【付録】ウェブサイト構築・運用のポイント

目次

はじめに 2
1. ウェブサイトを構築する上での注意点 3
1.1. ウェブサイト全体の情報セキュリティ対策 3
1.2. ソフトウェアのサポートライフサイクルを考慮したシステム計画 3
1.3. ウェブサイトの運用形態と設置場所についての考慮 5
コラム 「リスクの許容」 6
2. ウェブサイトの運用開始前の注意点 7
2.1. ウェブサイト全体の情報セキュリティが確保されていることの確認 7
2.2. ウェブサイトの運用管理体制の確認 7
2.3. ソフトウェア管理のための体制整備 8
コラム 「ウェブ健康診断仕様」 9
3. 運用開始後に取り組むべきこと 10
3.1. 脆弱性対策情報収集 10
3.2. アップデートする（修正パッチを適用する） 11
コラム 「自分で脆弱性診断を実施してみたい」 12

はじめに

本付録では本編が CMS に特化しウェブサイト構築・運用におけるセキュリティ対策の考え方を示したのに対し、ウェブサイトのライフサイクル全体を通じて求められる情報セキュリティ対策のチェック項目を解説している。特にウェブサーバーの選定において求められる、運用形態に合わせた“設置場所”について考察を示している点が特徴である。また、IPA では「安全なウェブサイトの作り方」[1]という、主にウェブアプリケーションのセキュリティ実装について詳述した資料も公開している。自組織のニーズに応じて、使い分けてほしい。

[1] 安全なウェブサイトの作り方：https://www.ipa.go.jp/security/vuln/websecurity.html

1. ウェブサイトを構築する上での注意点

ウェブサイトを構築する上で考慮すべき情報セキュリティのポイントは３つある。

- ウェブサイト全体の情報セキュリティ対策
- ソフトウェアのサポートライフサイクルを考慮したシステム計画
- ウェブサイトの運用形態と設置場所についての考慮

1.1. ウェブサイト全体の情報セキュリティ対策

運用中のウェブサイトに対して、新たな情報セキュリティ対策を実施すると、修正コストや機会損失が生じる可能性が高い。そのようなことを避けるためにも、構築（計画）の段階で対策の検討を行うことが賢明である。また、既存のウェブサイトに、新たにソフトウェアを追加で導入した結果、情報セキュリティレベルを低下させてしまう場合があり、これを避けなければならない。

なお、「ウェブサイト全体の情報セキュリティ対策」については、以下の項目を漏れなく考慮・検討する必要がある。

- ウェブサイト全体の情報セキュリティ要件を明確にする
- ソフトウェアは最新バージョンを利用する
- ウェブサイトの運用開始後の運用とメンテナンスの方法を明確にする
- 既に構築されているウェブサイト全体の情報セキュリティレベルを低下させないための対策を検討する

1.2. ソフトウェアのサポートライフサイクルを考慮したシステム計画

PC や家電などの「機器（ハードウェア）」が故障した場合、サポート期間内であれば修理、部品などの交換により、継続して使用が可能だろう。また、故障等が発生することにより経年劣化や寿命をある程度認識でき、買い替えを検討するだろう。一方、ソフトウェアの場合は、製品のサポートが切れてもソフトウェアが故障して使えなくなるとは限らない。しかし、サポートライフサイクル上でサポートが終了してしまうと、パッチの提供が受けられず、安全性が確保されなくなる。しかし機能が有効に動作するのであれば、そのまま使い続

けることは可能で、この点がハードウェアと同じにライフサイクル（寿命）を語れない点である。

ソフトウェアのサポート終了の身近な例として、Microsoft 社の OS「Windows XP」が挙げられる。同製品はサポートライフサイクルポリシーに基づき、2001 年の発売以降、延長を含め 2014 年 4 月までサポートが続き、問題を修正したパッチが提供されていた。しかし、サポート終了以降、同製品にはパッチは提供されていない。一般的にサポートが終了すると、脆弱性が見つかったとしても修正パッチは提供されず、使い続けることで情報セキュリティ上、大きな問題をはらみかねない。そのため、次代の製品への移行が求められる。

これと同様に、構築したウェブサイトの運用中に、CMS などソフトウェアのサポートが終了してしまうと、パッチが提供されなくなるため、問題を解消できず情報セキュリティ上のリスクが高まる（図 1-2-1）。これから稼動させる予定のウェブサイトの場合、組み込むソフトウェアのサポートライフサイクルを予め確認するよう努め、ウェブサイト運営中にサポートが終了する事態にならないよう、あらかじめ計画（見直しの時期を策定）することが重要である。

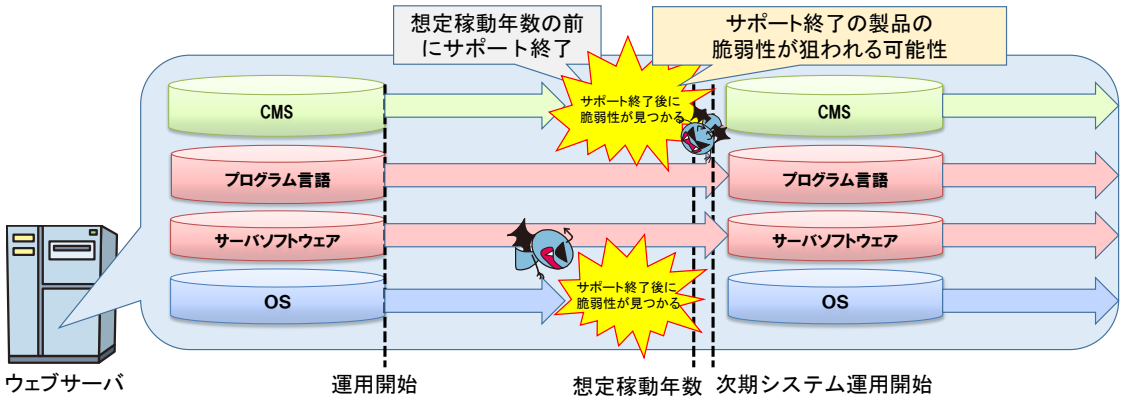


図 1-2-1 ウェブサイトで使用する製品にサポート切れが生じたイメージ

しかし、例えば OSS（オープンソースソフトウェア）は、サポートライフサイクルが明記されていないことも少なくない。さらに、利用者の減少や OSS コミュニティの解散、組織の買収によるサポート団体の消滅など、製品または製品の特定バージョンにおいて、長期に渡るサポートを期待することはなかなか難しい。OSS を利用する場合は、予期せぬサポート切れに備え、サポートが継続されているソフトウェアを使用した次期システムを予めに検討しておくのがよい。このように、ウェブサイトそのもののライフサイクルを意識してソフトウェアの選定とウェブサイトの運営期間を設定することが重要である。

1.3. ウェブサイトの運用形態と設置場所についての考慮

かつて、ウェブサイトは自組織内にサーバーを設置するのが一般的であったが、今では、レンタルサーバーやクラウドサーバーといった外部（第 3 者）が提供しているサービスを活用してウェブサイトを運用するケースも珍しくない。今やサーバーには様々な種類の運用形態があるため、自組織に見合ったサーバーの運用形態を選択する必要がある。気をつけるべき点としては、選択したサーバーの運用形態によって、ウェブサイト運営者のメンテナンス責任の範囲が異なることである。

サーバーの運用形態における管理対象項目ごとの、ウェブサイト運営者及びサーバー事業者の責任範囲は以下の表（1-3-1）の通りである。

表 1-3-1 サーバーの運用形態ごとの管理対象項目 [2]

管理対象項目	自組織内、IaaS、VPS	PaaS、レンタルサーバ	SaaS
パスワードの管理	運営者	運営者	運営者
カスタマイズ、他のウェブアプリケーション	運営者	運営者	－
拡張機能	運営者	運営者	事業者
CMS	運営者	運営者/事業者	事業者
ミドルウェア（ PHP、Apache 等）	運営者	事業者	事業者
OS	運営者	事業者	事業者

表中のサーバーの運用形態が右へ移るにつれ、ウェブサイト運営者は管理する対象が少なくて済む。しかし管理する必要がない代わりに、ウェブサイトのレイアウト変更や、運営者自らアップデートできないという、機能的な制約が生じる。既に運用中のウェブサイトがあれば、サーバーがどういったサーバー運用形態であるのか、そして情報セキュリティ要件を満たしているか確認してほしい。

[2] http://www.slideshare.net/ockeghem/wordcamptokyo2015?qid=afb2580e-f66b-4543-9e85-b1f01ac5d8eb&v=&b=&from_search=10 の内容を元に編集

コラム 「リスクの許容」

アップデートは CMS および利用しているソフトウェアの最新バージョンや修正パッチが公開されるたびに、行うことが理想ではあるが、予算や体制の制約から難しい場合がある。アップデートができないと脆弱性が残存する可能性がある。そのため、ウェブサイト全体に対して、どの様な情報セキュリティリスク（影響）があるかを判断し、どこまでの情報セキュリティリスクを許容できるかを検討する必要がある。情報セキュリティリスクを許容できない場合は、リスクを軽減するための回避策を検討する必要がある。仮に、情報セキュリティリスクを許容できず、回避策も取れない場合は、ウェブサイト自体を停止する事も視野に入れ、検討をする必要がある。したがって、どのような場合にどのような対応をするか、事前に方針・基準を策定しておく必要がある。

2. ウェブサイトの運用開始前の注意点

実際にウェブサイトの運用を開始する前には、以下を実施する必要がある。

- ウェブサイト全体の情報セキュリティが確保されていることの確認
- ウェブサイトの運用管理体制の確認
- ソフトウェア管理のための体制整備

2.1. ウェブサイト全体の情報セキュリティが確保されていることの確認

自組織の情報システムと同等の情報セキュリティ要件をウェブサイトにおいても満たしているのか確認する必要がある。もし、満たしていない場合はウェブサイトの運用開始は見送ることが賢明である。また、情報セキュリティ要件を漏れなく満たしているかどうかの確認には、情報セキュリティベンダーにセキュリティ脆弱性診断やセキュリティ監査を依頼することも検討してほしい。診断等を実施している企業は経済産業省から公開されている情報を参考にしてほしい。

情報セキュリティ監査制度
http://www.meti.go.jp/policy/netsecurity/is-kansa/

2.2. ウェブサイトの運用管理体制の確認

以下のウェブサイトの運用管理体制を策定、確認しておく必要がある。

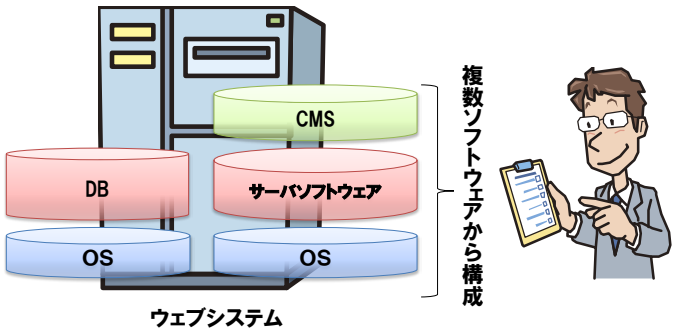
- ソフトウェアアップデート
- トラブル時の運用

ウェブサイトは複数のソフトウェアで構成されており、それぞれのソフトウェアに脆弱性が発見された場合、アップデートが必要となる。また、ウェブアプリケーションに不具合や、脆弱性が発見される場合もある。ほかにも、ウェブサイト内のコンテンツの更新や、リニューアル、ウェブサイトを利用しているハードウェア等にトラブルが発生する可能性もある。このようにウェブサイトの運用は常にメンテナンスが求められる。こうしたことへの対処のため、運用管理体制を策定して、日頃からトラブルが発生した場合を想定して訓練を実施しておくと、緊急事態発生時にも対応を円滑に進められる。詳細については、テクニカルウ

ォッチ「サーバー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」[3]を参考にして運用管理体制を策定してほしい。

2.3. ソフトウェア管理のための体制整備

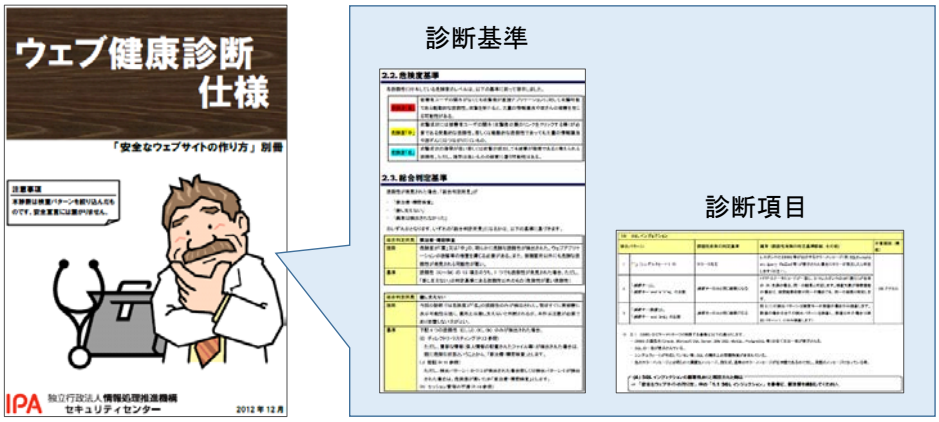
既述のとおり、ウェブサイトを構成するシステムには複数のソフトウェアが組み込まれている。このうち 1 つでも脆弱性があれば、ウェブサイトに対する情報セキュリティ上のリスクとなる。まず、どのソフトウェアを使用しているか棚卸しを行い、把握することが重要である。また、バージョン情報、サポートの有無など使用しているソフトウェアの情報を確認ができるようにリスト等を運用開始前に作成しておくことが望ましい。また、定期的にリストの更新をしておくことも忘れてはならない。



[3] IPA テクニカルウォッチ「サーバー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/files/000038393.pdf

コラム　「ウェブ健康診断仕様」

業者にウェブサイト制作を依頼した際、指定した情報セキュリティ要件を満たしているのかどうか、確認するために「検収」項目に要件を入れておくことが重要である。検収は発注内容と納品内容の要件全般の確認作業であるが、情報セキュリティ要件の確認も重要であり、その方法として発注者側で脆弱性診断を実施することを推奨する。たとえば IPA が公開している「ウェブ健康診断仕様」[4]に基づき発注者側が診断する。



この段階で脆弱性が見つかるということは、さらに別の、もしくは深刻な脆弱性が潜在している可能性がある。なおこの仕様書は、必要最小限の検査項目にとどめているため、この診断で脆弱性が見つからないからといって、安心安全宣言とは言えない点に注意が必要だ。万全を期すためには情報セキュリティベンダーに脆弱性診断を依頼することが望ましい。

[4] ウェブ健康診断仕様：https://www.ipa.go.jp/files/000017319.pdf

3. 運用開始後に取り組むべきこと

ウェブサイトの情報セキュリティレベルは、運用開始から時間が経過するにつれ、低下する。これは、ウェブサイトで利用しているソフトウェアに、運用開始時点では確認されていなかった攻撃手法や脆弱性が発見されるためである。

そのため、通常のウェブサイトの運営（コンテンツの更新、ウェブアプリケーションの追加等）作業に加えて、ウェブサイトの運用開始後にも、ウェブサイト全体の情報セキュリティレベルを維持する必要がある。それには以下のような取り組みが重要である。

■ 脆弱性対策情報収集

■ アップデートする（修正パッチを適用する）

3.1. 脆弱性対策情報収集

情報セキュリティレベルを維持するためには、利用しているソフトウェアを常に脆弱性対策がなされた最新の状態にする（アップデート）ことが重要である。そのためには、「2.3 使用しているソフトウェアの管理体制の確認」で把握したソフトウェアに、最新バージョンや修正パッチ（脆弱性対策情報）が公開されていないか、日ごろから情報の収集に努める必要がある。下記などを参考にして、常にウェブサイト運営者自身で脆弱性対策情報を収集することが重要である。

- ソフトウェア開発者の公式ウェブページの定期的な閲覧、もしくはメーリングリストに登録
- 脆弱性情報を収集している外部サービス（JVN iPedia や MyJVN[5]など）の活用
- 情報セキュリティの専門家による情報発信（SNS など）の活用

ここでポイントとなるのは、入手した脆弱性対策情報等の適用のタイミングである。パッチの適用でウェブサイトに不具合が生じてしまう可能性もあり、即時適用が必ずしも適切と言えない場合がある。そこで脆弱性等の影響範囲やその度合いに応じて都度、優先順位や妥当性を判断する必要がある。優先度をつけるためには以下の情報で判断するのがよい。

- 攻撃情報の有無

[5] MyJVN 脆弱性対策情報収集ツール：http://jvndb.jvn.jp/apis/myjvn/sysad.html

➢ 脆弱性を悪用された場合のウェブサイトへの影響

例えば、脆弱性対策情報を収集する過程で、脆弱性を狙った攻撃の発生情報を確認した場合、あるいはウェブサイトへの影響が大きいと判断された場合には、緊急対策の実施検討が求められる。その他の脆弱性対策情報については、定期的なメンテナンスにて対策を実施する。

また、あらかじめ組織内で優先度についての基準を設けておくことが重要である。判断材料としては、脆弱性の汎用的な評価手法である CVSS（共通脆弱性評価システム）を活用することができる。詳細は、テクニカルウォッチ「脆弱性対策の効果的な進め方（実践編）[6]」を参考に判断してほしい。

3.2. アップデートする（修正パッチを適用する）

収集した脆弱性対策情報をもとに、アップデートを実施する必要がある。アップデートの前に、以下の準備を実施しておきたい。

- アップデート手順を事前に検証
- アップデートに失敗した場合に備えて切り戻し手順を準備
- アップデート後の動作手順を準備
- 利用しているソフトウェアのリストを更新

注意しておきたいことは、アップデートによる影響である。ウェブサイトで利用している、CMS および、拡張機能をアップデート（もしくは修正パッチを適用する）するとウェブサイトが動かなくなるという話を聞く。売り上げに直結する EC サイトであれば、事業にとって大打撃である。そのようなウェブサイトでは、アップデートしても問題なく動作するか確認するためのテスト環境の用意を推奨する。アップデートに時間を要する場合は WAF（Web Application Firewall[7]）などの緩和策を用意しておくことが望ましい。

[6] IPA テクニカルウォッチ「脆弱性対策の効果的な進め方（実践編）」：https://www.ipa.go.jp/technicalwatch/20150331.html

[7] Web Application Firewall 読本：https://www.ipa.go.jp/security/vuln/waf.html

コラム　「自分で脆弱性診断を実施してみたい」

費用削減を目的として、自分でまず情報セキュリティ上の問題があるか調べてみたいという声をよく聞く。近年はオープンソースの脆弱性診断ツールが普及しているため、自組織のウェブサイトの脆弱性を検出するには有効的である。

しかし、忘れないでほしいのは、

- ツールを使用するにはノウハウが必要である
- 何も見つからなくても安全宣言とはいえない（発見できない脆弱性の存在）

ということである。最終的には、情報セキュリティベンダーに脆弱性診断をウェブサイト公開前や新しいページ公開前に実施してもらうことが望ましい。