性診断等のセキュリティ対応など

ガイドライン作成のための論点（案）

2．サイト自社構築・運用時における対策（前ページからの続き） ★は重点項目案

【構築・運用を外部委託する場合】

★③WAF（ウェブアプリケーションファイアウォール）をどう推奨すべきか？

・少なくとも現在、セキュリティ対策が十分でないサイトには、WAFの導入・運用を促すべきではないか？
・WAFを導入していたが、運用監視漏れ、設定ミスによる被害発生もあるとのこと。どう啓発するか？

★④Webサイトの改ざん検知ツールをどう推奨すべきか？

・少なくとも現在、セキュリティ対策が十分でないサイトには、 WAFとセットで、Webサイトの改ざん検知ツールの導入・運用を促すべきではないか？

★⑤サイバー保険の加入といざという時のありがたみをどうプロモーションすべきか？

・サイトオーナにサイバー保険の商品やその効用を理解してもらうことが必要

ガイドライン作成のための論点（案）

2．サイト自社構築・運用時における対策（前ページからの続き）　★は重点項目案

【構築・運用を内製する場合】

★①セキュリティ設計、公開前脆弱性診断をどう推奨すべきか？

・サイト構築時点で、必要なセキュリティ対策（セキュリティ設計、公開前脆弱性診断、コスト含む）をサイトオーナに認識してもらう必要がある。どのように推奨するのが効果的か？

★②脆弱性情報・注意喚起情報のモニタリング、セキュリティパッチの適用、定期的な脆弱性診断をどう推奨すべきか？

・サイト構築時点で、運用時に必要なセキュリティ対策（脆弱性情報・注意喚起情報のモニタリング、セキュリティパッチの適用、定期的な脆弱性診断、コスト含む）をサイトオーナに認識してもらう必要がある。どのように推奨するのが効果的か？

★③WAF（ウェブアプリケーションファイアウォール）をどう推奨すべきか？

・少なくとも現在、セキュリティ対策が十分でないサイトには、WAFの導入・運用を促すべきではないか？

・WAFを導入していたが、運用監視漏れ、設定ミスによる被害発生もあるとのこと。どう啓発するか？

ガイドライン作成のための論点（案）

2．サイト自社構築・運用時における対策（前ページからの続き） ★は重点項目案

【構築・運用を内製する場合】

★④Webサイトの改ざん検知ツールをどう推奨すべきか？

・少なくとも現在、セキュリティ対策が十分でないサイトには、 WAFとセットで、Webサイトの改ざん検知ツールの導入・運用を促すべきではないか？

★⑤サイバー保険の加入による、いざという時のありがたみをどうプロモーションすべきか？

・サイトオーナにサイバー保険の商品やその効用を理解してもらうことが必要

【その他】

★①一定期間のログの保存が、万が一の場合のフォレンジック調査の観点で重要

★②ECサイト管理画面へのアクセス制限が、万が一の場合の被害拡大抑止の観点で重要

・ IPアドレス制限、ログイン時の二要素認証を必須化すべきではないか？

★③インシデント発生時における対策が重要

ガイドライン作成のための論点（案）

3．本事業で作成したガイドラインをどう中小企業の経営者に効果的に届けるか？

★は重点項目案

★①作成ガイドの効果的な届け方（Best案)

・IPAチャネル、JCAチャネル、JADMAチャネルへの御願いを想定中。（具体的なお願いはこれから）他の効果的チャネルあれば、ご教示ください。