ECサイト構築・運用
セキュリテイガイドライン

Information-technology
Promotion
Agency, Japan
IPA

目次

はじめに

1 経営者の皆様へ

本ガイドラインは、EC サイト※1 を構築、運営されている中小企業の皆様に、EC サイトのセキュリティ対策を実施することがいかに重要であるかをご認識いただくため、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項目や、実務担当者が具体的に実践すべきセキュリティ対策の内容を、パッケージやスクラッチ開発による自社構築サイトを中心に記載したものです。

なお、本ガイドラインは各種法令に基づく文書ではなく、EC サイトを構築し運営されている皆様全員が遵守すべき項目を、主に技術的観点からまとめたガイドラインとしています。

※1 EC サイトには Amazon、楽天市場等のショッピングモールを利用した形態から自社 URL をもち、パッケージ、スクラッチ開発、SaaS 型 EC プラットフォーム※2 等を利用して構築されているサイトまで様々な構築形態が有ります。

※2 ASP カートシステム、EC サイト構築サービス、EC サイト構築プラットフォーム等、様々な名前で呼ばれています。

セキュリティ対策を疎かにした多くの EC サイトがサイバー被害に遭っていることをご認識ください！

EC サイトにおけるセキュリティ対策を疎かにして、ひとたび事故や被害を発生させてしまうと、EC サイトの長期間の閉鎖に伴う売上高の大幅な減少や、原因調査や被害の補償等、事故対応費用の支出による甚大な経済的損失が発生します。

EC サイトの閉鎖期間における売上高の平均損失額：1 社あたり約 5,700 万円
事故対応費用の平均額　　：1 社あたり約 2,400 万円

注 1）EC サイトの閉鎖期間における売上高の平均損失額は、個人情報保護委員会が実施した「EC サイトへの不正アクセスに関する実態調査」[1]（以下、「個情委調査」という。）による、従業者数 500 名以下の 44 社を対象とした場合の集計結果

注 2）事故対応費用の平均額は、IPA が実施した「EC サイトのセキュリティ対策のための調査業

[1] 個人情報保護委員会が実施した「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

務」（以下、「IPA 調査」という。）による、最近被害を受けた 19 社を対象とした場合の集計結果

いずれの調査結果からも、EC サイトでの事故や被害が引き起こす経済的損失が非常に大きいことが分かります。

中小企業の EC サイト運営においては、これらの経済的負担が経営を圧迫だけでなく、失われた顧客の信用を取り戻すことも容易ではないため、死活問題に発展することをご認識ください。

自社の EC サイトがサイバー攻撃の対象にならないと考え、セキュリティ対策を疎かにして EC サイトを構築や運用することは、大変危険です！

EC サイトのサイバー被害の発生原因の多くが、最新版へのバージョンアップ等によるアップデートの未実施や設定の不備によるものです。サイバー攻撃は一般の人からは見えにくく危機意識を持ちにくいですが、サイバー攻撃者はセキュリティ対策が不十分な EC サイトを抜け目なく見つけ出します。自社の EC サイトが、遅かれ早かれ攻撃対象となることを意識する必要があります。

EC サイトを構築する際に集客や売上を考えることはもちろん必要ですが、セキュリティ対策を併せて考えることが必須である（対策しないと事故に遭う）という意識を持つことが重要です。（「家の鍵が壊れているけどこの辺りは田舎なので泥棒はいないし大丈夫」という甘い考えがありますが、EC サイトは地球の裏側からも距離に関係無くインターネット経由で狙われるため通用しません。）

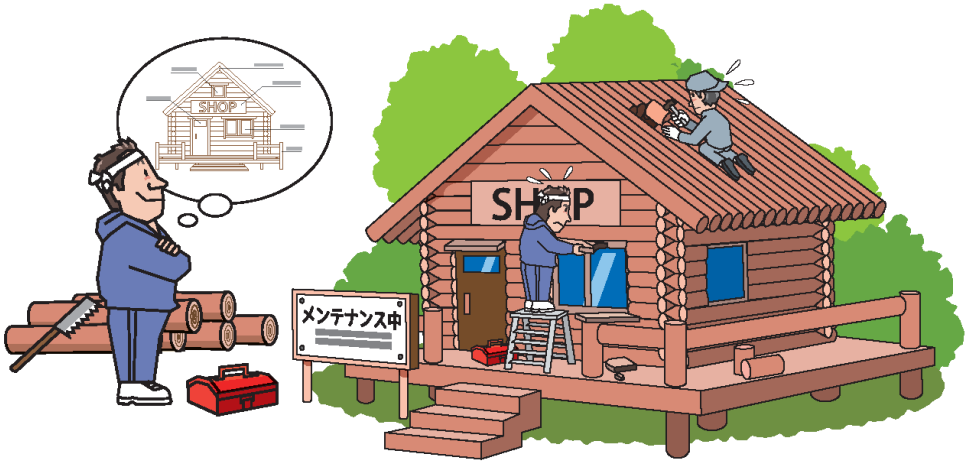
EC サイトは狙われている

セキュリティ対策と運用、保守コストを含めたトータルコストを考え、最適な EC サイトの形態の選定や外部委託先の活用を行うことが重要です！

これまでの EC サイトの売上増加や集客のみを優先する考え方から、セキュリティ事故を自分事（サイバー攻撃（事故・被害）は自分にも降りかかる災難である）として捉え、セキュリティを EC サイトの構築や運用の際の必須条件とするという考え方に変更してください。

EC サイト構築時点で必ずセキュリティ対策と運用、保守コストを見積り、運用や保守コストを含めたトータルコストを考えて、EC サイトの構築形態の選定や外部委託先の活用を適切に実施することが重要です。SaaS 型 EC プラットフォーム（以下、「SaaS 型サービス」という。）、ショッピングモールサービス（以下、「モール型サービス」という。）の利用や、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（コラム 2 を参照してください）の利用、セキュリティ対策における外部委託先の活用など、採りうる選択肢を幅広く検討いただければと思います。

自社構築サイト



2 本ガイドラインの対象

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や既に EC サイトを運営している経営者（SaaS 型サービスを利用して EC サイトを運営している経営者も含みます）、経営者から指示を受けた EC サイトを構築する責任者、運用担当者、関係者を想定読者としています。

また、外部委託先事業者も想定読者に含みます。

3 本ガイドラインの全体構成

本ガイドラインは、本編 2 部と付録により構成されます。付録には、本ガイドラインで用いている IPA 調査結果について、より詳しい内容が含まれています。

本ガイドラインの全体構成

構成		概要
本編	第 1 部　経営者編	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、自らの責任で実践しなければならない事項について説明しています。
	第 2 部　実践編	EC サイトにおけるセキュリティ対策を実践する責任者や担当者が、講じる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と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しています。
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 EC サイト運営事業者へのヒアリング調査結果の中から、特に参考になる事例を生の声として紹介しています。
	付録 2.　自社構築サイト（中小企業）50 社の脆弱性診断結果	中小企業の EC サイトにおけるセキュリティ対策状況を把握するために実施した脆弱性診断の結果を詳しく紹介しています。
	付録 3.　契約関係書類のひな形	外部委託先事業者と EC サイトの構築契約を締結する際に、外部委託先事業者に提示する仕様書の具体例を紹介しています。
	付録 4.　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一覧－	新規に構築する予定の EC サイトが、EC サイトの構築時におけるセキュリティ対策要件をどれぐらい実装しているか確認する際に用いるチェックリストを提供しています。
	付録 5.　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一覧－	運営中の EC サイトが、EC サイトの運用時におけるセキュリティ対策要件をどれぐらい実装しているか確認する際に用いるチェックリストを提供しています。

4 本ガイドラインの活用方法

「第 1 部　経営者編」は、EC サイトを新規に構築しようとしている経営者や、EC サイトを運営している経営者に、自社の EC サイトにおけるセキュリティ対策の必要性を認識するために読んでいただきたい内容です。

「第 2 部　実践編」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と担当者に、EC サイトの構築時や運用時において、必要となるセキュリティ対策を検討する上で、何を優先して対策していくか、自社の EC サイトの状況に見合った実践すべき対策の範囲や実現方法をどうすべきかを適切に決めるために読んでいただきたい内容です。

EC サイトのセキュリティ対策を実施するために、本ガイドラインをご一読いただき、対策が不十分な EC サイトは被害に遭う前にすみやかに対策を講じてください。

また、SaaS 型サービスを利用している場合も、自社の責任範囲となるセキュリティ対策がありますので、本ガイドラインをご一読いただき、対策が不十分な EC サイトは被害に遭う前にすみやかに確認と対策を講じてください。

本ガイドラインを利用するにあたり、EC サイトの運用形態や読者別に、参照していただきたい箇所と想定している対象者を表 1 に記載しておりますので、参考にしてください。「必読」は理解して頂きたい箇所、「推奨」は、ご一読いただきたい箇所を記載しております。

表 1　EC サイト運用形態毎のガイドライン参照箇所

＜＜新規に EC サイトを構築する場合＞＞			
■自社で構築・運営する場合			
	第一部	－	経営者：必読
	第二部	[1](1)(2) [2](1)(2) [3](1)(2)	責任者と担当者：必読 責任者と担当者：必読 責任者と担当者：必読
■外部委託先事業者に委託して構築・運営する場合			
	第一部	－	経営者：必読
	第二部	[1](1)(2) [2](1)(2) [3](1)(2)	責任者と担当者：必読 責任者と担当者：必読 責任者と担当者：必読
■外部サービス（SaaS 型/モール型サービス）を利用する場合			
	第一部	－	経営者：必読
	第二部	[1](1)(2) [2](4)	責任者と担当者：推奨 責任者と担当者：必読
＜＜EC サイトを運営中の場合＞＞			
■自社で運営している場合			
	第一部	－	経営者：必読
	第二部	[1](1)(2) [3](1)(2)	責任者と担当者：必読 責任者と担当者：必読
■外部委託先事業者に委託して運営している場合			
	第一部	－	経営者：必読
	第二部	[1](1)(2) [2](2)(3) [3](1)(2)	責任者と担当者：必読 責任者と担当者：必読 責任者と担当者：必読
■外部サービス（SaaS 型/モール型サービス）を利用している場合			
	第一部	－	経営者：必読
	第二部	[1](1)(2) [2](4)	責任者と担当者：推奨 責任者と担当者：必読

第１部　経営者編

経営者編では、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、実践しなければならない項目
とその背景について説明します。

1 EC サイトは常に攻撃対象として狙われている

昨今の EC サイトは、EC サイト構築パッケージや SaaS 型サービスを使って簡単に構築できるようになっています。また利用者の興味や関心を EC サイトに惹きつけ、購入を後押しするために、豊富な決済手段や、ポイントプログラム、商品レビューの書き込みや閲覧機能、FAQ 機能など、さまざまな機能が用意されています。

一方で、EC サイトの売上増加や集客にばかり気を配りすぎるあまり、大切なセキュリティ対策が疎かになっている事例が散見されています。こうした**セキュリティ対策が不十分な EC サイトは抜け目なく攻撃者に狙われ、被害に遭っており、経営者は経営責任を問われる結果となります**。

ここでは、EC サイトのセキュリティ対策の必要性について理解いただくために、次に挙げる 4 点を説明します。

- EC サイトにおけるサイバー被害の概要
- EC サイトが攻撃対象として狙われる事情
- 自社構築サイトの大半が本来すべきセキュリティ対策が未実施
- 52%の自社構築サイトがいつサイバー被害に遭ってもおかしくない状況

読んでいただいた後、サイバー被害が自社の EC サイトで起きないか、もしそうなったら自分達はどうなるのか、少しの時間、目を閉じて考えてください。経営者が安全に EC サイトを運営できるか、被害に遭わないですむかの第一歩です。

そのうえで、自社内で EC サイトのリスクとセキュリティ対策の必要性を、実務担当者を含めた部下と共有することが重要です。

(1) EC サイトに対するサイバー被害の概要

国内の EC サイトにおける個人情報とクレジットカード情報（個人情報、クレジットカード情報は、以下、「顧客情報」という。）の漏えい事故と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です。

日本クレジット協会の調べによると、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 億円に達しており、2016 年（142 億円）と比較すると 2 倍以上になっています。

また、2021 年の年間不正利用被害総額のうち、94%はクレジットカード番号盗用による被害額が占めており、EC サイトへのサイバー攻撃やフィッシング等によりサイバ

一攻撃者が入手したクレジットカード情報が不正利用されています。

経営者は、このような状況を認識し、EC サイトからの顧客情報の漏えいはもちろん、取引データ（仕入先情報を含む）等も含めて漏えい事故を起こさないようにすることが重要です。

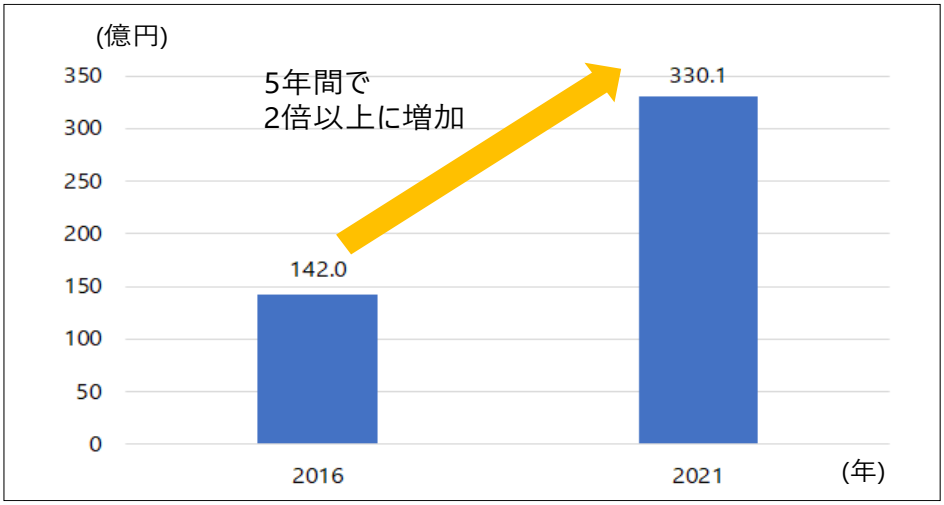


図 1　国内発行クレジットカードにおける年間不正利用被害総額の比較

参考情報 1　ひとたび事故や被害を発生させてしまうと、被害額はどれぐらいの金額になる？

不正アクセスを受けた EC サイト運営事業者の 40%以上で、**1,000 万円以上の損失金額が発生**しています。損失金額は、EC サイト上の取引規模や停止期間によりばらつきがあり、なかには、数億円の損失金額が発生した EC サイト運営事業者も見られます。（個情委調査）

最近被害を受けた EC サイト運営事業者 20 社を対象とした調査によると、**1 社あたりの顧客情報の平均漏えい件数は、約 3,800 件**です。また、そのうち 19 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 2,400 万円**にのぼります。（IPA 調査）

(2) EC サイトが攻撃対象として狙われる事情

サイバー攻撃者は抜け目ないです。セキュリティ対策が不十分な EC サイトを必ず見つけ出して、顧客情報等を盗み出し、その情報を様々なことに悪用します。EC サイトのサイバー被害が増えている背景としては、

①EC サイト構築パッケージ（プラグイン等の拡張機能を含む）や SaaS 型サービスを使って簡単に EC サイトを構築できるようになったこと

②個情委調査によると、サイバー被害を受けた EC サイトの 97%が自社構築サイト（EC サイト構築パッケージ、または、スクラッチで自社サイトを構築することを、

本ガイドラインでは自社構築サイトと定義します。SaaS 型サービスを利用されているサイトは自社構築に含みません）に集中していること

③自社構築サイトの中にはセキュリティ対策を考えていない、または、セキュリティ対策に十分な費用をかけていないサイトが多く、そのような EC サイトを狙った攻撃が増加していること

が挙げられます。

参考情報 2　**どのような特徴を持った EC サイトがサイバー被害に遭っている？**

不正アクセスを受け、サイバー被害が発生した EC サイト運営事業者の約 97%が、**自社構築サイト**です。（個情委調査）

最近被害を受けた EC サイト（20 サイト）の 75%が、**OSS（オープンソースソフトウェア）を主とする EC サイト構築パッケージや CMS の脆弱性を悪用されて被害が発生**しています。（IPA 調査）

※CMS（Contents Management System）は、Web サイト上で扱う画像やテキスト等のデジタルコンテンツに関する制作、編集、登録・公開等の作業を、管理者画面から簡単に行うことができるソフトウェアのことを指します。

(3) 自社構築サイトの大半は本来すべきセキュリティ対策が未実施

大半の中小企業の EC サイト運営事業者は、EC サイトのセキュリティ対策を行うことが必須である（対策しないと被害に遭う）という意識がなく、また継続的なセキュリティ対策（セキュリティ運用や保守）への経営資源の割り当ても不十分であるのが実情です。

個情委調査によると、不正アクセスを受け、被害に遭った EC サイト運営事業者のうち、外部委託先事業者に委託して EC サイトの運用や保守を実施していた事業者が 67%を占めますが、その 44%が、外部委託先との EC サイトの運用や保守にかかる契約書または仕様書の中にセキュリティ対策を記載していませんでした。

EC サイトへのセキュリティ対策を軽視している事業者が被害に遭っている状況を認識し、自社の EC サイトに対するセキュリティ対策状況を確認することが重要です。

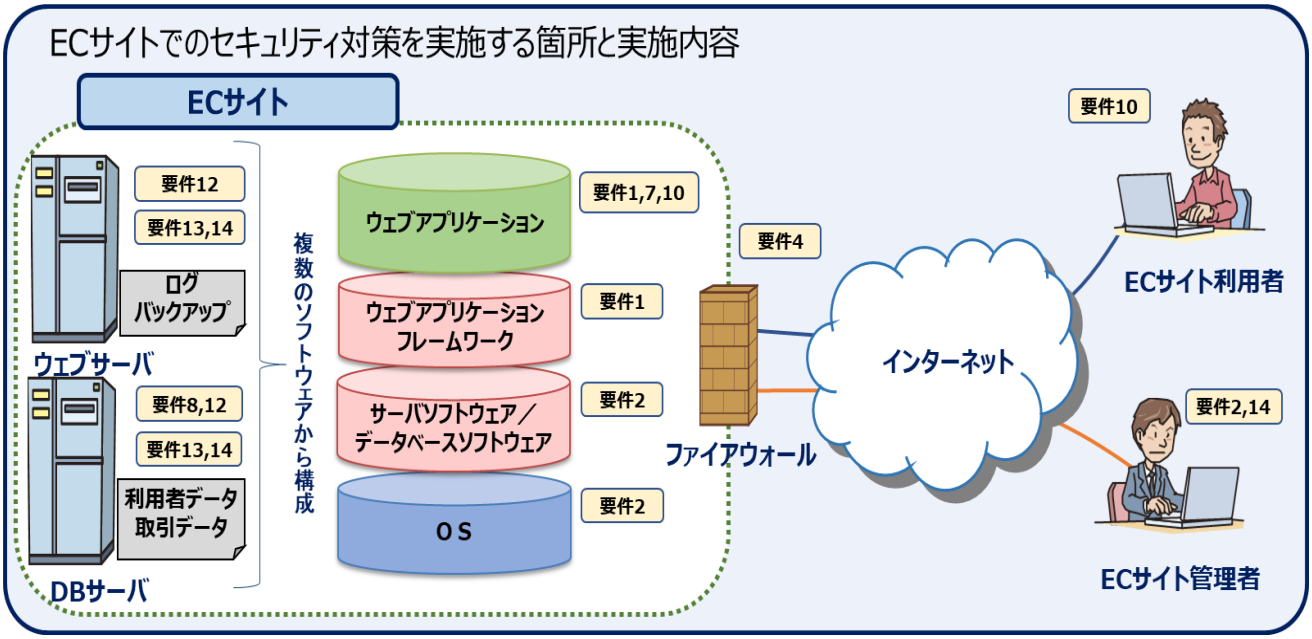
参考情報 3　**構築時や運用時を通したセキュリティ対策が実施できていない背景**

IPA 調査の結果、最近被害を受けた EC サイト（20 サイト）の 90%が、EC サイトの自社による保守または、外部委託先との EC サイトの運用や保守にかかる契約の締結を含めた運用時のセキュリティ対策を実施していないことが分かりました。なお、EC サイトへの継続的なセキュリティ対策が実施できない理由として、EC サイト運営事業者より、以下のような意見が挙げられました。（IPA 調査）

①EC 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いなかった（45%）

②外部委託先にセキュリティ対策を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（15%）
③事業全体の売上高に比較して、EC 事業による売上高の割合が低い（5%以下）ため、費用を掛けられなかった（15%）
④前任者が退職し、後任者における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であった（5%）

①～④に該当する EC サイトが被害に遭っています。被害を防ぐには、日頃からの対策が必要です。
また、①の意見は約半数から挙げられていることから、セキュリティ対策が必要であるという認識が普及していない現状が伺えます。



【要件 1】ウェブアプリケーションのセキュリティ対策	【要件 2】サーバ、管理端末のソフトウェアを最新化	【要件 4】管理画面、管理用ソフトウェアへのアクセス制限
【要件 7】利用者情報登録時等における不正ログイン対策	【要件 8】利用者の個人情報への安全管理措置	【要件 10】利用者のログイン時の二要素認証の導入
【要件 12】ログ、バックアップデータを保管	【要件 13】ログ、バックアップデータの保護対策	【要件 14】サーバ、管理端末のセキュリティ対策
【要件 3】【要件 5】【要件 6】【要件 9】【要件 11】その他のセキュリティ対策		

図 2　EC サイト（自社構築）の主なセキュリティ対策（構築時）の実施要件

(4) 52%の自社構築サイトはいつサイバー被害に遭ってもおかしくない状況

IPA では、中小企業の EC サイトにおけるセキュリティ対策状況を把握するため、50 社の EC サイトを対象として、2 種類の脆弱性診断（Web アプリケーション診断[2]、プラットフォーム診断[3]）を実施しました。各社で検出された脆弱性に関わる危険度[4]のうち、最高であったものを基準として集計した結果（1 つでも危険度「高」があれば、それを基準として、危険度「高」に該当する事業者としてカウントした結果）、Web アプリケーション診断において、危険度「高」が出ている事業者は、14 社（全体の 28%）、またプラットフォーム診断において、危険度「高」が出ている事業者は、21 社（全体の 42%）に上っています。さらに、9 社（全体の 18%）は、Web アプリケーション診断、プラットフォーム診断のいずれにおいても、危険度「高」が出ています。

このような重複分を考慮すると、50 社のうち、危険度「高」が出ている事業者は、26 社（全体の 52%）に上っており、いつサイバー被害に遭ってもおかしくない状況にあります。

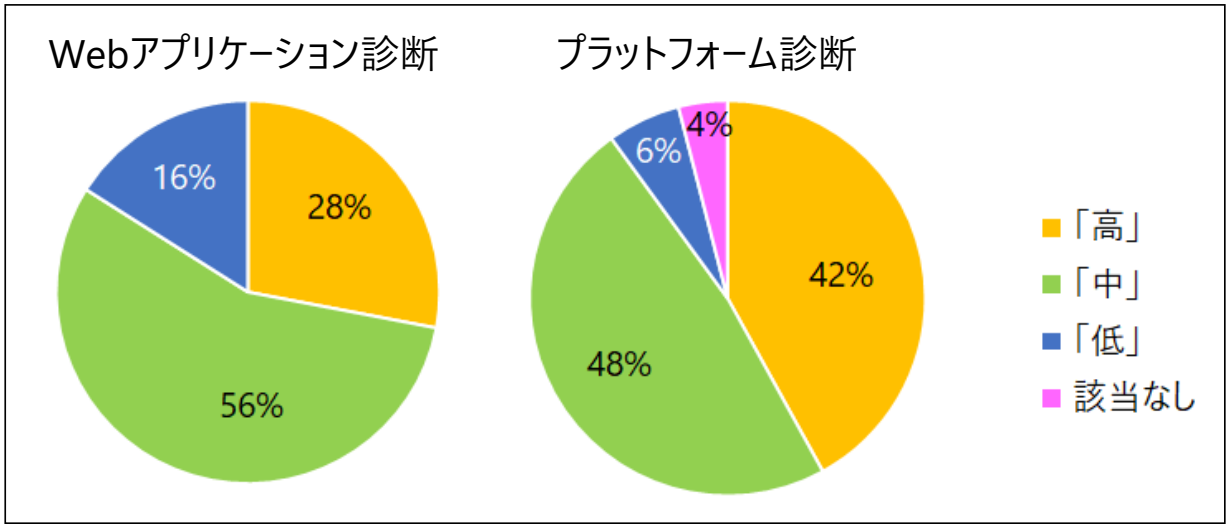


図 3　診断対象企業 50 社における危険度の最高位別にみた企業の割合

[2] Web サーバ上で動作するアプリケーションの脆弱性を診断するもの
[3] サーバやネットワーク機器等の OS やミドルウェアの脆弱性を診断するもの
[4] 直接被害に結びつく脆弱性を危険度「高」、複数の条件が揃った場合に被害に結びつく脆弱性を危険度「中」、現時点では被害に結びつかないが攻撃者に対し攻撃の手掛かりとなる情報を与えてしまう脆弱性を危険度「低」としています。

2 EC サイトのセキュリティ対策を疎かにして、セキュリティ事故・被害を発生させてしまうと、何が起きるか

顧客情報が外部に漏えいするセキュリティ事故を起こした場合、経営者の責任であることは言うまでもありません。経営者は、EC サイトの構築と運営に関して、「サイバーセキュリティが経営問題である」という認識を持つことが必要です。

ここでは、EC サイトにおけるセキュリティ対策を疎かにした代償は大きいことを、経営者に改めて認識していただくために、被害事例を参考に次に挙げる 3 点を説明します。

- EC サイトの運営事業者が受ける売上損失
- 事故対応費用にかかる大きな負担
- 66%の事業者が被害後、EC サイトを停止または SaaS 型/モール型に移行

経営者は、これらの被害事例を反面教師として、自社の EC サイトにおけるセキュリティ対策の必要性の認識を持ち、現在実施している対策の見直しや更なる対策強化に活かすことにより、EC サイトの構築と運営においても、経営者としての責任を積極的に果たしていくことが重要です。

セキュリティ事故による被害

(1) EC サイトの運営事業者が受ける売上損失

EC サイトにおけるセキュリティ対策を疎かにして、ひとたび事故や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だけでなく、売上高の回復には数年を要することになります。

被害にあった EC サイト 47 社を対象とした調査によると、1 社あたりの EC サイトの平均閉鎖期間は、8.6 か月間であり、長期間の閉鎖を余儀なくされています。(個情委調査)

また、EC サイトの閉鎖期間における売上高の損失額についてみると、従業員規模 300 名以下の 40 社を対象とした場合、1,000 万円以上の損失額が 26 社、3,000 万円以上の損失額が 9 社、1 億円以上の損失額が 4 社で発生しています。(個情委調査)

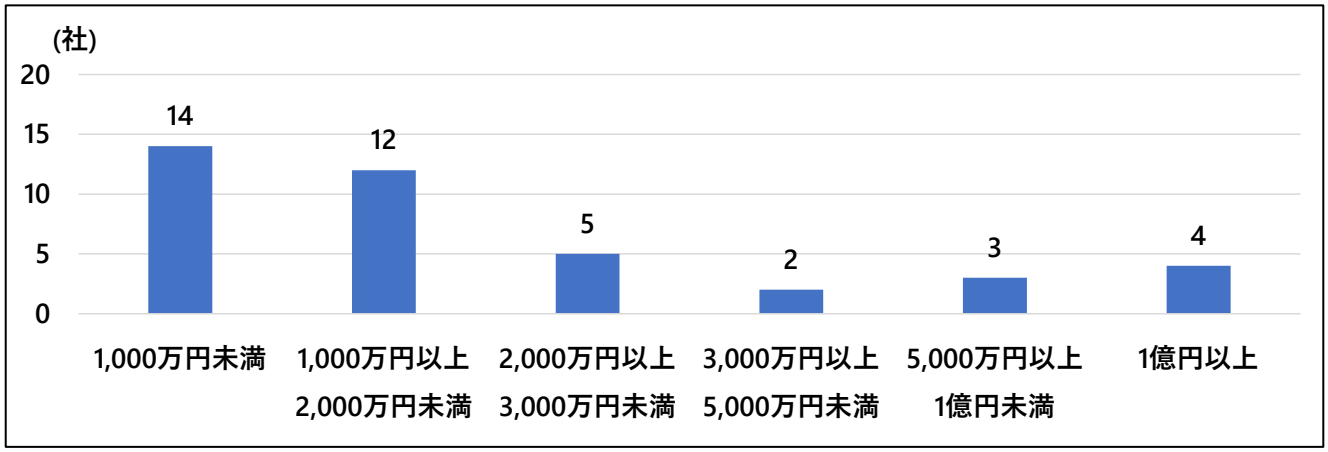


図 4　EC サイトの閉鎖期間における売上高の損失額の分布

ひとたび事故や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 サイトの閉鎖や事業の停止に追い込まれます。実際、不正アクセスを受けた EC サイトの運営事業者の 14%が EC サイトの再開を断念し、閉鎖が続いています。(個情委調査)

このような EC サイトの閉鎖や事業の停止は、特に中小企業で、EC サイトを運営する事業者にとっては死活問題に繋がることを十分認識する必要があります。

また、風評被害の影響で既に獲得していた顧客離れが進むと、事故や被害前の売上高に回復するまでに数年以上もの期間を必要とします。

被害を受けた EC サイトの運営事業者の中には、現在の EC サイト経由での売上高が、被害から 1 年半以上経ったにも関わらず、被害前の売上高の 50%以下に落ち込んでしまったところもあります。(IPA 調査)

事故や被害の影響は、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、事故対応費用の大きな負担や顧客からの信用失墜、ブランド毀損、風評被害に伴う離客など、多種多様です。EC サイトにおけるセキュリティ対策を疎かにした代償は大きいことを、経営者はご認識いただきたいと思います。

参考情報 4 **一度サイバー被害に遭うと顧客は戻らないことが多い？**

最近被害を受けた EC サイトの運営事業者においては、クレジットカード決済が使えなくなることにより、以下のような影響事例が見られた。（IPA 調査）

（事例 1）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するとともに、クレジットカード決済での利用者の 10%（利用者全体の 4～4.5%に相当）が離客してしまった

（事例 2）後払いや郵便振替に決済方法を変更し、手数料も自社の負担としたが、クレジットカード決済を利用できなければ商品を買わない顧客もいるため、売上高が減少してしまった

(2) 事故対応費用にかかる大きな負担

EC サイトの運営事業者が受ける経済的損失についてみた場合に、売上損失以外に影響が大きいのは事故対応費用です。事故対応費用として、フォレンジック調査やコールセンター設置にかかる費用、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、慰謝料といった費用の負担も重くのしかかります。

なかでも特に、賠償責任リスク（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）は、顧客情報の漏えい件数が増えれば増えるほど、大きくなるという傾向があります。

事故対応費用を支出した中小企業で、EC サイトを運営する事業者 19 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 万円となり、大きな負担になっています。顧客情報の漏えい件数により事故対応費用は大きく変動しますが、経営上大きな負担になる点について経営者は認識する必要があります。（IPA 調査）

参考情報 5 **事故対応費用って、何に、いくらかかる？**

A 社の場合（顧客情報の漏えい件数約 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
DM発送費用	25万円
その他費用	80万円
合計	600万円

B 社の場合（顧客情報の漏えい件数約 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
フォレンジック調査費用 コールセンター設置費用 その他費用	7,000万円
合計	9,800万円

※フォレンジック調査費用は、200 万円～600 万円が多く、費用は調査対象サーバ台数に依存します。（IPA 調査）

被害にあった EC サイトでは、以下の事故対応費用がかかっています。（個情委調査）

- クレジットカード再発行手数料（被害にあった EC サイトの 92%が負担をして、カード 1 枚当たり約 2000 円の回答が 6 割）
- その他費用として、セキュリティ強化費用、弁護士やコンサルティング費用

(3) 66%の事業者が被害後、EC サイトを停止または、SaaS 型/モール型サービスに移行

自社構築で EC サイトを運営していた事業者のほとんどが、被害後に EC サイトを再開するにあたって、自社構築では十分なセキュリティ対策の実施が予算面、管理要員面で不可能であると認識され、自社構築による EC サイトリニューアルを断念し、SaaS 型/モール型サービス等の別の形態の EC サイトに移行せざるを得なくなっています。

個情委調査によると、EC サイトを自社開発または外部委託先の活用により構築していた運営事業者の 52%が、被害後に SaaS 型/モール型サービスの利用に移行しています。

また一方で、被害を受けた EC サイト運営事業者の 14%が、EC サイトの運営停止に追い込まれています。EC サイトの運営停止がきっかけで、事業計画に大きな影響を与えてしまう事態も起こりうることを認識する必要があります。

上記の調査結果をまとめると、**被害企業の 66%(52%+14%)が、自社構築の形態での EC サイトセキュリティ対策はできないとあきらめ、SaaS 型/モール型サービス等への移行、または閉鎖されているという事実を重く受け止める必要があります。**逆に 34%の EC サイトは、「サービスに移行するとわが社にとって重要な独自性（カスタマイズ性）が失われるため、自社構築で追加予算をかけてでもセキュリティ対策を行う」と判断された経営者です。是非、被害に遭ってからではなく、経営者の皆様にはこの判断を被害に遭う前にしていただきたいと思います。

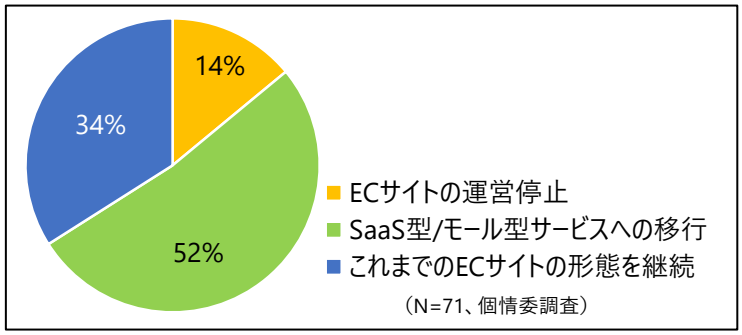


図 5　被害を受けた EC サイト運営事業者 66%が
EC サイトの運営を停止または SaaS 型/モール型サービスへ移行

参考情報 6　サイバー被害を受けた運営事業者は‥‥？

最近被害を受けた EC サイトの運営事業者（20 社）の多くが、顧客情報の漏えい事故を契機に、セキュリティ対策が必要条件であることを認識され、かつ、カスタマイズよりもセキュリティが重要であるという考えに至り、自社での対策の限界を把握された上で、50%が SaaS 型サービスの利用へ、15%がモール型サービスの利用へ移行しました。その一方で、残りの 35%は、深慮の上、カスタマイズ性の維持とセキュリティ対策の強化を選択されています。（IPA 調査）

是非被害を受ける前にセキュリティの重要性を認識される、脇のしまった経営者になっていただきたいと思います。

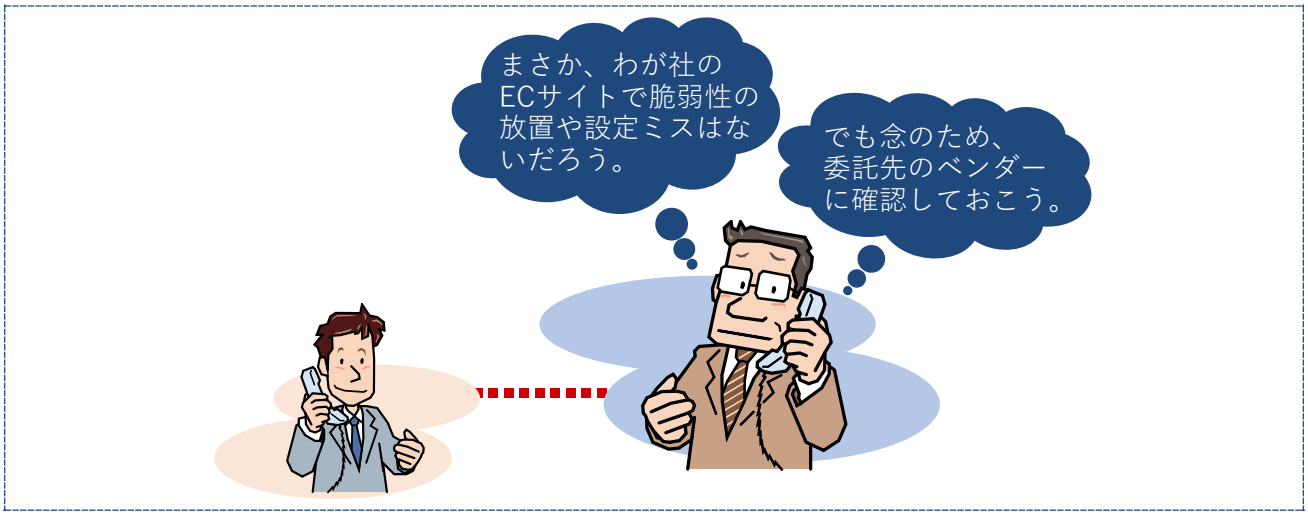
3 何が問題なのか

被害を受けたECサイトの運営事業者にヒアリングを行った結果、自社のECサイトがサイバー攻撃の対象になることはないと考え、セキュリティ対策を疎かにした状態で、EC サイトを構築や運用していたことが一番の大きな問題であると分かりました。（IPA 調査）

また、ECサイトのサイバー被害が発生した原因としては、ECサイトの脆弱性に対するアップデートの不十分が最も多く、次いでEC サイト構築パッケージやCMS 等の設定不備が多く挙げられています。（IPA 調査）

- EC サイト構築プログラムやCMS 等の脆弱性を放置していたこと、または最新版へのバージョンアップ等によるアップデートが十分に出来ていなかったこと（75%）
- 管理者画面へのログイン認証において、デフォルト設定の状態のままで運用していたこと（15%）
- 設定ミスによりWeb サーバの非公開ディレクトリが公開されていたこと(10%)

脆弱性対策や各種設定の確認といったセキュリティ対策の基本が疎かになっていた点が大きな問題であることを認識する必要があります。



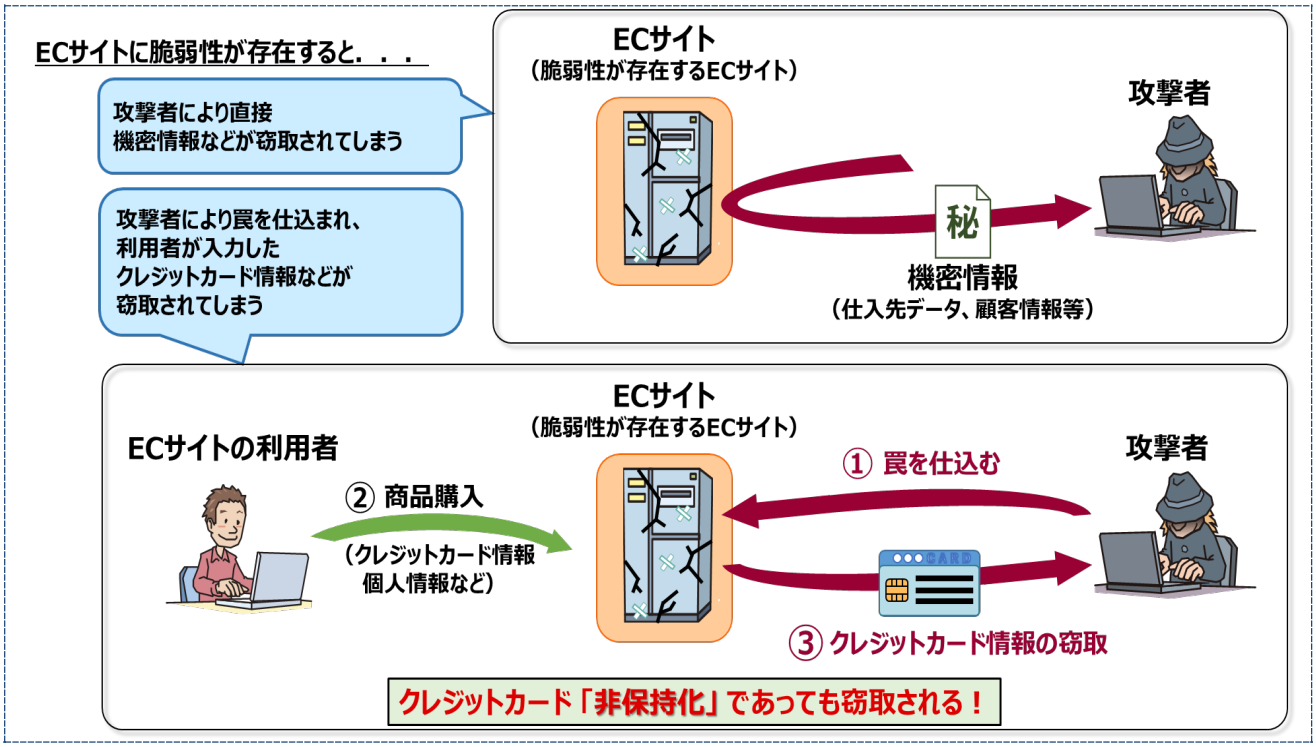
EC サイト構築プログラム等の脆弱性対策としては、修正プログラム（以下、「セキュリティパッチ」とする。）の適用や最新版へのバージョンアップ等によるアップデートが必要になります。

なお、脆弱性対策が実施しづらくなることを認識しないまま、機能面だけを考えてEC サイトのカスタマイズ（EC サイトの利用者の要望に応えるための新機能の開発や追加やシステム改修等）は行うべきではないことを認識する必要があります。

参考情報 7　EC サイトが受けるサイバー攻撃の手口にはどのようなものがある？

実際に被害を受けた EC サイトで見られたサイバー攻撃の手口としては、決済画面の改ざんを引き起こす脆弱性（37%）、SQL インジェクションの脆弱性（31%）といった、EC サイトの脆弱性の悪用が多くを占めています。その他では、EC サイトの管理者画面へのアクセス制限不備（15%）も原因となっています。（個情委調査）

また、最近は EC サイトの管理者画面へのアクセス制限不備に起因した決済画面への不正アクセスが多く報告されています。（IPA 調査）



参考情報 8　クレジットカード情報の非保持化対応の実施だけでは不十分です。EC サイトを改ざんされると、EC サイトからカード決済画面に移る手前でカード情報が盗まれます。

クレジットカード情報を保持しないようにしていても、クレジットカード情報は漏えいします。

通常 EC サイトの画面から入力されたクレジットカード情報は、決済代行会社（PSP※）が提供するシステム上で処理されるため、決済代行会社の責任範囲になります。しかし、EC サイトが改ざんされ、偽のカード決済画面が挿入されたりすると、決済代行会社が提供するシステムと別の画面で、クレジットカード情報の漏えいが発生し、EC サイト運営事業者の責任範囲になります。

このように、クレジットカード情報の非保持化を行ってもクレジットカード情報の漏えいは起こります。実際この手の被害が最近増えています。

したがって、クレジットカード情報の非保持化だけでなく、EC サイトそのものが改ざんされない対策が必須となります。

※PSP は、Payment Service Provider の略称です。

4 経営者は何をし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、EC サイトを構築し、運営する経営者が実行すべき項目について説明します。

IPA「中小企業の情報セキュリティ対策ガイドライン」にも記載されている 7 つの重要項目について、EC サイトに対しても以下のように実行することが、EC サイトのセキュリティ対策の基本になります。

まず、項目 1～4 で EC サイトはセキュリティ対策をしないとセキュリティ被害に遭うということを認識した上で、必要な予算と人材を確保し、EC サイトのセキュリティ対策を指示してください。また、指示した対策を対応方針に従って評価し、適切に見直しをするよう指示を出すことも重要です。

次に、項目 5～7 において、万が一、EC サイトの事故や被害が発生した場合に備えて、事前に対応方針・ルールの策定や外部委託先との連携等の緊急時の対応体制を整備することも必須です。また、サイト運用を外部委託先に委託している場合は契約等において、セキュリティ対策が盛り込まれているかどうか、チェックを実施してください。EC サイトに関する新しい攻撃手法や脅威がないか、最新のセキュリティ動向のチェックを実施してください。

項目 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
項目 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
項目 3	ECサイトを構築および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
項目 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
項目 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
項目 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
項目 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

上記の項目 1～7 を基に、本ガイドラインでは、経営者が認識し、実務担当者に実施させるべき取組を整理しました。EC サイトを新規に構築する場合、EC サイトを運営中の場合における取組を整理し、第 2 部にその取組の詳細を記載しています。実務担当者に以下の取組を必ず実施するよう指示をお願いします。

(1) 新規に EC サイトを構築する場合において実行すべき取組

EC サイトを新規に構築する場合においては、セキュリティ対策をないがしろにしてまで、EC サイトの売上増加や集客を優先するという考え方を変えることが必要です。EC サイトのセキュリティ対策は、顧客に EC サイトを安心して利用してもらうためだけでなく、EC サイトの事故や被害による既存顧客の信用失墜や離客を防ぐためにも必要になります。具体的には以下の取組が重要となります。

取組 1	EC サイトの開設計画時にセキュリティ対策および運用、保守コストを必ず見積り、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、講じるべきセキュリティ対策要件を把握し、必ずセキュリティ対策と運用、保守コスト（EC サイトの運用を継続する期間の費用）を見積ってください。

そのうえで構築時の費用も含めたトータルコストを算出し、EC サイトのセキュリティ対策の継続的な運用を考慮した上で、自社で構築することが本当に適当か、SaaS 型サービスやモール型サービスの活用を含めて、EC サイトの構築形態を選定してください。

取組 2	自社に人材がおらず、外部委託先の活用により EC サイトを自社構築する場合は、セキュリティ構築および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、脆弱性診断を必ず実施させてください。外部委託先の選定時において、構築後のセキュリティ運用、保守も併せて契約することが可能な委託先を選定してください。

EC サイトのセキュリティ運用、保守契約を外部委託先と必ず結んでください。運用、保守契約には、必要な動作環境（OS、ミドルウェア、プラグイン等）の最新版へのバージョンアップによる随時アップデート、攻撃のモニタリング等を含めてください。（第 2 部を参照ください。）

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確認が必要です。

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されていることを確認してください。

（注）ほとんどの中小企業の EC サイト運営事業者は自社 EC サイトの構築を外部委託先事業者に委託しており、上記「取組」は外部委託先の活用を想定した記述となっています。自社内で構築する場合は同等の対策を自社内で確実に実施してください。

(2) EC サイトを運営中の場合において実行すべき取組

EC サイトを運営中の場合においては、いつサイバー被害に遭ってもおかしくない状況を回避と改善することが必要です。具体的には以下の取組が重要となります。

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。

IPA「安全なウェブサイトの作り方」や、本ガイドの付録にある EC サイトの構築時や運用時における講じる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ってください。

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、応急処置を行う。

セキュリティ対策が不十分であることが分かり、対策実施には時間がかかる場合、その間の攻撃リスクを減らすため、応急処置（例：WAF（Web Application Firewall）実装、サイバー保険への加入）を実施してください。

なお、サイバー保険については、さまざまな種類・プランがあり、万が一の際の補償内容・金額やカバーされる脅威の範囲はもとより、事業性（売上高等）やセキュリティ対策状況、過去のインシデント被害経験等により保険料が決まるため、詳細は保険会社にご確認ください。

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、長期的（EC サイトの運用を継続する期間）なトータルコストを評価し、SaaS 型サービスやモール型サービスの利用も検討してください。

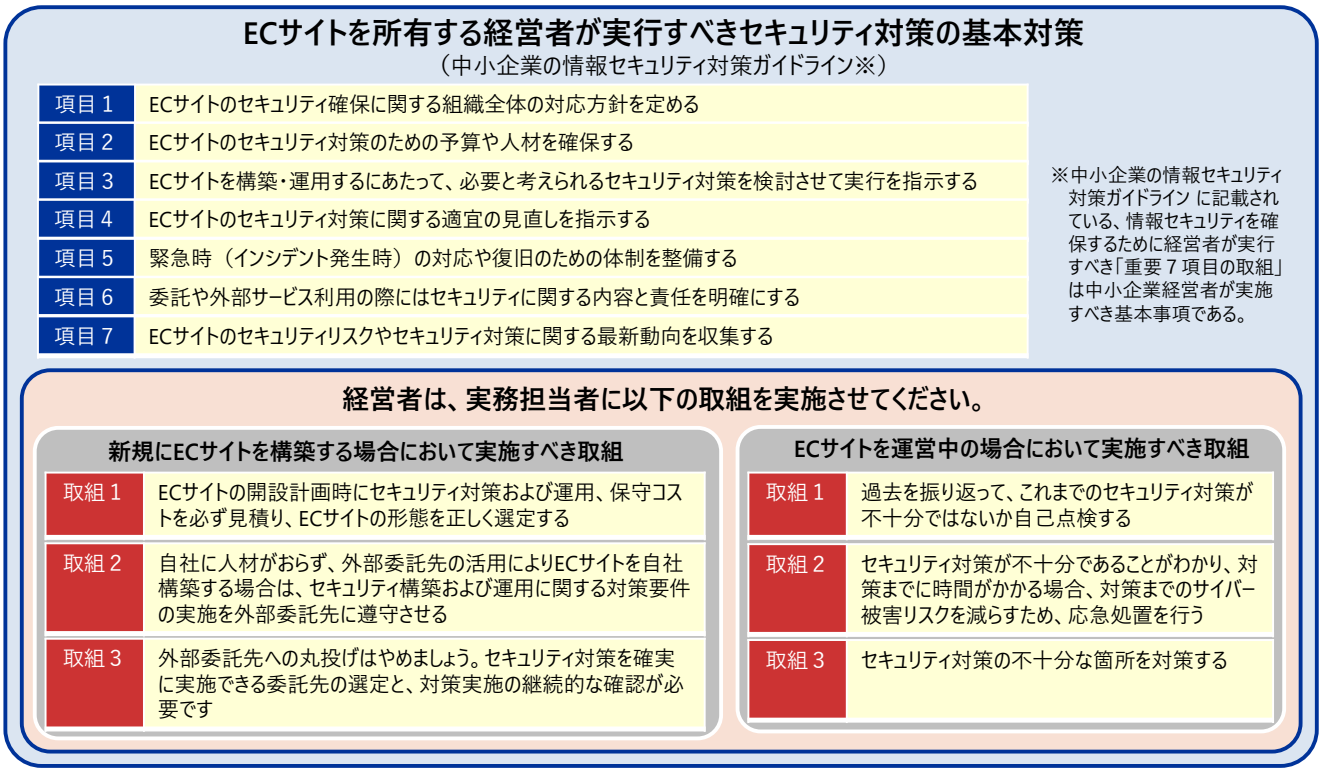


図 6　EC サイトのセキュリティ対策に関して
経営者が認識し実践しなければならない項目・取組の全体像

第２部　実践編

実践編では、EC サイトにおける**セキュリティ対策を実践する責任者及び担当者**が、講じる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します。

1 EC サイトの構築時及び運用時における講じるべきセキュリティ対策要件

セキュリティを考慮せずに構築・運用している EC サイトは、いつサイバー被害に遭ってもおかしくない状況に陥り、その運営事業者は、いつか必ずサイバー被害に遭い取り返しがつかない深刻なダメージを受けることになります（第 1 部を参考にしてください）。そうならないためには、EC サイトの構築時、運用時の各段階で EC サイトの安全性を高めることが必要です。

ここでは、自社の EC サイトの安全性を高めるために、講じるべきセキュリティ対策要件について説明します。

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

EC サイトにおけるセキュリティ対策を実践する責任者及び担当者は、これらのセキュリティ対策要件を、EC サイトを新規に構築する際の設計書や調達を行う際の要求仕様書に盛り込んだり、運営中の EC サイトにおけるセキュリティレベルを自己点検する際の評価項目として活用しリスクの高い問題に関して対策を行ったりすることにより、EC サイトのセキュリティ確保に向けた取組を推進していく責任を積極的に果たしていくことが重要です。また、自組織内で上記の対応が難しく、外部委託先事業者へ委託する際も、セキュリティ対策要件を活用し、セキュリティ確保に向けた対策を実施することが重要です。

(1) EC サイトの構築時におけるセキュリティ対策要件

EC サイトの構築時におけるセキュリティ対策要件は、以下に示す 14 の要件により構成されます。また、要件ごとに、求められるセキュリティの水準に応じて、「必須」、「必要」、「推奨」を定め、それぞれ表中の区分に表記しています。

「必須」は、EC サイト運営事業者が EC サイトのセキュリティを確保する上で早急かつ確実な対策実施が求められるものであり、実装が必須として求められる内容と定義しています。

また、「必要」は、事業の重要度、対策費用、対策までの期間、対策を実施しないことによる影響度等または、他の代替策を実施する等を考慮して導入時期を検討した上で実装が求められる内容と定義しています。

さらに、「推奨」は、EC サイト運営事業者がサイバー被害を受けるリスクの低減、

被害範囲の拡大防止、EC サイトを復旧する場合において、対策実施が求められるものであり、事業の重要度、影響度等を考慮した上で、EC サイト運営事業者が各自の責任において、その実装を検討すべき内容と定義しています。

表 2　EC サイトの構築時におけるセキュリティ対策要件一覧

No	セキュリティ対策要件（構築時）	区分
要件 1	「安全なウェブサイトの作り方」及び「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。	必須
要件 2	サーバ及び管理端末等で利用しているソフトウェアをセキュリティパッチ等により最新の状態にする。	必須
要件 3	EC サイトの公開前に脆弱性診断を行い、見つかった脆弱性を対策する。	必須
要件 4	管理者画面や管理用ソフトウェアへ接続する端末を制限する。	必須
要件 5	管理者画面や管理用ソフトウェアへ接続する端末のセキュリティ対策を実施する。	必須
要件 6	クレジット取引セキュリティ対策協議会が作成する「クレジットカード・セキュリティガイドライン」を遵守する。	必須
要件 7	サイト利用者情報の登録時及びパスワード入力時における、不正ログイン対策を実施する。	必須
要件 8	サイト利用者の個人情報に対して安全管理措置を講じる。	必須
要件 9	ドメイン名の正当性証明と TLS の利用を行う。	必須
要件 10	サイト利用者のログイン時における二要素認証を導入する。	必要
要件 11	サイト利用者のパスワードの初期化及び変更といった重要な処理を行う際、サイト利用者へ通知する機能を導入する。	必要
要件 12	Web サーバや Web アプリケーション等のログや、取引データ等のバックアップデータを保管する。	必要
要件 13	保管するログやバックアップデータを保護する。	推奨
要件 14	サーバ及び管理端末において、セキュリティ対策を実施する。	推奨

要件 1	「安全なウェブサイトの作り方」及び「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。

「安全なウェブサイトの作り方」及び「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、「脆弱性関連情報の届出制度」で届出の多かったものや攻撃による影響度が大きい脆弱性である、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ます。

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ますので、本書を参考にして EC サイトを構築してください。

なお、EC サイトの構築を委託する場合は、外部委託先事業者に、本書を参考にして構築することを依頼してください。

要件 2	サーバ及び管理端末等で利用しているソフトウェアをセキュリティパッチ等により最新の状態にする。

EC サイトを構築する場合、次のように利用しているソフトウェアへの脆弱性対策を実施することが重要です。

- 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してください。
- EC サイトを構成するソフトウェア（サーバと管理端末等の OS、ミドルウェアとライブラリ等、または、Web アプリケーションなど）を確認のうえ一覧にまとめ、それぞれのソフトウェアに関する脆弱性情報などセキュリティに関連する情報を収集して管理し、それらの情報の内容を把握してください。
- EC サイトの構築時に利用しているサーバ及び管理端末等の OS、ミドルウェア及びライブラリ等、または、Web アプリケーションや OSS などのソフトウェアについては、その時点の最新バージョンを使用してください。
- 利用しているソフトウェア等について、脆弱性情報を収集し、脆弱性の危険度が「高」の脆弱性については迅速に、危険度「中」は公開までにセキュリティパッチの適用や最新版へのバージョンアップによるアップデートを実施してください。アップデート実施後は、アップデートによりシステムへの影響が無いことを確認（動作検証）

してください。それ以外の脆弱性については、セキュリティパッチの適用や最新版へのバージョンアップを行うかどうかを、脆弱性によるシステムへの影響等を考慮して判断してください。

要件 3　EC サイトの公開前に脆弱性診断を行い、見つかった脆弱性を対策する。

EC サイトを新規に構築した際は、EC サイトを公開するまでに脆弱性対策を実施する期間を確保して、次のような第三者による EC サイトへの脆弱性診断を実施して、EC サイトに脆弱性が無いかを確認し、発見された危険度「高」、「中」の脆弱性への対策を行ったうえで公開してください。

- 脆弱性診断は、原則、第三者（外部委託先事業者、自社以外の第三者）による脆弱性診断を実施し、実施する脆弱性診断は、プラットフォーム診断、Web アプリケーション診断の 2 種類を実施してください。
- Web アプリケーション診断の実施範囲は、最低でも以下の画面について脆弱性診断を実施してください。
  ログイン画面、サイト利用者情報登録/変更画面、商品検索画面、注文・決済画面等
- 脆弱性診断を第三者に依頼する場合は、「情報セキュリティサービス基準適合サービスリスト（以下に URL を記載）」にある、「脆弱性診断サービス」に記載されている事業者を選定することを推奨しています。
  （https://www.ipa.go.jp/files/000067318.pdf）
  なお、自社等での脆弱性診断を実施する場合は、「コラム 3」における「脆弱性診断の実施者」の記載を参考にしてください。
- 脆弱性診断の診断結果として、実害に至る攻撃難易度を考慮した危険度は、一般的に「高」、「中」、「低」の 3 段階で分類されており、危険度「高」、「中」については、対策を行ったうえで EC サイトを公開してください。

要件 4　管理者画面や管理用ソフトウェアへ接続する端末を制限する。

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えいすると、サイト利用者の顧客情報や、注文・取引データ等が大量に漏えいすることに繋がるおそれがあるため、次のように厳重に管理することが重要です。

- 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・パスワードが不正に取得された場合に備えて、アクセスできる端末を制限するための IP アドレス接続制限や、アクセスできる利用者を制限するために、二要素認証（ID とパスワードによ

る認証後に SMS（ショートメッセージサービス）等での認証を行う方法）を導入してください。

要件 5　管理者画面や管理用ソフトウェアへ接続する端末のセキュリティ対策を実施する。

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マルウェアに感染すると、端末内部及び、当該端末がアクセス可能なサーバ等に保管しているサイト利用者の顧客情報や、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、アクセスする端末に対して、マルウェア対策ソフトウェアを導入し、リアルタイム検知の実施及び、定義ファイルの更新、端末のフルスキャン等の定期的（1 回/日を推奨）な実施や、USB メモリ等外部記憶媒体の利用制限を通じて、マルウェア感染防止対策を行うことが重要です。

要件 6　クレジット取引セキュリティ対策協議会が作成する「クレジットカード・セキュリティガイドライン」を遵守する。

クレジットカード決済を提供する場合には、割賦販売法におけるセキュリティ要求事項を反映した、クレジット取引セキュリティ対策協議会が作成する「クレジットカード・セキュリティガイドライン」（カード情報の非保持化、カード決済の EMV 3D セキュアの導入等）を遵守するとともに、契約するクレジットカード会社及び決済代行会社（PSP）とコミュニケーションを取り、常に最新のセキュリティ対策の実施を検討してください。

要件 7　サイト利用者情報の登録時及びパスワード入力時における、不正ログイン対策を実施する。

サイト利用者のパスワードが攻撃者に漏えいすると、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、次のような不正ログイン対策を実施することが重要です。

- サイト利用者がパスワードを登録する際に 10 文字以上、英大文字と小文字、数字、記号を組み合わせて、推測困難なパスワードを登録するようにしてください。また、推測されやすいパスワードは登録できないようにすることが重要です。
- ログイン用の ID とパスワードのすべてのパターンを機械的に繰り返し入力し、EC 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（10 回以下を推奨）を超えた場合はアカウント

をロックするようにしてください。

要件 8	サイト利用者の個人情報に対して安全管理措置を講じる。

個人情報保護法第二十三条（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（個人データの取扱規程の整備、個人データを保存するシステム、機器及び電子媒体等の盗難、漏えい等の防止、システム、機器へのアクセス制御、不正アクセス防止等）を講じることが重要です。

要件 9	ドメイン名の正当性証明と TLS の利用を行う。

EC サイト利用者が 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（正規のサイトであること）を確認できるようにするためには、証明書等を導入し正当性証明を行うこと、及び TLS（Transport Layer Security）の利用により通信を暗号化することが重要です。

要件 10	サイト利用者のログイン時における二要素認証を導入する。

なりすましなどによる不正ログインが行われる可能性が高い（ある）と判断した場合には、ID とパスワードを用いたサイト利用者の認証に加えて、安全性を高められる二要素認証（ID とパスワードによる認証後に SMS 等での認証を行う方法）を導入することが重要です。

要件 11	サイト利用者のパスワードの初期化及び変更といった重要な処理を行う際、サイト利用者へ通知する機能を導入する。

正規サイト等を装ったフィッシングサイトや、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、サイト利用者が気づかないうちに ID とパスワードを盗まれることがあります。そのため、なりすまされて登録情報を変更されたことにサイト利用者が気付くことができるようにするために、EC サイト利用者のメールアドレスの登録及び変更、パスワードの初期化及び変更、アカウントの登録及び削除、決済処理時といった重要な処理を実行した際に、メールや SMS 等を用いて、サイト利用者への通知を

行うことが重要です。

要件 12	Web サーバや Web アプリケーション等のログや、取引データ等のバックアップデータを保管する。

顧客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にフォレンジック調査会社に依頼します。フォレンジック調査で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（該当サーバ以外の外部ストレージサービスや、自社管理のサーバへの保管等）を過去 1 年間分保管しておくことが重要です。

フォレンジック調査の依頼先は、「情報セキュリティサービス基準適合サービスリスト」にある、「デジタルフォレンジックサービス」に記載されている事業者も参考にしてください（https://www.ipa.go.jp/files/000067319.pdf）。

また、レンタルサーバ事業者を利用する場合は、Web サーバのアクセスログ等の保管及び提供が行われることを確認することが重要です。

要件 13	保管するログやバックアップデータを保護する。

Web サーバのログ及び Web アプリケーションのログ、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、保管ログ及びデータ等への不正アクセスがあれば、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ります。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す。

要件 14	サーバ及び管理端末において、セキュリティ対策を実施する。

サーバ及び管理端末自体がマルウェアに感染すると、サーバや管理端末内部に保管しているサイト利用者の顧客情報や、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、マルウェア対策ソフトウェアを導入し、リアルタイム検知の実施及び、定義ファイルの更新、ファイル・メモリのスキャン等の定期的（1 回/日を推奨）な実施や、USB メモリ等外部記憶媒体の利用制限を通じて、マルウェア感染防止対策を行うことが重要です。

コラム１

（ご紹介）Web サーバにおける予防的対策

Web サーバへの設定で、実施しておくと良い設定をご紹介します。クロスサイト・スクリプティングや、クリックジャッキングという脆弱性により、悪意のあるスクリプトの読み込みや実行されることを制限する効果があるため、是非、Web サーバへ設定することをご検討してください。

【Content Security Policy（CSP）】

本設定することにより、ブラウザ側で影響を軽減することが可能となり、クロスサイト・スクリプティング攻撃、クリックジャッキング攻撃を軽減することができます。

レスポンスヘッダに下記の CSP ヘッダが出力されるよう設定してください。

設定例）Content-Security-Policy: script-src 'self' example.com;

【X-Frame-Options】

本設定をすることにより、ブラウザ側で影響を軽減することが可能となり、クリックジャッキング攻撃を軽減することができます。

レスポンスヘッダに下記の X-Frame-Options ヘッダが出力されるよう設定してください。

設定例）X-Frame-Options: DENY、X-Frame-Options: SAMEORIGIN

なお、X-Frame-Options ヘッダフィールドは、上記の Content Security Policy（CSP）のバージョン 1.1 の Frame-Options ディレクティブに置き換えることができます。そのため、現在、X-Frame-Options ヘッダの利用は推奨されておりません。Content Security Policy（CSP）をサポートしていないブラウザ（Internet Explorer11 以前のバージョン等）を利用している利用者への対応が必要な場合のみ、対策を実施してください。

【X-Content-Type-Option】

ブラウザ側で意図しないファイルを読み込む等の影響を軽減することが可能となり、クロスサイト・スクリプティング攻撃を軽減することができます。

レスポンスヘッダに下記の X-Content-Type-Option ヘッダが出力されるよう設定してください。

設定例）X-Content-Type-Options: nosniff

上記設定をすると、ウェブアプリケーションの動作に影響を与える可能性もありますので、設定をする際は、検証環境等で、ウェブアプリケーションに影響が無いかを十分に確認をしてから設定をするようにしてください。

(2) EC サイトの運用時におけるセキュリティ対策要件

EC サイトの運用時におけるセキュリティ対策要件は、以下に示す 7 つの要件により構成されます。なお、「必須」、「必要」、「推奨」という区分や定義については、(1)で前述したものと同じものです。

表 3　EC サイトの運用時におけるセキュリティ対策要件一覧

No	セキュリティ対策要件（運用時）	区分
要件 1	サーバ及び管理端末等で利用しているソフトウェアをセキュリティパッチ等により最新の状態にする。	必須
要件 2	EC サイトへの脆弱性診断を定期的及びカスタマイズを行った際に行い、見つかった脆弱性を対策する。	必須
要件 3	Web サイトのアプリケーションやコンテンツ、設定等の重要なファイルの定期的な差分チェックや、Web サイト改ざん検知ツールによる監視を行う。	必須
要件 4	システムの定期的なバックアップの取得及びアクセスログの定期的な確認を行い不正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。	必要
要件 5	重要な情報はバックアップを取得する。	必要
要件 6	WAF を導入する。	推奨
要件 7	サイバー保険に加入する。	推奨

要件 1	サーバ及び管理端末等で利用しているソフトウェアをセキュリティパッチ等により最新の状態にする。

ソフトウェアを安全な状態で利用するためには、その前提として、脆弱性情報に関する常日頃の情報収集が大切です。既に攻撃方法が見つかっていたり、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最新版へのバージョンアップによるアップデートを迅速に行うことが重要です。

それ以外の脆弱性に関しては、セキュリティパッチの適用や最新版へのバージョンアップを行うかどうかを、脆弱性によるシステムへの影響等を考慮して判断してください。

- EC サイトの構築時に利用している Web サーバ等の OS・ミドルウェア、プラグイン及びライブラリや、Web アプリケーションや OSS のソフトウェアについては、運用時点の最新版を使用してください。
- 利用しているソフトウェア等については、EC サイト運営事業者や外部委託先において最新の脆弱性情報を収集することが大切です。セキュリティ情報サイトでの定期的な情報収集をするとともに、ソフトウェアを提供している企業から脆弱性に関する情報収集方法が用意されている場合は必ず登録するようにしてください。
- 利用しているソフトウェア等で脆弱性が発見された場合、脆弱性情報を収集し、脆弱性の危険度が「高」の脆弱性については迅速に、危険度「中」は、3 ヶ月程度を目途にセキュリティパッチの適用や最新版へのバージョンアップによるアップデートを実施してください。アップデート実施後は、アップデートによりシステムへの影響が無いことを確認（動作検証）してください。

要件 2	EC サイトの脆弱性診断を定期的及びカスタマイズを行った際に行い、見つかった脆弱性を対策する。

EC サイトを構築後、新たな脆弱性が発見される・新たな脆弱性を作り込む可能性があるため、定期的及びカスタマイズを行った際に脆弱性診断を実施することが重要です。

- 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 Web アプリケーション診断を実施することが重要です。なお、診断箇所は、最低でも新機能の開発や追加やシステム改修等を行った箇所を対象とした診断を実施してください。
- 上記のような新機能の開発・追加やシステム改修等のカスタマイズ等を行っていない場合でも、OS やミドルウェア等の脆弱性は継続的に発見されているため、四半期に 1 回の頻度でプラットフォーム診断を実施することが重要です。
- 脆弱性診断の診断結果として、実害に至る攻撃難易度を考慮した危険度は、一般的に「高」、「中」、「低」の 3 段階で分類されており、危険度「高」の脆弱性については、迅速に対策を行うことを推奨しています。また、危険度「中」は、3 ヶ月程度を目途に対策を行うことを推奨しています。

要件 3	Web サイトのアプリケーションやコンテンツ、設定等の重要なファイルの定期的な差分チェックや、Web サイト改ざん検知ツールによる監視を行う。

不正アクセスやマルウェア感染により、Web サーバ内部に保管しているサイト利用者の顧客情報や、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 サーバの公

開ディレクトリ配下等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）や、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す。

要件 4	システムの定期的なバックアップの取得及びアクセスログの定期的な確認を行い不正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。

不正アクセスやマルウェア感染により、システムを改ざん、破壊された場合、EC サイトでの事業の継続が出来なくなる可能性があるため、システムのバックアップを１回/月取得することが重要です。また、EC サイトへの不審なログインの試行が増えたり、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不正アクセスの予兆が発生している場合もあります。このため、Web サーバのアクセスログを定期的に確認し、確認した結果、不正なアクセス（特定の IP アドレスからの大量のアクセス等）があれば、ファイアウォール等のネットワーク機器の設定でアクセスの制限等の対策を実施することが重要です。

Web サーバのアクセスログの定期的な確認は、IPA が提供する「ウェブサイトの攻撃兆候検出ツール iLogScanner」を利用して確認可能です。

※iLogScanner は、以下のウェブサイトから入手することができます。

https://www.ipa.go.jp/security/vuln/iLogScanner/index.html

要件 5	重要な情報はバックアップを取得する。

サイト利用者の顧客情報や仕入先情報、売上情報などの重要な情報がランサムウェアによって暗号化されると、EC サイトでの事業の継続が出来なくなる可能性があるため、重要な情報は 1 回/日にバックアップを取得（ネットワークに接続されていないオフライン環境へ保管）することが重要です。

要件 6	WAF を導入する。

既に見つかっている脆弱性に対して対応するまでに期間が必要な場合や、必要となるセキュリティ対策を実装するまでに期間が必要な場合が想定されます。対策をするまでの期間内にサイバー攻撃を受けることがないよう、応急処置として、WAF を導入することを推奨しています。（「コラム５：（ご紹介）WAF（Web Application Firewall）の活用方法」も参考にしてください。）

要件 7　サイバー保険に加入する。

万が一、EC サイトまたは、自社システム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を推奨しています。

サイバー保険については、IPA 調査でも顧客情報の漏えい事故を発生させてしまった EC サイトの多くが、被害後に加入していますが、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、被害が発生していない場合でも被害発生に備えて加入することを推奨しています。

コラム 2

（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

セキュリティ対策について、自社または構築事業者による対応で賄えない部分を補う際に採りうる選択肢として、「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」の活用を検討してください。著名な EC-CUBE、Welcart 等のソフトウェアを提供する事業者から提供されている場合があります。

【保守運用サービスの概要】

提供サービスの内容(※1)としては、一般的に以下が含まれています。

①サーバ、ミドルウェア等の仮想クラウドの環境提供

②EC サイト構築パッケージ、必要な全動作環境（OS、ミドルウェア、プラグイン）の最新版へのバージョンアップによるアップデート

③脆弱性検査の定期的な実施

④WAF による防御

⑤不正アクセスログの監視・注意喚起連絡

⑥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

※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、サービス提供事業者に必ず確認してください。

2 新規に EC サイトを構築する場合において確認・検討すべき事項

EC サイトにおけるセキュリティ対策を実践する責任者及び担当者は、EC サイトの構築時における「セキュリティ対策要件（構築時）」の内容を理解したうえで、必要となるセキュリティ対策を確認・検討し、それらの対策実装を計画的に進めていくことが必要です。

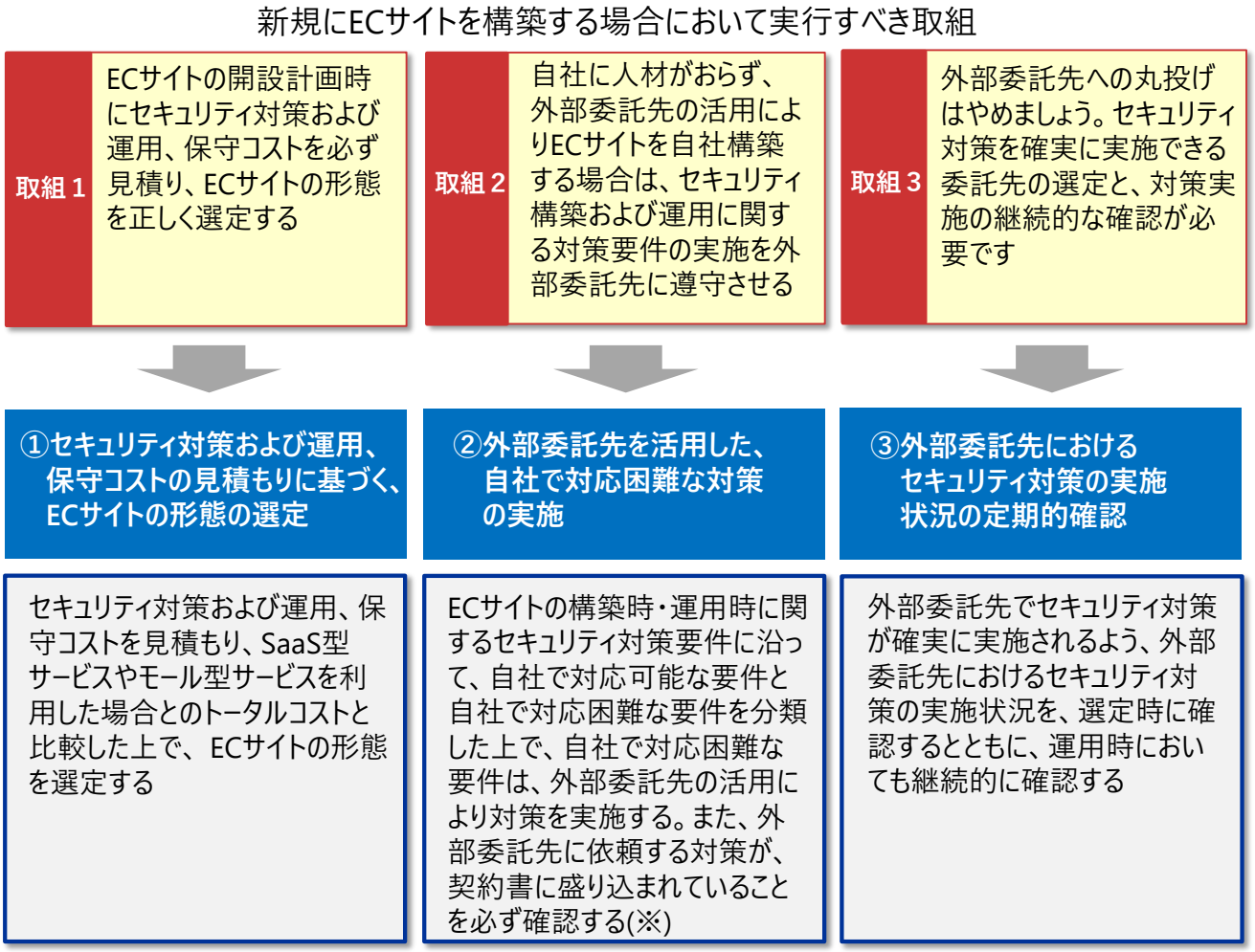
ここでは、必要となるセキュリティ対策を確認・検討する際の効果的な作業手順について理解を深めていただくために、次に挙げる 4 点に要約して説明します。

- 確認・検討にあたっての考え方
- 確認・検討手順
- 構築契約または運用・保守契約上の確認事項
- SaaS 型サービスの選定基準

これらを参考に、EC サイトの売上増加や集客のための検討と遜色がない、またはそれ以上のレベルで EC サイトにおける必要となるセキュリティ対策についても検討することが重要です。その際に、EC サイトの安全性を犠牲にしてまで、EC サイトを新規に構築しないという強い意識を持つことが必要です。

(1) 確認・検討にあたっての考え方

第 1 部の「4. 経営者は何をしなければならないか」で示した、経営者が新規に EC サイトを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及び担当者が、経営者と連携しつつ、それを具体的に実践してください。実践すべき内容は、以下の①～③になります。

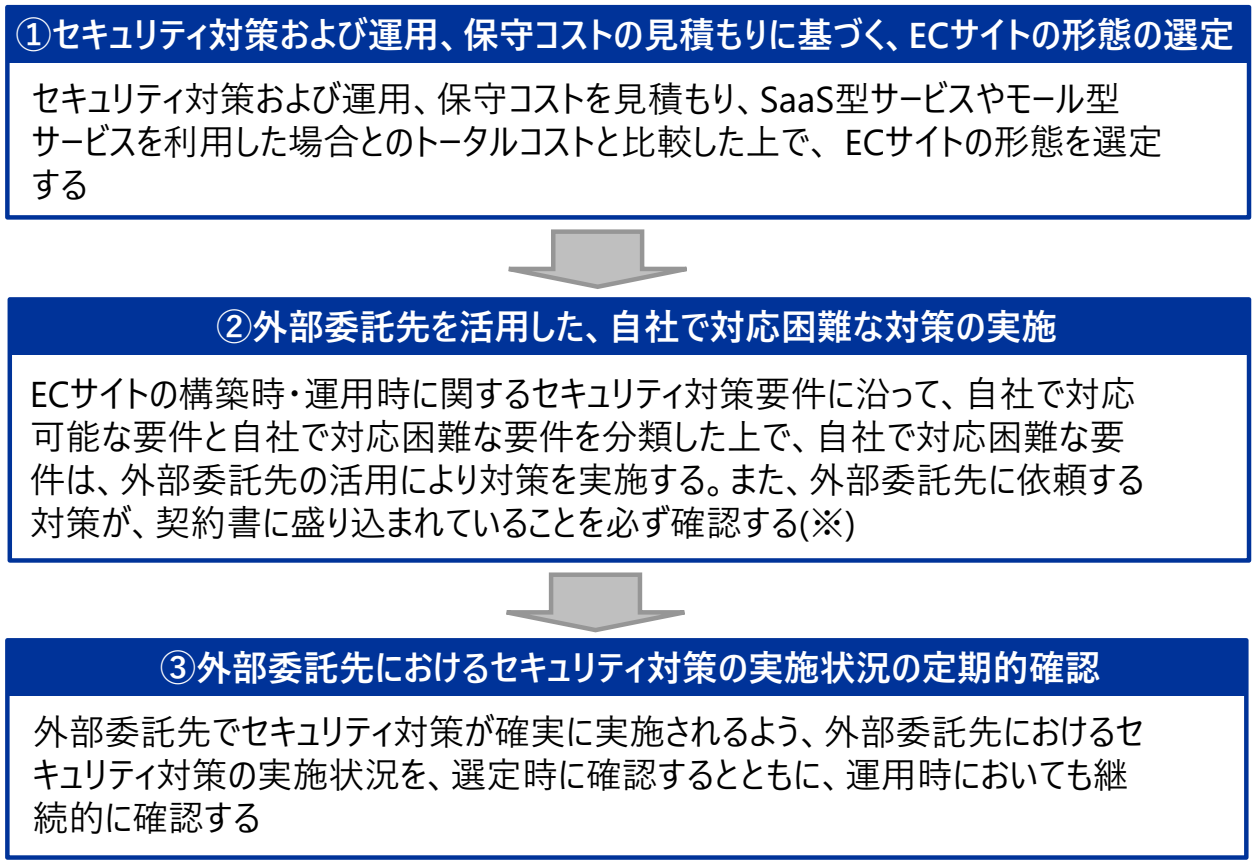


(※) 後述の「3. 構築契約または運用・保守契約上の確認事項」を参照してください。

図 7　新規に EC サイトを構築する場合において実務担当者が実践すべき内容

(2) 確認・検討手順

外部委託先の活用による自社構築がほとんどであるため、外部委託先の活用による自社構築 EC サイトにおける確認・検討手順を以下に示します。自社内での構築した場合は同等の対策を自社内で確実に実施してください。



（※）後述の「3. 構築契約または運用・保守契約上の確認事項」を参照してください。

図 8　外部委託先の活用による自社構築 EC サイトにおける確認・検討手順

① セキュリティ対策および運用、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対策および運用、保守コストを見積り、セキュリティ対策にかかるトータルコストを SaaS 型サービスやモール型サービスを利用した場合と比較した上で、 正しく EC サイトの形態を選定してください。

セキュリティ対策および運用、保守コストの見積りにおいては、「セキュリティ対策要件（運用時）」の「区分」が「必須」、「必要」として実施が求められているセキュリティ対策および運用項目とその費用感について以下を最低限の目安として参考にしてください。

参考情報 9　自社構築 EC サイトのセキュリティ対策および運用コストはいくらかかる？

自社構築 EC サイトにおいて必須として実施が求められるセキュリティ対策および運用項目（基本）

1. 脆弱性対策、運用	①最新の脆弱性情報の収集 ②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 ③自社 EC サイトへの影響度の確認 ④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最新版へのバージョンアップによるアップデート） ⑤システムの定期的なバックアップの取得 ⑥ログの取得・保管と定期的な確認による異常検出 ⑦脆弱性診断の実施 ⑧マルウェア対策ソフトの実装・運用
2. 脅威検知対策	⑨WAF の実装・運用 ⑩不正利用検知の実装・運用

上記のセキュリティ対策および運用項目（基本）にかかる費用感は、以下のとおりです。

- 上記①～⑥の費用感は、最低月額 2～5 万円程度
- 上記の⑦の費用感は、最低年額 100 万円以上（月額換算では、8 万円～）

上記より、自社構築 EC サイトの場合、最低でも月額 10 万円のセキュリティ対策および運用、保守コスト及び、自社内での人的コスト（セキュリティの専門家の雇用等）も含めて見込む必要があることを認識してください。

そのうえで、自社構築 EC サイトの場合と SaaS 型サービスやモール型サービスを利用した場合について、セキュリティ対策および運用、保守コストを含めたトータルコストを比較し、EC サイトの形態を正しく選定してください。

トータルコストの比較においては、一般的な事例をもとにした以下の傾向を参考にしてください。

表 4　セキュリティ対策および運用コストを含めたトータルコストの比較
（一般的な事例に基づく）

項目		EC サイト自社構築の場合	SaaS 型またはモール型サービスを利用した場合
カスタマイズ性		高い	中 (※1) ～ 低い
構築時コスト	セキュリティ以外の費用 (※2)	一般的に高い	低い
	セキュリティ費用	一般的に高い	低い
運用時コスト (※3)	セキュリティ以外の費用 (※4)	一般的に低い	自社構築と同等費用 ＋サービス使用料
	セキュリティ費用	最低月額 10 万円～	サービス使用料(自社構築よりも低い) (※5※6)

※1　SaaS 型サービスのカスタマイズ性は、サービス提供元により異なりますが、自社構築と比べると低くなります。

※2　EC サイトのハードウェア/ソフトウェア構成検討、EC サイトの構成/機能設計、製造、テスト等

※3　決済手数料等は除いています。

※4　商品入替、キャンペーン、サイト改修等

※5　SaaS 型サービスを利用する場合には、PCI DSS に準拠しているサービスを必ず選定してください。

※6　EC サイトのカスタマイズ等により、自社固有の動的ページを作り込んでいる場合、自社固有の部分に対してはセキュリティ対策および運用コスト（脆弱性診断等）を見込んでください。

コラム 3

（ご紹介）脆弱性診断を実施する上で参考にしていただきたいこと

【脆弱性診断の目的】

脆弱性診断は、EC サイトがサイバー攻撃を受けて被害を招く元となる脆弱性が存在していないかを調べるために行う、とても重要で必要な工程となります。もし、脆弱性が見つかった場合、脆弱性による EC サイトへの影響度を確認する必要があります。見つかった脆弱性の危険度及び、脆弱性による EC サイトへの影響度により、対応の要否を判断して、対応をすることが重要となります。

【脆弱性診断の種類】

脆弱性診断は、診断対象、診断方法によって、以下のものがあります。

＜診断対象＞

・プラットフォーム診断：サーバやネットワーク機器等の OS やミドルウェアを診断します。

・Web アプリケーション診断：Web サーバ上で動作するアプリケーションを診断します。

＜診断方法＞

・ツールによる診断：ツールにより自動で診断します。ツールによって診断できる範囲が異なります。ツールには無償のものと有償のものがあります。

・手動による診断：人手により診断します。

・ハイブリッド診断：ツールでの診断が難しい箇所（人による判断が必要な場合）を人手で行うといった両者を組み合わせて診断します。

※手動による診断は、ツールによる診断に比べて費用が高額となります。手動による診断は、ツールでは見つけられない脆弱性を発見でき、ツールによる診断と組み合わせる事で結果として精度の高い診断が可能です。

【脆弱性診断の実施者】

ツールで自動的に診断できる部分があるとはいえ、ツールの使用や診断結果を判断するため、脆弱性診断を行う人はそれなりのスキルが必要になります。自社に脆弱性診断を実施する技術者がいない場合は、脆弱性診断サービスの利用を検討してください。

なお、特定非営利活動法人日本ネットワークセキュリティ協会の日本セキュリティオペレーション事業者協議会のセキュリティオペレーションガイドライン WG(WG1)と、OWASP JAPAN 主催の共同ワーキンググループである「脆弱性診断士スキルマッププロジェクト」では、脆弱性診断を行う技術者に求められるスキルマップとシラバスなどを整備していますので、参考にしてください。

脆弱性診断士スキルマップシラバス

https://github.com/OWASP/www-chapter-japan/tree/master/skillmap_project#

②外部委託先を活用した、自社で対応困難な対策の実施

新規に構築する予定の EC サイトが、第 2 部の 1.（1）EC サイトの構築時におけるセキュリティ対策要件をどれぐらい実装しているか、表 5 に示す「構築時チェックリスト」を用いて確認してください。（表 5 のセキュリティ対策要件は表 2 と同一です）

具体的な作業としては、「構築時チェックリスト」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（表 5 の赤枠部分）を分類し、双方を明確化してください。そのうち自社で対応困難な要件（表 5 の赤枠部分）は、外部委託先の活用で対応すべき要件となりますので、外部委託先の活用により対策を実施してください。

表 5　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一覧－

要件 No	セキュリティ対策要件（構築時）	区分	自社で対応可能な要件	外部委託先の活用で対応すべき要件
1	「安全なウェブサイトの作り方」及び「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。	必須	✓	
2	サーバ及び管理端末等で利用しているソフトウェアをセキュリティパッチ等により最新の状態にする。	必須		✓
3	EC サイトの公開前に脆弱性診断を行い、見つかった脆弱性を対策する。	必須	✓	
4	管理者画面や管理用ソフトウェアへ接続する端末を制限する。	必須	✓	
5	管理者画面や管理用ソフトウェアへ接続する端末のセキュリティ対策を実施する。	必須		✓
6	クレジット取引セキュリティ対策協議会が作成する「クレジットカード・セキュリティガイドライン」を遵守する。	必須	✓	
7	サイト利用者情報の登録時及びパスワ 対策を実施する。			✓
8	サイト利用者の個人情報に対して安全管		✓	
9	ドメイン名の正当性証明と TLS の利用を行う。	必須	✓	
10	サイト利用者のログイン時における二要素認証を導入する。	必要	✓	
11	サイト利用者のパスワードの初期化及び変更といった重要な処理を行う際、サイト利用者へ通知する機能を導入する。	必要		✓
12	Web サーバや Web アプリケーション等のログや、取引データ等のバックアップデータを保管する。	必要		✓
13	保管するログやバックアップデータを保護する。	推奨		

✓はサンプルです。

14	サーバ及び管理端末において、セキュリティ対策を実施する。	推奨		

分類した結果からみて、EC サイトの構築時において、望ましい対応は以下のとおりです。

- 1～9 の「必須」項目はすべてのチェックが埋まっていることを必ず確認してください。
- 10～12 の「必要」項目は可能な限りチェックが埋まっていることを確認してください。
- 13 と 14 の「推奨」項目は、チェックが埋まっていることが望ましいです。
- なお、自社で対応困難な「必須」要件を、外部委託先の活用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す。

次に、新規に構築する予定の EC サイトと同様、運営中の EC サイトについても、第 2 部の 1.(2)EC サイトの運用時におけるセキュリティ対策要件をどれぐらい実装しているか、表 6 に示す「運用時チェックリスト」を用いて確認してください。(表 6 のセキュリティ対策要件は表 3 と同一です)

具体的な作業としては、「運用時チェックリスト」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（表 6 の赤枠部分）を分類し、双方を明確化してください。そのうち自社で対応困難な要件（表 6 の赤枠部分）は、外部委託先の活用で対応すべき要件となりますので、外部委託先の活用により対策を実施してください。

表 6　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一覧－

要件 No	セキュリティ対策要件（運用時）	区分	自社で対応可能な要件	外部委託の活用で対応すべき要件
1	サーバ及び管理端末等で利用しているソフトウェアをセキュリティパッチ等により最新の状態にする。	必須	✓	
2	EC サイトへの脆弱性診断を定期的及び[redacted]つかった脆弱性を対策する。			✓
3	Web サイトのアプリケーションやコンテン[redacted]的な差分チェックや、Web サイト改ざん[redacted]			✓
4	システムの定期的なバックアップの取得及びアクセスログの定期的な確認を行い不正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。	必要	✓	

✓はサンプルです。

5	重要な情報はバックアップを取得する。	必要		✓
6	WAF を導入する。	推奨		
7	サイバー保険に加入する。	推奨		

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

- 1～3 の「必須」項目はすべてのチェックが埋まっていることを必ず確認してください。
- 4 と 5 の「必要」項目は可能な限りチェックが埋まっていることを確認してください。
- 6 と 7 の「推奨」項目は、チェックが埋まっていることが望ましいです。

このように構築時/運用時チェックリストは、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。

なお、自社で対応可能な要件と外部委託先の活用で対応すべき要件との切り分け方法について悩まれた場合は、以下のような例を参考にしてください。

（例 1）EC サイト構築時における管理者画面保護対策（EC サイトの構築時におけるセキュリティ対策要件 4 と 5）や利用者保護対策（同要件 7、8、9、10 と 11）など、自社でも比較的取り組みやすいセキュリティ対策については、極力自社で対応し、その実装の正しさを第三者による脆弱性診断にて確認し、指摘のあった不十分な箇所を修正する

（例 2）EC サイト運用時における脆弱性対策（EC サイトの運用時におけるセキュリティ対策要件 1 と 2）など、最新の脆弱性や攻撃手法への対応のために、自社において新しい知識やスキルの習得が求められる対策で、かつ対応要員を確保できない場合については、EC サイトの構築事業者が提供する EC サイトのセキュリティ運用・保守契約の利用によりカバーする

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、外部委託先に委託する自社のセキュリティ対策を、選定時には実施可能かを確認するとともに、運用時においても継続的に実施状況を確認してください。確認すべきセキュリティ対策は以下のとおりです。

- 運用時チェックリストの 1～5 の実施状況を定期的に確認してください。

- 確認頻度の目安としては、以下を参考にしてください。
  (1 の確認頻度) 随時
  (2 の確認頻度) プラットフォーム診断は、少なくとも四半期に 1 回程度
  Web アプリケーション診断は、新機能の開発や追加やシステム改修等を行ったタイミングで実施
  (3 の確認頻度) 少なくとも週に 1 回程度
  (4 の確認頻度) 少なくとも週に 1 回程度
  (5 の確認頻度) 少なくとも週に 1 回程度

(3) 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・検討手順/②外部委託先を活用した、自社で対応困難な対策の実施」において、構築時/運用時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、外部委託先事業者へ委託する場合は、必ず構築契約/運用・保守契約にかかる、契約関係書類（見積書や調達時の要求仕様書、契約書等）の記載内容に、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してください。

- 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す。
- 特に、脆弱性対応を含む、EC サイトの運用・保守契約を、外部委託先事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す。

①最新の脆弱性情報の収集

【情報収集先となる主なサイト】

- JVN iPedia 脆弱性対策情報データベース（IPA）
  https://jvndb.jvn.jp/index.html
- 重要なセキュリティ情報一覧（IPA）
  https://www.ipa.go.jp/security/announce/alert.html
- サイバーセキュリティ注意喚起サービス（IPA）
  https://www.ipa.go.jp/security/vuln/icat.html
- JVN（Japan Vulnerability Notes）（JPCERT/CC、IPA）
  https://jvn.jp/
- 注意喚起（JPCERT/CC）
  https://www.jpcert.or.jp/at/

②収集した脆弱性情報の中から、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

③公表された脆弱性の危険度の調査

④外部契約先が担当する自社 EC サイトへの影響度の確認

⑤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最新版へのバージョンアップによるアップデート）

⑥EC サイトのシステムの定期的なバックアップの取得

⑦ログの取得・保管と定期的な確認による異常検出

EC サイトの構築契約の仕様書の具体例の一つを付録 3 に示します。

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して、見積書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。

(4) SaaS 型サービスの選定基準と利用時に必要となる対策

前述した「(2)確認・検討手順/①セキュリティ対策および運用、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 型サービスを選定した場合、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ります。

【SaaS 型サービスの選定基準】

- 選定したサービスが PCI DSS に準拠していることを確認してください。（当該サービスの運営事業者のホームページやパンフレット等に情報が公表されていない場合は、サービスの営業窓口に問い合わせて確認してください）

また、SaaS 型サービスを選択した場合でも、セキュリティ対策が不要ということではありません。SaaS 型サービスの管理画面を乗っ取られると、EC サイトに不正ログインされ被害が発生します。

また、カスタマイズした部分（SaaS 型サービス利用で独自の処理を追加したホームページを作成している場合）に関しては自社構築サイトと同等レベルのセキュリティ対策を行う必要があります。

EC サイト運営事業者は、上記を理解した上で以下のセキュリティ対策を必ず実施してください。

【SaaS 型サービス利用時に注意すべきセキュリティ対策】

- 管理画面の乗っ取りを未然に防ぐため、SaaS 型サービスの管理画面や管理用ソフトウェアへアクセスする管理端末を利用する従業員を極力最低限に限定し、かつ、管理端末からのアクセス時は二要素認証と IP アドレスや端末 ID による接続制限の導入等を必須としてください。
- 管理端末において、セキュリティ対策（マルウェア対策ソフトウェアの導入、USB メモリ等外部記憶媒体の利用制限、OS、ソフトウェアの最新版へのアップデート等）を実施し、管理端末のサイバー攻撃者からの乗っ取りを防いでください。

コラム４

「SaaS 型サービスなのでセキュリティは何もしなくて大丈夫」は大きな間違いです。

第 1 章の参考情報２で「不正アクセスを受け、サイバー被害が発生した EC サイト運営事業者の約 97%が、自社構築サイト」であるとの調査結果がありますが、「SaaS 型サービスなのでセキュリティは大丈夫」と考えるのは正しくありません。大変残念なことに、数は少ないですが、SaaS 型サービスでもサイバー攻撃被害が発生しています。

ここまで読まれた読者の皆様はセキュリティ対策の重要性をご理解されたと思います。万が一でも被害にあわないためには、SaaS 型サービス選定時は上記「SaaS 型サービスの選定基準」に従い選定し、【SaaS 型サービス利用時に注意すべきセキュリティ対策】を必ず実施してください。

3 運営中の EC サイトにおいて確認･検討すべき事項

EC サイトにおけるセキュリティ対策を実践する責任者及び担当者は、EC サイトの運用時における「セキュリティ対策要件（運用時）」の内容を理解したうえで、必要となるセキュリティ対策を確認・検討し、それらの対策実装を計画的に進めていくことが必要です。

ここでは、必要となるセキュリティ対策を確認・検討する際の効果的な作業手順について理解を深めていただくために、次に挙げる 2 点に要約して説明します。

- 確認･検討にあたっての考え方
- 確認･検討手順

これらを参考に、運営中の EC サイトが抱えるサイバー被害リスクに対して、対策が不十分であった過去を振り返りつつ、改めて基本に立ち返って必要となるセキュリティ対策を確認し、すぐにできる対策から着実に進めていくことが重要です。また、対策の実装に時間を要する場合は、サイバー被害リスクを軽減するための応急処置についても併せて検討することが重要です。

その際、セキュリティは経営の中核事項ではないと考える経営者の誤った認識を正しい方向に導き、セキュリティ意識改革を実現することが成功への近道になります。

また、セキュリティ対策を含め、自社のみで EC サイトを運用することが難しい運営事業者においては、効果的な対策を効率よく実装するうえで、外部委託先と適正な運用・保守契約等を締結することや、EC サイトのカスタマイズを諦め SaaS 型サービスやモール型サービスを利用することも一つの有力な選択肢となりうるということを認識してください。売上増加や集客と同じようにセキュリティを経営の中核事項として EC サイトの形態を検討することが最も重要です。

(1) 確認・検討にあたっての考え方

第 1 部の「4. 経営者は何をしなければならないか」で示した、経営者が EC サイトを運営中の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及び担当者が、経営者と連携しつつ、それを具体的に実践してください。実践すべき内容は、以下の①～③になります。

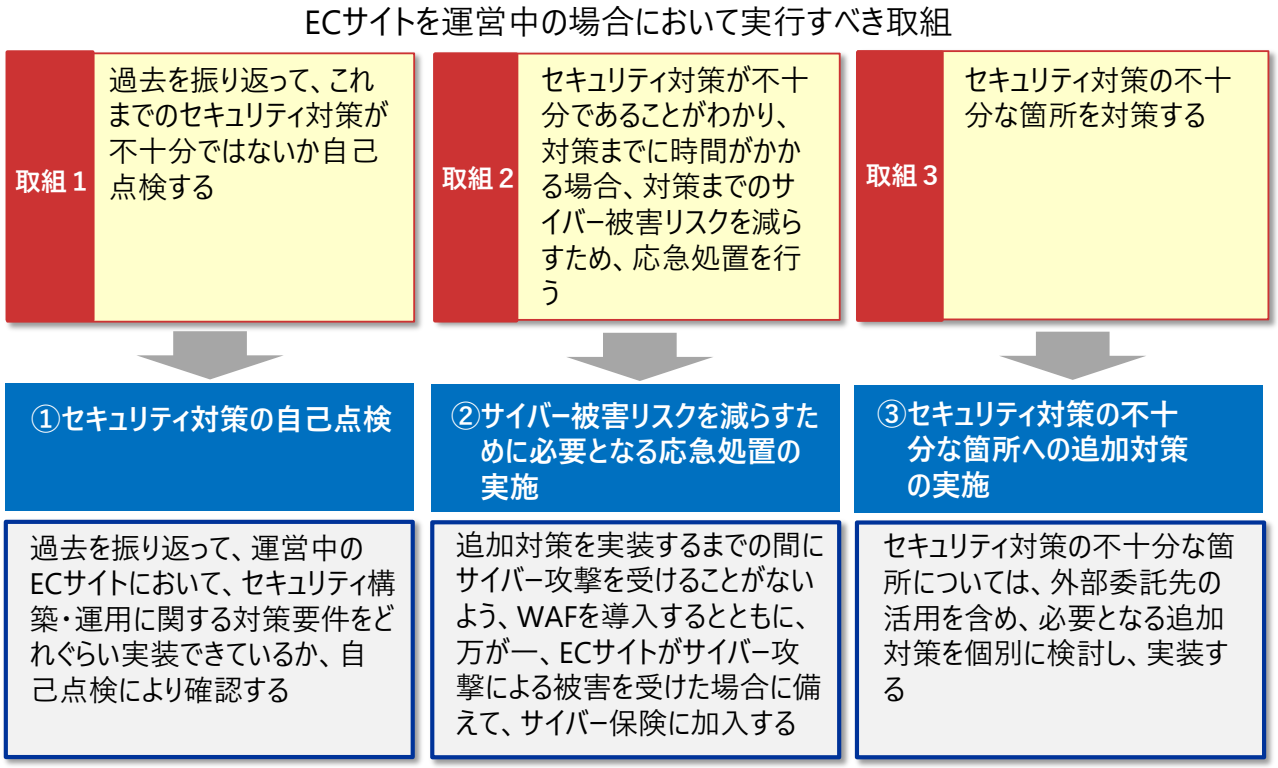


図 9　EC サイトを運営中の場合において実務担当者が実践すべき内容

(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します。

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

↓

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、外部委託先の活用を含め、必要となる追加対策を個別に検討し、実装する

図 10　運営中の EC サイトにおける確認・検討手順

① セキュリティ対策の自己点検

表 7 に示す「運営中 EC サイト向け構築時チェックリスト」を用いて、運営中の EC サイトが、第 2 部の 1.（1)EC サイトの構築時におけるセキュリティ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してください。(表 7 のセキュリティ対策要件は表 2 と同一です)

具体的には、「運営中 EC サイト向け構築時チェックリスト」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、双方を明確化してください。そのうち未実装の要件は、自社で対応できない場合に外部委託先の活用で対応すべき要件となりますので、外部委託先の活用により対策を実施してください。

表 7　運営中 EC 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一覧－

要件 No	セキュリティ対策要件（構築時）	区分	実装済みの要件	対策完了時にチェック
1	「安全なウェブサイトの作り方」及び「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。	必須	✓	
2	サーバ及び管理端末等で利用しているソフトウェアをセキュリティパッチ等により最新の状態にする。	必須		✓
3	EC サイトの公開前に脆弱性診断を行い、見つかった脆弱性を対策する。	必須	✓	
4	管理者画面や管理用ソフトウェアへ接続する端末を制限する。	必須	✓	
5	管理者画面や管理用ソフトウェアへ接続する端末のセキュリティ対策を実施する。	必須		✓
6	クレジット取引セキュリティ対策協 ィガイドライン」を遵守する。	必須	✓	
7	サイト利用者情報の登録時及び 策を実施する。	必須		✓
8	サイト利用者の個人情報に対して安全管理措置を講じる。	必須	✓	
9	ドメイン名の正当性証明と TLS の利用を行う。	必須	✓	
10	サイト利用者のログイン時における二要素認証を導入する。	必要	✓	
11	サイト利用者のパスワードの初期化及び変更といった重要な処理を行う際、サイト利用者へ通知する機能を導入する。	必要		✓
12	Web サーバや Web アプリケーション等のログや、取引データ等のバックアップデータを保管する。	必要		✓
13	保管するログやバックアップデータを保護する。	推奨		
14	サーバ及び管理端末において、セキュリティ対策を実施する。	推奨		

✓はサンプルです。

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

- 「対策完了時にチェック」欄は外部委託先等に問合せの上、「実施済みの要件」欄と合わせて、1～9 の「必須」項目がすべて埋まるようにしてください。
- 10～12 の「必要」項目は可能な限りチェックが埋まっていることを確認してください。
- 13 と 14 の「推奨」項目は、チェックが埋まっていることが望ましいです。

同様に、表 8 に示す「運営中 EC サイト向け運用時チェックリスト」を用いた自己点検による確認についても併せて実施してください。（表 8 のセキュリティ対策要件は表 3 と同一です）

表 8　運営中 EC 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一覧－

要件 No	セキュリティ対策要件	区分	実装済みの要件	対策完了時にチェック
1	サーバ及び管理端末等で利用しているソフトウェアをセキュリティパッチ等により最新の状態にする。	必須	✓	
2	EC サイトへの脆弱性診断を定期的及びカスタマイズを行った際に行い、見つかった脆弱性を対策する。	必須		✓
3	Web サイトのアプリケーションやコンテンツ、設定等の重要なファイルの定期的な差分チェックや、Web サイ	必須		✓
4	システムの定期的なバックアッ 行い不正アクセス等があればア	必要	✓	
5	重要な情報はバックアップを取得する。	必要		✓
6	WAF を導入する。	推奨		
7	サイバー保険に加入する。	推奨		

✓はサンプルです。

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

- 「対策完了時にチェック」欄は外部委託先等に問合せの上、「実施済みの要件」欄と合わせて、1～3 の「必須」項目がすべて埋まるようにしてください。
- 4 と 5 の「必要」項目は可能な限りチェックが埋まっていることを確認してください。
- 6 と 7 の「推奨」項目は、チェックが埋まっていることが望ましいです。
- 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 型サービスへの移行を含め、善処策を検討してください。

このように運営中 EC サイト向け構築時/運用時チェックリストは、継続して自社で EC サイトを運営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、応急処置として、WAF を導入することが推奨されます。

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ます。

- WAF を選定する際には、「コラム５　(ご紹介)WAF(Web Application Firewall)の活用方法」を参照してください。

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、外部委託先の活用を含め、必要となる追加対策を個別に検討し、実装してください。

- 前述の第 2 部の 2.③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、外部委託先を活用する場合、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す。

コラム 5

（ご紹介）WAF（Web Application Firewall）の活用方法

【WAF は何ができるのか】

WAF は、外部から脆弱性を悪用した攻撃に対して、攻撃通信を遮断して、Web サーバを防御することが可能です。しかし、WAF はすべての攻撃を遮断できる訳ではなく、決済画面上でのランダムなクレジットカード番号等の入力を有効性が確認されるまで何度も繰り返し、他人のクレジットカード番号等を割り出すクレジットマスター攻撃に代表されるような、正規の操作を自動的に繰り返すプログラムを利用した攻撃や、Web アプリケーションの脆弱性を悪用するものではない攻撃（ネットワークや OS、ミドルウェアに対する攻撃等）は遮断する事はできません。

【WAF の種類】

WAF には、製品・サービスとして、以下の物があります。

製品・サービス	特徴
クラウド型	第三者が提供するクラウド型の WAF サービスで、サービス提供者が提供する WAF を経由することで検査を行い、Web サーバへの通信を遮断する
アプライアンス型	組織内のネットワーク内に専用の機器として WAF を設置し、Web サーバへの通信を遮断する
ソフトウェア型	組織が運用する Web サーバ内に、ソフトウェアとして WAF をインストールし、Web サーバへの通信を遮断する

【WAF を利用することによる効果と考慮事項】

WAF を利用することによる主な効果と考慮事項は、以下です。

効果	考慮事項
○クロスサイト・スクリプティングや SQL インジェクションなどの Web アプリケーションの脆弱性を悪用する攻撃や、ボットネットからの DDoS 攻撃等から、自社 EC サイトを防御できる。	○WAF をより効果的に運用するために必要となる検知ポリシーの設定作業や、検知ポリシー適用後に発生する誤検知を減らすためのチューニング作業を有効なものとするには、時間と労力、コストが必要となる

○自らが行う必要がないクラウド型の WAF や、レンタルサーバに標準機能として搭載され、on/off のシンプルな操作で利用可能な WAF など、さまざまな製品・サービスが提供されており、短期間で自社 EC サイトを防御できる。	○検知ポリシーの内容が、提供事業者によって決められているような WAF を利用する場合、自社 EC サイト向けのカスタマイズが効かないため、誤検知が発生しやすくなる。 ○共用サーバを利用して、EC サイトを構築している場合、自社 EC サイト向けにカスタマイズした検知ポリシーの設定作業やチューニング作業ができない。

【WAF を利用するにあたっての注意点】

① WAF で防御できない攻撃が存在する点や、検知ポリシーの設定内容によって、遮断できる攻撃のカバー範囲や検知精度にレベルの違いが生じる点について認識し、WAF が万能ではないことや、WAF の各種製品・サービス間の攻撃検知性能が均質ではないことを正しく理解する必要があります。
上記を考慮し、あくまでも、根本的な対策を実施するまでの間や、他のセキュリティ対策への追加的な対策として、WAF を利用してください。

② 高いレベルのスキルが求められる検知ポリシーの設定・チューニングについては、設定ミスが起きないように、提供事業者との調整のもとで適切な設定を行うことや、EC サイトを狙う攻撃の変化や、EC サイトのリニューアルやカスタマイズの状況に応じて、定期的に見直しを行うことを認識する必要があります。

WAF を利用するにあたっては、以下の資料も参考にしてください。
・Web Application Firewall の導入に向けた検討項目
https://www.ipa.go.jp/files/000072484.pdf

お わ り に

国内の EC サイトにおける顧客情報の漏えい事故と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です。これ以上の事故・被害の拡大に歯止めをかけるため、EC サイト運営事業者は、セキュリティ対策を疎かにした状態で、EC サイトを構築・運用することを控えてください。

その一方で、EC サイトの形態も、それに伴って必要となるセキュリティ対策もさまざまであり、EC サイト運営事業者の中には、自社の EC サイトでどんな対策をやれば良いのか分からないという事業者も多くいます。さらに、予算上の制約を抱える中小企業で、EC サイトを運営する事業者においては、費用を出来る限り低く抑えながら、講じるべき対策を実施することが求められます。

本ガイドラインは、このような状況を踏まえ、EC サイトの構築時及び、運用時において、必要となるセキュリティ対策を検討する上で、何を優先して対策していくか、自社の EC サイトの状況に見合った実践すべき対策の範囲や実現方法をどうすべきかを適切に決めていく際の考え方や手順を取り上げて解説しています。経営者が実務担当者に対し、セキュリティ対策を実施する指示を出す際や、実務担当者が適切なセキュリティ対策を実践する際やそのために必要な予算を確保する際に、本ガイドラインをご活用いただければ幸いです。

また、EC サイト構築事業者等においては、実務担当者からセキュリティ対策の実装・運用を依頼された際に、本ガイドラインをご活用いただき、ご対応いただければ幸いです。

本ガイドライン作成にあたり、「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」の座長である慶應義塾大学　土居範久　名誉教授をはじめ、委員の皆様方より貴重なご助言を賜りました。また、経済産業省や個人情報保護委員会より調査データの提供や EC サイト構築事業者等ヒアリング先の紹介についてご協力をいただきました。さらに、多くの事業者にヒアリングや脆弱性診断にご協力いただきました。ここに厚く御礼申し上げます。

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

座長	土居 範久	慶應義塾大学　名誉教授
委員	上野 宣	株式会社トライコーダ　代表取締役
	大河内 貴之	クレジット取引セキュリティ対策協議会 テクニカルグループ 分科会　座長、Secure・Pro株式会社　代表取締役
	岡村 久道	弁護士法人英知法律事務所　弁護士、国立情報学研究所　客員教授、京都大学大学院医学研究科　非常勤講師
	小林 雅人	NRIセキュアテクノロジーズ株式会社 DXセキュリティコンサルティング事業本部 DXセキュリティ事業部　グループマネージャー
	島貫 和久	クレジット取引セキュリティ対策協議会 テクニカルグループ　議長、三菱UFJニコス株式会社 経営企画本部　エグゼクティブ・フェロー
	筒井 浩二朗	ひまわりセキュア株式会社　代表取締役
	三浦 千宗	公益社団法人 日本通信販売協会　理事・事務局長

（五十音順、敬称略）

オブザーバ

経済産業省 商務情報政策局 サイバーセキュリティ課

経済産業省 商務情報政策局 商務・サービスグループ 商取引監督課

経済産業省 商務情報政策局 商務・サービスグループ 消費・流通政策課

個人情報保護委員会事務局　監視・監督室

一般社団法人日本クレジット協会

事務局

独立行政法人情報処理推進機構

株式会社野村総合研究所

本ガイドラインで用いている主な用語の説明

【第 1 部　経営者編に初めて出てくる用語】

管理者画面

サービスの運用を目的として、顧客情報や売上情報等のデータを管理するための画面を指す。

自社構築サイト

EC サイト構築パッケージ、または、スクラッチで自社サイトを構築することを、本ガイドラインでは自社構築サイトと定義します。SaaS 型サービスを利用されているサイトは、本ガイドラインでは自社構築に含みません。

スクラッチ開発

システム開発のひな形であるパッケージ等を用いずに、一からオリジナルのシステムを開発することを指す。

セキュアコーディング

ソフトウェアを開発する際、ハッカー等の悪意のある攻撃者や、マルウェア等の攻撃に耐えうる、堅牢なプログラムを構築することを指す。

パッケージ

システムのひな形を指す。ひな形を使用する、または一部をカスタマイズする等して、システム開発を行うことをパッケージ開発と呼ぶ。

非公開ディレクトリ

サーバ等にファイルを保管する場所（ディレクトリ）のうち、アクセス制限等を用いて、特定のユーザー以外からのアクセスが不可能なよう設定した領域を指す。

フォレンジック調査

Web サイトへの不正アクセス等のインシデントが発生した際に、被害状況の把握や原因究明等を行い、法的証拠を得るために行われる、鑑識調査やデータ解析のことを指す。

本ガイドラインにおいては、EC サイト運営事業者が不正アクセスや顧客情報流出等の被害にあった際に、被害状況の把握や原因究明を実施するために、専門企業に依頼・実施する調査を指す。

ミドルウェア

コンピュータを構成する要素の一つで、基本機能を提供する OS と、OS だけではできない特別なことを提供するアプリケーションとの間に存在するソフトウェアを指す。

モール型サービス

1 つの EC サイト上に、多数のショップが商店街（モール）のように存在している形態の EC サービスを指す。

ランサムウェア

コンピュータを使用不能にする等して、元に戻すことと引き換えに身代金を要求するサイバー攻撃に用いられるソフトウェアを指す。

CMS

Contents Management System（コンテンツ管理システム）の略で、Web サイト上で扱う画像やテキスト等のデジタルコンテンツに関する制作、編集、登録・公開等の作業を、管理者画面から簡単に行うことができるソフトウェアのことを指す。

OSS

Open Source Software の略で、ソースコードが公開されており、無償で誰でも自由に改変、再配布が可能なソフトウェアを指す。

SaaS 型サービス

SaaS とは、Software as a Service の略で、サービス提供者が保有するクラウドサーバ上にあるソフトウェアを、利用者がインターネットを経由して利用することが出来るサービスのことを指す。

WAF

Web Application Firewall の略で、Web アプリケーションの脆弱性を悪用した攻撃から Web サイトを保護するセキュリティ対策のことを指す。

クリックジャッキング

Web サイト上に隠蔽・偽装したリンクやボタンを設置し、サイト訪問者を視覚的に騙してクリックさせる等意図しない操作を誘発することで、顧客情報やクレジットカード情報等を意図的に収奪する手法のサイバー攻撃を指す。

クロスサイトスクリプティング

サイトに設置されたフォームにユーザーが情報を入力・送信する際に、埋められた悪質な HTML スクリプトが実行され、入力された情報に加え Cookie 情報なども攻撃者に収集されてしまう等、Web サイトの脆弱性を利用したサイバー攻撃を指す。

証明書

サーバ証明書の略で、ウェブサイトの運営者の実在性を確認し、ブラウザとウェブサーバ間で通信データの暗号化を行うための電子証明書を指す。

通常、ドメインの所有者の情報や、暗号化通信に必要な鍵、発行者の署名データが含まれます。例として、ドメイン認証証明書、組織認証証明書、EV サーバ証明書等が挙げられる。

二要素認証

ID・パスワードによる認証実施後に、その他の方法（SMS 等）での認証を行うことを指す。

マルウェア

コンピュータに悪影響をもたらす悪意のある動作をさせるコードやソフトウェアを指す。

Content Security Policy

本設定を行うことにより、ブラウザ側で影響を軽減することが可能となり、クロスサイト・スクリプティング攻撃、クリックジャッキング攻撃を軽減することができる。

DDoS 攻撃

Distributed Denial of Service 攻撃の略称で、攻撃対象となる Web サーバ等に対して、複数のコンピュータから大量のデータを送付し、正常なサービス提供を妨

げる行為を指す。

EMV 3D セキュア

クレジットカードの不正利用を防ぐための本人認証サービスを指す。

https

Hypertext Transfer Protocol Secure の略で、通信経路での第三者による情報の盗聴や改ざんのリスクを防止することが出来る暗号化通信の一種のことを指す。

https にすることで、通信経路での第三者による情報の盗聴や改ざんのリスクを防止することができる。

OS コマンド・インジェクション

Web サイト上で、不正なデータを入力し、Web サーバ側で想定していない動作をさせるサイバー攻撃を指す。

PCIDSS

Payment Card Industry Data Security Standard の略で、クレジットカードの利用者の情報保護を目的として、クレジットカードを決済方法として具備する店舗や、クレジットカード発行体・国際ブランド等の関連するステークホルダーが遵守すべき情報セキュリティ基準のことを指す。

SQL インジェクション

アプリケーションのセキュリティ上の不備を意図的に利用し、アプリケーションが想定しない言語を入力・実行させることにより、データベースを不正に操作する攻撃方法を指す。

TLS

Transport Layer Security の略で、安全性の高い通信を行うため、公開鍵認証や共通鍵暗号等の機能を提供する仕組みを指す。

X-Content-Type-Option

本設定を行うことにより、ブラウザ側で意図しないファイルを読み込む等の影響を軽減することが可能となり、クロスサイト・スクリプティング攻撃を軽減することができる。

X-Frame-Options

本設定を行うことにより、ブラウザ側で影響を軽減することが可能となり、クリックジャッキング攻撃を軽減することができる。

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 EC サイトの運営事業者にヒアリングを実施した際に担当者から寄せられた生の声について紹介しますので、今後の対策検討において参考にしてください。

Q1 被害に繋がる一連の問題事象の中で、根本原因は何でしたか？

A 社

OSS の EC サイト構築プログラムの脆弱性や、クレジットカード決済機能を自社で運用するリスクについての理解が不十分であった。前任者から運用担当を引き継いだ際に、実装の中身まで確認していなかったが、想像していたよりも、実際にはセキュリティ対策が行われていなかった。

B 社

OSS の EC サイト構築プログラムの古いバージョンを利用して EC サイトを構築していた。無料で利用できる診断ツールを利用して脆弱性診断を行った結果、脆弱性が見つかったが、最新バージョンでリニューアルする計画があったため、古いバージョンで見つかった脆弱性については修正する必要はないと考えてしまい、疎かにしてしまった。

C 社

EC サイト構築プログラムの脆弱性が公表されたが、標準の機能では実現できないようなカスタマイズを行った箇所が EC サイトに多く含まれていたため、バージョンアップ対応が難しくなり、迅速に対処することができなかった。

D 社

付き合いの長い外部委託先事業者に、EC サイトの構築や運用・保守を委託しており、EC サイト構築プログラムの脆弱性が公表された際の対策についても依頼していたが、外部委託

先の得意な分野ではなかったため、対策が十分ではなかった。

E 社

セキュリティ運用を含めた EC サイトの構築と運用・保守について、特定の担当者による属人的な対応に依存していたが、その担当者の退職やそれに伴う社内での引継ぎの不十分により、EC サイト構築プログラムの脆弱性対策が疎かになってしまった。

Q2 被害が確認された後の対応において、困ったことは何でしたか？

F 社

クレジットカード決済の再開のためには、フォレンジック調査での指摘事項に対して、すべて対応する必要があるが、予算の確保が厳しく、また社内でクレジットカード決済にこだわらなくてもよいという意見も出たため、当面はクレジットカード決済の再開を見送るという経営判断に至った。

G 社

EC サイトの構築を外部委託先事業者に委託していた。フォレンジック調査により、外部委託先の構築内容がずさんで瑕疵があったことが判明したが、外部委託先との契約書には、瑕疵担保責任の存続期間は 1 年間と記載されており、被害発覚時に構築後 3 年程度経過していたこともあり、外部委託先に賠償請求することが出来なかった。

H 社

被害者の多くは初めての経験でショックを受け、どこに相談すればよいか分からないほど思考停止に陥る。被害発生当時、今後、事業に対しどのような影響が及ぶのか、お詫び文の公表までにどのようなプロセスを経るのか等全く状況が分からない中で、客観的なアド

バイスがもらえる信頼できる相談先を見つけることが出来なかった。

I 社

フォレンジック調査を行う際に、利用していたレンタルサーバ事業者より Web サーバのアクセスログ等の提供や管理者画面等へのアクセス権限の付与を断られたため、フォレンジック調査会社に対して、調査に必要となる十分なログやデータを提供することが出来なかった。

Q3 当時の被害を振り返って、「被害を受ける前に、これだけは実施しておけばよかった」と後悔している対策はありましたか？

J 社

EC サイトのセキュリティ対策を担当する部署も人材も存在しないという組織構造上の欠陥と、セキュリティ対策を外部委託先事業者任せにしていたことが被害を招いた。社内のセキュリティ人材を育成し、EC サイトの脆弱性対応やセキュリティ対策への感度を高めることが必要であった。

K 社

EC サイトの運用・保守を自社で行っていた。被害発生当時、EC サイト構築プログラムの脆弱性について公表されているプレスリリースを頻繁に閲覧することは業務上の負担となっていたため、主要なもののみ確認していた。すべての脆弱性を確認・把握し、対応することが必要であった。

L 社

EC サイトの構築を委託した外部委託先事業者の設定ミスで非公開のディレクトリが公開領域にあり、被害を受けた。外部委託先の選定時に、費用と提供機能の観点を重視し、セ

キュリティの観点を重視していなかった。外部委託先事業者のセキュリティ知識を確認することが必要であった。

M社

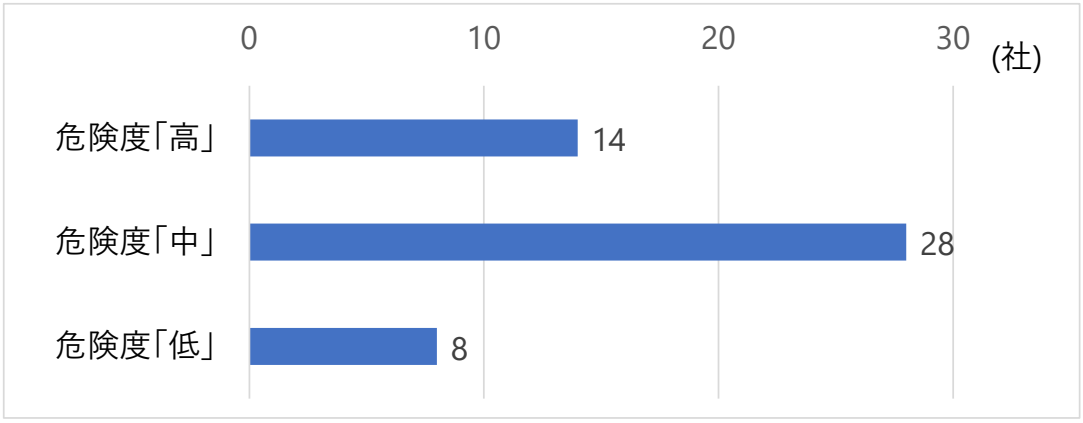
サイバー保険に加入していたことにより、SaaS型サービスへの移設、WAFの新規導入・運用等のセキュリティ対策の強化等に係る費用をほぼ賄うことができた。一方で、現在加入しているサイバー保険では、カテゴリごとに補償額の金額に上限があり、一部で賄えない部分もあったため、保険金額の増額が必要と感じ、現在検討している。

N社

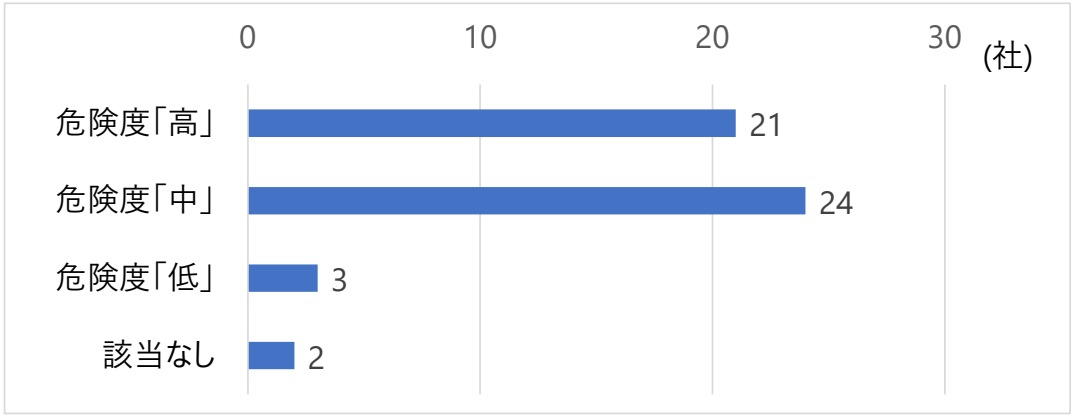
管理者画面にアクセスする際の管理者IDとパスワードをデフォルトのまま運用していたことや、管理者IDとパスワードを複数の担当者で使い回しして利用していたことが被害の根本的な原因である。アクセス権限の設定や管理者パスワードの定期的な更新等の管理者画面の運用方法に関するルール化がずさんであってはいけない。

付録 2. 自社構築サイト(中小企業)50 社の脆弱性診断結果

Web アプリケーション診断及び、プラットフォーム診断において検出された脆弱性に関わる危険度のうち、最高であったものを基準にして整理した企業数（例えば、1 つでも危険度「高」があれば、それを基準として、危険度「高」に該当する企業としてカウントしています）を以下に示す。



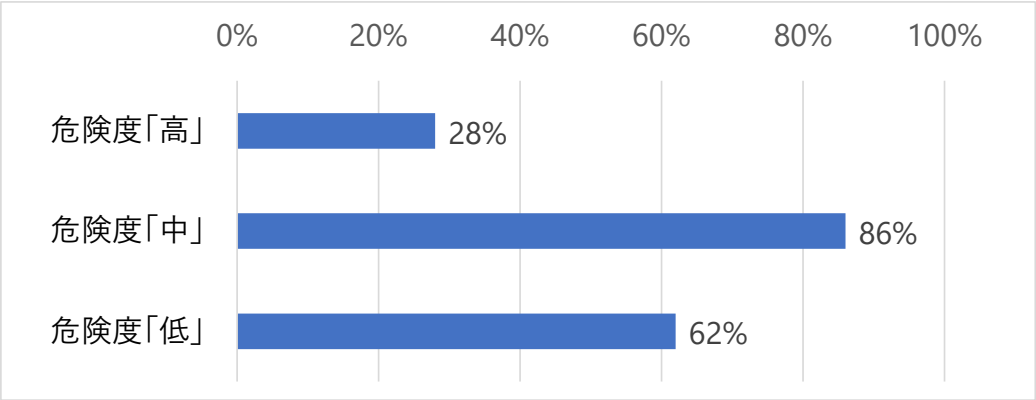
Web アプリケーション診断における危険度の最高位別にみた企業数(調査対象企業 50 社)



プラットフォーム診断における危険度の最高位別にみた企業数（調査対象企業 50 社）

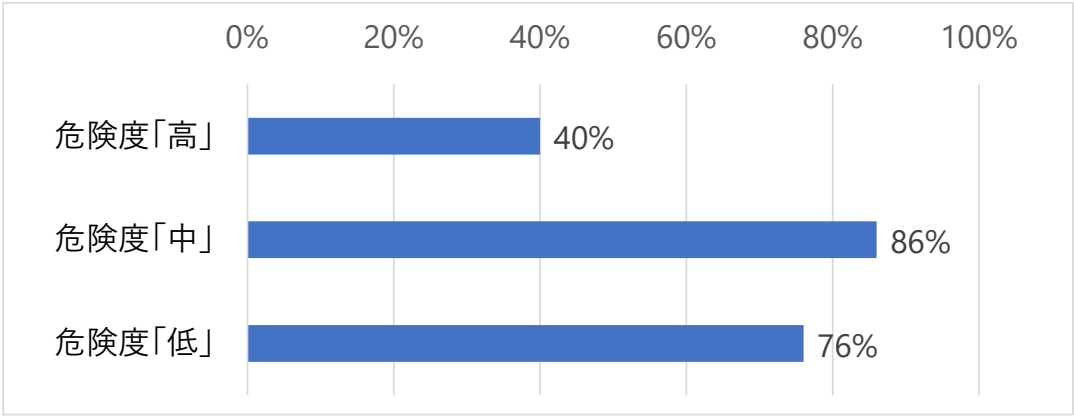
次に、診断対象企業 50 社を対象とした Web アプリケーション診断及び、プラットフォーム診断において検出された脆弱性に関して、危険度別にみた企業数の割合を以下に示します。

Web アプリケーション診断において、危険度「高」、「中」、「低」の脆弱性が検出された企業の割合はそれぞれ 28%、86%、62%となっています。



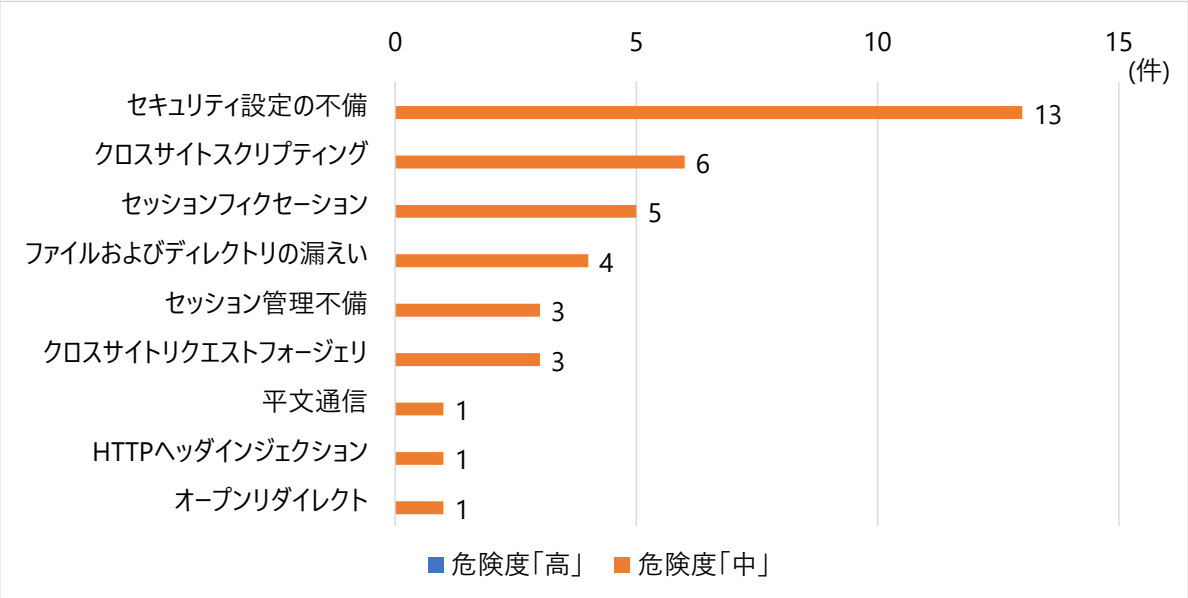
Web アプリケーション診断における危険度別にみた企業の割合 (診断対象企業 50 社)

他方、プラットフォーム診断において、危険度「高」、「中」、「低」の脆弱性が検出された企業の割合はそれぞれ 40%、86%、76%となっています。

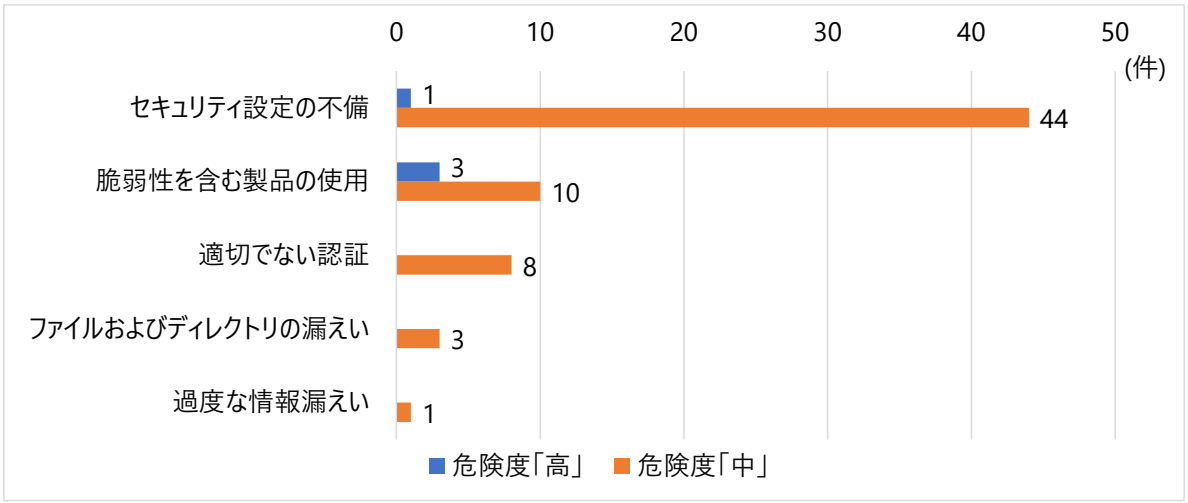


プラットフォーム診断における危険度別にみた企業の割合 (診断対象企業 50 社)

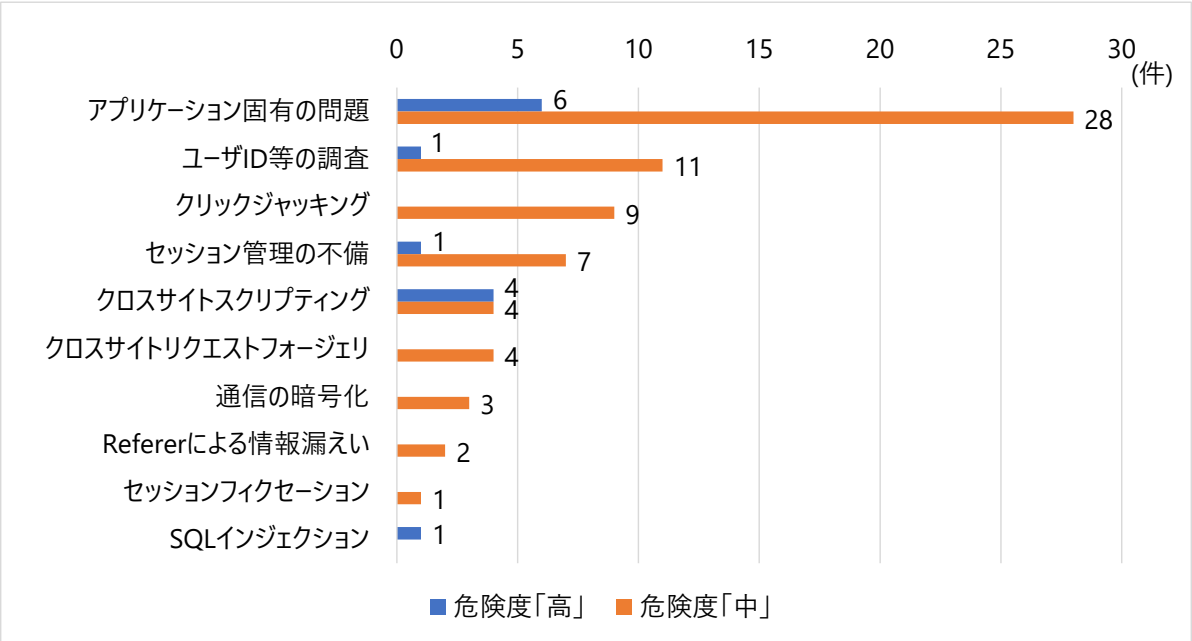
Web アプリケーション診断及び、プラットフォーム診断について、危険度「高」「中」ごとの検出件数が多い脆弱性のカテゴリを以下に示します。なお、脆弱性診断を実施した事業者は 2 社あり、診断事業者によって、脆弱性のカテゴリが異なることから、診断事業者ごとに、脆弱性カテゴリ別の検出件数を示します。



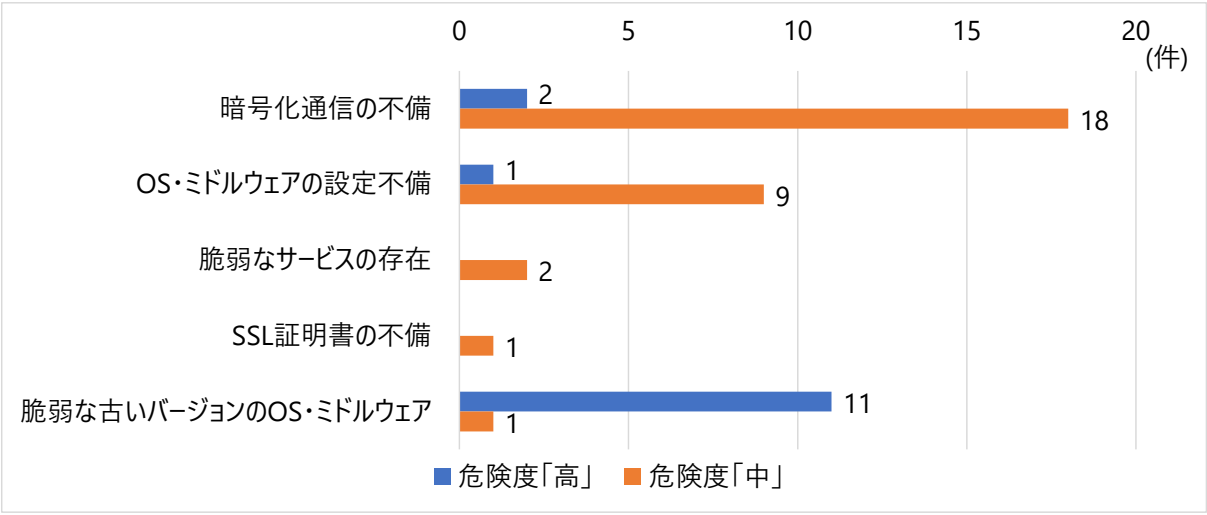
Web アプリケーション診断における延べ検出数上位の脆弱性カテゴリ
（診断事業者 A が実施した診断対象企業 20 社の集計結果）



プラットフォーム診断における延べ検出数上位の脆弱性カテゴリ
（診断事業者 A が実施した診断対象企業 20 社の集計結果）



Web アプリケーション診断における延べ検出数上位の脆弱性カテゴリ
（診断事業者 B が実施した診断対象企業 30 社の集計結果）



プラットフォーム診断における延べ検出数上位の脆弱性カテゴリ
（診断事業者 B が実施した診断対象企業 30 社の集計結果）

付録 3. 契約関係書類のひな形

このひな形は、外部委託先との契約にあたって仕様書の一部として組み込んで利用するためのものです。
対象サーバ の範囲など、自社の構築内容に沿って内容は変更してください。
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、構築時点で提供されているセキュリティパッチを適用（適用するパッチはシステムへの影響等を考慮して判断）すること。対象となるサーバは以下のとおり。

  【対象サーバ】　Web サーバ、DB サーバ等

- 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、利便性が著しく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】　Web サーバ、DB サーバ等

- 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、個人情報及び機密情報等の情報が出力されない様に出力する情報は考慮すること。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】　Web サーバ、DB サーバ等

- 外部に公開するサーバ（Web サーバ等）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】　Web サーバ等

- 外部に公開するサーバ（Web サーバ等）内に機密データ等を保持する場合については、情報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】　Web サーバ等

- 納入前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、検出さ

れた脆弱性等の対策を実施し、その結果をレポートにして提出すること。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（Firewallや、ルータ等）に対する脆弱性診断）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】　Webサーバ、DBサーバ等

● 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】　Webサーバ等

付録 4. 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一覧－

要件No	セキュリティ対策要件（構築時）	区分	自社で対応可能な要件	外部委託先の活用で対応すべき要件
1	「安全なウェブサイトの作り方」及び「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。	必須		
2	サーバ及び管理端末等で利用しているソフトウェアをセキュリティパッチ等により最新の状態にする。	必須		
3	EC サイトの公開前に脆弱性診断を行い、見つかった脆弱性を対策する。	必須		
4	管理者画面や管理用ソフトウェアへ接続する端末を制限する。	必須		
5	管理者画面や管理用ソフトウェアへ接続する端末のセキュリティ対策を実施する。	必須		
6	クレジット取引セキュリティ対策協議会が作成する「クレジットカード・セキュリティガイドライン」を遵守する。	必須		
7	サイト利用者情報の登録時及びパスワード入力時における、不正ログイン対策を実施する。	必須		
8	サイト利用者の個人情報に対して安全管理措置を講じる。	必須		
9	ドメイン名の正当性証明と TLS の利用を行う。	必須		
10	サイト利用者のログイン時における二要素認証を導入する。	必要		
11	サイト利用者のパスワードの初期化及び変更といった重要な処理を行う際、サイト利用者へ通知する機能を導入する。	必要		
12	Web サーバや Web アプリケーション等のログや、取引データ等のバックアップデータを保管する。	必要		
13	保管するログやバックアップデータを保護する。	推奨		
14	サーバ及び管理端末において、セキュリティ対策を実施する。	推奨		

※赤枠部分は、自社で対応困難な場合にチェックを入れます。チェックが入ったセキュリティ対策要件は、外部委託先の活用により対策を実施してください。

付録 5. 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一覧－

要件No	セキュリティ対策要件（運用時）	区分	自社で対応可能な要件	外部委託先の活用で対応すべき要件
1	サーバ及び管理端末等で利用しているソフトウェアをセキュリティパッチ等により最新の状態にする。	必須		
2	EC サイトへの脆弱性診断を定期的及びカスタマイズを行った際に行い、見つかった脆弱性を対策する。	必須		
3	Web サイトのアプリケーションやコンテンツ、設定等の重要なファイルの定期的な差分チェックや、Web サイト改ざん検知ツールによる監視を行う。	必須		
4	システムの定期的なバックアップの取得及びアクセスログの定期的な確認を行い不正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。	必要		
5	重要な情報はバックアップを取得する。	必要		
6	WAF を導入する。	推奨		
7	サイバー保険に加入する。	推奨		

※赤枠部分は、自社で対応困難な場合にチェックを入れます。チェックが入ったセキュリティ対策要件は、外部委託先の活用により対策を実施してください。

参考資料

参考資料 1. クレジットカード・セキュリティガイドライン

【作成主体】

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）

【情報収集先のサイト】

https://www.j-credit.or.jp/security/document/index.html

参考資料 2. 安全な Web サイトの作り方

【作成主体】

独立行政法人情報処理推進機構

【情報収集先のサイト】

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

参考資料 3. Web システム／Web アプリケーションセキュリティ要件書

【作成主体】

特定非営利活動法人日本ネットワークセキュリティ協会の日本セキュリティオペレーション事業者協議会のセキュリティオペレーションガイドライン WG（WG1）と、OWASP Japan 主催の共同ワーキンググループ

【情報収集先のサイト】

https://github.com/OWASP/www-chapter-japan/tree/master/secreq

参考資料 4. 中小企業の情報セキュリティ対策ガイドライン

【作成主体】

独立行政法人情報処理推進機構

【情報収集先のサイト】

https://www.ipa.go.jp/security/keihatsu/sme/guideline/

参考資料 5. EC サイトへの不正アクセスに関する実態調査

【作成主体】

個人情報保護委員会

【情報収集先のサイト】

https://www.ppc.go.jp/files/pdf/ecsite_report.pdf

EC サイト構築・運用セキュリティガイドライン
2023 年 3 月

独立行政法人 **情報処理推進機構**
〒113-6591
東京都文京区本駒込二丁目 28 番 8 号文京グリーンコートセンターオフィス
URL https://www.ipa.go.jp
電話 03-5978-7527　　FAX 03-5978-7552
E-mail vuln-inq@ipa.go.jp