IPA Technical Watch

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
～組織の実情にあったウェブサイトを構築・運用するために～

2018 年 5 月

独立行政法人情報処理推進機構
技術本部 セキュリティセンター

内容

はじめに （Executive Summary）

今や企業や組織においてウェブサイトの利活用は、事業展開や重要な経営戦略の一部として機能している。特に EC サイトによるウェブ通販を生業としている組織においては、ウェブサイトの公開が停止すると収益に大きく影響してしまう。さらに、企業情報のみの公開で重要な情報は保有していないウェブサイトの場合でも、ウェブサイトの利用者にウイルスを配布するサイトに改ざんされてしまうといった被害が考えられる。このような被害が発生すれば、ウェブサイトの公開停止のみならず、企業や組織の信用失墜につながる。

このような状況の中、1990 年代以降、個人や企業を問わず安価なレンタルサーバサービスやクラウドサービスを利用することにより、サーバやネットワーク装置の購入をすることなくウェブサイトを構築することが可能となった。また、SaaS[1]型クラウドサービス等の登場により、ウェブアプリケーションを開発することなくウェブサイトを運営することも可能となっており、企業は容易にウェブサイトを開設できるが、運用管理について十分な検討を行わずウェブサイトを運用していると、先に述べたような被害が発生し、大きな損害へと繋がってしまう。

ウェブサイトを運営するためには、どのようなシステム形態で構築するか、どのような運用形態で管理していくか、の二つを決定することが重要であり、それには様々な形態の選択肢が存在している。本書では、この両者を合わせた形態を、ウェブサイトの「運営形態」と総称することとする。

現在では様々な組織がそれぞれの状況に合わせウェブサイトを構築・運営することができるようになった。しかしながら、ウェブサイトの運営形態に合わせたセキュリティ対策が認識されていないためか、IPA には運営形態を問わずウェブサイトの脆弱性について届け出が行われている。

ウェブサイトをどのような形態で運営するかによって、運営にかかる費用が変化するのはもちろん、運営者が実施する作業内容が異なるため、運営者に求められる技術レベルも変化する。また、運営形態毎にウェブサイト上でどのような機能を提供できるか、ウェブサイトをどこまで自由に変更できるか、どのようなセキュリティ対策が必要になるかについても異なる。特に企業のウェブサイトでは個人情報を取り扱うことも多く、サイト運営者はセキュリティが継続的に維持され、最新の脅威に対し対策が出来ているかどうかに気を配る必要がある。運営者はウェブサイトを構築する前に運営形態毎の特徴を理解し、組織の状況に応じた運営形態を選定する必要がある。

このような状況に対し、IPA にてそれぞれの運営形態がどのような特徴を持ち、セキュリティを維持する上で留意すべきかといった情報が公開されているか調査を行ったが、一般に公開された資料は確認できなかった。

[1] Software as a Service の略称

こうした背景を受け、本テクニカルウォッチでは、

- ウェブサイトの運営形態の種類と特徴
- 運営形態毎の選定のアプローチ方法
- 運営形態毎に検討が必要なセキュリティ上のポイント

を解説している。本書を**安全なウェブサイト構築・運営**を実現するための一助として役立ててもらいたい。

対象読者と活用範囲

本書は、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。特に開発者や運用管理者の体制や業務内容や工数を決定づけるのが、ウェブサイトの企画段階であり、一番重要なフェーズである。本書はその企画段階において、どのような選択肢があり、それぞれの特徴や長短比較等を詳細に解説して、組織の内情やウェブサイトの要件に合った検討や選択選定ができることを目的の一つとしている。

具体的な活用の方法としては、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。

また、一方で、既に構築、運用されているウェブサイトにおいて、どの運用形態が採用されているかを改めて省みて、その運用形態において、考慮しなくてはならないことが実施されているかを検証するためにも、参考にして頂くことを期待している。

本書では、１章で代表的なウェブサイト運営形態の特徴を解説し、２章で実際に運営形態の選定を行うためのアプローチ方法について解説している。どの運営形態がよいか検討したうえで考慮すべきセキュリティ対策について３章で紹介している。

ウェブサイト運営のライフサイクル

ウェブサイト運営のライフサイクルを本書では下記のように分類している[2]。本書は、後の工程にも大きく影響する「1. 企画」フェーズにおいて、ウェブサイトの運営形態の検討と選定を支援する情報を提示している。なお、他の工程の各フェーズにおいて参考となる資料やツールに関しては、【付録 A】に示すので、合わせて参照頂きたい。

1.企画	ウェブサイトを公開するにあたり、ウェブサイトにて提供したい内容および、機能について検討・決定するフェーズ
2.設計	「1. 企画」にて決定した内容を実現するために「3. 実装/構築」にて必要となる設計を行うフェーズ
3.実装/構築	「2. 設計」にて作成した内容をもとに基盤の構築、および、アプリケーションの作成を行うフェーズ
4.テスト	「3. 実装/構築」の成果物に対して、「2. 設計」で決定した内容で正しく動作するかを確認するフェーズ
5.運用/利用	ウェブサイトを公開し続けるために必要な保守管理や監視を行うフェーズ
6.廃棄	ウェブサイトの公開を停止し、システムやデータ、機器を適切な手段を用いて削除/破棄するフェーズ

ウェブサイト運営形態の選定の重要性

ウェブサイトの運営を開始しようとした場合、前述のライフサイクル「1.企画」の段階では、初めに以下の点を明確する必要がある。

- ウェブサイトの目的
- ウェブサイトにて提供するサービス

ウェブサイトでどのようなサービスを提供するかによって、選定できる運営形態が制限されてしまう場合が存在する。例えば、SaaS ではサービスの提供者が用意した機能しかウェブサイトでは提供できないため、独自の機能を実装することができない。

しかし、SaaS が提供する画面デザインや機能では、十分なサービスを提供できないなどの問題が生じる場合がある。このような問題を解決するためには、ウェブサイト運営者が独自に適切なインフラを調達することや、OS の選定、独自のウェブアプリケーションの開発等が必要になる。この場合では SaaS とは異なり、前述のライフサイクル「5.運用/利用」フェーズにおいてウェブサーバで使用するソフトウェアの管理等の業務が発生する。加えて、セキュリティ対策としてもソフトウェアの脆弱性検査やセキュリティパッチの適用といった業務が発生する。

[2] 本書では、ウェブサイトの運営に必要な業務をウェブサイト運営形態の選定から、ウェブサイトで使用した情報の廃棄までと位置付けている。

このように、ウェブサイトの企画が運営形態の選定やウェブサイトの保守管理といった後のフェーズの作業内容に密接に関係するため、企画の段階でどのようなサービスを提供するかを明確にするとともに、後続のフェーズでどのような作業が発生するか、その作業を誰がどのように対応するかについても想定しておく必要がある。その上で、作業分担に合致する運営形態を選定することが、安全なウェブサイト運営において極めて重要となる。

各章節の想定読者

本書の解説内容は多岐に渡るため、各節の想定読者を下記の表に示す。

想定読者 / 章・節		経営者	ウェブサイト企画者	ウェブサイト開発者	ウェブサイト管理者
1章					
	1.1	○	○	○	○
	1.2	○	○	○	○
2章					
	2.1	○	○	○	○
	2.2		○	○	○
	2.3		○	○	
	2.4		○	○	
	2.5		○	○	○
	2.6		○	○	○
3章					
	3.1			○	
	3.2			○	○

- 想定読者の役割
  - 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

本書におけるウェブサイトの運営形態について、ウェブサイトを運営するサーバやネットワーク基盤を、どのように調達・管理しているかによって分類したものである。本書では下記の表 1-1 の 6 種類の運営形態について解説する。

表 1-1　運営形態の分類と説明

運営形態	運営形態の説明	サービス提供者の例（注 1）
モール	ウェブサイトの公開に必要な機能や運用を一括してレンタルできる運営形態。 ASP 型のウェブサイトが複数集まって運営されている。	Amazon マーケットプレース[3] 楽天市場[4] Yahoo!ショッピング[5]
ASP SaaS 型クラウドサービス	ウェブサイトの公開に必要な機能や運用を一括してレンタルできる運営形態。 SaaS 型クラウドサービスでは ASP と比較して、性能の自由度が高い。	shopserve[6] salesforce.com[7] ASP i-do[8] MODD Web Service[9]
PaaS 型クラウドサービス レンタルサーバ(注２)	サービス提供者が管理するウェブサーバをレンタルする運営形態。 ハードウェアや OS 等のプラットフォームをレンタルすることができる。	さくらインターネット[10] GMO クラウド[11] NTT コミュニケーションズ[12] アマゾンウェブサービス[13]
IaaS 型クラウドサービス	サービス提供者が管理するハードウェアをレンタルする運営形態。 サーバやネットワークなどのインフラの性能を詳細に指定しレンタルすることができる。	IDC Frontier[14]
ハウジング	機器の設置場所と通信環境をレンタルし、サイト運営者が使用する機材を設置する運営形態。 ソフトウェアの導入やサーバの運用は各組織で実施する。	富士通[15] セコムトラストシステムズ[16]
オンプレミス	ネットワークやサーバを自社で用意し、自社の施設内で運用する運営形態。	―

- 用語の説明
  - サービス提供者：ウェブサイトを構築・運営するサービスを提供する組織
  - サイト運営者：サービス提供者のサービスを利用する等して、ウェブサイトを運営する組織

[3] Amazon マーケットプレース：https://services.amazon.co.jp/sell-on-amazon-marketplace.html
[4] 楽天市場：https://www.rakuten.co.jp/ec/
[5] Yahoo!ショッピング：https://business-ec.yahoo.co.jp/shopping/
[6] shopserve：https://sps.estore.jp/
[7] salesforce.com：https://www.salesforce.com/jp/
[8] ASP i-do：https://www.i-do.ne.jp/index.html
[9] MODD Web Service：https://www.modd.com/
[10] さくらインターネット：https://www.sakura.ad.jp
[11] GMO クラウド：https://private.gmocloud.com
[12] NTT コミュニケーションズ：http://www.ntt.com/index.html
[13] アマゾンウェブサービス：https://aws.amazon.com/jp/
[14] IDC Frontier：https://www.idcf.jp/
[15] 富士通：http://www.fujitsu.com/jp/
[16] セコムトラストシステムズ：http://www.secomtrust.net/

（注１）ホームページを確認した範囲での例を示したものであり、当該サービスが複数の運営形態を提供しているケースもある。
（注２）レンタルサーバの運営形態では、サービス提供者により PaaS[17]型クラウドサービスに近いサービス内容や、IaaS[18]型クラウドサービスに近いサービス内容である等様々なため、本書では PaaS 型クラウドサービスに近いサービスとして取り扱う。

本章では、ウェブサイト運営形態の概要について解説し、それぞれで検討が必要なセキュリティ対策について解説する。

1.1. 様々な運営形態が登場した背景

1993 年に HTML[19]ブラウザが開発[20]されたことで、世界的にインターネットの利用人口が増加した。

日本国内でネットワーク通信が使用されるようになったのは 1984 年[21]であり、インターネットの普及が始まったのは 1990 年頃である。当時は大学や企業単位でサーバが構築（オンプレミス）され、FTP[22]によるファイル転送や SMTP[23]によるメールの送信が主流であった。

その後、国内ではインターネット環境の整備や PC の普及により、1995 年頃からインターネット通販事業が行われるようになった[24]。これにより、個人や企業でウェブサイトを運営したいという需要が高まり、日本国内では 1996 年にレンタルサーバが登場したとされる。その一方で、1997 年頃から独自にサーバを構築することなく、インターネット通販ページを作成することができるサービスとして、ASP[25]や SaaS による EC サイト構築サービスが登場した。これは、インターネット利用者が増えたことにより、より小規模の組織でもウェブサイトを作成したいという要望が増加したためと考えられる。

2006 年頃からよりサイト運営者のニーズに合った規模で、より速やかにレンタルサービスを提供できる形として、クラウドサービスが世界的に提供されるようになった。特に、2006 年にはアマゾンウェブサービスの提供が始まり、よりサイト運営者のニーズに合わせた計算資源やネットワーク環境の調達が可能となった。これは、サーバを構成する CPU やメモリの性能が向上したこと、サーバの仮想化技術が進歩したことにより、それ以前と比較してクラウドサービスの提供が容易になったことが要因であると考えられる。また、ASP や SaaS では提供で

[17] Platform as a Service の略称
[18] Infrastructure as a Service の略称
[19] HyperText Markup Language の略称
[20] 90 年代の歴史的ブラウザ展示と "Web ブラウザ年表"最新版の配布：https://www.mozilla.jp/blog/entry/10547/
[21] JPNIC アーカイブス インターネット歴史年表：https://www.nic.ad.jp/timeline/
[22] File Transfer Protocol の略称
[23] Simple Mail Transfer Protocol の略称
[24] 日本のホスティング・マーケットの歴史と現状を探る：http://www.itmedia.co.jp/products/hyperbox/special/031215.html
[25] Application Service Provider の略称

きない、独自のサービスを提供したいというニーズが常に存在したこともクラウドサービスが発達した要因であると考えられる。

1.2. 各運営形態の特徴

ウェブサイトの開設にあたって、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は、以下の 6 項目が挙げられる。

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

これらの項目は、必ずしも単独ではなく、相関関係がある。ウェブサイトを公開する組織は、組織における予算や技術を加味して①～⑥に対応可能かを検討する必要がある。この検討結果によって運用形態の選択肢が自ずと絞られてくる。

運営形態についてこの６つの項目を検討する中で、①については自由度に関係するものであるため大きい（より優れている）ことが望まれるものだが、他の②～⑥はコストや工数を示すものであるためより小さい（もしくは少ない）ことが望まれる項目である。

各運営形態とこれらの項目からみた優劣の対応の比較を表 1-2-1 に示す。この表は典型的な概観や傾向を示しているものである。表が示すように、ASP や SaaS 型クラウドサービスによって提供されるサービスを活用することで、ウェブサイトの運用ができればサイト運営者の負担は軽減されるが、逆にウェブサイトで提供できる機能は、サービス提供者によって提供もしくは追加が許容される範囲に限られる。また、⑤の維持・運営に必要な費用（ランニングコスト）については、サービスのレベルで費用に幅があることと、自前のウェブサイトであればサーバやアプリケーションには費用発生はなくとも保守や運用体制にコストが生じる等複雑であるので、一般的な傾向を示しているものである。

表 1-2-1　運営形態毎の選定項目の比較

項目番号	ウェブサイト開設・運営に関わる項目 ＼ 運営形態		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		補足事項
①	ウェブサイトの機能の自由度	低									高	(注1) ECサイトの場合、月々の売上の一部が維持費用に課金される場合がる。
②	ウェブサイト開設までの日数	短									長	
③	ウェブサイト開設のため調達が必要な物品数	少									多	
④	ウェブサイト開設・運営に必要な人的資源	少									多	
⑤	ウェブサイト開設に必要な費用	少									多	
	ウェブサイトの維持・運営に必要な費用	少	(注1)	(注1)	(注1)						多	
⑥	検討が必要なセキュリティ対策項目	少									多	

優 ■■■■■■■■ 劣

左側の色の項目程、優れていることを示す。

※上記の表は各運営形態の典型的な例をもとに比較しているため、
サービスや導入機材によっては実際の優劣が変わる場合が存在する。

以降本節では、各運営形態の概要と特徴の大枠について解説する。各観点と項目に対しては、2 章でより詳細に解説する。

1.2.1. モール、ASP、SaaS 型クラウドサービスの特徴

ウェブサイトを運営するために必要なサービスを一括して契約でき、機器の調達やサーバ構築の必要がないことから、導入からサービス開始までの期間が短い。自組織内に専用設備を設置する必要がなく、基本的な運用はサービス提供者が実施するため、組織内で発生するウェブサイト運用管理のための工数が少ない。一方で、ウェブサイトで提供できるサービスや、ウェブサイトのレイアウトについての自由度等は、サービス提供者が用意した範囲に限られるため低い。

下記の表 1-2-2 にて本運営形態のメリットとデメリットを示す。

表 1-2-2　モール、ASP、SaaS でのメリットとデメリット

メリット	デメリット
・EC サイト等を運営するための、決済機能をサービス提供者が提供している場合が多い ・ウェブサイト開設までの期間が短い ・サイト運営者がソフトウェアやハードウェアの管理をしなくてよい ・サイト運営や EC サービスについてのサポートサービスが提供されている場合がある ・セキュリティ対策の業務負荷が極めて少ない	・ウェブサイトで提供可能なサービスが限られる ・ウェブサイトデザインの自由度が低い ・サイト運営者が希望するセキュリティ対策の追加ができない

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

PaaS 型クラウドサービスでは、上記のレンタルサーバと異なり、仮想的なサーバとしての機能をレンタルすることができる。ハードウェア単位のレンタルであるレンタルサーバの運営形態と異なり、サーバとしての処理性能や保存領域を細かく調整することができ、運用中であっても性能を変更することが可能である。また、一部のサービスでは仮想的ネットワークを構成できる機能も存在する。

レンタルサーバのサービスでは、サーバ単位での使用契約となるため、サーバ上にインストールするソフトウェアをサイト運営者が自由に選択することが可能である。また、ハードウェアの管理はサービス提供者が行うため、サーバの設置や電源確保、ネットワーク環境の整備といった作業をサイト運営者が行う必要がない。これにより、独自開発のサービスの提供が可能でありながら、ハードウェアの初期導入に関わるサイト運営者の作業負担がない。

IaaS 型クラウドサービスの場合では、レンタルするサーバについて、CPU やメモリ等の構成をサービス提供者が提示する範囲で任意に選択することができる。これにより、PaaS 型クラウドやレンタルサーバよりもより詳細にサーバの仕様を決定することができる。一方で、上記 2 つのサービスと異なり、初期の状態では OS までの導入となるため、ミドルウェアやアプリケーションはサイト運営者が調達し導入する必要がある。

下記の表 1-2-3 に本運営形態のメリットとデメリットを示す。

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

メリット	デメリット
・ウェブサイトのシステムやソフトウェアの構成が自由 ・サービス利用中にサーバの容量や処理性能を変更できる(PaaS/IaaS 型クラウドサービス) ・サイト運営者による機器導入作業が不要 ・サイト運営者がハードウェアを管理する必要がない	・サーバで使用するソフトウェアをサイト運営者が用意する必要がある[26] ・OS やミドルウェアの設定、アップデートの管理をサイト運営者が行う必要がある ・導入したソフトウェアのアップデートやパッチ適用はサイト運営者が行う必要がある ・セキュリティ対策はサイト運営者が検討し、実施する必要がある

[26] 一般的には、PaaS 型クラウドサービスとレンタルサーバではミドルウェアまでがサービス提供者より提供され、IaaS 型クラウドサービスでは OS までがサービス提供者によって提供される。

1.2.3. ハウジング、オンプレミスの特徴

他の運営形態と異なり、どのメーカのサーバやネットワーク機器を使用するか、どのようなネットワーク構成にするか、冗長化構成等について最も自由度が高い。一方で、ハードウェアの維持管理やネットワークの維持、障害対応等はサイト運営者がすべて実施する必要がある。このことから、管理の委託等を含め組織で十分な知識を有した管理者を用意し、管理体制を構築することが前提の運営形態である。

下記の表 1-2-4 に本運営形態のメリットとデメリットを示す。

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

メリット	デメリット
・機能やサービスの設計が自由 ・ハードウェア、ソフトウェアの選択が自由 ・ネットワーク構成が自由 ・冗長化やバックアップの構成が自由	・ウェブサイト運営に必要な機器を自組織で選定し、調達する必要がある ・組織で機器の管理者を確保する必要がある ・他の運営形態に対して、初期構築費用、運用コストが高い ・セキュリティ対策はリスクに応じて実施する必要があり、パッチ適用等を含めセキュリティの維持運用する体制が必要である

1.2.4. 業種による利用傾向

どのような企業がどの運営形態をとるか、一概に解説することはできない。企業の業態や組織規模や体制など運営者側の制約もあり、またそれぞれの運営形態毎にどのようなサービスが可能か異なり、更には運営に必要な知識や技術水準も異なるためである。

そのため、２章では、運営形態の選定のアプローチを解説するが、以下では、それぞれの運営形態に対して、活用実績や選定理由等に対するサービス利用者の声を簡単に紹介する。

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。

[27] 楽天市場　ネットショップ成功事例：https://www.rakuten.co.jp/ec/interview/
[28] IDC Frontier クラウド導入事例：https://www.idcf.jp/cloud/case/

2. 各運営形態の選定に向けたアプローチ

本章では、ウェブサイトの構築に向け各組織が運営形態を選定する際に、どのようなアプローチで検討を行うべきかについて解説する。2.1 節では、運営形態の選定のアプローチ方法について具体的に例示し、2.2 節以降で 2.1 節のアプローチから得られた結果が適切かどうか確認するための、各運営形態の特徴を解説している。

2.1. 運営形態の選定のアプローチについて

ウェブサイトを構築するにあたり、どのような観点で運営形態を検討すべきかについては、1.2 節にて説明した 6 つの項目を踏まえて、実現したい機能やサービスをはじめとして組織の体制や予算、セキュリティ対策の知識等から検討が必要である。

企業等でウェブサイトを構築する場合、運営形態の選定方針として大きく分けると、『実現したい機能を優先して運営形態を選定する方針』と、『組織内でウェブサイトの運用・維持ができる運営形態を優先する方針』の 2 つの方針が考えられる。

下記の図 2-1-1 は前者の、『実現したい機能を優先して運営形態を選定する方針』に従って運営形態を選定する場合のフローである。

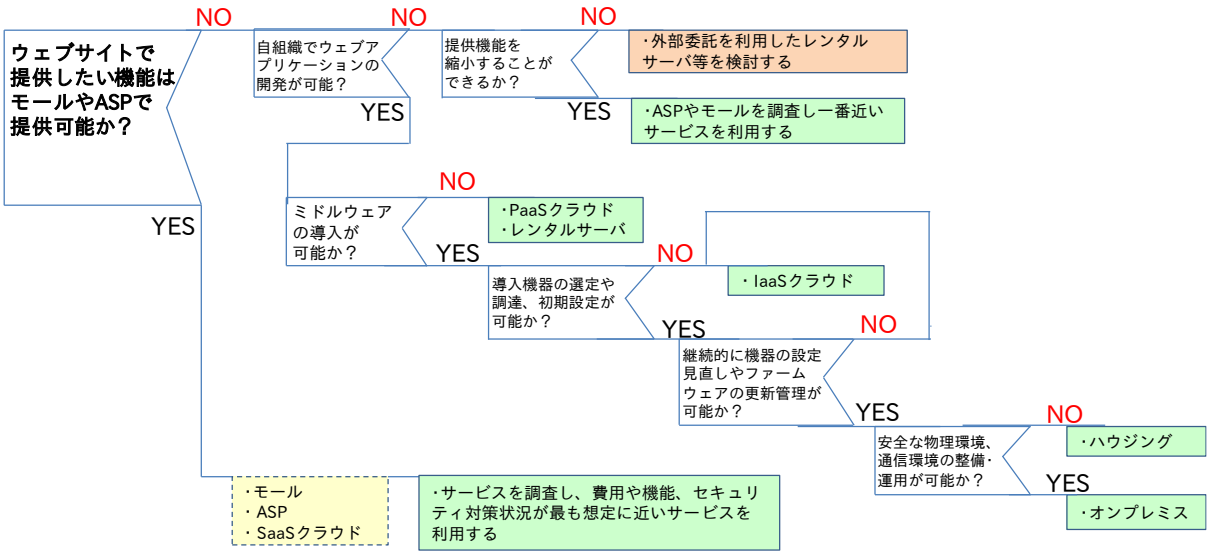

図 2-1-1 実現したい目的を優先した観点における選定フロー

上記のフローではまず初めに、ウェブサイトで提供したい機能が、モールや ASP といったサービスを利用することで実現できるかどうかを調査している。提供したい機能が、モール等を利用することで実現できるのであれば、具体的なサービス提供者の選択を始める。

モール等では提供したい機能を導入できない場合、独自にウェブアプリケーションの開発やウェブサーバの構築を検討する。この場合、自組織内でウェブサイトの構築やウェブアプリケーションを開発できるか検討する必要があり、自組織内で開発ができない場合はウェブサイトで提供

するサービスについて見直しを行う。例えば、提供予定のサービスを縮小することでモールや ASP によって提供されている機能の範疇に収まらないかについて調査し、収まるのであれば、条件に当てはまるサービスを利用するといった方針についての検討を行う。提供するサービスを縮小できないのであれば、ウェブアプリケーションの開発やウェブサーバの構築、運用といった業務を外部の業者に委託し、レンタルサーバ等の運営形態でウェブサイトを運営することの検討に移る。

ウェブアプリケーションを自組織内で開発する場合や、外部の業者に委託する場合は、レンタルサーバやハウジング、オンプレミス等の運営形態から、組織の状況に対応した運営形態の検討を行う。その場合は、ミドルウェアの設定が可能であることや、ネットワーク機器を自組織で管理できるか、といった観点から検討を行い、セキュリティを維持し続けられる形態を選択する必要がある。

次に、下記の図 2-1-2 は、『組織内でウェブサイトの運用・維持ができる運営形態を優先する方針』に従って運営形態を選定する場合のフローである。

下記のフローではまず、以下 4 つの判断基準について対応可能か判断を行っている。

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

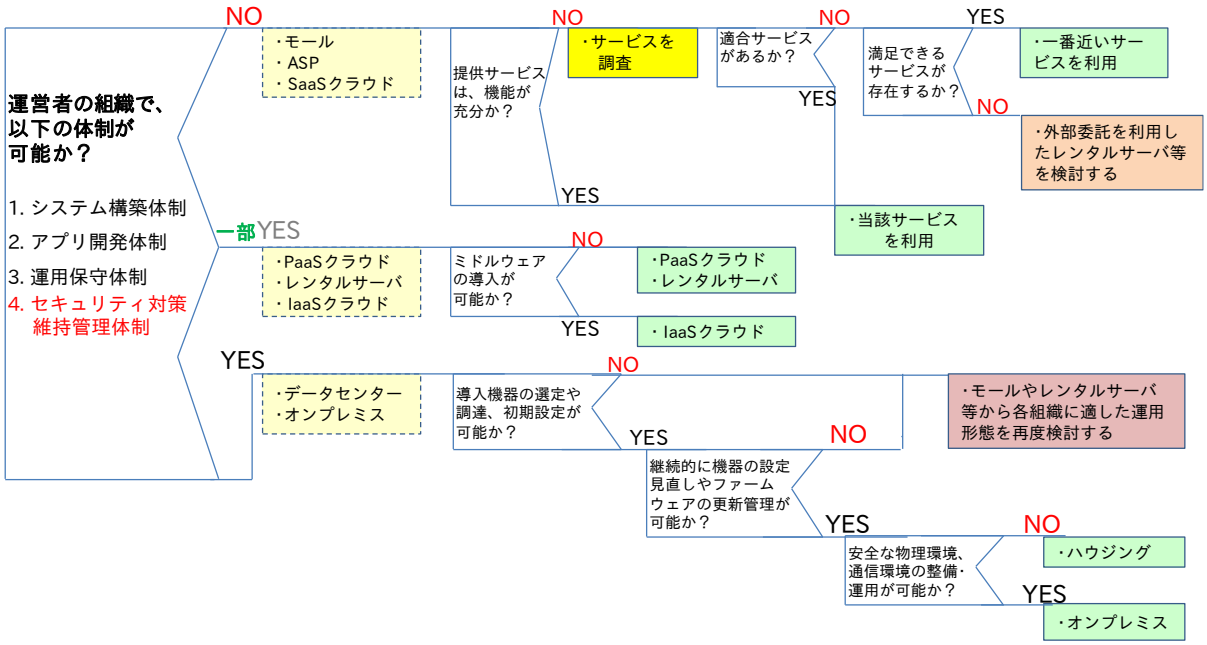

図 2-1-2　運用・維持を優先した観点における選定フロー

1 の判断基準は、サーバやネットワーク機器の設定や接続等といった、ウェブサイトを公開するために必要なシステムの構築ができるかである。オンプレミスやハウジングの運営形態を選定する場合、サイト運営者がサーバの初期設定やネットワーク整備を行わなくてはならない。ま

た、レンタルサーバの場合でもサーバについては初期設定をサイト運営者の責任で実施する必要がある。

２の判断基準は、ウェブサーバ上で使用するウェブアプリケーションを開発するか、調達することで、サーバに導入することができるかである。オンプレミスやレンタルサーバではサイト運営者がウェブサイトの構築を行う必要があり、サーバのセキュリティについてもサイト運営者が対策を講じる必要がある。

３の判断基準は、ウェブサーバの構築後の運用保守体制をサイト運営者が構築できるかである。この場合の運用保守とは、ウェブサイトのコンテンツの更新ではなく、サーバ上で使用しているソフトウェアやアプリケーションのアップデートや、ログの確認、障害対応等を示している。ウェブサーバ上で使用しているソフトウェア製品にパッチが公開された場合は、その適用を行う必要があり、パッチの適用によってサーバ上のその他の製品に影響がないか、事前に調査する等が必要となる。また、独自に開発したアプリケーションの場合でも、脆弱性等の問題が見つかることがある。このような場合は修正を行う必要がある。

４の判断基準は、ウェブサイトの運営に際してセキュリティ対策の実施や維持管理ができる体制を構築できるかである。例えば、セキュリティ対策機器の導入やサーバに不正なアクセスが行われていないかをログから調査する体制を構築すること等が考えられる。

上記の４項目に対し、実施可能であるかを検討すると、その結果から大きく３つの結果に分かれる。具体的には上記４項目について、『全く実施できない』、『一部なら実施できる』、『すべて実施できる』に分類される。『一部なら実施できる』というのは、ネットワーク機器の管理やセキュリティ機器の導入はできないが、サーバの構築やアプリケーションの導入はできる、というような状況を想定している。
３つの分類によって、次の段階で具体的なサービスの選定に進む。例えば、４項目について『全く対応できない』という場合、モールや ASP、SaaS 型クラウドサービスを検討するという選定に進む。この場合、ウェブサイトに実装する予定の機能がサービス提供者によって提供されているかを確認する必要がある。確認した結果、希望する機能が提供されていない場合、代替する機能の調査が必要になる。代替可能な機能がなければ提供する機能を縮小する等の対応を検討する。あるいは、自組織以外に開発と運用を委託する形でレンタルサーバ等を利用するといった方法を検討する必要がある。

『組織内でウェブサイトの運用・維持ができる運営形態を優先する方針』と、『実現したい目的を優先して運営形態を選定する方針』の２つの観点での選定を解説したフローチャートである。図 2-1-1 と図 2-1-2 を、『ウェブサイト構築』、『ウェブサイト運用』『セキュリティインシデント発生時』『セキュリティインシデント対応体制』の観点からより詳細に解説したフローチャートは、本書の【付録 B】に記載しているので合わせて参考にしてほしい。
これらの運営形態の選定に関するフローチャートはあくまで一例であり、選定に際し重要視する観点が異なれば、そのアプローチも異なってくる。

2.2. 運営形態毎の自由度

表 1-1 に掲載した運営形態では、それぞれにサイト運営者が変更可能な項目の自由度が異なる。それぞれの自由度については、下記にて解説する。

・モール、ASP、SaaS 型クラウドサービス

最も自由度が低い運営形態はモールである。中でもモールはウェブサイトで使用するソフトウェアはサービス提供者が提供するものに限定され、ウェブサイトのデザインも変更可能な箇所が限られることが多い。また、ウェブサイトで提供可能な機能もサービス提供者によって限定されている。

次に自由度が低いのは ASP である。モールと比較しウェブサイトのデザイン等の自由度は広がっている場合が多いが、使用するソフトウェア等は変更できず、提供可能な機能が限定される点はモールと同様である。また、モールではサービスを利用したサイト運営者のウェブサイトを横断的に検索する機能が提供されているが、ASP ではこのような機能がない。

SaaS 型クラウドサービスについては、ウェブサイトのデザインや機能が限定されておらず、サービス提供者に開発を委託可能な場合もある。しかしながら、どの程度自由に開発できるかについては、サービス提供者によって異なる。

これらの自由度の少なさは、後に掲載する表 2-3-1 にも記載するように、サービス運営者が用意したウェブアプリケーションが事前に用意されており、これらを利用するためである。換言すると、典型的なビジネスモデル群に対するアプリケーションが用意されており、その範囲内に提供サービスを合わせることになる。

以下では、両極端にある運営形態の構成を解説する。

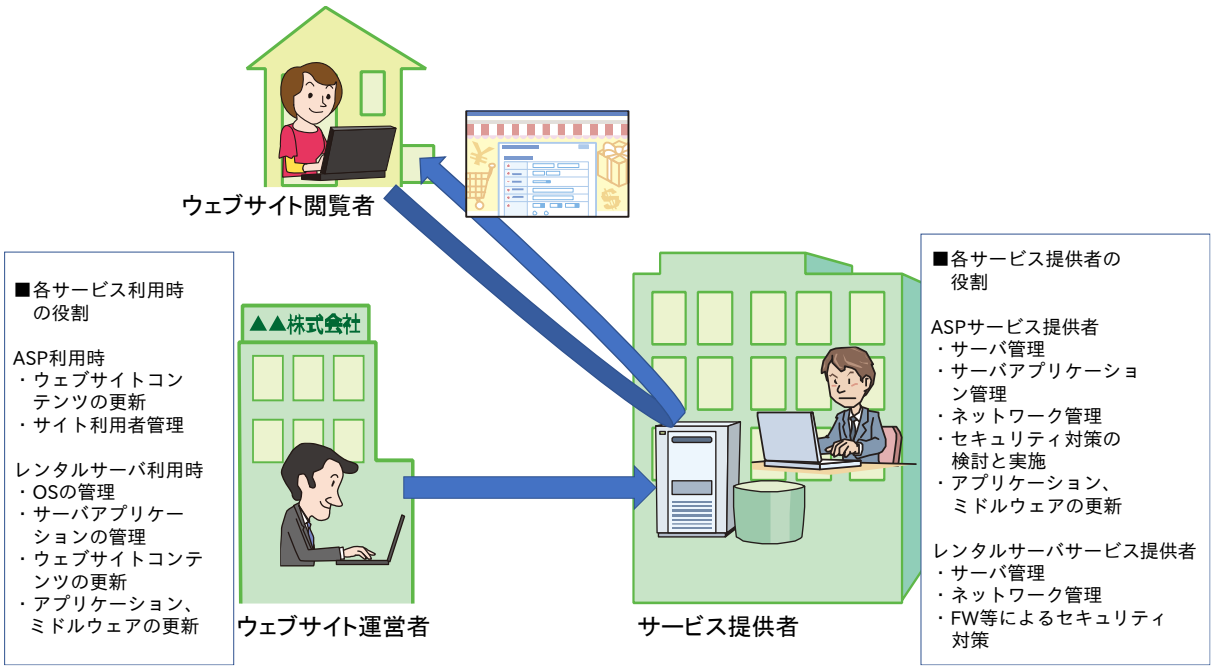

図 2-2-1 ASP やレンタルサーバでのウェブサイト運営

・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

上記のモールや SaaS 型クラウドサービス等より自由度が高い運営形態が、レンタルサーバや PaaS 型のクラウドサービス、IaaS 型クラウドサービスである。レンタルサーバやクラウドサービスではサーバとしての機能が提供され、その上で使用するウェブアプリケーションはサイト運営者が独自に用意することができる。これらのサービスでは、サービス提供者が OS 等のソフトウェアもあわせて提供している。

・ハウジング、オンプレミス

ハウジングを利用する運営形態やオンプレミスの運営形態では、実際に使用するサーバやネットワーク装置をサイト運営者が自由に選択することができる。これにより、冗長化構成やバックアップの取得といった構成を自由に決定することができる。一方で他の運営形態とは異なり、ハードウェアの維持管理のための作業が発生する。

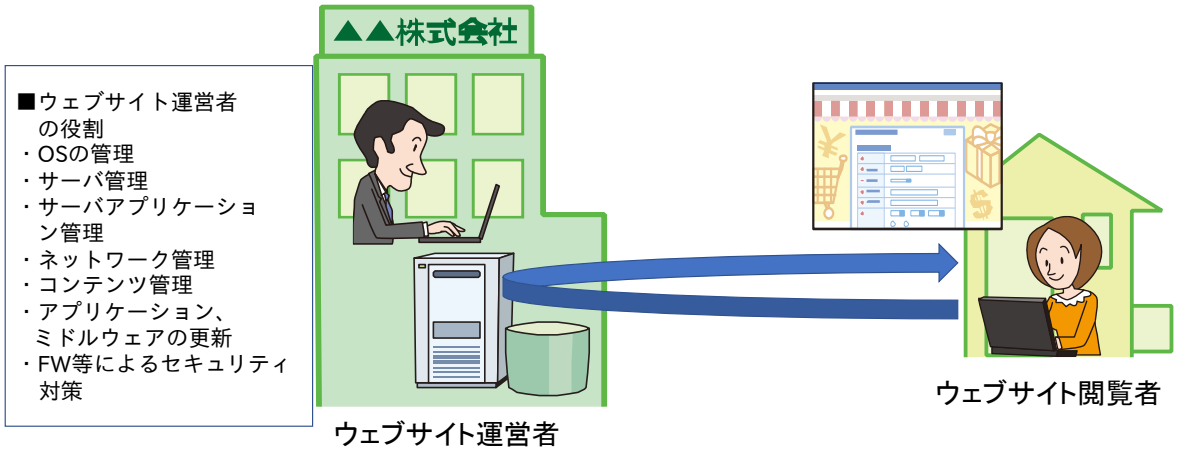

図 2-2-2　オンプレミスのウェブサイト運営

2.3. 運営形態毎に調達が必要となる機材

1.2 節で説明したようにウェブサイトの運営形態によって、サイト運営者が管理する範囲が異なるため、運営形態毎にサイト運営者が用意しなければならない対象も異なる。下記の表に各運営形態で調達が必要な対象を示す。「○」となっている箇所が各形態で調達が必要な項目である。

表 2-3-1 運営形態毎に調達が必要な機材

運営形態 / 調達項目	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
サーバ室				○
電源管理				○
ネットワーク回線			△ (注 1)	○
サーバ、OS			○	○
ミドルウェア		△ (IaaS のみ調達が必要)	○	○
ウェブ アプリケーション		○	○	○
コンテンツ	○	○	○	○

- 記号の意味
  ○：サイト運営者が調達する必要がある機材
  △：サービス提供者との契約内容によって、サイト運営者による調達が必要な機材

（注１）ハウジングの場合、サーバラックまでの回線はサービス提供者が敷設を行うが、サーバラック内での回線やネットワーク機器の導入については、サイト運営が実施する必要がある。

2.4. 運営形態毎に発生する費用項目

各運営形態において発生する費用項目を下記の表 2-4-1 に示す。表 2-4-1 に記載した費用は一例であり、サービス提供者によって発生する費用に差異がある。なお、オンプレミスでの運営形態では、自組織内のサーバ室の状態や使用する機器、ネットワーク回線の契約状況等により実際の費用は大きく異なる。

表 2-4-1　運営形態毎に必要となる費用

運営形態 / 費用項目	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
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	○	○	△ (ハウジングのみ)

- 記号の意味
  ○：サイト運営のために発生する費用
  △：運営形態によっては、サイト運営のために発生する費用

2.5. 運営形態毎の責任範囲

本項では、システム実現形態から典型的な責任範囲を述べるが、必ずしも記載の内容だと断定するものではない。実態は、契約事項や契約内容に依存するものである。

基本的な責任の所在は概ね下記の表 2-5-1 に記載したとおりと考えられる。

表 2-5-1　運営形態毎の責任範囲[29]

運営形態 / 被害例	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
サービスの停止		△	○
データの破壊・消去		○	○
情報漏洩	△	○	○
改ざん	△	○	○

- 記号の意味
  ○：サイト運営者の責任と判断されるもの
  △：状況によってはサイト運営者の責任と判断されるもの

・ASP、モール、SaaS 型クラウドサービス

顧客情報等のデータの破壊・消去については、サービス提供者の責任になると考えられる。ASP や、モール等のサービスでは、ウェブサイトを運営するためのアプリケーションやサーバはサービス提供者により管理されているため、サイト運営者がウェブアプリケーションやミドルウェアのアップデートや修正を行うことができないからである。ウェブアプリケーション等に脆弱性等の技術的問題が存在することで、サービスの停止や、サーバ上のデータの破壊・消去等による被害の責任はサービス提供者にあると考えられる。また、個人情報の漏洩やウェブサイトの改ざんに関しても、ウェブアプリケーションやミドルウェアに脆弱性が存在したことによって被害が発生した場合はサービス提供者の責任であると考えられる。一方で、サイト運営者による管理画面等のパスワードの管理が不十分であり、パスワードを盗まれる等して不正に管理者としてログインされ被害が生じた場合は、サイト運営者の責任と考えられる。

・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

ASP やモールと異なり、サーバ上で使用する OS やウェブアプリケーションはサイト運営者が用意し、運用する形態であるため、ソフトウェアに存在する脆弱性を悪用した攻撃によって生じるデータの破壊や情報漏洩、ウェブサイトの改ざん等の被害は、サイト運営者の責任であると考えられる。一方で、ネットワーク機器の故障やネットワーク機器の脆弱性を悪用されてサービスが停止した場合は、サービス提供者の責任と考えられるが、サイト運営者が管理するウェブアプ

[29] https://www.slideshare.net/ockeghem/wordcamptokyo2015?qid=afb2580e-f66b-4543-9e85-b1f01ac5d8eb&v=&b=&from_search=10 の内容をもとに編集

リケーションに脆弱性が存在し、脆弱性を悪用されることで発生したサービスの停止のような場合はサイト運営者の責任になると考えられる。

ASP やモール等の場合と異なり、ウェブサイトの構築や運用を外部の専門業者に委託することも可能であるが、この場合でも最終的な管理責任はサイト運営者となる。

・ハウジング、オンプレミス

ネットワーク機器やサーバといったハードウェア、サーバ上で使用するソフトウェアはすべてサイト運営者が調達し、導入することになるため、機器障害やソフトウェア障害等の責任はすべてサイト運営者の問題とみなされる。導入時に機器を自由に選択できる一方、その管理・運用はすべてサイト運営者が実施する必要がある。

前述の管理・運用には、サーバやネットワーク機器の物理的な管理も含まれ、オンプレミスの場合はサーバルームへの入退室管理等の物理的な盗難・破壊に対する対策も、サイト運営者の責任で実施する必要がある。一方、ハウジングの場合、入退室の管理についてはサービス提供者により実施される。いずれの場合においても、他の運営形態と異なり、ハードウェアの故障についてもサイト運営者の責任となる。

PaaS 型クラウドサービス等と同様に、ウェブサイトの構築や運用を外部の専門業者に委託することも可能であるが、この場合でも最終的な管理責任はサイト運営者となる。

【コラム】　「契約の免責事項」

ASP やモールのサービスでは契約時の免責事項として、以下のような条項が存在することがある。

- 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

上記の条項では、サービス提供者による作業やサイバー攻撃等による被害によって、サイト運営者に何らかの損害が発生した場合でも、サービス提供者は一切の責任を負わないという契約条項となっている。

しかしながら、過去の判例では上記のようなサービス提供者の免責範囲を限定していないような条文が存在したとしても、サービス提供者の故意や重過失が認められる場合はその責任を完全に免責されるという訳ではなく、一定の範囲において賠償すべきという判例が存在する[30]。

前述のような契約条項が存在する場合、サービス提供者と免責範囲や保証範囲について詳細に確認すべきである。

[30] 平成１２年（ワ）第１８４６８号損害賠償請求事件,平成１２年（ワ）第１８７５３号仮払金返還請求事件：http://www.courts.go.jp/app/files/hanrei_jp/947/005947_hanrei.pdf

2.6. 各運営形態で検討が必要なセキュリティ対策

これまでで解説したように、運営形態毎に調達が必要な機材やサイト運営の際の役割が大きく異なる。これにより、各運営形態で検討が必要なセキュリティ対策も異なる。本項では運営形態毎の責任範囲やセキュリティ対策について解説する。

サイト運営者が各運営形態において検討すべきセキュリティ対策項目一覧を表 2-6-1 に示す。本表は、運営形態毎に示しているが、「△」の個所は、サービス提供者によりオプションサービスとして一部機能が提供されているケースがあることを示している。

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				運用形態			
区分	分類		代表的対策例	モール ASP SaaS	PaaS レンタルサーバ IaaS	データセンタ	オンプレミス
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		△（アプリ）	○	○
		監視	・ログ収集、分析		△	○	○
		ｲﾝｼﾃﾞﾝﾄ対応	・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	○	○	○	○

サイト運営者対応　○：対応の検討が必要
△：一部対応の検討が必要

実施すべきセキュリティ対策は大きく分けて、システム自体のセキュリティを維持するための「システムセキュリティ対策」と業務を遂行・運用していく上で必要となる「業務セキュリティ対策」の２つに分けられる。

「システムセキュリティ対策」はさらに「技術的対策」、「運用管理的対策」、「人的対策」に分かれる。「技術的対策」はセキュリティの維持のためにシステムを保護する環境やどのような機器やソフトウェアを導入するべきかという観点に立った対策で、物理的、ネットワーク、アプリケーションの各区分が含まれる。「運用管理的対策」は、ウェブサイト運営時に脆弱性による被害に遭わないため定期的なソフトウェアアップデートの計画や、攻撃兆候や攻撃発生時に影響の

調査ができるようログを保存し、被害が発生していないかログ分析するといった対策、万が一被害が発生した際のセキュリティインシデント対応等が含まれる。「人的対策」はウェブサイト運営に携わる職員に対し、情報の取り扱いポリシーやコンテンツ更新ルール等を定め、普段から実践するように教育を施し、ポリシーに沿った業務が行われているか監査を行うといった対策が含まれる。

表 2-6-1 に示す「○」や「△」のついたセキュリティ対策を各運営形態では、運営者の人員（もしくは一部委託）によって対応する必要がある。例えば、監視等は専門の事業者への委託や、運用人員をアウトソースするケースも考えられる。

以下では、運営形態毎に行うべき基本的な対策と要点について解説する。

・ASP、モール、SaaS 型クラウドサービス

上記の表に示すように、ASP、モール、SaaS 型クラウドサービスではサイト運営者がシステムセキュリティ対策を実施する必要がない。これは、サービス提供者がサーバやウェブアプリケーション等を一括して提供するためである。逆にこれは、セキュリティ対策の検討・実施をサービス提供者に依存するともいえるため、十分なセキュリティ対策を行っているサービス提供者を選択することが必要である。

・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

サイト運営者によるウェブアプリケーションやデータベースソフトウェア等の管理が必要となる。そのため、サイト運営者が使用するウェブアプリケーション等の脆弱性を調査し、必要に応じてアップデートを行うといった対策を講じる必要がある。場合によってはソフトウェア製品としての WAF[31]やサービス提供者が提供するセキュリティ対策の利用を検討することも必要である。

・ハウジング

サーバ上で使用する OS やウェブアプリケーションといった全てのソフトウェアの管理をサイト運営者が実施する必要がある。また、IDS[32]/IPS[33]、WAF 等のセキュリティ製品の導入やウェブサイトのアクセスログ等の収集を行い、攻撃兆候を分析するといった対策も必要である。サービス提供者によっては、ネットワークセキュリティに関わる部分をサービスとして提供しているケースもあるので、その活用も考慮してサービス事業者を選定する必要がある。

・オンプレミス

ハウジングで必要な対策に加え、サーバやネットワーク機器の物理的なセキュリティ等全てのセキュリティ対策を実施する必要がある。

[31] Web Application Firewall の略
[32] Intrusion Detection System の略
[33] Intrusion Prevention System の略

運営形態の選定の際には、サイト運営者が上記の対策を実施・維持することができるかを検討し、維持し続けられる運営形態を選定することが、安全なウェブサイトの構築・運営において重要となる。

本節の対策についての詳細や、本節で解説した以外のセキュリティ対策については、次の３章において解説する。

【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」

既知の脆弱性とは、ソフトウェア製品の開発者が問題を認識しており、修正等の対応をすでに行っている脆弱性のことである。IPA に対し、このような既知の脆弱性が存在するウェブサイトの届出があることから、日本国内にも既知の脆弱性が放置されたウェブサイトが未だ存在していると考えられる。

アプリケーションのアップデートを行わなかったことで、全世界で広く使用されている CMS[34]の「WordPress」が狙われる被害が発生した。これは、2017 年２月に発生した被害であり、全世界で 160 万件の改ざん被害が発生したと言われている。この被害では、製品開発者が脆弱性を修正したバージョンを１月末時点で公開していたにもかかわらず被害が発生した。このことから、多くのウェブサイトで「WordPress」の自動更新機能を無効にして運用しており、サイト運営者がアップデート情報に気が付かなかったか、気が付いていてもアップデートをすぐに実施していなかったと考えられる。

IPA では、2008 年２月から 2013 年９月の間に脆弱性の届出のあったウェブサイトにおいて、よく用いられるサーバ関連ソフトウェア３種に関して、使われていたバージョンをチェックした。その結果、サポートの終了したバージョンを使い続けているウェブサイトが多数存在していることが判明した[35]。サポートが終了したバージョンでは、脆弱性が発見されてもその対策情報は提供されない。そのため、サポートが終了した製品を使い続けていれば、脆弱性を抱えたままウェブサイトが運営されてことになる。

サポート切れの製品が使われる要因としては、セキュリティを維持していくための運用体制や計画が不十分なことで、サポートが継続している製品を購入する予算が確保されていないことが考えられる。また、アップデートが実施できない原因には、ウェブサイトのメンテナンス計画が整備されていないことで、ウェブサイトを停止することができず、アップデートが先延ばしにされてしまうことが考えられる。

---

[34] Content Management System の略称

[35] IPA テクニカルウォッチ：「サーバソフトウェアが最新版に更新されにくい現状および対策」：https://www.ipa.go.jp/security/technicalwatch/20140425.html

3. セキュリティ対策要件および強化のポイント

２章までにウェブサイト運営形態を選択する際の６つの項目と、各運営形態の特徴、運営形態選択のアプローチについて解説した。2.6 節では、各運営形態におけるセキュリティ対策に対して、外形的な対応の要否について解説した。しかし、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。

本章では、いずれのウェブサイト運営形態で実現するとしても、セキュリティ面で外形的な対応の要否だけでは捉えきれないセキュリティ上の要件や強化のポイントについて解説する。ASP 等のサービスを選択する場合には、サービス提供者により提供されるセキュリティ対策の要件を確認する上で活用頂きたい。

3.1. 実現する機能、サービスに対する考慮のポイント

本節では、それぞれのウェブサイトで実現される典型的な機能、提供するサービスに対して要求されるセキュリティ要件や対策内容について解説する。

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

企業等の組織が公開するウェブサイトの中には、個人情報の漏洩といった被害が想定されなくても、航空機の運行スケジュールといった公益性の高い情報や公共インフラ等に関する情報が掲載されている場合がある。このような情報が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。

ウェブサイトの改ざんによる被害では上記以外にも、ウェブサイトのプログラムが改ざんされることにより、ウイルス等の不正なプログラムをウェブサイトの利用者に配布するように仕立て上げられる場合がある。近年でも、企業のウェブサイトが利用者をランサムウェアの配布サイトに誘導するように改ざんされた事例が存在する。この場合では、ランサムウェアの感染対象に誰を意図していたのかは不明であるが、サイト運営者の取引先が標的にされていた可能性もある。

以上に述べたように、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。

このような状況から、企業等が公開する全てのウェブサイトで改ざん防止の対策が求められる。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。ウェブサイトを狙った攻撃では、ウェブサイトで使用されているソフトウェアに脆弱性の修正情報が公開された場合、脆弱性を悪用した攻撃が急速に増加

したことが報告されている[36]。このことからも、ソフトウェア開発者が公開する根本的対策の実施を早急に検討する必要がある。

上記の対策は、モールや ASP の運営形態を利用する場合でも例外ではない。しかし、これらの運営形態では、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であり、サイト運営者が関与することができない。そのため、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である。サイト運営者がサービス提供者を調査する際には、「セキュリティは万全です」といった表面的な文句で安心するのではなく、具体的にどのようなセキュリティ対策を実施しているかを確認するべきである。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。

ウェブサイトが 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。このことから、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。一例として、日本国内のサービス提供者であれば PCI DSS[37]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 Security Standards 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。しかし、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。

---

[36] WordPress の脆弱性対策について：https://www.ipa.go.jp/security/ciadr/vul/20170206-wordpress.html
[37] Payment Card Industry Data Security Standard の略称
[38] PCI DSS とは：http://www.jcdsc.org/pci_dss.php

また、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としては、以下のような原因が考えられる。

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

上記の１や２のように、簡単なパスワードを使用している場合や、個人名や住所、生年月日から推測されやすいパスワードを使用していた場合、総当たりや SNS 情報等からパスワードを推測されることが考えられる。また、他のウェブサービスと同じパスワード使用していた場合は、他のウェブサービスからパスワードが盗まれた場合に連鎖的に被害が発生することが報告されている[39]。

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

SNS サイトや掲示板サイトでは、サイト利用者が任意の情報を書き込む機能があり、それを第三者が閲覧することができる機能を提供している。これらのウェブサイトでは投稿者の身元を確認することはまれであり、身元を隠したまま悪意ある情報を書き込むことが可能である。また、悪意ある情報を誰でも参照できるため、与える影響が大きい。従って、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。

このほかにも、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には、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。

また、この他の攻撃には、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

[39] 2013 年 8 月の呼びかけ：https://www.ipa.go.jp/security/txt/2013/08outline.html

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

画像投稿サイトやファイルのアップロードサイト等では、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

本節では、ウェブサイトを運営するにあたって、特にセキュリティ上で強化が必要となる典型的な項目に対して、その強化のポイントについて解説する。

3.2.1. 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

外部からのネットワークに対する攻撃および、外部からの不正アクセスに対する対策をする上で、強化すべきポイントとしては、大きく分けると、以下の２点である。

・外部からの攻撃が発生しているかの把握（攻撃の検知等）
・外部からの攻撃からの防御（攻撃の遮断等）

まず、外部からの攻撃が発生しているかを把握（攻撃の検知等）する方法と、その際の注意すべき点について、次の通り解説する。

ウェブサイトに対するインターネットからの攻撃をいち早く検知・遮断する対策として、IDS/IPS、WAF といったセキュリティ製品の導入が考えられる。

具体的な導入手段としては、利用しているサービス提供者のオプションサービスを利用する場合と、サイト運営者が独自に、セキュリティ製品を導入するという方法がある。

どちらの方法を選択したとしても、IDS/IPS や WAF 等のセキュリティ製品を導入した場合は、ウェブサイト毎に検知対象の通信を調整する必要がある。これを実施しないと、誤検知や検知漏れが生じる可能性があるためである。

サービス提供者のオプションサービスを利用する場合は検知対象の調整を受けられるかを確認する必要がある。

また、独自にソフトウェア製品をサーバに導入する場合は、サイト運営者自身で検知対象の調整を行う必要がある。自身で IDS 等の調整を行う場合、ある程度の期間の通信や検知に関するログを取得し、ログの内容から誤検知（過検知や検知漏れ）について精査を行う必要がある。

次に、外部からの攻撃を防御（攻撃の遮断等）する方法と、その際の注意すべき点について、以下で解説する。

IPS、WAF 等を用いて攻撃の遮断を行う場合、正規のサイト利用者の通信が遮断されないようにすることが重要である。正規のサイト利用者の誤検知を完全に防ぐことは困難であるが、できる限り誤検知を減らすことが必要である。そのためには検知内容を担当者が精査し、誤検知でないか確認し、ネットワーク環境の変化に合わせ柔軟に検知条件の調整を行う運用ができる SOC[40]等の体制を構築し、運営する必要がある。

しかしながら、SOC の構築や運営にはネットワークやセキュリティ、セキュリティ製品の知識がある人員が必要になるため、小規模な組織では体制を構築することが極めて困難である。このような場合の代案として、機器の導入や監視、運用を委託できるマネージド・セキュリティ・サービスの利用があげられる。

IPS の他に、攻撃元の IP アドレスが判明している場合は、FW[41]を用いて通信を遮断することも可能である。この場合も、IDS/IPS 等と同様に過去の通信ログから攻撃者であるか慎重に調査を行い、FW に遮断する IP アドレスを登録する必要がある。

どちらの対策を導入する場合においても、一定の知識や技術が必要となるため、組織内に十分な人員や知識が蓄積されていない場合は、マネージド・セキュリティ・サービス等の外部サービスを利用し、専門家に委託したほうが安全かつトータルコストが低いウェブサイト運営につながると考えられる。

[40] Security Operation Center の略称
[41] FireWall の略称

(2) DDoS[42]攻撃対策

大量のアクセスが集中してしまうことにより、ウェブサイトのサービスが妨害されてしまう DDoS 攻撃は、EC サイトでは特にサービス継続の観点で対策が重要視される項目と言える。対策のポイントとしては、下記の観点で検討する必要がある。

・攻撃通信をネットワークに入れないためにどうするか

DDoS 攻撃の場合、大量の通信がウェブサイトに集中するため、ウェブサイトが存在するネットワークに攻撃通信が侵入するだけで、ネットワークの帯域が枯渇し、サービス停止につながる。そのため、ネットワークに侵入する前に遮断する必要がある。

具体的な対策としては、レンタルサーバ等のサービス提供者がオプションサービス等で、DDoS 対策を提供している場合もあるが、提供されていない場合はサイト運営者自身で対策を検討する必要がある。サイト運営者自身で対策する場合、セキュリティの専門企業が提供するクラウド型の DDoS 対策サービスを利用するといった対策が考えられる。しかし、このようなサービスは月額費用が発生するため、ウェブサイトの目的によって対策の要否を検討する必要がある。

例えば、EC サイトであればウェブサイトのサービス停止は企業の減収に直結する。場合によっては、数百万円から数千万円の被害となることも考えられる。このようなウェブサイトであれば、専門企業による DDoS 対策を導入することは十分に有益であると言える。しかし、企業情報のみを掲載した直接収益を生じないウェブサイトであれば、DDoS 攻撃による被害は企業イメージの棄損や一時的な情報発信の停止となり、金銭被害は発生しないと考えられる。このように、DDoS 対策をどこまで行うかについては、ウェブサイトの機能と想定被害を検討し、ウェブサイト毎に判断を行う必要がある。

(3) なりすまし対策

3.1.2 項でもなりすましによる不正ログインについて取り上げたが、運営形態に合わせ以下の 2 つの観点で対策が必要である。

・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

上記の対策は、サイト運営者だけではなく、サイト利用者に対しても実施・普及の啓発を行う必要がある。

まず、サイト運営者が実施すべき対策について以下で解説する。

ウェブサイトのシステムで使用するパスワードが短く簡単なパスワードや、第三者から推測されやすいパスワードの場合、総当たり式にログインを試行されることで不正にログインされる危険性が高くなる。そのため、サイト運営者は他者が類推できない、長く複雑なパスワードを設定することが対策の第一である。その上で、パスワードを描いたメモを卓上に放

[42] Distributed Denial of Service attack の略称

置しない、誰でも閲覧できるファイルに保存しないといった基本的な対策の遵守が必要である。特に、モールや ASP の運営形態でサイト運営者自身が実施できる対策は、パスワード管理体制の強化のみとなるため、前述の基本的な対策の徹底が重要である。

また、万が一パスワードが漏洩してしまった場合に備えた対策として接続方式、認証方式を強化することや、VPN[43]接続を利用することを検討すべきである。レンタルサーバやハウジング、一部のオンプレミス環境の場合、サイト運営者とウェブサーバが同じ拠点にないことから、SSH[44]や管理用ウェブページを用いてウェブサイトの管理を行う場合がある。このような運用では、モール等と同様にパスワードの管理を厳重にするとともに、暗号鍵を用いた認証や、VPN 接続を使用してのサーバへのログインに限定するといった対策が必要である。

次に、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。

基本的な対策として、サイト運営者と同様に、使用するパスワードが短く簡単なパスワードや、第三者から推測されやすいパスワードを使用しないように普及・啓発する必要がある。なりすましによる不正ログインは、正規のサイト利用者の通信と判別することが困難である。このため、決済情報等の重要情報が盗まれた場合でも、サイト管理者や正規のサイト利用者が被害に気付き難い。よって、不正ログインの被害を防ぐため、ウェブサイトで短く簡単なパスワードを設定できないようにウェブアプリケーション側で制限する等の対策が必要である。

しかし、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、以下のような問題が生じる可能性がある。

・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

よってサイト運営者は安全と利便性とのバランスを調整し、落としどころを探る必要がある。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。

これは、ログインの際にあらかじめ設定したパスワード以外に、一定時間で変更されるパスワードをトークンやメールにて通知する等して、パスワード以外の方法での本人確認を行う認証方式である。近年では、なりすましによって多額の被害の発生が予見されることや、ウェブサイトユーザの資産を守る観点から、このような認証がサービス提供者によって提供されている場合がある。ASP 等の運営形態でこのような認証が利用できる場合は、利用を検討すべきである。レンタルサーバやオンプレミスではウェブアプリケーションを開発する際に、導入を検討すべきと言える。

[43] Virtual Private Network の略称
[44] Secure Shell の略称

(4) 重要情報の保護対策

EC サイトや会員制サイト等、個人情報や決済情報を取り扱うウェブサイトの場合、これらの情報を安全に保管することは必須の対策ある。重要情報の保護について、注意すべき点は大きく分けると次の 3 点について検討が必要である。

・データベースをインターネット公開領域(いわゆる DMZ[45])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

まず、データベースをインターネット公開領域に配置しないことの重要性について以下で解説する。

ウェブサーバに個人情報等を保存したデータベースが同居していると、インターネットから攻撃を受けた際、ウェブアプリケーションや OS の脆弱性が悪用されることで容易にデータベースから情報を抜き取られる危険性がある。また、ウェブサーバとデータベースが同居していなくても、インターネットに公開しているネットワーク上にデータベースサーバが存在していれば、インターネット上から直接データベースサーバを攻撃されてしまう危険性がある。このような理由から、データベースをインターネットの公開領域外のネットワークに設置することが、情報の保護において最初に実施すべき対策である。

具体的な方法としては、サイト運営者の組織のネットワークを、目的別に以下のようなセグメントに分離し、ネットワークの境界に存在するファイアーウォールやルータによってそれぞれのセグメント間の通信を適切に制限することで、攻撃からのリスクを低減することができる。

・公開セグメント　：ウェブサーバを設置した、インターネットからアクセス可能なネットワーク
・サーバセグメント：データベースサーバ等を設置した、特定のサーバや端末からのアクセスだけを受け付けるネットワーク
・業務用セグメント：一般職員が利用するネットワーク

次に、重要情報の暗号化について、以下で解説する。

EC サイトや会員制サイト等では個人情報や決済情報を取り扱うため、ウェブサイトに保存された情報を安全に保管することは重要な対策の一つである。個人情報を保護するための対策には、インターネットからの攻撃だけでなく、組織内の端末にウイルスを感染させ、踏み台にする手口や、物理的にハードディスクを盗み出すといった手口についても対策を講じる必要がある。

前述の手口への対策として、先に述べた組織内のネットワークの分離を行うことの他に、データベースデータベースソフトウェアの機能等を利用しデータファイルを暗号化する対策方法がある。データファイルが暗号化されていれば、攻撃者にデータファイルを窃取されたとしても、データファイルの内容を参照される可能性を減らすことができ、情報漏洩を防ぐ

[45] DeMilitarized Zone の略称

ことにつながる。暗号化による保護は、データベースのバックアップファイルに対しても実施する必要がある。

しかし、データファイルの暗号化を行うことでデータベースの応答性に影響が生じることが考えられるため、ウェブサイト構築時に影響の調査を行うことが望ましい。

次に、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、以下で解説する。

サイト利用者が不正なウイルスや不正なウェブサイトに誘導されてしまった場合の対策として、ウェブサイト上での重要な操作の前に再度パスワードによる認証が求められる構成であることが望ましい。

例えば、ウェブサイトに作りこまれやすい脆弱性として、クロスサイト・スクリプティングがある。この脆弱性が存在した場合、サイト利用者に偽の情報を参照させる他に、不正なスクリプトを用いてサイト利用者から Cookie 等の認証情報が盗み取られる被害が考えられる。攻撃者が盗み取った認証情報を用いて、正規の利用者になりすましてログインすることで、不正な決済や、ウェブサイトに登録されている個人情報が窃取されることにつながる。しかし、このような場合でも、決済や登録情報の参照・変更に際してパスワードによる認証を必須とする構成であれば、正規のサイト利用者が被害にあう可能性を減らすことができる。

(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。例えば、システムの冗長化等の対策を実施しておくことが必要である。事業継続を目的とした対策には以下の２点等が存在する。

・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

まず、予備システムを設置することの必要性について以下で解説する。

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。

バックアップデータを定期的に取得する必要性について、次の通り解説する。

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。

バックアップの取得間隔をどのように決定するかについては、【補足 3】で解説している。

3.2.2. その他の対策の観点

3.2.1 項では、すべてのウェブサイトにおいて実施するべき対策を解説した。本項では、3.2.1 項で解説した対策に加え、セキュリティの一層の強化や維持のために実施を検討すべき対策について解説する。

(1) ログの収集、分析

インターネットからの攻撃を未然に防ぐためには、いち早く攻撃の兆候を察知する必要がある。攻撃者は、攻撃を行う前にウェブサイトに脆弱性が存在するかの調査をし、攻撃の際に送る攻撃通信の内容を変えながら攻撃を行う場合がある。このような攻撃の兆候をいち早く察知するためには、通信ログやアクセスログを取得し、解析を行うことが有効である。

ハウジングやオンプレミスといった運営形態では、サーバのみならず、ネットワーク機器についてもサイト運営者自身で管理する必要がある。そのため、サーバに対し不審なアクセスが発生していないか等についても、サイト運営者が調査する必要がある。例えば、業務時間外にサイト運営者の組織内からサーバに対しログインが行われていたり、ファイルのアップロードが試みられていたりする場合、組織内の端末が踏み台となって不正アクセスが行われている疑いがある。

どのようなログを取得するか、取得したログの取り扱いをどうすべきかについては、【補足 2】にて解説している。

(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 NISC[46]、海外であれば NIST[47]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
・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

まず、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という観点について、以下で説明する。

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。

次に、必須ではない自発的なセキュリティ基準への準拠について、以下で説明する。

先に説明したように、実装するウェブサービスに関連したセキュリティ基準や、業界で定めたセキュリティ基準があればそれに準拠したサービス提供者を選択する必要がある。しかし、決済機能を持たないウェブサイトや業界が定めたセキュリティ基準がない場合は、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。

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。参考となる資料について、一部を【付録 A】に掲載している。

(3) セキュリティ専門事業者の活用

安全なウェブサイトの構築や運用に際しては、注意すべき事項がソフトウェアからハードウェアまで多岐に渡るため、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。

[46] 内閣サイバーセキュリティセンター(National center of Incident readiness and Strategy for Cybersecurity の略称)
[47] 米国国立標準技術研究所(National Institute of Standards and Technology の略称)

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

企業等の組織がウェブサイトを活用し、企業情報の公開や通販サイトでの販売活動を行うことは当たり前になっており、ウェブサイトは情報の公開に留まらず企業の販売活動においても重要な位置を占めるようになった。

かつては自組織内でサーバを管理し、必要なアプリケーションをインストールする等してウェブサイトを構築・運営する必要があったが、近年ではサイト運営者がサーバを管理せずともさまざまな方法でウェブサイトを公開することができるようになった。また、ウェブサイトのデザインやサービス内容、日々の運営についても専門の企業に委託することができ、サイト運営者が直接関与する必要はなくなっている。

このように、ウェブサイト構築・運営のハードルが下がり、運営形態の選択肢が増えた一方で、サイト運営者が運営形態を選定する際にどのような点に着目すべきか、運営形態毎にどのようなセキュリティ対策を実施すべきかについて、本書では解説している。ウェブサイト構築にあたって運営形態を選定するための６つの項目（機能、期間、調達、体制、費用、セキュリティ）を整理し、各運営形態のそれらに対する比較を明らかにし、選定のフローとポイントについて述べている。

ウェブサイトの構築や運営のハードルが下がったことにより、ウェブサイト運営の手間は軽減されたが、発生した問題の責任が軽減されることはなく、サイト運営者の責任とみなされる。また、ウェブサイトを狙ったセキュリティ上の脅威は減少するどころか増加する一方である。従って、以前よりもサイト運営者に求められるセキュリティに関する責任は増加しているといえる。

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。

本書が、組織において、安心安全で効果的なウェブサイト運営を実現する上での一助になることを期待している。

補足資料

各運営形態の特徴やセキュリティ上注意すべき項目については、２章で解説したとおりである。本章では２章で解説した内容に加え、すべての運営形態で共通して検討すべき項目について解説する。

【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

ウェブサイトの運営の際には、下記のログを取得しておくことが望ましい。

表 補足 2-1　ログの種類と内容

ログの種類	取得場所	取得可能な運営形態	ログの内容
ログイン履歴	ウェブサーバ	全て	ウェブサーバや管理画面へのログイン履歴
アクセスログ	ウェブサーバ	全て	ウェブページへのアクセス記録
通信ログ	ネットワーク上	ハウジング IaaS 型クラウドサービス オンプレミス	ネットワーク上で発生した通信の記録

前表のログを残しておくことで、定期的に不正アクセスや攻撃を意図した通信が発生していないか、調査することが可能となる。また、実際に情報漏洩等の被害が発生した際、ログを残しておくことで、どのような情報が漏洩したかといった被害範囲の確認が可能になる。

ログを取得する際は以下の点に注意することが必要となる。

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

①については、不必要なログを取得しないための確認である。実際の例では、パスワードやクレジットカード情報等がウェブサイトへのアクセスログとして、サイト運営者が意図していない状態で保存されており、このログが窃取されたことで情報漏洩につながったという事件が存在した。

②については、攻撃者がウェブサーバに不正侵入した場合、自身がアクセスしたことを隠ぺいするためログを削除することが考えられる。これを防ぐため、ウェブサーバのアクセスログを Syslog[48]等の方法を用いて、別のサーバに保存し削除されないようにするといった対策が必要である。

ASP やモール等の場合、ログイン履歴やアクセスログはサービス提供者が管理しており、サイト運営者がすべてを参照できない場合も考えられる。サービス提供者を選択する段階で、ログをどこまで参照できるか確認し、多くのログを提供してもらえることも選択の基準にすることも必要と考える。

【補足 3】バックアップの取得間隔について

バックアップは定期的に取得し、できる限り最新のデータをバックアップしておくことが望ましい。バックアップの取得間隔はウェブサイト上で提供するサービスによって異なるため、各サイト運営者が業務影響等を考慮して取得間隔を決定する必要がある。

例えば、ひと月に 1 回のペースでバックアップを取得すれば、OS の構成情報が破壊されたり、ランサムウェアに感染し OS が起動できなくなったりした場合でも、長くても 1 か月前の状態に復元することができる。

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。

[48] ログメッセージを転送するための通信規格。

【付録 A】ウェブサイト構築・運営に関する参考資料

下記の表 A-1 は「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。これらの資料はウェブ上で一般に公開されているものである。

表 A-1 各フェーズにおける参考資料一覧

フェーズ	No	資料名称	URL(翻訳版が存在する場合は、翻訳版を掲載)	発行元
1.企画	1	情報セキュリティ 10 大脅威 2017	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	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/	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	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	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	IPA
	7	ソフトウエア管理ガイドライン	http://www.meti.go.jp/policy/netsecurity/downloadfiles/softkanri-guide.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	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	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	Delta Risk Limited Liability Company

1.企画	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	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	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/	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	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	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	IPA
	18	Web Application Firewall 読本	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	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	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	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	データベース・セキュリティ・コンソーシアム

2.設計	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	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	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	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	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	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/	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	IPA
	31	CERT C コーディングスタンダード	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	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	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	IPA
	35	システム監査企業台帳	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	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	JPCERT/CC
	39	CSIRT ガイド	http://www.jpcert.or.jp/csirt_material/operation_phase.html	JPCERT/CC

5.運用/利用	40	高度サイバー攻撃への対処におけるログの活用と分析方法	https://www.jpcert.or.jp/research/apt-loganalysis.html	JPCERT/CC
	41	コンピュータインシデント対応ガイド	https://www.ipa.go.jp/security/publications/nist/index.html	米国国立標準技術研究所
6.廃棄	42	システム管理基準	http://www.meti.go.jp/policy/netsecurity/new_systemauditG.html	経済産業省
	43	特定個人情報の適正な取扱いに関するガイドライン（事業者編）	https://www.ppc.go.jp/legal/policy/	個人情報保護委員会
	44	連邦政府情報システムおよび連邦組織のためのセキュリティ管理策とプライバシー管理策	https://www.ipa.go.jp/security/publications/nist/index.html	米国国立標準技術研究所
	45	媒体のサニタイズに関するガイドライン	https://www.ipa.go.jp/security/publications/nist/index.html	米国国立標準技術研究所
	46	DoD 5220.22-M	ー (2018 年 5 月現在、ウェブ上での公開なし)	米国国防総省

【付録 B】複数の観点による運営形態の選定アプローチ

下記の図 B-1、図 B-2、図 B-3、図 B-4 は、2.1 節にて解説した観点とはまた異なる観点で選定を行うフローチャートである。2.1 節で選定した運営形態が、他の観点から選択しても組織に適した運営形態であるか確認するために利用してほしい。

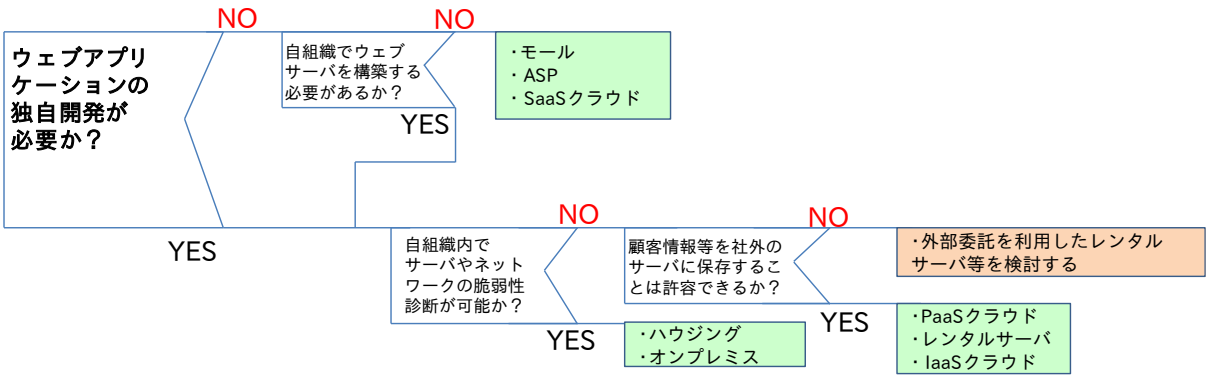

図 B-1 ウェブサイト構築時の観点に基づくフローチャート

上記の図 B-1 は『ウェブサイト構築時にどこまで対応が可能か』、という観点における選定のフローチャートである。この観点では、組織内でサーバを構築する必要があるかといった観点や、ネットワーク管理などを実施できるかについて検討する必要がある。

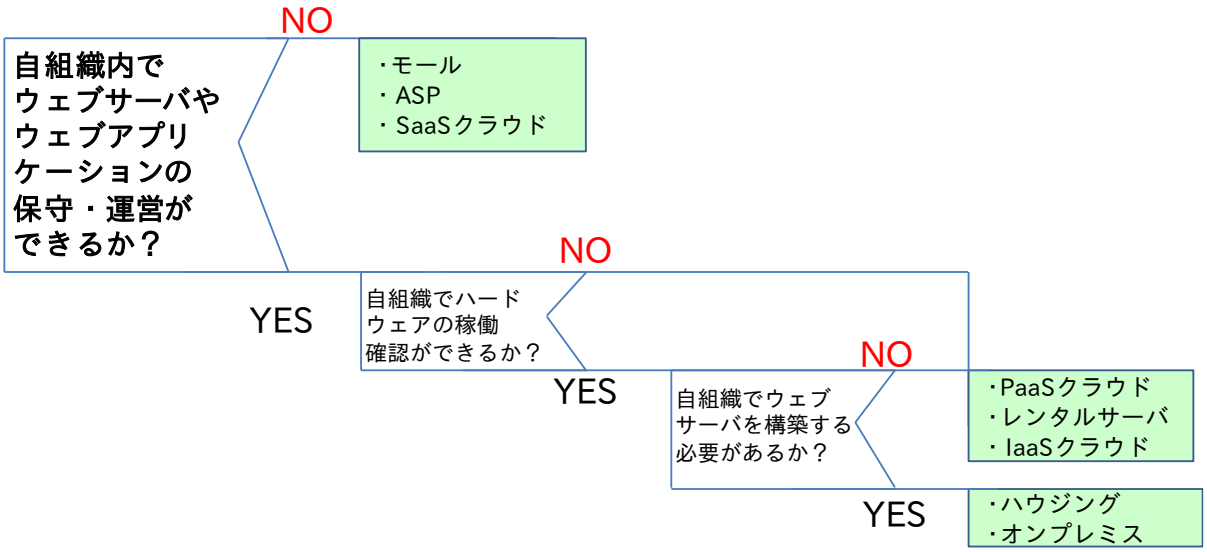

図 B-2 ウェブサイト運用時の観点に基づくフローチャート

上記の図 B-2 は『ウェブサイト運用時にどこまで対応が可能か』、という観点における選定のフローチャートである。この観点では、保守対応やサーバの正常性確認、攻撃兆候の調査が可能であるかについて検討する必要がある。

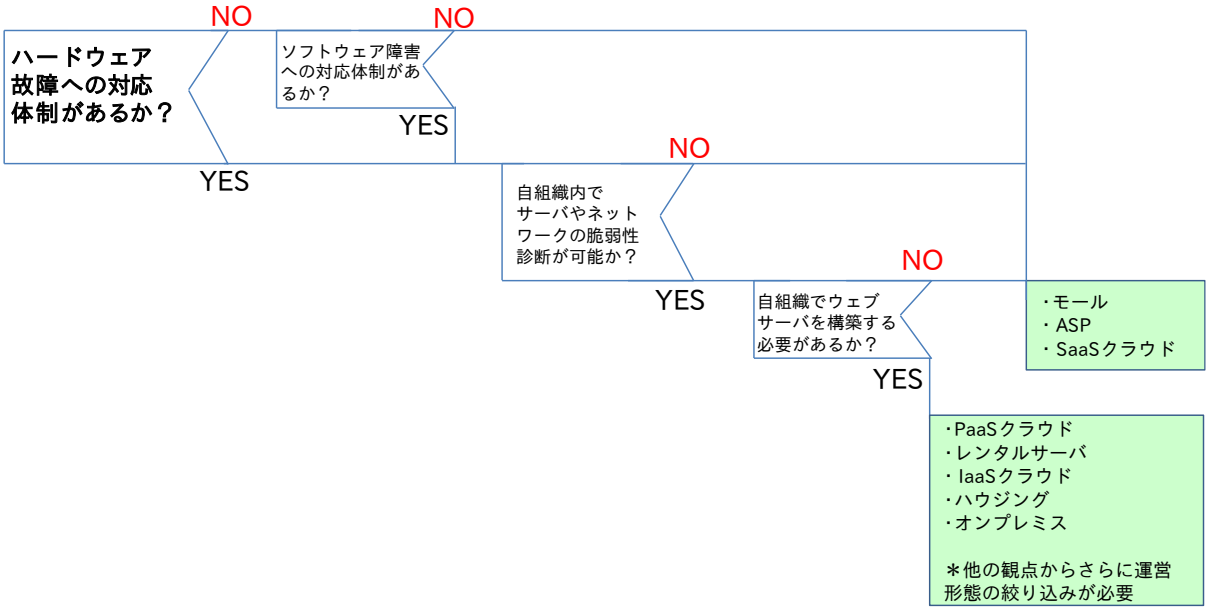

図 B-3 セキュリティインシデント発生時の観点から見たフローチャート

上記の図 B-3 は『セキュリティインシデント発生時にどこまで対応が可能か』、という観点におけるフローチャートである。この観点では、障害対応を始めとして、被害範囲の調査や発生事象への問い合わせ、情報公開等への対応が可能であるかについて検討する必要がある。

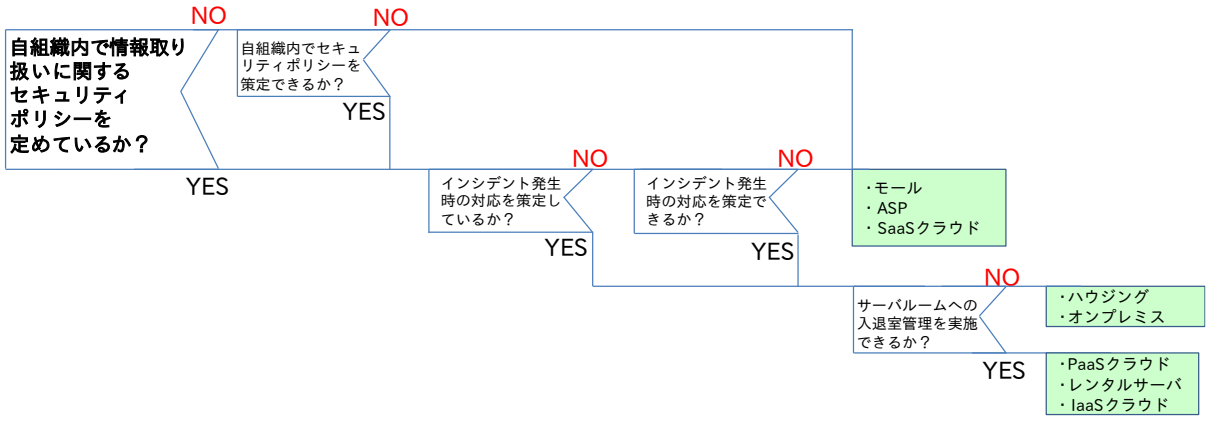

図 B-4 セキュリティインシデント対応体制構築の観点から見たフローチャート

上記の図 B-4 は『セキュリティインシデント対応体制を構築可能か』か、という観点におけるフローチャートである。この観点では、セキュリティポリシーやセキュリティインシデント発生時の対応方針の策定、機器管理体制の構築が可能であるかについて検討する必要がある。

IPA テクニカルウォッチ

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 ～組織の実情にあったウェブサイトを構築・運用するために～

[発　　行]　2018 年 5 月 30 日
[著作・制作]　独立行政法人情報処理推進機構 セキュリティセンター

編集責任　桑名 利幸

執筆者　熊谷 悠平
協力者　徳丸 浩　金野 千里　渡辺 貴仁　板橋 博之　塩田 英二　扇沢 健也
田村 智和　小林 桂　菅原 尚志　鹿野 一人　大塚 龍彦