Sec01-02-10 ウェブサイト開設等における運営形態の選定方法に関する手引き

|  |
| --- |
| **Hyperlinks:** |
| <https://www.ipa.go.jp/files/000066952.pdf> |

# 改版履歴

|  |
| --- |
|  |

## 2020年5月14日　加筆訂正

# 【2018年5月IPA】

|  |
| --- |
|  |

# はじめに （Executive Summary

# 対象読者と活用範囲

## ウェブサイトの運営者を主な対象読者としている。ウェブサイトの運営にあたっては、経営者、企画者、開発者、運用管理者等がそれぞれの立場で関与することになる。

## 自組織でウェブサイトを構築する際に組織の内情や実施可能なセキュリティ対策、セキュリティインシデント発生時の対応可能範囲等をもとに運営形態を選定する他、ウェブサイトの構築を外部委託するケースでは、運営形態に応じて必要となるセキュリティ対策項目の選定と発注要件の決定に活用して頂くことも想定している。

# ウェブサイト運営のライフサイクル

|  |
| --- |
|  |

## 1.企画

|  |
| --- |
|  |

## 2.設計

## 3.実装/構築

## 4.テスト

## 5.運用/利用

|  |
| --- |
|  |

## 6.廃棄

# ウェブサイト運営形態の選定の重要性

|  |
| --- |
|  |

# 各章節の想定読者

## 経営者：ウェブサイトの運営方針や、組織としてのセキュリティの全体的な方針を決定する者を指す。

## ウェブサイト企画者：ウェブサイトで提供するコンテンツや、サービス,具体的なセキュリティ方針を企画・決定する立場の者を指す。

|  |
| --- |
|  |

## ウェブサイト開発者：ウェブサーバの構築や、ウェブアプリケーションの開発、方針に従ったセキュリティ対策の実装に携わる者を指す。

## ウェブサイト管理者：構築されたウェブサイトを保守・運用管理する立場の者を指す。

|  |
| --- |
|  |

# 1. ウェブサイトの運営形態について

## 表1-1 運営形態の分類と説明

|  |
| --- |
|  |

### モール

### ASP SaaS 型クラウドサービス

|  |
| --- |
|  |

### PaaS 型クラウドサービス レンタルサーバ

### IaaS 型クラウドサービス

|  |
| --- |
|  |

### ハウジング

### オンプレミス

|  |
| --- |
|  |

## 1.1. 様々な運営形態が登場した背景

|  |
| --- |
|  |

## 1.2. 各運営形態の特徴

|  |
| --- |
|  |

### 運営形態を検討、選定する上で、選定を判断する観点や指標

|  |
| --- |
|  |

#### ①機能：計画しているウェブサイトの機能を満たせるか、機能の自由度はどれだけあるか

|  |
| --- |
|  |

#### ②期間：開設までに要する期間（工数）、サービスインの計画との整合性

#### ③調達：運営するために調達が必要となる物理環境、機材、ソフトウェア等

|  |
| --- |
|  |

#### ④体制：開設、運営していくのに必要となる人的資源、体制

|  |
| --- |
|  |

#### ⑤費用：開設での一次費用、運用における経年費用、トータル費用等

#### ⑥セキュリティ：安全な運用を維持するために対応すべきセキュリティ対策

### 表1-2-1 運営形態毎の選定項目の比較

|  |
| --- |
|  |

#### ①ウェブサイトの機能の自由度

#### ②ウェブサイト開設までの日数

|  |
| --- |
|  |

#### ③ウェブサイト開設のため調達が必要な物品数

#### ④ウェブサイト開設・運営に必要な人的資源

|  |
| --- |
|  |

#### ⑤-1ウェブサイト開設に必要な費用

|  |
| --- |
|  |

#### ⑤-2ウェブサイトの維持・運営に必要な費用

|  |
| --- |
|  |

#### ⑥検討が必要なセキュリティ対策項目

|  |
| --- |
|  |

### 1.2.1 モール、ASP、SaaS 型クラウドサービスの特徴

#### 表1-2-2 モール、ASP、SaaS でのメリットとデメリット

|  |
| --- |
|  |

### 1.2.2 PaaS 型クラウドサービス、レンタルサーバ、IaaS 型クラウドサービスの特徴

|  |
| --- |
|  |

#### 表1-2-3 PaaS、レンタルサーバ、IaaS でのメリットとデメリット

### 1.2.3 ハウジング、オンプレミスの特徴

#### 表1-2-4 ハウジング、オンプレミスでのメリットとデメリット

### 1.2.4 業種による利用傾向

|  |
| --- |
|  |

#### ウェブサイトで公開されている各運営形態の情報27を参照すると、

#### ASP やモールの運営形態を選ぶ場合は、

##### ウェブサイト運営サービスに付加される別のサービスを利用できることが選定の理由として挙げられていた。サーバの構築や運営の技術を持たない個人商店や中小企業等の利用が多くみられ、そういった企業がEC サイトを出店する際に、サポートサービスのEC サイト経営の相談サービス等が提供されていることを選定の基準にしているとのコメントが見られた。

|  |
| --- |
|  |

#### レンタルサーバやクラウドの場合は、

|  |
| --- |
|  |

##### ASP やモールと異なり独自のドメインを取得するサービスが提供されており、企業紹介のウェブサイトを導入する際に利用されているようである。選定の理由として挙げられているのは導入するサービスや使用するソフトウェアを自由に選択できる点である28。機材管理の工数が必要ないこと、サービスの提供開始までに要する時間が短いこと、特にクラウドの場合は処理性能等のスケーラビリティが確保されていることがある。

# 2. 各運営形態の選定に向けたアプローチ

|  |
| --- |
|  |

## 2.1. 運営形態の選定のアプローチについて

|  |
| --- |
|  |

### 図2-1-1 実現したい目的を優先した観点における選定フロー

|  |
| --- |
|  |

### 図2-1-2 運用・維持を優先した観点における選定フロー

|  |
| --- |
|  |

#### 判断基準

|  |
| --- |
|  |

##### 1.システム構築体制

|  |
| --- |
|  |

##### 2.アプリ開発体制

|  |
| --- |
|  |

##### 3.運用保守体制

|  |
| --- |
|  |

##### 4.セキュリティ対策維持管理体制

|  |
| --- |
|  |

## 2.2. 運営形態毎の自由度

### 図 2-2-1 ASP やレンタルサーバでのウェブサイト運営

|  |
| --- |
|  |

### 図 2-2-2 オンプレミスのウェブサイト運営

## 2.3. 運営形態毎に調達が必要となる機材

|  |
| --- |
|  |

### 表 2-3-1 運営形態毎に調達が必要な機材

|  |
| --- |
|  |

### サーバ室

|  |
| --- |
|  |

### 電源管理

|  |
| --- |
|  |

### ネットワーク回線

|  |
| --- |
|  |

### サーバ、OS

|  |
| --- |
|  |

### ミドルウェア

|  |
| --- |
|  |

### ウェブアプリケーション

|  |
| --- |
|  |

### コンテンツ

|  |
| --- |
|  |

## 2.4. 運営形態毎に発生する費用項目

|  |
| --- |
|  |

### 表2-4-1 運営形態毎に必要となる費用

|  |
| --- |
|  |

### サーバ室の整備費用

|  |
| --- |
|  |

### ネットワーク回線の敷設費用

|  |
| --- |
|  |

### ネットワーク機器の購入費用

|  |
| --- |
|  |

### サーバの購入費用

|  |
| --- |
|  |

### ウェブアプリケーションの開発費用・購入費用

|  |
| --- |
|  |

### ウェブサーバの構築費用

|  |
| --- |
|  |

### ウェブサイトの運用管理費用

|  |
| --- |
|  |

### サービス利用費用、課金

|  |
| --- |
|  |

## 2.5. 運営形態毎の責任範囲

### 表2-5-1 運営形態毎の責任範囲

|  |
| --- |
|  |

### サービスの停止

|  |
| --- |
|  |

### データの破壊・消去

|  |
| --- |
|  |

### 情報漏洩

|  |
| --- |
|  |

### 改ざん

## 【コラム】 「契約の免責事項

|  |
| --- |
|  |

### メンテナンスまたは不慮の事故等により、サービス停止等によるサービス利用者の逸失利益や損害について、提供者は一切の責任を負わないものとする

|  |
| --- |
|  |

### 不測の事故等により、サービス利用者のサーバ上に蓄積されているデータが喪失、流失、損壊等が発生した場合、提供者は一切の責任を負わないものとする

|  |
| --- |
|  |

## 2.6. 各運営形態で検討が必要なセキュリティ対策

|  |
| --- |
|  |

### 表2-6-1 運営形態毎に検討すべきセキュリティ対策

|  |
| --- |
|  |

### セキュリティ対策項目

|  |
| --- |
|  |

#### システムセキュリティ対策

|  |
| --- |
|  |

##### 技術的対策

###### 物理

|  |
| --- |
|  |

・サーバ室

|  |
| --- |
|  |

・入退管理

|  |
| --- |
|  |

###### ネットワーク

|  |
| --- |
|  |

・FW　・IDS/IPS

|  |
| --- |
|  |

・WAF ・VPN

|  |
| --- |
|  |

・ウイルス対策製品

|  |
| --- |
|  |

・サンドボックス型製品

|  |
| --- |
|  |

・DDoS対策

|  |
| --- |
|  |

###### アプリケーション

・改ざん検知

・認証　・アクセス制御

|  |
| --- |
|  |

・データ保護

|  |
| --- |
|  |

##### 運用管理的対策

|  |
| --- |
|  |

###### セキュリティパッチ

|  |
| --- |
|  |

・パッチ適用

|  |
| --- |
|  |

・仮想パッチ適用

|  |
| --- |
|  |

###### 監視

|  |
| --- |
|  |

・ログ収集、分析

|  |
| --- |
|  |

###### インシデント対応

|  |
| --- |
|  |

・バックアップ

・切り分け ・抜線

|  |
| --- |
|  |

##### 人的対策

|  |
| --- |
|  |

###### 要員教育

|  |
| --- |
|  |

・ポリシー教育

|  |
| --- |
|  |

・技術教育

|  |
| --- |
|  |

#### 業務セキュリティ対策

|  |
| --- |
|  |

##### 社員教育

|  |
| --- |
|  |

###### ・リテラシー教育

|  |
| --- |
|  |

##### ユーザ・顧客管理

|  |
| --- |
|  |

###### ・ポリシー教育

|  |
| --- |
|  |

###### ・情報取扱い規則

|  |
| --- |
|  |

##### コンテンツ管理

|  |
| --- |
|  |

###### ・コンテンツ更新ルール

|  |
| --- |
|  |

## 【コラム】 「既知の脆弱性が存在するウェブサイトに関する届出」

# 3. セキュリティ対策要件および強化のポイント

|  |
| --- |
|  |

## 各セキュリティ対策が、どのような要件を満たすべきか、どの程度の強度レベルを必要とするか、等については、構築するウェブサイトにおいて実現する機能やサービスや事業モデルによって、大きく異なってくる。

|  |
| --- |
|  |

## 3.1. 実現する機能、サービスに対する考慮のポイント

### 3.1.1 企業等の組織が公開するウェブサイトでのポイント

|  |
| --- |
|  |

#### 改ざんされることで、サイト利用者が不利益を被る場合が考えられる。また、偽の情報を掲載されてしまったことで、サイト運営者の信用失墜が発生する。

#### ウェブサイト改ざんの被害は、運営組織の大小や掲載されている情報の内容によらず、事業継続の大きな障害となりうる。このことから、「我社のウェブサイトには漏洩して問題がある情報はない」というケースにおいても、簡単に安心することはできない。

|  |
| --- |
|  |

#### 改ざん被害にあわないためには、ウェブサイトで使用しているソフトウェアを常に最新の状態に保つことが、第一の対策となる。

#### モールやASP の運営形態

|  |
| --- |
|  |

##### ソフトウェアのアップデートはサービス提供者が実施する対策

|  |
| --- |
|  |

##### サービス提供者を選定する段階で、外部機関によるペネトレーションテストを定期的に実施していたり、ウェブサイト改ざん検知の機能を提供していたりするサービス提供者を選択することが重要

|  |
| --- |
|  |

##### 例えば、「外部の●●社の脆弱性診断を毎年実施し、脆弱性が検出されないことを確認している」といった、明確な対策状況の回答が得られることが望ましい。

|  |
| --- |
|  |

### 3.1.2 EC サイトでのポイント

|  |
| --- |
|  |

#### EC サイト等では決済機能を提供するため、ウェブサイト上でクレジットカード情報や、口座情報等の取り扱いが必要である。万が一、EC サイトで不正アクセスや情報漏洩等が発生した場合、サイト利用者のみならず、関係している組織に対しても、重大な被害が発生する。

|  |
| --- |
|  |

#### ASP やモール、SaaS 型クラウドサービスを利用して運営する場合

|  |
| --- |
|  |

##### 決済機能を含む様々なプログラムはサービス提供者によって実装されるものである。そのため、サイト運営者による攻撃を検知するためのプログラムの実装や、脆弱性の修正等の管理をすることができない

|  |
| --- |
|  |

##### サービス提供者を選択する時点で、外部からの攻撃を検知・遮断するための監視システムを導入しているか、業界団体や政府機関が定めるセキュリティ基準に準拠した対策を行っているかについて調査する必要がある。

|  |
| --- |
|  |

##### 日本国内のサービス提供者であればPCI DSSへの準拠について確認が必須である38

###### PCI DSS は、国際クレジットカード国際カードブランド5 社が共同で設立したPCI SecurityStandards Council によって運用、管理されている基準であり、日本国内ではクレジットカード情報を自社内で取り扱う企業に対して、2018 年3 月までにPCI DSS へ準拠することが義務となっている。

|  |
| --- |
|  |

#### レンタルサーバやPaaS・IaaS 型のクラウドサービス、ハウジング、オンプレミスの運営形態の場合

|  |
| --- |
|  |

##### 決済機能はサイト運営者が何らかの形で導入する必要がある。たとえば、自組織で決済機能を開発する方法や、クレジットカード会社が提供するサービスを利用するといった方法が考えられる。

|  |
| --- |
|  |

##### ウェブサイトに独自に決済機能を開発する場合、自組織内で機微な情報を取り扱う必要が発生する。

|  |
| --- |
|  |

##### これによりPCI DSS 準拠へのセキュリティ対策・維持の負荷が増大するため、外部の決済代行会社に決済機能を委託することで、サイト運営者の負担を軽減することも一考である。

|  |
| --- |
|  |

サイト運営者は悪意ある第三者がサイト利用者になりすまして商品の購入や、他者の決

##### 済情報を盗み取ることができないようにすることも必要である。

|  |
| --- |
|  |

##### 正規の利用者になりすまして情報を盗み取る場合、正規のサイト利用者と攻撃者を識別することが困難である。

|  |
| --- |
|  |

###### なりすましの被害を受ける原因

|  |
| --- |
|  |

1. 簡単で短いパスワードを設定していた

|  |
| --- |
|  |

2. 個人情報から類推しやすいパスワードを設定していた

|  |
| --- |
|  |

3. 他のウェブサービスで同じパスワードを設定していた

|  |
| --- |
|  |

###### なりすましを防ぐためには、3.2 節で説明するサイト運営者側の対策だけでなく、サイト利用者に対して簡単なパスワードの禁止やパスワードの使いまわしをしないこと等の啓発が必要である。

|  |
| --- |
|  |

### 3.1.3 SNS サイトや掲示板サイト等でのポイント

|  |
| --- |
|  |

#### 悪意ある書き込みや改ざんには十分留意する必要がある。

|  |
| --- |
|  |

#### 例えば、クロスサイト・スクリプティングの脆弱性の場合

|  |
| --- |
|  |

##### 攻撃者がスクリプトを含む内容を投稿することで偽の情報を表示されてしまう。このような被害を防ぐために、投稿される内容にスクリプトが含まれていれば、ウェブサイト上にそのまま出力しないよう特定の記号はエンコードして表示する必要がある。

|  |
| --- |
|  |

#### クロスサイト・リクエスト・フォージェリの脆弱性がある場合

##### サイト利用者が意図しない操作を実行させられてしまう可能性が存在し、結果的に登録情報の書き換えや、意図しない内容を投稿させられてしまうといった被害につながる。

|  |
| --- |
|  |

##### これを防ぐために、登録情報の変更等の重要な処理の際にはパスワードの再入力を求めることや、外部のウェブサイトから転送された通信であるか調査する機能を実装する等の対策が必要である。

|  |
| --- |
|  |

#### この他の攻撃

|  |
| --- |
|  |

##### 他者のセッションを乗っ取り、他人になりすまして記事を投稿する等がある。その対策としては、攻撃者によるセッションID の推測や、被害者に任意のセッションID を使用させない（セッションID の固定をさせない）ウェブアプリケーションの設計にすることが必要である。

|  |
| --- |
|  |

### 3.1.4 画像投稿サイト等のファイルアップロードサイトでのポイント

#### 違法なファイルをアップロードされる以外にも、実行形式のファイルをアップロードされてしまうことにより、アップロードサイトのサーバ上で不正なファイルを実行されてしまう可能性がある。

#### このようなことが可能な場合、スクリプトを含むファイルをアップロードし、外部からそのファイルを参照することで、任意のスクリプトをサーバ上で実行されてしまう被害が考えられる。

#### スクリプトを実行されることで、ウェブサイトの改ざんや、サーバの設定の改ざんにつながる可能性がある。

|  |
| --- |
|  |

#### また、ウイルスを含むファイルをアップロードされた場合、サーバにウイルスが感染し、外部から不正な命令を受け付けるようにされてしまう可能性もある。

|  |
| --- |
|  |

#### このようなリスクを回避するために、アップロード可能なファイル形式を制限するだけでなく、アップロードされたサーバ上でファイルのウイルスチェックを行う等の対策を講じることが必要である。

|  |
| --- |
|  |

#### また、特定のユーザ以外にアクセスを許可しないファイルが、誰でもURL を直接指定することで閲覧できてしまうといった、アクセス制限不備の問題が考えられる。

|  |
| --- |
|  |

#### このような脆弱性がある場合、アップロードされたファイルが不特定多数のサイト利用者から参照可能になってしまう。

|  |
| --- |
|  |

#### この場合、個人を特定できてしまう情報を含むファイルが、URL を直接指定するだけで参照できるといった被害が発生する。

|  |
| --- |
|  |

#### このような被害を防止するために、ファイルのアクセス制限を適切に設定することが求められる。

|  |
| --- |
|  |

## 3.2. セキュリティ強化のポイント

|  |
| --- |
|  |

### 技術的な対策の観点

|  |
| --- |
|  |

#### (1) ネットワーク攻撃、不正アクセス対策

|  |
| --- |
|  |

##### ・外部からの攻撃が発生しているかの把握（攻撃の検知等）

|  |
| --- |
|  |

###### Subtopic

##### ・外部からの攻撃からの防御（攻撃の遮断等）

|  |
| --- |
|  |

###### Subtopic

|  |
| --- |
|  |

#### (2) DDoS攻撃対策

|  |
| --- |
|  |

##### ・攻撃通信をネットワークに入れないためにどうするか

|  |
| --- |
|  |

#### (3) なりすまし対策

|  |
| --- |
|  |

##### ・パスワードの管理体制の強化

|  |
| --- |
|  |

##### ・使用する接続方式、認証方式の強化

|  |
| --- |
|  |

##### サイト利用者に普及・啓発すべき対策について以下で解説する。

|  |
| --- |
|  |

###### 長く複雑なパスワードを設定するようにサイト利用者に要求すれば

・パスワードを使いまわす可能性の増加

|  |
| --- |
|  |

・利便性の低下によるサイト利用者の減少

|  |
| --- |
|  |

###### その一つの答えとして、次に解説する二要素認証や二段階認証が存在する。

|  |
| --- |
|  |

#### (4) 重要情報の保護対策

|  |
| --- |
|  |

##### ・データベースをインターネット公開領域(いわゆるDMZ45)に配置しない

|  |
| --- |
|  |

##### ・重要情報の暗号化

|  |
| --- |
|  |

##### ・情報を変更、参照する際の再認証

|  |
| --- |
|  |

##### 重要情報の暗号化について

|  |
| --- |
|  |

##### ウェブサイトに登録した情報を変更、参照する際の再認証の必要性について

|  |
| --- |
|  |

#### (5) 事業継続対策

|  |
| --- |
|  |

##### サーバ等の機材故障やインターネット上から攻撃を受けた場合にウェブサイトの停止期間を最小化するためには、事業継続計画（Business continuity planning）を検討する必要がある。

|  |
| --- |
|  |

##### 事業継続を目的とした対策には以下の２点等が存在

|  |
| --- |
|  |

###### ・予備システムを設置する

|  |
| --- |
|  |

###### ・バックアップを定期的に取得する

|  |
| --- |
|  |

##### ・予備システムを設置する

|  |
| --- |
|  |

###### インターネットからの攻撃が行われ、サーバが破壊されてしまった場合、データやサービスの復旧には長期間の作業が必要となる。このような場合に、破壊されたサーバと同一の構成の予備システムがあれば、ウェブサイト復旧までの時間を大幅に削減することが可能である。

|  |
| --- |
|  |

###### 注意すべき点として、予備システムを有効に活用するためには、主となるサーバと可能な限り同じデータを持ち、同一のソフトウェアバージョンに揃える必要がある。

|  |
| --- |
|  |

###### また、予備システムが主となるサーバとは別の拠点に設置されていれば、大規模な地域災害時への対策にも繋がる。

|  |
| --- |
|  |

###### 前述の予備システムを設置できない場合は、次に説明するバックアップの取得が重要になる。

##### ・バックアップを定期的に取得する

|  |
| --- |
|  |

###### インターネット上から攻撃を受け、ウェブサーバが破壊された際に、ウェブサーバや重要情報のバックアップを取得していればバックアップデータを元にウェブサイトを速やかに復旧することができる。

|  |
| --- |
|  |

###### 多くの場合、バックアップを取得するために専用のソフトウェアを購入する必要はなく、OS の機能としてバックアップを取得することができる。

|  |
| --- |
|  |

###### しかし、バックアップデータを取得していても、ウェブサーバ上に保管していれば、ウェブサーバが攻撃を受けた際に同時にバックアップデータも破壊されてしまう可能性がある。

|  |
| --- |
|  |

###### また、バックアップデータを盗まれることで、攻撃者が偽サイトを作成することを可能にしてしまうことも考えられる。サーバ上に保管していない場合でも、ネットワークに接続された端末に保管されていれば、ウイルスがネットワークに侵入した際にバックアップデータが破壊・窃取を受ける可能性がある。

|  |
| --- |
|  |

###### 以上の理由から、バックアップデータは外付けハードディスク等に保存し、ネットワークから切り離して保管しておくことが望ましい。

|  |
| --- |
|  |

### その他の対策の観点

|  |
| --- |
|  |

#### (1) ログの収集、分析

|  |
| --- |
|  |

#### (2) 各種基準への準拠

|  |
| --- |
|  |

##### 近年では、ウェブサイトへの攻撃による被害に対応した保険商品等が提供されている。しかし、このような保険に加入する場合は、保険企業やセキュリティ関連組織等が定める基準に準拠したウェブサイト運用が行われていることが条件となっている場合が多い。

|  |
| --- |
|  |

##### また、ウェブサイトの性質やウェブサイト上で取り扱う情報によっては、所轄官庁が取り扱いの基準を定めている場合がある。

##### 国内であれば、経済産業省やNISC46、海外であればNIST47等の公的機関がセキュリティ要件について様々なガイドラインや基準を定めている。

|  |
| --- |
|  |

##### サービス提供者を選択する際に注意すべき点として、以下の２点を挙げる。

|  |
| --- |
|  |

###### ・関係する団体が定める必須のセキュリティ基準を満たしているか

|  |
| --- |
|  |

EC サイト等の決済機能を有するウェブサイトであれば、使用する決済機能を提供する企業や、業界団体が定めるセキュリティ基準基準を満たしているかについて確認が必要である。

|  |
| --- |
|  |

代表例として、PCI DSS がある。3.1.2 項でも解説した通り、国内でクレジットカードの決済機能を導入する場合は、PCI DSS に準拠することが求められる。

|  |
| --- |
|  |

この他に、サイト運営者が所属する業界や団体が定めるセキュリティ基準がないか確認し、その基準を満たしているサービス提供者を選択すべきである。

|  |
| --- |
|  |

###### ・必須ではないが、自発的にセキュリティ基準に則った対策を実施しているか

|  |
| --- |
|  |

サービス提供者が自発的に何らかの基準に従ったセキュリティ対策を実施しているか、という観点で選択を行うべきである。

|  |
| --- |
|  |

サービス提供者が自発的に何らかの基準に従ったセキュリティ対策を実施しているか

|  |
| --- |
|  |

一例をあげると、モールやASP のサービス提供者を選択する場合であれば、総務省が定めた「ASP・SaaS における 情報セキュリティ対策ガイドライン」に準拠しているか、といった観点で確認することが考えられる。

|  |
| --- |
|  |

これは、ASP やSaaS のサービス提供者に対し、実施すべきセキュリティ対策について解説した資料である。

|  |
| --- |
|  |

着目すべき基準については、ウェブサイトのサービス内容や運営形態によっても変わるため、サイト運営者自身で調査することが必要である。

|  |
| --- |
|  |

#### (3) セキュリティ専門事業者の活用

|  |
| --- |
|  |

##### 情報セキュリティを専門としない組織が独自に脆弱性診断や脆弱性対策を行うことは困難と考えられる。そのため、脆弱性の検査を行う情報セキュリティ専門の企業による診断を受けることが望ましい。

|  |
| --- |
|  |

##### レンタルサーバ等では、サーバの構築をサイト運営者自身で行う必要がある。

|  |
| --- |
|  |

##### また、サイト運営者によっては、使用するウェブアプリケーションを独自に開発する場合もあり、サーバや独自開発のウェブアプリケーションに脆弱性を作りこんでいないか、十分に検査する必要がある。

|  |
| --- |
|  |

##### しかしながら、サイト運営者自身で脆弱性の検査を十分に行うことは困難であると考えられる。

|  |
| --- |
|  |

##### 特にハウジングやオンプレミスによる運営形態では、サーバだけでなくネットワーク機器等にも脆弱性がないか調査する必要がある。

|  |
| --- |
|  |

##### このような場合には、脆弱性の検査を専門としたセキュリティ企業に、サーバやウェブアプリケーションの脆弱性検査の委託を検討する必要がある。セキュリティ専門企業については、経済産業省が「情報セキュリティ監査企業台帳」を公開している。

|  |
| --- |
|  |

#### (4) サービス終了時の情報の破棄

##### サーバの機器故障やウェブアプリケーションの老朽化、事業方針の変更等により、ウェブサイトの運用の終了や、次期システムへ移行する時期が訪れる。

|  |
| --- |
|  |

##### このような際に適切にデータの破棄が行われていない場合、ハードウェアを取得した第三者によって重要情報が盗み取られる被害が想定される。このような被害を防ぐため、重要情報や情報記録媒体の破棄について対応を検討しておく必要がある。

|  |
| --- |
|  |

##### モールやASP、レンタルサーバ等ではウェブサイトのプログラムのみならず、サイト利用

##### 者の個人情報についても、サービス提供者の管理するサーバ上で管理される。そのため、ウェブサイトの運営を終了し、ASP 等の利用契約を解除する際、データの破棄・消去をサービス提供者がどのように取り扱いしているかについて、サービス提供者の選択時に確認する必要がある。

|  |
| --- |
|  |

##### 例えば、使用していたサーバのハードディスクの破壊について証明書を発行する、米国国防総省が定めるDoD 5220.22-M に従ったデータの消去を保証しているといった観点がある。

|  |
| --- |
|  |

##### 各組織がハードウェアを管理するオンプレミス等の運営形態の場合は、前述の規格に沿って組織内でデータの削除やハードディスクの破壊を実施、または専門業者に依頼しての実施を検討する必要がある。

|  |
| --- |
|  |

# おわりに

|  |
| --- |
|  |

## ウェブサイトで提供したいサービスや運営形態の手軽さだけでなく、日々の運営でセキュリティを維持し続けることができるかといった点についても目を向けて頂き、安全なウェブサイトの運営が可能な運営形態を選定するようにしてほしい。

|  |
| --- |
|  |

# 補足資料

|  |
| --- |
|  |

## 【補足1】ウェブサイト構築・運営の委託について

|  |
| --- |
|  |

### 中小企業をはじめとして、ウェブサイトの構築や運営を外部企業に委託する場合が数多く存在している。ASP やモールの運営形態が目的と合致せず、自組織内でウェブサイトを作成する技術がない場合は正しい選択である。

### しかしながら、外部企業にウェブサイトの構築を委託した際、契約内容にウェブサイトの脆弱性検査や運用開始後に脆弱性が見つかった場合の対応が盛り込まれておらず、脆弱性を抱えたままコンテンツの更新だけが行われているウェブサイトが存在しており、IPA に対して届出が行われている。

|  |
| --- |
|  |

### このようなウェブサイトを運営するサイト運営者に脆弱性の連絡を行った際、組織内で修正できないためウェブサイトを構築した企業に依頼する場合がある。

### しかし、修正のための追加費用が発生してしまうことが原因で対応が行われないという事態が発生している。

### ウェブサイトに存在する脆弱性への対応は組織毎に判断すべき内容であるが、重大な問題を抱えたまま運営し、個人情報の流出等が発生する場合もあるため、可能な限り脆弱性は解消することが望ましい。

|  |
| --- |
|  |

### 前述したような事例となることを避けるために、ウェブサイト構築・運営を委託する際には、契約する際の項目に脆弱性の検査や脆弱性が見つかった場合の対応を明確に記載することが望ましいといえる。

|  |
| --- |
|  |

## 【補足2】ログの取得について

|  |
| --- |
|  |

### ログイン履歴

|  |
| --- |
|  |

### アクセスログ

|  |
| --- |
|  |

### 通信ログ

### ログを取得する際は以下の点に注意する

|  |
| --- |
|  |

#### ①意図しないログが残っていないか調査する

|  |
| --- |
|  |

#### ②取得場所以外の場所にログを保存する

|  |
| --- |
|  |

## 【補足3】バックアップの取得間隔について

|  |
| --- |
|  |

### 実際にバックアップの取得期間をどのように設定するべきかについては、ウェブサイトの運用計画を定める段階で、ウェブサイトの目的や更新頻度等からどれぐらいの期間のデータの喪失を許容できるかといった観点で定めることが必要である。

# 【付録A】ウェブサイト構築・運営に関する参考資料

|  |
| --- |
|  |

## 「ウェブサイト構築のライフサイクル」の各フェーズで参考となる資料を一覧にまとめた表である。

|  |
| --- |
|  |

## 1.企画

|  |
| --- |
|  |

### 1 情報セキュリティ10 大脅威 2018

#### https://www.ipa.go.jp/security/vuln/10threats2018.html

|  |
| --- |
| **Hyperlinks:** |
| <https://www.ipa.go.jp/security/vuln/10threats2017.html> |

#### IPA

|  |
| --- |
|  |

### 2 情報セキュリティ白書

|  |
| --- |
|  |

#### https://www.ipa.go.jp/security/publications/hakusyo/2017.html

|  |
| --- |
|  |

|  |
| --- |
| **Hyperlinks:** |
| <https://www.ipa.go.jp/security/publications/hakusyo/2017.html> |

#### IPA

|  |
| --- |
|  |

### 3 中小企業の情報セキュリティ対策ガイドライン

|  |
| --- |
|  |

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

|  |
| --- |
|  |

|  |
| --- |
| **Hyperlinks:** |
| <https://www.ipa.go.jp/security/keihatsu/sme/guideline/> |

#### IPA

|  |
| --- |
|  |

### 4　中小企業のためのクラウドサービス安全利用の手引き

|  |
| --- |
|  |

#### https://www.ipa.go.jp/security/cloud/tebiki\_guide.html

|  |
| --- |
|  |

|  |
| --- |
| **Hyperlinks:** |
| <https://www.ipa.go.jp/security/cloud/tebiki_guide.html> |

#### IPA

|  |
| --- |
|  |

### 5 ウェブサイト構築事業者のための脆弱性対応ガイド

|  |
| --- |
|  |

#### https://www.ipa.go.jp/security/fy20/reports/vuln\_handling/index.html

|  |
| --- |
|  |

|  |
| --- |
| **Hyperlinks:** |
| <https://www.ipa.go.jp/security/fy20/reports/vuln_handling/index.html> |

#### IPA

|  |
| --- |
|  |

### 6 セキュリティ担当者のための脆弱性対応ガイド

|  |
| --- |
|  |

#### https://www.ipa.go.jp/security/fy22/reports/vuln\_handling/index.html

|  |
| --- |
|  |

|  |
| --- |
| **Hyperlinks:** |
| <https://www.ipa.go.jp/security/fy22/reports/vuln_handling/index.html> |

#### IPA

|  |
| --- |
|  |

### 7 ソフトウエア管理ガイドライン

#### http://www.meti.go.jp/policy/netsecurity/downloadfiles/softkanriguide.htm

|  |
| --- |
|  |

|  |
| --- |
| **Hyperlinks:** |
| <http://www.meti.go.jp/policy/netsecurity/downloadfiles/softkanriguide.htm> |

#### 経済産業省

|  |
| --- |
|  |

### 8 効果的なサイバー防御のためのCIS クリティカルセキュリティコントロール

|  |
| --- |
|  |

#### https://sans-japan.jp/resources/CriticalSecurityControls.html

|  |
| --- |
|  |

|  |
| --- |
| **Hyperlinks:** |
| <https://sans-japan.jp/resources/CriticalSecurityControls.html> |

#### Center For Internet Security

|  |
| --- |
|  |

### 9 事業継続計画策定ガイドライン

#### http://www.meti.go.jp/policy/netsecurity/secdoc/contents/seccontents\_000039.html

|  |
| --- |
|  |

|  |
| --- |
| **Hyperlinks:** |
| <http://www.meti.go.jp/policy/netsecurity/secdoc/contents/seccontents_000039.html> |

#### 経済産業省

|  |
| --- |
|  |

### 10 経営者が知っておくべきセキュリティリスクと対応について

|  |
| --- |
|  |

#### https://www.jpcert.or.jp/research/aptrisk.html

|  |
| --- |
|  |

|  |
| --- |
| **Hyperlinks:** |
| <https://www.jpcert.or.jp/research/aptrisk.html> |

#### Delta Risk Limited Liability Company

|  |
| --- |
|  |

### 11 システム開発ライフサイクルにおけるセキュリティの考慮事項

|  |
| --- |
|  |

#### https://www.ipa.go.jp/security/publications/nist/index.html

|  |
| --- |
|  |

|  |
| --- |
| **Hyperlinks:** |
| <https://www.ipa.go.jp/security/publications/nist/index.html> |

#### 米国国立標準技術研究所

|  |
| --- |
|  |

### 12 データベースセキュリティガイドライン

|  |
| --- |
|  |

#### http://www.db-security.org/report/guideline\_seika.html

|  |
| --- |
|  |

|  |
| --- |
| **Hyperlinks:** |
| <http://www.db-security.org/report/guideline_seika.html> |

#### データベース・セキュリティ・コンソーシアム

|  |
| --- |
|  |

### 13 DB 内部不正対策ガイドライン

#### http://www.db-security.org/report/ag\_seika.html

|  |
| --- |
|  |

#### データベース・セキュリティ・コンソーシアム

### 14 Payment Card Industry（PCI）データセキュリティ基準 (PCI DSS)

|  |
| --- |
|  |

#### https://ja.pcisecuritystandards.org/minisite/env2/

|  |
| --- |
|  |

|  |
| --- |
| **Hyperlinks:** |
| <https://ja.pcisecuritystandards.org/minisite/env2/> |

#### PCI Security Standards Council

|  |
| --- |
|  |

### 15 連邦政府の情報および情報システムに対するセキュリティ分類規格

|  |
| --- |
|  |

#### https://www.ipa.go.jp/security/publications/nist/index.html

|  |
| --- |
|  |

|  |
| --- |
| **Hyperlinks:** |
| <https://www.ipa.go.jp/security/publications/nist/index.html> |

#### 米国国立標準技術研究所

|  |
| --- |
|  |

### 16 政府機関の情報セキュリティ対策のための統一基準（平成28 年度版）

|  |
| --- |
|  |

#### https://www.nisc.go.jp/active/general/kijun28.html

|  |
| --- |
|  |

|  |
| --- |
| **Hyperlinks:** |
| <https://www.nisc.go.jp/active/general/kijun28.html> |

#### 内閣サイバーセキュリティセンター

|  |
| --- |
|  |

## 2.設計

|  |
| --- |
|  |

### 17 ウェブサイト改ざんの脅威と対策

|  |
| --- |
|  |

#### https://www.ipa.go.jp/security/technicalwatch/20140829.html

|  |
| --- |
|  |

|  |
| --- |
| **Hyperlinks:** |
| <https://www.ipa.go.jp/security/technicalwatch/20140829.html> |

#### IPA

|  |
| --- |
|  |

### 18 Web Application Firewall 読本

|  |
| --- |
|  |

#### https://www.ipa.go.jp/security/vuln/waf.html

|  |
| --- |
|  |

|  |
| --- |
| **Hyperlinks:** |
| <https://www.ipa.go.jp/security/vuln/waf.html> |

#### IPA

|  |
| --- |
|  |

### 19 安全なウェブサイトの作り方

|  |
| --- |
|  |

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

|  |
| --- |
|  |

|  |
| --- |
| **Hyperlinks:** |
| <https://www.ipa.go.jp/security/vuln/websecurity.html> |

#### IPA

|  |
| --- |
|  |

### 20 攻撃者に狙われる設計・運用上の弱点についてのレポート

#### https://www.ipa.go.jp/security/technicalwatch/20140328.html

|  |
| --- |
|  |

#### IPA

|  |
| --- |
|  |

### 21 インシデント対応マニュアルの作成について

|  |
| --- |
|  |

#### https://www.jpcert.or.jp/csirt\_material/build\_phase.html

|  |
| --- |
| **Hyperlinks:** |
| <https://www.jpcert.or.jp/csirt_material/build_phase.html> |

#### JPCERT/CC

|  |
| --- |
|  |

### 22 情報資産の重み-対策レベル対応表

|  |
| --- |
|  |

#### http://www.db-security.org/report.html

|  |
| --- |
| **Hyperlinks:** |
| <http://www.db-security.org/report.html> |

#### データベース・セキュリティ・コンソーシアム

|  |
| --- |
|  |

### 23 DB セキュリティガイドライン-他フレームワーク対応表

#### http://www.db-security.org/report.html

|  |
| --- |
|  |

|  |
| --- |
| **Hyperlinks:** |
| <http://www.db-security.org/report.html> |

#### データベース・セキュリティ・コンソーシアム

### 24 ITシステムのためのリスクマネジメントガイド

|  |
| --- |
|  |

#### https://www.ipa.go.jp/security/publications/nist/index.html

|  |
| --- |
| **Hyperlinks:** |
| <https://www.ipa.go.jp/security/publications/nist/index.html> |

#### 米国国立標準技術研究所

|  |
| --- |
|  |

### 25 連邦情報システムのためのセキュリティ計画作成ガイド 改訂第1 版

|  |
| --- |
|  |

#### https://www.ipa.go.jp/security/publications/nist/index.html

|  |
| --- |
|  |

|  |
| --- |
| **Hyperlinks:** |
| <https://www.ipa.go.jp/security/publications/nist/index.html> |

#### 米国国立標準技術研究所

|  |
| --- |
|  |

## 3.実装/構築

|  |
| --- |
|  |

### 26 安全なウェブサイトの作り方

|  |
| --- |
|  |

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

|  |
| --- |
| **Hyperlinks:** |
| <https://www.ipa.go.jp/security/vuln/websecurity.html> |

#### IPA

|  |
| --- |
|  |

### 27 ウェブサイト改ざんの脅威と対策

|  |
| --- |
|  |

#### https://www.ipa.go.jp/security/technicalwatch/20140829.html

|  |
| --- |
| **Hyperlinks:** |
| <https://www.ipa.go.jp/security/technicalwatch/20140829.html> |

#### IPA

|  |
| --- |
|  |

### 28 攻撃者に狙われる設計・運用上の弱点についてのレポート

|  |
| --- |
|  |

#### https://www.ipa.go.jp/security/technicalwatch/20140328.html

|  |
| --- |
|  |

|  |
| --- |
| **Hyperlinks:** |
| <https://www.ipa.go.jp/security/technicalwatch/20140328.html> |

#### IPA

### 29 IPA セキュア・プログラミング講座

|  |
| --- |
|  |

#### https://www.ipa.go.jp/security/awareness/vendor/programming/

|  |
| --- |
|  |

|  |
| --- |
| **Hyperlinks:** |
| <https://www.ipa.go.jp/security/awareness/vendor/programming/> |

#### IPA

|  |
| --- |
|  |

### 30 ウェブサイトにおける脆弱性検査手法の紹介（ソースコード検査編）

|  |
| --- |
|  |

#### https://www.ipa.go.jp/security/technicalwatch/20140306.html

|  |
| --- |
|  |

|  |
| --- |
| **Hyperlinks:** |
| <https://www.ipa.go.jp/security/technicalwatch/20140306.html> |

#### IPA

### 31 CERT C コーディングスタンダード

|  |
| --- |
|  |

#### https://www.jpcert.or.jp/sc-rules/

|  |
| --- |
|  |

|  |
| --- |
| **Hyperlinks:** |
| <https://www.jpcert.or.jp/sc-rules/> |

#### JPCERT/CC

|  |
| --- |
|  |

### 32 連邦政府情報システムのためのセキュリティ管理策アセスメントガイド

|  |
| --- |
|  |

#### https://www.ipa.go.jp/security/publications/nist/index.html

|  |
| --- |
|  |

|  |
| --- |
| **Hyperlinks:** |
| <https://www.ipa.go.jp/security/publications/nist/index.html> |

#### 米国国立標準技術研究所

|  |
| --- |
|  |

## 4.テスト

|  |
| --- |
|  |

### 33 安全なウェブサイトの作り方

|  |
| --- |
|  |

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

|  |
| --- |
| **Hyperlinks:** |
| <https://www.ipa.go.jp/security/vuln/websecurity.html> |

#### IPA

|  |
| --- |
|  |

### 34 ウェブサイトにおける脆弱性検査手法(ウェブアプリケーション検査編)

|  |
| --- |
|  |

#### https://www.ipa.go.jp/security/technicalwatch/20160928-2.html

|  |
| --- |
|  |

|  |
| --- |
| **Hyperlinks:** |
| <https://www.ipa.go.jp/security/technicalwatch/20160928-2.html> |

#### IPA

|  |
| --- |
|  |

### 35 システム監査企業台帳

|  |
| --- |
|  |

#### http://www.meti.go.jp/policy/netsecurity/sys-kansa/

|  |
| --- |
|  |

|  |
| --- |
| **Hyperlinks:** |
| <http://www.meti.go.jp/policy/netsecurity/sys-kansa/> |

#### 経済産業省

|  |
| --- |
|  |

### 36 情報セキュリティ監査企業台帳

|  |
| --- |
|  |

#### http://www.meti.go.jp/policy/netsecurity/is-kansa/

|  |
| --- |
|  |

#### 経済産業省

|  |
| --- |
|  |

## 5.運用/利用

### 37 ウェブサイト運営者のための脆弱性対応ガイド

|  |
| --- |
|  |

#### https://www.ipa.go.jp/security/fy19/reports/vuln\_handling/index.html

|  |
| --- |
| **Hyperlinks:** |
| <https://www.ipa.go.jp/security/fy19/reports/vuln_handling/index.html> |

#### IPA

|  |
| --- |
|  |

### 38 インシデントハンドリングマニュアル

|  |
| --- |
|  |

#### http://www.jpcert.or.jp/csirt\_material/operation\_phase.html

|  |
| --- |
| **Hyperlinks:** |
| <http://www.jpcert.or.jp/csirt_material/operation_phase.html> |

#### JPCERT/CC

|  |
| --- |
|  |

### 39 CSIRT ガイド

|  |
| --- |
|  |

#### http://www.jpcert.or.jp/csirt\_material/operation\_phase.html

|  |
| --- |
|  |

|  |
| --- |
| **Hyperlinks:** |
| <http://www.jpcert.or.jp/csirt_material/operation_phase.html> |

#### JPCERT/CC

|  |
| --- |
|  |

# 【付録B】複数の観点による運営形態の選定 アプローチ

|  |
| --- |
|  |

## 図B-1 ウェブサイト構築時の観点に基づくフローチャート

|  |
| --- |
|  |

## 図B-2 ウェブサイト運用時の観点に基づくフローチャート

|  |
| --- |
|  |

## 図B-3 セキュリティインシデント発生時の観点から見たフローチャート

|  |
| --- |
|  |

## 図B-4 セキュリティインシデント対応体制構築の観点から見たフローチャート

|  |
| --- |
|  |