

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

# EC加盟店サイトセキュリティガイドライン 骨子（案）

2022年10月17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加盟店サイトセキュリティガイドラインの目次構成

## ■はじめに

### ■ 第一部 経営者編

1. ECサイトが常に攻撃対象として狙われている（ECサイト攻撃からの被害事例、調査結果を踏まえて）
2. ECサイトのセキュリティ対策を疎かにすると何が起きるのか（ECサイトの脆弱な点、調査結果を踏まえて、対策をしないと何が起きるのか）
3. 何が問題なのか
4. 経営者は何をやらなければならないのか

※**第一部では、ECサイトにおけるセキュリティ対策に関して、経営者が認識し、自らの責任で考えなければならない事項について説明する。**そのため、経営者向けのメッセージを図表、イラスト等を活用して分かりやすく伝える。

### ■ 第二部 実践編

#### 第1章 ECサイトの構築時及び運用時における最低限満たすべきセキュリティ対策要件

1. ECサイトの構築時におけるセキュリティ対策要件
2. ECサイトの運用時におけるセキュリティ対策要件

※**第二部では、ECサイトにおけるセキュリティ対策を実践する責任者・担当者が、最低限満たすべきセキュリティ対策要件に関して認識し、ECサイトの安全な構築・運用を実践するうえで検討・確認すべき事項について説明する。**そのため、検討・確認を行うために必要となる手順を図表等を活用して分かりやすく伝える。

# EC加盟店サイトセキュリティガイドラインの目次構成

## ■ 第2章 ECサイトを新規に構築する場合において検討・確認すべき事項

1. 確認・検討にあたっての考え方
2. 確認・検討手順
  - (1) セキュリティ運用・保守コストの見積もりに基づく、ECサイトの形態の選定
  - (2) 外部委託を活用した、自社で対応困難な対策の実施
  - (3) 外部委託先におけるセキュリティ対策の実施状況の定期的確認
3. 構築契約または運用・保守契約上の確認事項  
※契約に係る問題点、契約のあり方、注意事項
4. SaaS型ECプラットフォームの選定基準

## ■ 第3章 運営中のECサイトにおいて検討・確認すべき事項

1. 確認・検討にあたっての考え方
2. 確認・検討手順
  - (1) セキュリティ対策の自己点検
  - (2) サイバー被害リスクを減らすために必要となる応急処置（保険的対策）の実施
  - (3) セキュリティ対策の不十分な箇所への追加対策の実施

## ■ 最後に

## ■ 付録

- ・ 付録1 被害を受けたECサイトからの生の声一覧
- ・ 付録2 自社構築サイト（中小企業）50社の脆弱性診断結果
- ・ 付録3 WAF（Web Application Firewall）選定時の注意事項

はじめに

## はじめに（案）

1. 経営者の皆様
2. 本ガイドラインの想定読者
  - 本ガイドラインは、中小企業で、ECサイトを新規に構築しようとしている経営者及びECサイトを運用している経営者を想定読者とする。
  - また、経営者から指示を受けたECサイトの構築・運用担当者、関係者および外部委託事業者も想定読者に含めるものとする。
3. 本ガイドラインの全体構成
4. 本ガイドラインの活用方法

第一部 経営者編

# 第一部 経営者編

## 1. ECサイトは、常に攻撃の対象として狙われている

国内における、EC加盟店におけるクレジットカード情報・個人情報の漏えい事故、それに伴うクレジットカードの不正利用被害の発生が後を絶たない状況

### ■ 日本クレジット協会

- 2021年における国内発行クレジットカードにおける年間不正利用被害総額は、**約330億円**  
※2021年の特殊詐欺事件（オレオレ詐欺等）による被害総額約280億円を大きく上回る
- 2021年の年間不正利用被害総額に対する番号盗用の被害割合は、**約94%**

### ■ 個人情報保護委員会/ECサイトへの不正アクセスに関する実態調査※

- 具体的な損失金額は、ECサイト上の取引規模や停止期間のよりばらつきがあるが、1,000万円以上の損失が40%以上で、数億円の損失が発生した事業者もみられた。

### ■ 本調査（直近で被害を受けたECサイトへのヒアリング調査）

- 被害企業19社を対象とした集計によると、1社あたりの個人情報・クレジットカード情報の平均漏えい件数は、**約4,100件**
- 被害企業16社を対象とした集計によると、1社あたりの平均被害額は、**約2,460万円**

被害が拡大している背景には、①オープン・ソース・ソフトウェア（OSS）のECサイト構築プログラムやプラグインを使って簡単にECサイトを構築できるようになったこと、②一方、自社構築サイトはセキュリティ対策が不十分であるため、脆弱性を狙った攻撃が増加していること、の2つの状況がある

### ■ 個人情報保護委員会/ECサイトへの不正アクセスに関する実態調査

- 不正アクセスを受けたECサイトの運営事業者の**約97%**が、**自社構築サイトで被害**が発生

### ■ 本調査（直近で被害を受けたECサイトへのヒアリング調査）

- 被害を受けたECサイトの**約71%**が、**OSSのECサイト構築プログラムやCMSの脆弱性を悪用されて被害**が発生

※個人情報保護委員会/ECサイトへの不正アクセスに関する実態調査 [https://www.ppc.go.jp/files/pdf/ecsite\\_report.pdf](https://www.ppc.go.jp/files/pdf/ecsite_report.pdf)

# 第一部 経営者編

## 1. ECサイトは、常に攻撃の対象として狙われている

ECサイト構築においてセキュリティ対策をすることが必須（対策しないと事故にあう）という意識がない。また、継続的なセキュリティ対策に経営資源を割り当てていない。

- 個人情報保護委員会/ECサイトへの不正アクセスに関する実態調査
  - ・ 不正アクセスを受けたECサイトの運営事業者の約97%が、自社構築サイトで被害が発生
  - ・ 自社で保守・運用を実施しているのは、21%、外部委託は、67%、特に実施していないは、11%
  - ・ 契約書・仕様書等でセキュリティ対策を記載しているのは、4%、記載はしているが具体的ではないが、21%、記載なしが44%、不明・無回答が31%
- 本調査（直近で被害を受けたECサイトへのヒアリング調査）
  - ・ 被害を受けたECサイトの約72%が、ECサイトへの継続的なセキュリティ対策（ECサイトの自社による保守または、外部委託先との保守契約の締結等）を実施していない
  - ・ セキュリティ対策が出来ない理由として、以下の様な意見も散見された
    - 事業全体の売上に比較して、EC事業での売上の割合が低い（5%以下）ため費用を掛けられない
    - ECサイトの運営で主にセキュリティ対策の必要性を認識している人員がない
    - 前任者が退職し、セキュリティ対策の引継ぎや知見のキャッチアップが不十分
    - 依頼しているつもりであったが、外部委託先では認識されていなかった

本事業での調査結果によると中小企業の○%がいつ(明日かも)サイバー被害にあってもおかしくない状況

- 本調査（直近で被害を受けたECサイトへのヒアリング調査）
  - ・ 50社への脆弱性診断の状況を活用。第3回委員会に向け精査・分析中。



# 第一部 経営者編

## 2. ECサイトのセキュリティ対策を疎かにすると何が起きるのか

【被害】セキュリティ対策を疎かにして、ひとたび事故・被害を発生させてしまうと、ECサイトが閉鎖に追い込まれ、ECサイト経由での売上高が大幅に減少する

- 個人情報保護委員会/ECサイトへの不正アクセスに関する実態調査
  - ECサイトを閉鎖した47社を対象とした集計によると、1社あたりのECサイトの平均閉鎖期間は、約8.6か月間
  - 従業員規模100名以下の34社を対象とした集計によると、1社あたりのECサイト閉鎖期間における売上高の平均損失額は、約1,600万円。従業員規模300名以下の48社を対象とした集計によると、1社あたりのECサイト閉鎖期間における売上高の平均損失額は、約6,300万円
  - ひとたび事故・被害を発生させてしまうと、クレジットカード決済機能の停止にとどまらず、ECサイトの閉鎖・事業の停止に追い込まれるケースが多い。特に中小規模のEC加盟店にとっては事業の停止は死活問題となる可能性がある
  - 不正アクセスを受けた後に、14%が現在、ECサイトの運営を取り止めている
- 本調査（直近で被害を受けたECサイトへのヒアリング調査（事例））
  - 現在のECサイト経由での売上高は、被害前の売上高の50%以下
  - ECサイト利用者の40～45%がクレジットカード決済での利用者であり、主流であったため、売上高が大幅に減少した。また、クレジットカード決済での利用者の10%（全体の4～4.5%）が離客した
  - 後払いや郵便振替に決済方法を変更し、手数料も自社負担としたが、クレジットカード決済を利用できなければ買わない顧客もいるため、売上高が減少した

# 第一部 経営者編



## 2. ECサイトのセキュリティ対策を疎かにすると何が起きるのか

【被害】 事故対応費用として、クレジットカードの再発行手数料、不正利用被害の補償額、フォレンジック調査にかかる費用、コールセンター設置にかかる費用、慰謝料といった費用の負担も重くのしかかる

### ■ 個人情報保護委員会/ECサイトへの不正アクセスに関する実態調査

- 不正アクセスを受けたECサイトの運営事業者の事故対応費用として以下がある。
  - フォレンジック調査等の調査費用（100万～500万が多く、特に200万～249万が多い）
  - クレジットカード差替え手数料（約92%が負担をして、1件当たり約2000円の回答が6割）
  - 顧客への見舞金の支払い・見舞品の送付（約25%が負担を実施）
  - その他発生費用として、セキュリティ強化費用、弁護士・コンサルティング費用他が発生

### ■ 本調査（直近で被害を受けたECサイトへのヒアリング調査）

- 事故対応費用を支出した中小規模のEC加盟店16社を対象とした集計によると、1社あたりの事故対応費用の平均額は、**約2,400万円**

#### A社（漏えい件数：約3千件）

カードの不正利用被害補償額・再発行手数料	250万円
フォレンジック調査費用	170万円
コールセンター設置費用	75万円
弁護士相談費用	40万円
DM発送費用	25万円
その他費用	40万円
合計	600万円

#### B社（漏えい件数：約1万件）

カードの不正利用被害補償額・再発行手数料	2,800万円
お詫び品（Quoカード、自社製品）費用	6,300万円
フォレンジック調査費用	} 700万円
コールセンター設置費用	
お詫び品の郵送費用	
その他費用	
合計	9,800万円

# 第一部 経営者編

## 2. ECサイトのセキュリティ対策を疎かにすると何が起きるのか

【被害】さらに、風評被害の影響で既に獲得していた顧客の離客が進むと、事故・被害前の売上高に回復するまでに長期化を余儀なくされる

- 個人情報保護委員会/ECサイトへの不正アクセスに関する実態調査
  - ECサイトの停止期間は、半年以上1年未満という回答が最も多かった
- 本調査（直近で被害を受けたECサイトへのヒアリング調査（事例））
  - 現在のECサイト経由での売上高は、被害前の売上高の50%以下（再掲）
- 中小規模のEC加盟店における被害の影響
  - 事故・被害の影響は、ECサイト閉鎖期間中における売上高の減少にとどまらず、事故対応費用の過重な負担や風評被害に伴う既顧客の離客など、多種多様であり、セキュリティ対策を疎かにした代償は高くつく




# 第一部 経営者編

## 2. ECサイトのセキュリティ対策を疎かにすると何が起きるのか

【事後対応】被害後、自社ではセキュリティ対策が不可能であると認識し、ECサイトを移設せざるを得なくなった

### ■ 個人情報保護委員会/ECサイトへの不正アクセスに関する実態調査

- 自社開発・外部委託サイトの約半分が、クラウド型サービス・ショッピングモール型サービスへ移行した
- 自社開発・外部委託サイトの14%が、ECサイトの運営停止に追い込まれた

	不正アクセス前	不正アクセス後	
自社開発・外部委託	97%	31%	 66%減
クラウド型サービス・ショッピングモール型サービス	3%	55%	 52%増
ECサイトの運営停止	—	14%	 14%増

### ■ 本調査（直近で被害を受けたECサイトへのヒアリング調査）

- 個人情報・クレジットカード情報の漏えい事故を契機に、カスタマイズよりもセキュリティの方が重要であるという考えに至り、SaaS型プラットフォームサービスやショッピングモールサービスの利用へ移行（被害を受けたECサイトの約53%がSaaS型ECプラットフォームの利用へ移行、約18%がショッピングモール型サービスの利用へ移行）

# 第一部 経営者編

## 3. 何が問題なのか

セキュリティ対策を考慮せずに、ECサイトを構築・運用している事が大きな問題である  
(ECサイト被害の発生原因は、アップデートが不十分なため)

- 個人情報保護委員会/ECサイトへの不正アクセスに関する実態調査
  - 不正アクセスの直接な原因として、SQLインジェクションの脆弱性（31%）、決済画面の改ざんを引き起こす脆弱性（37%）といった、ECサイトの脆弱性に対する不正アクセスが多くを占めている
  - このほか、ECサイトの管理画面へのアクセス制限不備が15%となっている
- 本調査（直近で被害を受けたECサイトへのヒアリング調査）
  - 被害を受けたECサイトの被害の発生原因として最も多いのが、ECサイト構築プログラムやCMS等の脆弱性を放置している（アップデートが出来ていない）（被害を受けたECサイトの約71%）
  - 次いで被害の発生原因として多いのが、以下の2つ
    - 管理者画面へのログイン認証における、デフォルト設定の状態のままでの運用（約18%）
    - 設定ミスによるWebサーバーの非公開ディレクトリの公開（約12%）
  - ECサイトの利用者の要望に応える、新機能の開発・追加やシステム改修等のカスタマイズが、構築プログラム等の迅速なバージョンアップ対応や、SaaS型ECプラットフォームへの移行の妨げになっている（約12%）
- その他（記載予定）
  - SQL、XSS、管理者画面への攻撃手口を図示して説明をする（経営者が理解できるように記載）
  - クレジットカード情報の非保持化対応を実施していてもクレジットカード情報が漏えいする場合もあることについて、記載する

# 第一部 経営者編

## 4. 経営者は何をやらなければならないのか

ECサイトのセキュリティ確保のために、経営者が実行すべき事項・取組は以下のとおり。

### ECサイトを所有する経営者が実行すべきセキュリティ対策の基本対策 (中小企業の情報セキュリティ対策ガイドライン 第3版※)

事項1	ECサイトのセキュリティ確保に関する組織全体の対応方針を定める
事項2	ECサイトのセキュリティ対策のための予算や人材を確保する
事項3	ECサイトを構築・運用するにあたって、必要と考えられるセキュリティ対策を検討させて実行を指示する
事項4	ECサイトのセキュリティ対策に関する適宜の見直しを指示する
事項5	緊急時（インシデント発生時）の対応や復旧のための体制を整備する
事項6	委託や外部サービス利用の際にはセキュリティに関する内容と責任を明確にする
事項7	ECサイトのセキュリティリスクやセキュリティ対策に関する最新動向を収集する

※中小企業の情報セキュリティ対策ガイドライン 第3版に記載されている、情報セキュリティを確保するために経営者が実行すべき「重要7項目の取組」は中小企業経営者が実施すべき基本事項である。

経営者は、実務担当者に以下の取組を実施させてください。

#### ECサイトを新規に構築する場合において実施すべき取組

取組1	ECサイトの開設計画時にセキュリティ対策・運用コストを必ず盛り込み、ECサイトの形態を正しく選定する
取組2	自社に人材がおらず、外部委託によりECサイトを自社構築する場合は、セキュリティ構築・運用に関する対策要件の実施を外部委託先に遵守させる
取組3	外部委託先への丸投げはやめましょう。セキュリティ対策を確実に実施できる委託先の選定と、対策実施の継続的モニタリングが必要です

#### ECサイトを運営中の場合において実施すべき取組

取組1	過去を振り返って、これまでのセキュリティ対策が不十分ではないか自己点検する
取組2	セキュリティ対策が不十分であることがわかり、対策までに時間がかかる場合、対策までのサイバー被害リスクを減らすため、応急処置（保険的対策）を行う
取組3	セキュリティ対策の不十分な箇所を対策する

### ■ ECサイトを新規に構築する場合において実行すべき取組

#### 取組 1

ECサイトの開設計画時にセキュリティ対策・運用コストを必ず盛り込み、ECサイトの形態を正しく選定する。

- ECサイト自社構築時は、最低限満たすべきセキュリティ対策要件を把握し、必ずセキュリティ運用・保守コストを見積ってください。
- そのうえで自社構築が本当に適当か、SaaS型ECサイト構築サービスやショッピングモールサービスの活用を含めて、ECサイトのタイプを選定ください。

#### 取組 2

自社に人材がおらず、外部委託によりECサイトを自社構築する場合は、セキュリティ構築・運用に関する対策要件の実施を外部委託先に遵守させる。

- ECサイトの構築時、外部委託先にセキュアコーディング、脆弱性診断等を必ず実施させてください。
- ECサイトのセキュリティ保守契約（環境の随時アップデート、攻撃状況の監視等）を外部委託先と必ず結んでください。（第2部のチェックシートを活用させてください）

#### 取組 3

外部委託先への丸投げはやめましょう。セキュリティ対策を確実に実施できる委託先の選定と、対策実施の継続的なチェックが必要です。

- セキュリティ対策は当然費用を伴います。契約時（仕様書、見積等）において、必要なセキュリティ対策を明記し、納品時、運用時に契約どおり実施していることを確認しましょう。

（注）中小企業はほとんどの事業者が外部委託による自社構築を行っており、上記「取組」は外部委託を想定した記述となっています。内作の場合は同等の対策を自社内で確実に実施下さい。

### ■ ECサイトを運営中の場合実行すべき取組

#### 取組 1

過去を振り返って、これまでのセキュリティ対策が不十分ではないか自己点検する。

- 安全なウェブサイトの作り方(改訂第7版)や、ECサイトの構築時及び運用時における最低限満たすべきセキュリティ対策要件をまとめたチェックシートを活用して、自社のECサイトにおけるセキュリティ対策の自己点検を行きましょう。

#### 取組 2

セキュリティ対策が不十分であることがわかり、対策までに時間がかかる場合、対策までのサイバー被害リスクを減らすため、応急処置（保険的対策）を行う

- セキュリティ対策が不十分であることがわかり、対策実施には時間がかかる場合、その間のサイバー被害リスクを減らすため、保険的対策（例：WAF実装、サイバー保険への加入）を実施しましょう。

#### 取組 3

セキュリティ対策の不十分な箇所を対策する。

- セキュリティ対策の不十分な箇所を対策し、あわせて、トータルコストを評価し、SaaS型ECサイト構築サービスやショッピングモールサービスの利用を検討しましょう。



## 第二部 実践編

# 第1章 ECサイトの構築時及び運用時における 最低限満たすべきセキュリティ対策要件

# 第1章 ECサイトの構築時及び運用時における最低限 満たすべきセキュリティ対策要件



## 1. ECサイトの構築時におけるセキュリティ対策要件

No	セキュリティ対策要件	区分
要件1	委託業者からECサイトの納品を受ける前に、脆弱性診断の実施によりECサイトに脆弱性がないかどうかを確認するとともに、見つかった脆弱性について最低でも、危険度「中」以上は対策すること。	必須
要件2	「安全なウェブサイトの作り方 改訂第7版」および「セキュリティ実装チェックリスト」に準拠して、ECサイトを構築すること。	必須
要件3	WebサーバーのOS・ミドルウェアや、Webアプリケーションやオープンソースのプログラムのソースコード等に関わる脆弱性情報を収集し、利用するプログラムへの脆弱性対応として、セキュリティパッチの適用や新バージョンへのアップデートを実施すること。	必須
要件4	管理者画面や管理用ソフトウェアへのアクセスにおいて、適切なセキュリティ対策（IPアドレスや端末IDによる接続制限、二段階認証・二要素認証の導入等）を実施すること。	必須
要件5	管理者画面や管理用ソフトウェアへのアクセス可能な端末において、適切なセキュリティ対策（ウイルス対策ソフトの導入、USBメモリ等外部記憶媒体の利用制限等）を実施すること。	必須
要件6	ECサイト上でのユーザー登録やアカウント登録において、不正ログイン対策(推測困難なパスワードの利用や、パスワード等の入力間違いの回数が一定数を超えた場合のアカウントロックの導入等)を実施すること。	必須
要件7	ユーザー認証機能の強度を高めるため、ログイン時における二段階認証・二要素認証を導入すること。	必須
要件8	ユーザーのメールアドレスの登録・変更やパスワードの登録・リセット・変更、アカウントの削除といった重要な処理を行う際に、ユーザーへのメール通知を行うこと。	必須
要件9	クレジットカード業界ルール（カード情報非保持化、カード決済のEMV 3Dセキュアへの移行）を遵守すること。	必須
要件10	ECサイトの運用を通じて取得される配送先（氏名、住所等）等のサイト利用者に関する個人情報に対して安全管理措置を講じること。	必須
要件11	WebサーバーやWebアプリケーションのログや、取引データ等のバックアップデータを過去1年間分保管すること。（万が一の被害時に備えて保管する事が必要）	必須
要件12	ログ出力機能、保管されるログ、バックアップ機能、保管されるバックアップデータに対して、不正アクセスができないよう保護する対策を実施すること。	必須
要件13	Webサーバーにおいて、セキュリティ対策（ウイルス対策ソフトの導入や、USBメモリ等外部記憶媒体の利用制限等）を実施すること。	必須
要件14	証明書（ドメイン認証証明書、組織認証証明書、EV SSLサーバー証明書等）の導入によるTLSの利用により、第三者機関(CA)によるドメイン名の正当性証明を行うこと。	必須

# 第1章 ECサイトの構築時及び運用時における最低限 満たすべきセキュリティ対策要件



## 1. ECサイトの構築時におけるセキュリティ対策要件

### 要件1

委託業者からECサイトの納品を受ける前に、脆弱性診断の実施によりECサイトに脆弱性がないかどうかを確認するとともに、見つかった脆弱性について最低でも、危険度「中」以上は対策すること。

- 脆弱性診断では、確認された脆弱性に関して、実害に至る攻撃難易度を考慮した危険度を、「高」、「中」、「低」の3段階で分類しており、危険度「中」以上については、迅速に対策を行うことを推奨している。

### 要件2

「安全なウェブサイトの作り方 改訂第7版」および「セキュリティ実装チェックリスト」に準拠して、ECサイトを構築すること。

- 「安全なウェブサイトの作り方 改訂第7版」および「セキュリティ実装チェックリスト」では、「ウェブアプリケーションのセキュリティ実装」として、SQL インジェクション、OS コマンド・インジェクションやクロスサイト・スクリプティング等11種類の脆弱性を取り上げ、それぞれの脆弱性で発生しうる脅威や特に注意が必要なウェブサイトの特徴等を解説し、脆弱性の原因そのものをなくす根本的な解決策、攻撃による影響の低減を期待できる対策を示している。
- また、「ウェブサイトの安全性向上のための取り組み」として、ウェブサーバのセキュリティ対策やフィッシング詐欺を助長しないための対策等7つの項目を取り上げ、主に運用面からウェブサイト全体の安全性を向上させるための方策を示している。

### 要件3

WebサーバのOS・ミドルウェアや、Webアプリケーションやオープンソースのプログラムのソースコード等に関わる脆弱性情報を収集し、利用するプログラムへの脆弱性対応として、セキュリティパッチの適用や新バージョンへのアップデートを実施すること。

- 脆弱性情報などセキュリティに関連する情報を公表しているECサイト構築プログラムを選定することが重要である。
- ECサイトの構築時に用いるWebサーバのOS・ミドルウェアや、Webアプリケーションやオープンソースのプログラムについては、その時点の最新バージョンにアップデートされたものを使用することが重要である。

# 第1章 ECサイトの構築時及び運用時における最低限 満たすべきセキュリティ対策要件



## 1. ECサイトの構築時におけるセキュリティ対策要件

### 要件4

管理者画面や管理用ソフトウェアへのアクセスにおいて、適切なセキュリティ対策（IPアドレスや端末IDによる接続制限、二段階認証・二要素認証の導入等）を実施すること。

- 管理者画面や管理用ソフトウェアにアクセスするためのID・パスワードが攻撃者に漏洩すると、サイト利用者の個人情報や、注文・取引データ等の漏えいに繋がるおそれがあるため、厳重に管理することが重要である。
- 万が一、管理者画面や管理用ソフトウェアのID・パスワードが不正に利用された場合に備えて、IPアドレスによる接続制限や、二段階認証・二要素認証を導入することが重要である。
- さらに、管理者画面や管理用ソフトウェアへの不正アクセス防止対策を強化するにあたっては、端末IDによる接続制限や二要素認証を併せて導入することが推奨される。

### 要件5

管理者画面や管理用ソフトウェアへのアクセス可能な端末において、適切なセキュリティ対策（ウイルス対策ソフトの導入、USBメモリ等外部記憶媒体の利用制限等）を実施すること。

- 管理者画面や管理用ソフトウェアへのアクセスに用いる端末がウイルスに感染すると、端末内部に保管しているサイト利用者の個人情報や、注文・取引データ等が外部に送信されるおそれがあるため、ウイルス対策ソフトの導入や、USBメモリ等外部記憶媒体の利用制限を通じて、ウイルス感染防止対策を行うことが重要である。

### 要件6

ECサイト上でのユーザー登録やアカウント登録において、不正ログイン対策(推測困難なパスワードの利用や、パスワード等の入力間違いの回数が一定数を超えた場合のアカウントロックの導入等)を実施すること。

- サイト利用者の会員パスワードが攻撃者に漏洩すると、サイト利用者の個人情報や、注文・取引データ等の漏えいに繋がるおそれがあるため、8桁以上、英字と数字と記号を組み合わせ、推測困難なパスワードを利用することが重要である。
- また、ログイン用のIDとパスワードのパターンを推測して、すべてのパターンを機械的に繰り返し入力し、サイト利用者のIDとパスワードを盗み出すという総当たり攻撃に備えて、パスワード等の入力間違いの回数が一定数を超えた場合のアカウントロックを導入することも重要である。

# 第1章 ECサイトの構築時及び運用時における最低限 満たすべきセキュリティ対策要件



## 1. ECサイトの構築時におけるセキュリティ対策要件

**要件7** ユーザー認証機能の強度を高めるため、ログイン時における二段階認証・二要素認証を導入すること。

- なりすましによる不正ログインの対策を強化するにあたっては、IDとパスワードを用いたユーザー認証よりも、安全性を高められる二段階認証二要素認証を導入することが重要である。

**要件8** ユーザーのメールアドレスの登録・変更やパスワードの登録・リセット・変更、アカウントの削除といった重要な処理を行う際に、ユーザーへのメール通知を行うこと。

- 正規のアカウント登録サイト等を装ったフィッシングサイトや、登録済みのパスワードの変更等を行うように不正に誘導するフィッシングメールに騙されて、ユーザーが気づかぬうちにIDとパスワードを盗まれてしまうことがないよう、ユーザーのメールアドレスの登録・変更やパスワードの登録・リセット・変更、アカウントの削除といった重要な処理を行う際に、ユーザーへのメール通知を行うことが重要である。

**要件9** クレジットカード業界ルール（カード情報非保持化、カード決済のEMV 3Dセキュアへの移行）を遵守すること。

- 改正割賦販売法におけるセキュリティ要求事項を反映した、一般社団法人日本クレジット協会が公表する「クレジットカード・セキュリティガイドライン【3.0版】」等のクレジットカード業界ルールに遵守して、必要となるセキュリティ対策を行うことが重要である。

**要件10** ECサイトの運用を通じて取得される配送先（氏名、住所等）等のサイト利用者に関する個人情報に対して安全管理措置を講じること。

- 改正個人情報保護法の第二十三条（安全管理措置）に基づき、ECサイトの運用を通じて取り扱う個人データの漏えい、滅失又は毀損の防止その他の個人データの安全管理のために必要かつ適切な措置を講じることが重要である。

# 第1章 ECサイトの構築時及び運用時における最低限 満たすべきセキュリティ対策要件



## 1. ECサイトの構築時におけるセキュリティ対策要件

**要件 1 1** WebサーバーやWebアプリケーションのログや、取引データ等のバックアップデータを過去1年間分保管すること。

- 万が一、個人情報・クレジットカード情報の漏えい事故を発生させてしまった場合には、事故の原因究明のためのフォレンジック調査が必要となる。また、フォレンジック調査会社に調査を依頼し、原因究明を徹底的に行うためには、調査に必要なデータが十分に揃っていることが必要となるため、WebサーバーやWebアプリケーションのログや、取引データ等のバックアップデータを過去1年間分保管しておくことが重要である。
- レンタルサーバー事業者を利用する場合は、万が一の場合にWebサーバーのアクセスログ等の提供がされることを確認することが重要である。

**要件 1 2** ログ出力機能、保管されるログ、バックアップ機能、保管されるバックアップデータに対して、不正アクセスができないよう保護する対策を実施すること。

- WebサーバーやWebアプリケーションのログや、取引データ等のバックアップデータを過去1年間分保管していても、保管ログ・データ等への不正アクセスの痕跡・証拠があれば、前述したフォレンジック調査による原因究明に支障が生じ、誤った結果が導かれるおそれがある。このため、ログ出力機能、保管されるログ、バックアップ機能、保管されるバックアップデータに対して、不正アクセスができないよう保護する対策を実施することが重要である。

**要件 1 3** Webサーバーにおいて、セキュリティ対策（ウイルス対策ソフトの導入や、USBメモリ等外部記憶媒体の利用制限等）を実施すること。

- Webサーバー自体がウイルスに感染すると、サーバー内部に保管しているサイト利用者の個人情報や、注文・取引データ等が外部に送信されるおそれがあるため、ウイルス対策ソフトの導入や、USBメモリ等外部記憶媒体の利用制限を通じて、ウイルス感染防止対策を行うことが重要である。

# 第1章 ECサイトの構築時及び運用時における最低限 満たすべきセキュリティ対策要件



## 1. ECサイトの構築時におけるセキュリティ対策要件

### 要件14

証明書（ドメイン認証証明書、組織認証証明書、EV SSLサーバー証明書等）の導入によるTLSの利用により、第三者機関(CA)によるドメイン名の正当性証明を行うこと。

- ユーザーが気づかぬうちにIDとパスワードを不正に窃取するフィッシングサイトではないことを、サイト利用者が確認できるようにするためには、証明書（ドメイン認証証明書、組織認証証明書、EV SSLサーバー証明書等）の導入によるTLSの利用により、第三者機関(CA)によるドメイン名の正当性証明を行うことが重要である。



# 第1章 ECサイトの構築時及び運用時における最低限 満たすべきセキュリティ対策要件



## 2. ECサイトの運用時におけるセキュリティ対策要件

No	セキュリティ対策要件	区分
要件1	WebサーバーのOS・ミドルウェアや、Webアプリケーションやオープンソースのプログラムのソースコード等に関わる脆弱性情報を収集し、利用するプログラムへの脆弱性対応として、セキュリティパッチの適用や新バージョンへのアップデートを実施すること。	必須
要件2	システムの定期的なバックアップの取得及び、ログの定期的な確認、確認した結果、不正なアクセス等があれば、アクセスの制限等の対策を実施すること。	必須
要件3	脆弱性診断の定期的な実施によりECサイトに脆弱性がないかどうかを確認して、最低でも、危険度「中」以上は対策を行うこと。	必須
要件4	Webサイト改ざんの攻撃からECサイトを保護するため、Webサーバーのwwwディレクトリ配下のアプリケーションやコンテンツ等のファイルについて、定期的な差分チェック（ファイル整合性監視）を行うこと。（または必要に応じて、Webサイト改ざん検知ツールを導入し、適切な運用を行うこと）	必須
要件5	WAF（Web Application Firewall）を導入すること（1.2.3.4が実施出来ないタイミングに備え、保険的対策としてWAFを導入する）	推奨
要件6	万が一、Webサイトがサイバー攻撃等による被害を受けた場合に備えて、サイバー保険に加入すること。	推奨

# 第1章 ECサイトの構築時及び運用時における最低限 満たすべきセキュリティ対策要件



## 2. ECサイトの運用時におけるセキュリティ対策要件

### 要件1

WebサーバーのOS・ミドルウェアや、Webアプリケーションやオープンソースのプログラムのソースコード等に関わる脆弱性情報を収集し、利用するプログラムへの脆弱性対応として、セキュリティパッチの適用や新バージョンへのアップデートを実施すること。

- 既に攻撃方法が見つかったり、被害の存在が広く知られていたりするなど、危険度の高い脆弱性に関しては、セキュリティパッチの適用や新バージョンへのアップデートを迅速に行うことが重要である。

### 要件2

システムの定期的なバックアップの取得及び、ログの定期的な確認、確認した結果、不正なアクセス等があれば、アクセスの制限等の対策を実施すること。

- 個人情報・クレジットカード情報の漏えい事故を発生させる可能性のあるECサイトには、ECサイトへの不正ログインが増えたり、システム上で対応されていない不正な注文ができたりするという予兆が発生している場合もある。このため、ログの定期的な確認、確認した結果、不正なアクセス等があれば、アクセスの制限等の対策を実施することが重要である。

### 要件3

脆弱性診断の定期的な実施によりECサイトに脆弱性がないかどうかを確認して、最低でも、危険度「中」以上は対策を行うこと。

- Webサーバーなどのプラットフォームは、定期的に脆弱性診断を実施することが重要である。
- Webアプリケーションは、少なくとも、ECサイトの利用者の要望に応じて、新機能の開発・追加やシステム改修等のカスタマイズを行ったときには、その都度脆弱性診断を実施することが重要である。
- また、上記のようなカスタマイズを高頻度で行っている場合は、概ね四半期に1回の頻度で定期的に脆弱性診断を実施することが重要である。
- 脆弱性診断では、確認された脆弱性に関して、実害に至る攻撃難易度を考慮した危険度を、「高」、「中」、「低」の3段階で分類しており、危険度「中」以上については、迅速に対策を行うことを推奨している。

# 第1章 ECサイトの構築時及び運用時における最低限 満たすべきセキュリティ対策要件



## 2. ECサイトの運用時におけるセキュリティ対策要件

### 要件4

Webサイト改ざんの攻撃からECサイトを保護するため、Webサーバーのwwwディレクトリ配下のアプリケーションやコンテンツ等のファイルについて、定期的な差分チェック（ファイル整合性監視）を行うこと。（または必要に応じて、Webサイト改ざん検知ツールを導入し、適切な運用を行うこと）

- 不正アクセスやウイルス感染により、Webサーバー内部に保管しているサイト利用者の個人情報や、注文・取引データ等を外部に送信する不正なプログラムが、Webサーバーのwwwディレクトリ配下に仕掛けられた場合でも、それを検知できるように、定期的な差分チェック（ファイル整合性監視）を行うこと（または必要に応じて、Webサイト改ざん検知ツールを導入し、適切な運用を行うことが重要である）。

### 要件5

要件1～4が実施できないタイミングに備え、保険的対策として、WAF（Web Application Firewall）を導入すること。

- 要件1～4が実施できないタイミングとして、既に見つかった脆弱性に対して対応するまでの間や、必要となるセキュリティ対策を実装するまでの間が想定される。その間にサイバー攻撃を受けることがないよう、保険的対策として、WAF（Web Application Firewall）を導入することが推奨される。

### 要件6

万が一、Webサイトがサイバー攻撃等による被害を受けた場合に備えて、サイバー保険に加入すること。

- WAF（Web Application Firewall）以外にも、万が一、ECサイトがサイバー攻撃による被害を受けた場合に備えて、サイバー保険に加入することが推奨される。
- サイバー保険については、個人情報・クレジットカード情報の漏えい事故を発生させてしまったEC加盟店の多くが、被害後に加入しており、損害賠償や事故対応費用の負担、収益の減少を補う効果が認められることから、加入を継続することが推奨される。

## (ご紹介) ECサイト向けホスティング付きセキュリティ保守運用サービス

セキュリティ対策の1方法として「ECサイト向けホスティング付きセキュリティ保守運用サービス」の活用を検討ください。Welcart等のECサイト構築パッケージベンダから提供されています。

### 【本保守運用サービスの概要】

#### ・提供サービスの内容※1

- ・サーバ、ミドル等の仮想クラウドの環境提供
- ・ECサイト構築パッケージ、必要な全動作環境（OS、ミドル）のアップデート
- ・脆弱性検査を定期的を実施
- ・WAFによる防御
- ・不正アクセスログの監視・注意喚起連絡
- ・アップデートによりECサイトの動作に影響が出た場合のサイト改修

※1 サービスによっては、提供されていない、または有料オプションの機能もありますので提供ベンダに必ず確認ください。

※2 IPAが現時点把握している該当サービスはWelHost（Welcart向け）  
ただともに100サイト以下(普及していない)。普及阻害の要因は費用。

※3 Welcart(WordPressのプラグイン) ECサイト数：2 - 3万

## 第2章 ECサイトを新規に構築する場合において 検討・確認すべき事項

# 第2章 ECサイトを新規に構築する場合において検討・確認すべき事項

## 1. 確認・検討にあたっての考え方

第一部の「4. 経営者は何をやらなければならないか」で示した、経営者がECサイトを新規に構築する場合において実行すべき取組について、ECサイトにおけるセキュリティ対策を実践する責任者・担当者が、経営者と連携しつつ、それを具体的に実践してください。

### ECサイトを新規に構築する場合において実行すべき取組

取組1

ECサイトの開設計画時にセキュリティ対策・運用コストを必ず盛り込み、ECサイトの形態を正しく選定する

取組2

自社に人材がおらず、外部委託によりECサイトを自社構築する場合は、セキュリティ構築・運用に関する対策要件の実施を外部委託先に遵守させる

取組3

外部委託先への丸投げはやめましょう。セキュリティ対策を確実に実施できる委託先の選定と、対策実施の継続的なチェックが必要です

(1) セキュリティ運用・保守コストの見積もりに基づく、ECサイトの形態の選定

セキュリティ対策・運用コストを見積もり、SaaS型ECプラットフォームやショッピングモールサービスを利用した場合とのトータルコストと比較した上で、ECサイトの形態を選定する

(2) 外部委託を活用した、自社で対応困難な対策の実施

セキュリティ構築・運用に関する要件に沿って、自社で対応可能な要件と自社で対応困難な要件を分類した上で、自社で対応困難な要件は、外部委託の活用により対策を実施する

(3) 外部委託先におけるセキュリティ対策の実施状況の定期的確認

外部委託先でセキュリティ対策が確実に実施されるよう、外部委託先におけるセキュリティ対策の実施状況を、選定時に確認するとともに、運用時においても継続的にチェックする

# 第2章 ECサイトを新規に構築する場合において検討・確認すべき事項

## 2. 確認・検討手順

外部委託による自社構築がほとんどであるため、外部委託による自社構築における確認・検討手順を以下に示す。

### (1) セキュリティ運用・保守コストの見積もりに基づく、ECサイトの形態の選定

セキュリティ対策・運用コストを見積もり、SaaS型ECプラットフォームやショッピングモールサービスを利用した場合とのトータルコストと比較した上で、ECサイトの形態を選定する



### (2) 外部委託を活用した、自社で対応困難な対策の実施

セキュリティ構築・運用に関する要件に沿って、自社で対応可能な要件と自社で対応困難な要件を分類した上で、自社で対応困難な要件は、外部委託の活用により対策を実施する。また、外部委託先に依頼する対策が、契約書に盛り込まれていることを必ず確認する



### (3) 外部委託先におけるセキュリティ対策の実施状況の定期的確認

外部委託先でセキュリティ対策が確実に実施されるよう、外部委託先におけるセキュリティ対策の実施状況を、選定時に確認するとともに、運用時においても継続的にチェックする

※後述の「3. 構築契約または運用・保守契約上の確認事項」を参照

(注) 中小企業はほとんどの事業者が外部委託による自社構築を行っており、上記「取組」は外部委託を想定した記述となっています。内作の場合は同等の対策を自社内で確実に実施下さい。

### 2. 確認・検討事項

#### (1) セキュリティ運用・保守コストの見積もりに基づく、ECサイトの形態の選定

自社構築ECサイトのセキュリティ運用コストを見積り、SaaS型ECプラットフォームやショッピングモールサービスを利用した場合とのトータルコストと比較した上で、正しくECサイトの形態を選定する。

##### ① 自社構築ECサイトのセキュリティ運用コストの見積り


【自社構築ECサイトにおいて実施必須なセキュリティ運用項目（基本）】


###### ■ 脆弱性対策、運用

- 最新の脆弱性情報の収集
- 自社ECサイトに関連した、対策が必要となる脆弱性情報の特定
- 自社ECサイトへの影響度の確認
- 公表された脆弱性への対処（セキュリティパッチの適用やアップデート等による修正）
- システムの定期的なバックアップの取得
- ログの取得・保管と定期的な確認による異常検出
- 脆弱性診断の実施およびペネトレーションテストの実施
- ウイルス対策ソフトの実装・運用

###### ■ 脅威検知対策

- WAFの実装・運用
- AI不正利用検知の実装・運用

 の費用感は2～5万円／月

 の費用感は100万円／年～

上記より自社構築ECサイトの場合、最低でも10万円/月のセキュリティ運用コストを見込む必要有り。



### 2. 確認・検討事項

#### (1) セキュリティ運用・保守コストの見積もりに基づく、ECサイトの形態の選定

#### ② トータルコストを比較した上での ECサイトの形態の選定

セキュリティ運用コストを含めたトータルコストを比較、ECサイトの形態を正しく選定ください。

項目		ECサイト自社構築の場合	SaaS型ECプラットフォームまたはモジュール使用の場合
カスタマイズ性		高	低
構築時コスト	セキュリティ以外	一般的に高	低
	セキュリティ費用	一般的に高	低
運用時コスト	セキュリティ以外※2	一般的に低	左記 + SaaS使用料※3
	セキュリティ運用	最低10万円/月～	基本0※1

※1 PCIDSSに準拠しているプラットフォームを必ず選定ください。またカスタマイズ等によりECサイト固有の動的Pageを作り込んでいる場合、固有部分に対してはセキュリティ運用コスト(脆弱性診断等)を見込んでください。

※2 商品入替、キャンペーン、サイト改修等

※3 月々の固定費 + 決済手数料を含む

## 第2章 ECサイトを新規に構築する場合において検討・確認すべき事項

### 2. 確認・検討事項

#### (2) 外部委託を活用した、自社で対応困難な対策の実施

以下の「自社対応確認チェックリスト」を用いて、新規に構築する予定のECサイトが、第二部のECサイトの構築時及び運用時における最低限満たすべきセキュリティ対策要件への準拠性について、どれぐらい考慮されているか、確認する。

- 具体的には、自社対応確認チェックリストに記載されたセキュリティ対策要件に沿って、**自社で対応可能な要件**と**自社で対応困難な要件**を分類し、双方を明確化する。

#### 構築時チェックリスト – ①ECサイトの構築時におけるセキュリティ対策要件の確認 –

No	セキュリティ対策要件	自社で対応可能な要件	外部委託で対応する要件
1	委託業者からECサイトの納品を受ける前に、脆弱性診断の実施によりECサイトに脆弱性がないかどうかを確認するとともに、見つかった脆弱性について最低でも、危険度「中」以上は対策すること。	✓	
2	「安全なウェブサイトの作り方 改訂第7版」および「セキュリティ実装チェックリスト」に準拠して、ECサイトを構築すること。		✓
3	WebサーバーのOS・ミドルウェアや、Webアプリケーションやオープンソースのプログラムのソースコード等に関わる脆弱性情報を収集し、利用するプログラムへの脆弱性対応として、セキュリティパッチの適用や新バージョンへのアップデートを実施すること。	✓	Sample
4	管理者画面や管理用ソフトウェアへのアクセスにおいて、適切なセキュリティ対策（IPアドレスや端末IDによる接続制限、二段階認証・二要素認証の導入等）を実施すること。	✓	
5	管理者画面や管理用ソフトウェアへのアクセス可能な端末において、適切なセキュリティ対策（ウイルス対策ソフトの導入、USBメモリ等外部記憶媒体の利用制限等）を実施すること。		✓

## 第2章 ECサイトを新規に構築する場合において検討・確認すべき事項

### 2. 確認・検討事項

#### (2) 外部委託を活用した、自社で対応困難な対策の実施

##### 構築時チェックリスト – ①ECサイトの構築時におけるセキュリティ対策要件の確認 –

No	セキュリティ対策要件	自社で対応可能な要件	外部委託で対応する要件
6	ECサイト上でのユーザー登録やアカウント登録において、不正ログイン対策(推測困難なパスワードの利用や、パスワード等の入力間違いの回数が一定数を超えた場合のアカウントロックの導入等)を実施すること。	✓	
7	ユーザー認証機能の強度を高めるため、ログイン時における二要素認証・多要素認証を導入すること。		✓
8	ユーザーのメールアドレスの登録・変更やパスワードの登録・リセット・変更、アカウントの削除といった重要な処理を行う際に、ユーザーへのメール通知を行うこと。	✓	
9	クレジットカード業界ルール（カード情報非保持化、カード決済のEMV 3Dセキュアへの移行）を遵守すること。	✓	
10	ECサイトの運用を通じて取得される配送先（氏名、住所等）等のサイト利用者に関する個人情報に対して安全管理措置を講じること。	✓	Sample
11	WebサーバーやWebアプリケーションのログや、取引データ等のバックアップデータを過去1年間分保管すること。（万が一の被害時に備えて保管する事が必要）		✓
12	ログ出力機能、保管されるログ、バックアップ機能、保管されるバックアップデータに対して、不正アクセスができないよう保護する対策を実施すること。		✓
13	Webサーバーにおいて、セキュリティ対策（ウイルス対策ソフトの導入や、USBメモリ等外部記憶媒体の利用制限等）を実施すること。	✓	
14	証明書（ドメイン認証証明書、組織認証証明書、EV SSLサーバー証明書等）の導入によるTLSの利用により、第三者機関(CA)によるドメイン名の正当性証明を行うこと。	✓	

全てのチェックが埋まっていることを必ず確認ください。

## 第2章 ECサイトを新規に構築する場合において検討・確認すべき事項

### 2. 確認・検討事項

#### (2) 外部委託を活用した、自社で対応困難な対策の実施

#### 運用時チェックリスト – ②ECサイトの運用時におけるセキュリティ対策要件の確認 –

No	セキュリティ対策要件	自社で対応可能な要件	外部委託で対応する要件
1	WebサーバーのOS・ミドルウェアや、Webアプリケーションやオープンソースのプログラムのソースコード等に関わる脆弱性情報を収集し、利用するプログラムへの脆弱性対応として、セキュリティパッチの適用や新バージョンへのアップデートを実施すること。	✓	
2	システムの定期的なバックアップの取得及び、ログの定期的な確認、確認した結果、不正なアクセス等があれば、アクセスの制限等の対策を実施すること。		✓
3	脆弱性診断の定期的な実施によりECサイトに脆弱性がないかどうかを確認して、最低でも、危険度「中」以上は対策を行うこと。	Sample	✓
4	Webサイト改ざんの攻撃からECサイトを保護するため、Webサーバーのwwwディレクトリ配下のアプリケーションやコンテンツ等のファイルについて、定期的な差分チェック（ファイル整合性監視）を行うこと。（または必要に応じて、Webサイト改ざん検知ツールを導入し、適切な運用を行うこと）	✓	
5	WAF（Web Application Firewall）を導入すること（1.2.3.4が実施出来ないタイミングに備え、保険的対策としてWAFを入れることを推奨）		
6	万が一、Webサイトがサイバー攻撃等による被害を受けた場合に備えて、サイバー保険に加入すること。		

1～4のすべてのチェックが埋まっていることを必ず確認ください。5と6は、チェックが埋まっていることが望ましいです。

### 2. 確認・検討事項

#### (2) 外部委託を活用した、自社で対応困難な対策の実施

分類した結果からみて、ECサイトの構築時・運用時において、推奨される対応は以下のとおり。

- ✓ 自社ですべて対応可能である場合のみ、自社でECサイトを構築・運用することが可能である。
  - ✓ 自社で対応困難な必須の要件が一部でも含まれる場合は、対応困難な要件を補うために外部委託を活用することが必要になる。
  - ✓ なお、自社で対応困難な必須の要件を、外部委託で補うことが難しい状況で、新規のECサイトを自社構築しないことが重要である。
- 
- このように自社対応確認チェックリストは、自社のみでECサイトを構築・運用することが可能であるか、また外部委託先に依頼する必要があるセキュリティ対策が何かを確認するために活用してください。

### 2. 確認・検討事項

#### (3) 外部委託先におけるセキュリティ対策の実施状況の定期的確認

外部委託先でセキュリティ対策が確実に実施されるよう、外部委託先におけるセキュリティ対策の実施状況を、選定時に確認するとともに、運用時においても継続的に実施状況を確認する。確認すべきセキュリティ対策は以下のとおり。

- 運用時チェックリストの1)～4)の実施を定期的に確認する

## 第2章 ECサイトを新規に構築する場合において検討・確認すべき事項

### 3. 構築契約または運用・保守契約上の確認事項

#### ■ 構築契約または運用・保守契約上の確認事項

前述した2. 確認・検討事項/ (2) 外部委託を活用した、自社で対応困難な対策の実施において、自社対応確認チェックリストを用いて確認を行った結果、自社で対応困難な要件に分類されたセキュリティ対策要件について、外部業者へ委託する場合は、必ず契約内容（構築契約、運用・保守契約、見積等の内容）に、当該セキュリティ対策要件が盛り込まれていることを確認する。

- 構築契約または運用・保守契約に盛り込まれたセキュリティ対策要件であっても、必ず自社の義務と外部委託先の免責事項や、万が一、事故が発生した場合の責任や対応方法を確認することが重要である
- 特に、脆弱性対応を含む、ECサイトの運用・保守契約を、外部委託業者と締結する場合には、以下の要求事項が盛り込まれていることを確認することが重要である。
  - 最新の脆弱性情報の収集
  - 契約先が担当する自社ECサイトに関連して、必要となる情報の特定
  - 契約先が担当する自社ECサイトへの影響度の確認
  - 公表された脆弱性への影響度の調査
  - 公表された脆弱性への対処（セキュリティパッチの適用やアップデート等による修正）
  - ECシステムの定期的なバックアップの取得
  - ログの取得・保管と定期的な確認による異常検出

## 第2章 ECサイトを新規に構築する場合において検討・確認すべき事項



### 3. 構築契約または運用・保守契約上の確認事項

- 以下は、ECサイトの構築契約の仕様書の具体例の一つです（なお、仕様書をECサイト運営者側で作成しない場合においては、構築時／運用時チェックリストに委託先実施項目を明記させ、見積に当該チェックシートを添付する契約の形態も代案として可能です）

セキュリティ対策における作業については、具体的なセキュリティ対策を当社に提示し、承認を得てから作業すること。

- すべてのサーバの要塞化を行うこと。具体的には、不要なソフトウェアの削除、不要なサービスの停止、不要な通信ポートの閉鎖、不要なアカウントの削除、適切なパスワードの設定、セキュリティパッチの適用等を実施すること。対象となるサーバは以下のとおり。【対象サーバ】 ○○○サーバ
- ウェブサーバに対するセキュリティ対策については、IPAが発行している「安全なウェブサイトの作り方」のセキュリティ実装の項目を網羅すること。あわせて、セッションはログイン成功からログアウトまでとし、ログアウト後はセッション情報を破棄すること。セキュリティ対策を施すことにより、利便性が損なわれないように考慮すること。対象となるサーバは以下のとおり。【対象サーバ】 ○○○サーバ
- 監査や事故不具合の追跡の為にログを出力すること。ただし、個人情報等の機密情報が漏えいすることのない情報にとどめること。ログが不正に参照・変更・削除されないよう保護すること。ログの安全な保管方法（媒体、保管フォーマット、保管場所等）を定めること。対象となるサーバは以下のとおり。【対象サーバ】 ○○○サーバ
- 外部に公開するサーバの侵入対策を施すこと。また、侵入された場合に検知ができること。対象となるサーバは以下のとおり。【対象サーバ】 ○○○サーバ
- 外部に公開するサーバに保持するデータについては、漏えいが発生した場合に備えデータの難読化や暗号化を施すこと。対象となるサーバは以下のとおり。【対象サーバ】 ○○○サーバ
- 納入時にすべてのサーバに対して第三者によるセキュリティ診断を行い、その結果をレポートして提出すること。セキュリティ診断はすべてのサーバに対してプラットフォーム診断（サーバやネットワーク機器に対するセキュリティ診断）を、ウェブアプリケーションを提供するサーバにはウェブアプリケーションのセキュリティ診断も行うこと。プラットフォーム診断を行う対象のサーバは以下のとおり。【対象サーバ】 ○○○サーバ
- ウェブアプリケーションのセキュリティ診断対象のサーバは以下のとおり。【対象サーバ】 ○○○サーバ



## 第2章 ECサイトを新規に構築する場合において検討・確認すべき事項



### 4. SaaS型ECプラットフォームの選定基準

前述した2. 確認・検討事項/ (1) セキュリティ運用・保守コストの見積もりに基づく、ECサイトの形態の選定において、SaaS型ECプラットフォームを選定した場合、以下のセキュリティ対策の実施状況について確認する必要がある。

- PCIDSS準拠であること

## 第3章 運営中のECサイトにおいて検討・確認すべき事項

## 1. 確認・検討にあたっての考え方

第一部の「4. 経営者は何をやらなければならないか」で示した、経営者がECサイトを既に自社構築し運用している場合において実行すべき取組について、ECサイトにおけるセキュリティ対策を実践する責任者・担当者が、経営者と連携しつつ、それを具体的に実践してください。

### 運営中のECサイトにおいて実行すべき取組

取組 1

過去を振り返って、これまでのセキュリティ対策が不十分ではないか自己点検する

(1) セキュリティ対策の自己点検

過去を振り返って、運営中のECサイトにおいて、セキュリティ構築・運用に関する対策要件をどれぐらい実装できているか、自己点検により確認する

取組 2

セキュリティ対策が不十分であることがわかり、対策までに時間がかかる場合、対策までのサイバー被害リスクを減らすため、応急処置（保険的対策）を行う

(2) サイバー被害リスクを減らすために必要となる応急処置（保険的対策）の実施

追加対策を実装するまでの間にサイバー攻撃を受けることがないよう、WAFを導入するとともに、万が一、ECサイトがサイバー攻撃による被害を受けた場合に備えて、サイバー保険に加入する

取組 3

セキュリティ対策の不十分な箇所を対策する

(3) セキュリティ対策の不十分な箇所への追加対策の実施

セキュリティ対策の不十分な箇所については、外部委託の活用を含め、必要となる追加対策を個別に検討し、実装する

## 2. 確認・検討手順

運営中のECサイトにおける確認・検討手順を以下に示す。

### (1) セキュリティ対策の自己点検

過去を振り返って、運営中のECサイトにおいて、セキュリティ構築・運用に関する対策要件をどれぐらい実装できているか、自己点検により確認する



### (2) サイバー被害リスクを減らすために必要となる応急処置（保険的対策）の実施

追加対策を実装するまでの間にサイバー攻撃を受けることがないように、WAFを導入するとともに、万が一、ECサイトがサイバー攻撃による被害を受けた場合に備えて、サイバー保険に加入する



### (3) セキュリティ対策の不十分な箇所への追加対策の実施

セキュリティ対策の不十分な箇所については、外部委託の活用を含め、必要となる追加対策を個別に検討し、実装する

# 第3章 運営中のECサイトにおいて検討・確認すべき事項



## 2. 確認・検討事項

### (1) セキュリティ対策の自己点検

以下の「実装確認チェックリスト」を用いて、運営中のECサイトが、第二部／第1章のECサイトの構築時及び運用時における最低限満たすべきセキュリティ対策要件を、どれぐらい実装しているか、自己点検により確認する。

- 具体的には、実装確認チェックリストに記載されたセキュリティ対策要件に沿って、**実施済みの要件と未実装の要件を分類し**、双方を明確化する。

#### 運営中サイト向け構築時チェックリスト – ①ECサイトの構築時におけるセキュリティ対策要件実施の確認 –

No	セキュリティ対策要件	実装済みの要件	対策完了時にチェック
1	委託業者からECサイトの納品を受ける前に、脆弱性診断の実施によりECサイトに脆弱性がないかどうかを確認するとともに、見つかった脆弱性について最低でも、危険度「中」以上は対策すること。	✓	
2	「安全なウェブサイトの作り方 改訂第7版」および「セキュリティ実装チェックリスト」に準拠して、ECサイトを構築すること。		✓
3	WebサーバーのOS・ミドルウェアや、Webアプリケーションやオープンソースのプログラムのソースコード等に関わる脆弱性情報を収集し、利用するプログラムへの脆弱性対応として、セキュリティパッチの適用や新バージョンへのアップデートを実施すること。	✓	Sample
4	管理者画面や管理用ソフトウェアへのアクセスにおいて、適切なセキュリティ対策（IPアドレスや端末IDによる接続制限、二段階認証・二要素認証の導入等）を実施すること。	✓	
5	管理者画面や管理用ソフトウェアへのアクセス可能な端末において、適切なセキュリティ対策（ウイルス対策ソフトの導入、USBメモリ等外部記憶媒体の利用制限等）を実施すること。		✓

# 第3章 運営中のECサイトにおいて検討・確認すべき事項



## 2. 確認・検討事項

### (1) セキュリティ対策の自己点検

#### 運営中サイト向け構築時チェックリスト – ①ECサイトの構築時におけるセキュリティ対策要件実施の確認 –

No	セキュリティ対策要件	実装済みの要件	対策完了時にチェック
6	ECサイト上でのユーザー登録やアカウント登録において、不正ログイン対策(推測困難なパスワードの利用や、パスワード等の入力間違いの回数が一定数を越えた場合のアカウントロックの導入等)を実施すること。	✓	
7	ユーザー認証機能の強度を高めるため、ログイン時における二段階認証・二要素認証を導入すること。		✓
8	ユーザーのメールアドレスの登録・変更やパスワードの登録・リセット・変更、アカウントの削除といった重要な処理を行う際に、ユーザーへのメール通知を行うこと。	✓	
9	クレジットカード業界ルール（カード情報非保持化、カード決済のEMV 3Dセキュアへの移行）を遵守すること。	✓	
10	ECサイトの運用を通じて取得される配送先（氏名、住所等）等のサイト利用者に関する個人情報に対して安全管理措置を講じること。	✓	Sample
11	WebサーバーやWebアプリケーションのログや、取引データ等のバックアップデータを過去1年間分保管すること。（万が一の被害時に備えて保管する事が必要）		✓
12	ログ出力機能、保管されるログ、バックアップ機能、保管されるバックアップデータに対して、不正アクセスができないよう保護する対策を実施すること。		✓
13	Webサーバーにおいて、セキュリティ対策（ウイルス対策ソフトの導入や、USBメモリ等外部記憶媒体の利用制限等）を実施すること。	✓	
14	証明書（ドメイン認証証明書、組織認証証明書、EV SSLサーバー証明書等）の導入によるTLSの利用により、第三者機関(CA)によるドメイン名の正当性証明を行うこと。	✓	

※「対策完了時にチェック」欄は外部委託先等に問合せの上全件項目が埋まるようにチェック下さい。

# 第3章 運営中のECサイトにおいて検討・確認すべき事項



## 2. 確認・検討事項

### (1) セキュリティ対策の自己点検

#### 運営中サイト向け運用時チェックリスト – ②ECサイトの運用時におけるセキュリティ対策要件実施の確認 –

No	セキュリティ対策要件	実装済みの要件	対策完了時にチェック
1	WebサーバーのOS・ミドルウェアや、Webアプリケーションやオープンソースのプログラムのソースコード等に関わる脆弱性情報を収集し、利用するプログラムへの脆弱性対応として、セキュリティパッチの適用や新バージョンへのアップデートを実施すること。	✓	
2	システムの定期的なバックアップの取得及び、ログの定期的な確認、確認した結果、不正なアクセス等があれば、アクセスの制限等の対策を実施すること。		✓
3	脆弱性診断の定期的な実施によりECサイトに脆弱性がないかどうかを確認して、最低でも、危険度「中」以上は対策すること。		✓
4	Webサイト改ざんの攻撃からECサイトを保護するため、Webサーバーのwwwディレクトリ配下のアプリケーションやコンテンツ等のファイルについて、定期的な差分チェック（ファイル整合性監視）を行うこと。（または必要に応じて、Webサイト改ざん検知ツールを導入し、適切な運用を行うこと）	✓	
5	WAF（Web Application Firewall）を導入すること（1.2.3.4が実施出来ないタイミングに備え、保険的対策としてWAFを導入する）		✓
6	万が一、Webサイトがサイバー攻撃等による被害を受けた場合に備えて、サイバー保険に加入すること。		

Sample

※「対策完了時にチェック」欄は外部委託先等に問合せの上、1～4の必須項目が埋まるようにチェック下さい。

### 2. 確認・検討事項

#### (1) セキュリティ対策の自己点検

分類した結果からみて、ECサイトの構築時・運用時において、推奨される対応は以下のとおり。

- ✓ すべて実施済みであるか確認ください。すべての必須要件がチェック済みの場合は、継続して自社でECサイトを構築・運用してかまいません。
  - ✓ 未実装の必須要件が一部でも含まれる場合は、未実装の要件を補うために、追加対策を個別に検討することが必要になります。対策を至急検討してください。
  - ✓ なお、必須要件の一部でも対策できない場合は、SaaS型ECプラットフォームへの移行を含め、善処策を検討ください。
- このように実装確認チェックリストは、継続して自社でECサイトを運用することが可能であるか、追加対策として個別に検討する必要があるセキュリティ対策が何かを確認するために活用してください。



### 2. 確認・検討事項

#### (2) サイバー被害リスクを減らすために必要となる応急処置（保険的対策）の実施

必要となる追加対策を実装するまでの間にサイバー攻撃を受けることがないよう、保険的対策として、WAF（Web Application Firewall）を導入することが推奨される。

また、万が一、ECサイトがサイバー攻撃による被害を受けた場合に備えて、サイバー保険に加入することが推奨される。

- WAF（Web Application Firewall）を選定する際には、付録3 WAF（Web Application Firewall）選定時の注意事項を参照すること。

## 第3章 運営中のECサイトにおいて検討・確認すべき事項



### 2. 確認・検討事項

#### (3) セキュリティ対策の不十分な箇所への追加対策の実施

セキュリティ対策の不十分な箇所については、外部委託の活用を含め、必要となる追加対策を個別に検討し、実装する。

- 前述の第二部／第2章／(3) 外部委託先におけるセキュリティ対策の実施状況の定期的確認に記載したとおり、外部委託を活用する場合、外部委託先でセキュリティ対策が確実に実施されるよう、外部委託先におけるセキュリティ対策の実施状況を、選定時に確認するとともに、運用時においても継続的に確認することが必要である。

# 付録

- 付録1 被害を受けたECサイトからの生の声一覧
  - 被害を受けた原因の傾向等について記載する。
  
- 付録2 自社構築サイト（中小企業）50社の脆弱性診断結果
  - 脆弱性診断の結果として、危険度「高」以上のもの、危険度「中」以上のもの、危険度「小」のみものの割合等について記載する。
  
- 付録3 WAF（Web Application Firewall）選定時の注意事項
  - 設定次第で、WAFが機能しない場合があることについて記載する。

## 参考資料

---

- クレジットカード・セキュリティガイドライン
- 安全なWebサイトの作り方
- Webシステム／Webアプリケーションセキュリティ要件書