ウェブサイト運営のファーストステップ

～ウェブサイト運営者がまず知っておくべき

脅威と責任～

2019 年 3 月

IPA 独立行政法人情報処理推進機構
Information-technology Promotion Agency, Japan

■はじめに

インターネットの普及に伴い、ウェブサイトも急速に増加・発展しましたが、その一方で、情報漏えいなどの被害が後を絶ちません。これはウェブサイトを安全に維持するための、適切な運営が行われていないことが一因です。

本資料は、初めてウェブサイトを開設したウェブサイト運営者と IT コンサルタントとのやり取りを通して、ウェブサイトを運営する上で避けては通れない脅威や責任について学んでいただき、安全なウェブサイト運営を検討するためのきっかけとして、ご活用いただくことを目的としています。

■想定読者

・今後ウェブサイトの開設を予定されている方

・現在ウェブサイトを運営している方

■登場人物紹介

A 商事 部長

A 商事におけるウェブサイト運営の責任者(意思決定者)。

この度、コーポレートサイトを開設することとなり、ウェブサイト開発と運用を手掛ける事業者(委託先)と契約した。

ウェブサイト運営ついては、素人。

〇×コンサルティング株式会社 IT コンサルタント

A 商事社長の知人。

ウェブサイト運営経験があり、A 商事社長からウェブサイト運営に関する部長の相談に乗るよう頼まれた。

■目次

■プロローグ

「ようやく我が社のウェブサイトが完成したぞ！」
「ウェブサイトを公開するだけで自社 PR になるなんて、奮起して作った甲斐があったというものだ！」
「これで放っておいても仕事がじゃんじゃんくるぞ。」

「ちょっと待ってください！ウェブサイトは完成が終わりではないですよ！」
「むしろ、ウェブサイトは公開してからが重要で、運営という重要な仕事が待っています。」

「えっ、ウェブサイトって公開したら終わりでしょ？」
「ようやく公開するところまで漕ぎつけたから、これから祝杯を上げるつもりだったのに。」

「いいえ。」
「閲覧者がウェブサイトを安全に利用できるように、運営者にはすべきことが沢山あり、責任重大です。」
「お気持ちは分かりますが、今日は祝杯の前に、ウェブサイトにおける脅威と運営者の責任について理解していってください。」

■ウェブサイトにおける脅威って？

「それで、ウェブサイトを安全にしておく責任がどうとかいう話だったけど、具体的にどういうことなの？」

「はい。まず、責任の話の前に、ウェブサイトにまつわるトラブル(脅威)を考えてみましょう。」
「ウェブサイトで思いあたるトラブル(脅威)にはどのようなものがあるでしょうか？」

「うーん。」
「個人情報漏えいとか？よくニュースでも攻撃を受けて漏えいしたとかやっているのをみるよ。」

「わあ、よくご存じですね。」
「確かに情報漏えいは、ウェブサイトにとって非常に大きな脅威といえるでしょう。」
「他にも、ウェブサイトを改ざんされてしまったり、他のウェブサイトを攻撃するための踏み台とされてしまったりするなどの脅威がよく知られていますね。」

「ああ、なんか聞いたことはあるような。」

「これらは一般的にセキュリティ上の脅威と呼ばれるものですが、主にウェブサイトの脆弱性(ぜいじゃくせい)を攻撃者によって悪用されてしまうことで発生しています。」

「脆弱性？」

「ウェブサイトを構成するソフトウェアや設定上の問題が原因となるセキュリティ上の『弱点』のことですね。」
「代表的な脆弱性については、末尾の参考文献で紹介している『知っていますか？脆弱性』にて、わかりやすく解説していますので、後ほどそちらをご確認いただくのがよいでしょう。」

「へー、でも、そういうのはウェブサイトを構築した委託先の責任なんだから、うちは関係ないでしょ。」
「うちの会社はお金を払って、ウェブサイトについては全て任せてるんだから、全部委託先がなんとかしてくれるんじゃないの。」

「外部の事業者にウェブサイトの構築を委託されたようですね。」
「それでは、ウェブサイトにおける責任の所在と、委託先との責任範囲について、次からはそれぞれ触れていきましょう。」

■ポイント
ウェブサイトにおける脅威は、ウェブサイトの脆弱性が原因となっていることが多い。
脆弱性とは、ウェブサイトにおけるセキュリティ上の弱点のこと。

■ウェブサイトで発生した問題は委託先の責任？

「例えば、委託先が構築した御社のウェブサイトの脆弱性が原因で、利用者の個人情報が流出してしまった場合、責任の所在はどこにあるでしょうか？」

「さっきも言ったけど、脆弱性を作ったのは構築を行った委託先の責任なんだから、運営者は関係ないでしょ。」

「ところが、そういうわけにもいかないのです。」
「ウェブサイト利用者からすると、ウェブサイトの責任者はウェブサイト運営者であるため、被害にあった利用者は、運営者のせいで問題が発生したととらえます。このため、たとえウェブサイトの構築や運用を外部の事業者に委託していたとしても、安全を確保していなかったとして運営者の責任が問われることとなります。」
「委託先のせいだ、と言っているだけでは、ウェブサイト運営を丸投げしている運営者として利用者から批判を浴びてしまいますよ。」

「えっ、そうなの？それじゃあ、我関せずじゃダメってこと？」

「残念ながら、その通りです。」
「もし、情報漏えいが発生してしまった場合、ウェブサイト運営者は、信用を大きく失墜させてしまうだけでなく、運営責任を果たしていなかったとして、訴訟の対象となる可能性もあります。社会的責任が問われるのです。」

「訴訟だなんて脅かさないでよ！だけど、実際にそういうことが起きるかもしれないってことかぁ。」

■ポイント
ウェブサイトの責任者は、ウェブサイト運営者である。開発を外部の事業者に委託したウェブサイトであったとしても、情報漏えいなどの問題が発生した場合は、ウェブサイト運営者の運営責任が問われる。

■委託先は本当に何でも屋？

「続いて、ウェブサイト運営者と委託先の責任範囲についてですね。」

「さっきの話で、ウェブサイトの責任者は運営者だ、ということは分かったけど、やっぱり我々じゃ技術的なことはよくわからないから、対応は全部委託先に任せるしかないでしょ。」
「もしかして、これもダメなの？」

「脆弱性の対応を委託先に依頼することは問題ありませんが、依頼する上で気を付けなければならないことがあります。」

「気を付けること？」

「1つ目は、委託先が対応可能なのは、契約の範囲内に限られるため、何でもかんでも委託先に任せられるというわけではないということです。」
「例えば、事前にウェブサイトの脆弱性対策における取り決めを結んでいない場合などは、納入後に脆弱性が発見されても、対応してもらえない場合や、有償での対応となる可能性があります。」

「あー、そりゃそうか。」
「どういう契約内容だったかなぁ。」

「ウェブサイトの構築を委託すると、全て委託先が対応してくれると錯覚してしまいがちですが、委託先とのトラブルを避けるためにも、双方の責任範囲を明確にしてウェブサイトを運営することが重要ですね。」
「特に保守契約がない場合は、基本的にウェブサイト運営者自らが問題に対処しなければなりません。先ほどおっしゃられていたように、ウェブサイトで問題が発生しても、ご自身での対応が難しい場合は、技術的なサポートが受けられる保守契約を結んでおくことが基本となります。」
「あとで、もう一度契約内容を確認しておくとよいでしょう。」

「そうするよ…。」

「２つ目は、”委託先に対応を依頼すること”が脆弱性対応のゴールではないということです。」

「肩の荷が下りる安心感からか、委託先に依頼をすると、そのまま任せきりになってしまう運営者もいらっしゃるのですが、先ほどご説明した通り、ウェブサイトの責任者は運営者ですので、『委託先に対応を任せたから、その後のどうなったのかは知らない』というような状況は運営責任を果たしているとは言えません。」

「うむむ…、確かに。」

「脆弱性に対し、何らかの対処をして初めて対応完了ですので、委託先に依頼する場合でも、影響範囲の確認や、対応方針の検討、予算や対応スケジュールの調整など、ウェブサイト運営者も一緒になって対応しなければならないことはたくさんあります。」
「このため、積極的に委託先と連携を取りながら、対処する必要があるということを覚えておいてください。」

「言われなかったら、任せきりになっていたかも。」
「肝に銘じておきます。」

■ポイント
委託先は契約内での対応しか行えないため、保守契約などで明確に対応範囲を取り決めておく必要がある。また、脆弱性などの対応を依頼する場合でも、対応完了までは、委託先と連携を取り、協力して対処すること。依頼してそのまま放置してはならない。

■本当にウェブサイトに脆弱性は存在するの？

「ウェブサイトで問題が発生すると運営者が責任を負わなきゃいけないってことは分かったけど、でも、それってウェブサイトに脆弱性があることが前提の話だよね？」
「プロの事業者にわざわざ委託して作ってもらってるんだから、そもそも脆弱性なんて存在しないんじゃないの。」

「もちろん、存在しない可能性も考えられますが、それでも、全くのゼロというのはなかなか難しいかもしれません。」

「というのも、脆弱性はウェブサイトを構築する際の設計ミスや考慮不足などによって、結果的に作りこまれてしまうので、経験豊富な開発事業者であっても、脆弱性が全く存在しないウェブサイトの構築は、容易ではないのです。また、場合によっては、新たな攻撃手法が見つかることで、これまで問題ないとされていた箇所が脆弱性となってしまう可能性もあります。」

「ですから、脆弱性は存在するものと想定してウェブサイト運営を行った方が賢明ですね。」

「あることを想定して、といわれてもなぁ。」

「一度作りこんでしまった脆弱性を自分たちだけで見つけることは、困難ですからね。」

「取りうる手段としては、別途コストが発生しますが、疑似攻撃を行うことで脆弱性を発見するウェブアプリケーション診断を行うという方法があります。」

「他には、ウェブサイトを閲覧している第三者が脆弱性を発見して運営者に報告してくれるといった場合もありますので、ウェブサイト上に運営者の適切な連絡先を公開しておくとよいでしょう。」

「ウェブサイトの構築で結構費用もかかったし、今はウェブサイト診断を行う余裕はないなぁ。」

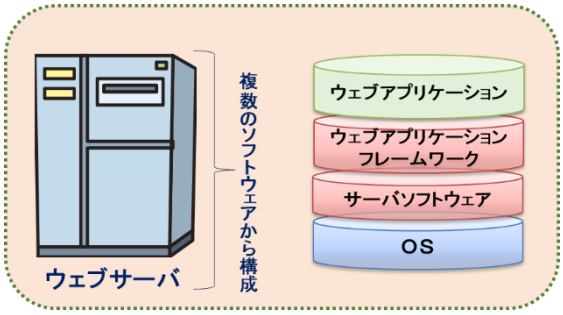
「とりあえず、連絡先についてはしっかりしたものを公開しておくよ。」

「ウェブアプリケーション診断の実施も、今後の課題として検討してくださいね。」

「それから、言いにくいのですが、実はその他にも、ウェブサイトには、今後運営していく中で新たに脆弱性が発生する可能性があるのです。」

「えぇ、まだ何かあるの？」

「実はウェブサイトを構築する際に開発されるウェブアプリケーションの他にも、ウェブサイトは様々なソフトウェアが動作することで成り立っているのですよ。」
「このソフトウェアに、新たな脆弱性が発見されることがあります。」



「つまり、ウェブサイトはそのソフトウェアと、自社で開発したウェブアプリケーションの混合物ってこと？」
「脆弱性が見つかるなら、そんなソフトウェアは使わないってことはできないの？」

「使わないという選択肢もありますが、ウェブサイト開発において使用されるソフトウェアは、非常に有用な機能が多く備えられているため、ゼロからウェブサイトを構築するのに比べて、開発の手間を大きく省くことが可能なのです。よって、ウェブサイト開発ではよく使われています。」
「別の言い方をすれば、便利だからこそ、利用者も多く、多くの人に使用されることで、潜んでいる脆弱性も発見されやすいといえます。」
「脆弱性が発見されることは、修正されてより安全になるということで、必ずしも悪いことではないのです。」

「なるほどなぁ。」

「話が逸れましたが、このようにソフトウェアにおいても、脆弱性が新たに発見されることが少なからずあります。」
「攻撃者も、多くの利用者がいるソフトウェアの脆弱性を積極的に狙ってきますので、脆弱性が残ったまま放置しておくと…。」

「攻撃の対象になるかもしれないと…。」

「そういうことですね。」
「ソフトウェアは、基本的には脆弱性の情報が公開されると同時に、開発者から脆弱性の修正されたバージョンも公開されるので、ウェブサイトでどのようなソフトウェアが使用されているか、きちんと把握し、脆弱性情報が公開されたら、速やかにソフトウェアの更新を行うことが大切です。」

■ポイント

脆弱性の存在しないウェブサイトは現実的ではないため、存在することを想定したウェブサイト運営をすることが望ましい。脆弱性には大きく分けて 2 種類のタイプがある。

1. ウェブアプリケーション開発において作りこんでしまう脆弱性
2. ウェブサイトで使用しているソフトウェアにおいて今後新たに発見される脆弱性

- 1. について、ウェブアプリケーション診断などで発見できる場合がある。
- 2. については、開発者から脆弱性対策情報が公開されるため、速やかにソフトウェアバージョンアップなどの対処を行う必要がある。

■大手のウェブサイトだけが攻撃者に狙われる？

「これまでの話から脆弱性があると、攻撃される危険があるってことだよね。」
「でも、そもそもウェブサイトを攻撃するような人たちって、うちみたいな中小企業のウェブサイトも狙ってくるの？」
「ニュースとかだと、大手の企業が攻撃されたとかって話しか見たことないけど。」

「確かに、大手企業の情報漏えい事件などの方が報道される機会が多い傾向にあるのは事実ですね。」
「ただし、だからと言って、中小企業のウェブサイトが攻撃の対象外というわけではありません。」
「国内のウェブサイトに関する改ざんなどの報告を受け付けているJPCERT/CC によると、毎月 100 件近くのウェブサイト改ざんに関する報告が寄せられているそうです。」

JPCERT/CC インシデント報告対応レポート
https://www.jpcert.or.jp/ir/report.html

「100 件！？そんなに？」

「もちろん、報告されているものは、氷山の一角と考えられますので、実際にはもっと数多くのウェブサイトが被害にあっていると推測されます。」
「特に近年は、ウェブサイトへの攻撃の大部分が自動化され、攻撃者自らが手を煩わせなくとも、容易に脆弱性のあるウェブサイトを調査し、攻撃を行うことが可能となってきているので、油断は禁物ですね。」

「そうなんだ。じゃあ今問題がないからといって、気を抜くわけにはいかないね。」

「また、実際に攻撃が行われてしまった場合、現場は大騒ぎとなってしまいますので、その中で冷静かつ迅速に対応を行うには事前準備が不可欠です。」
「そのため、予め、脆弱性が見つかった場合や、万が一攻撃を受けてしまった場合に、誰が担当となって、どのように対応するのかを取り決めておくとよいでしょう。」

「うーん、確かに対応チームを作って備える必要がありそうだなぁ。」
「後で社内でも相談してみるよ。」

■ポイント
ウェブサイトの大小にかかわらず、脆弱性が存在すれば攻撃者に狙われる可能性がある。
万が一、攻撃を受けた場合に備えて、担当者や対応方針を取り決めておくとよい。

■エピローグ

「いかがだったでしょうか。」
「ウェブサイトは公開して終わりじゃないということが、ご理解いただけましたか？」

「うん。自分の考えの甘さに気づかされたよ。」

「いろいろと大変な部分もありますが、ウェブサイトを公開することによる恩恵は、やはり大きなものです。」
「しかし、運営する上では、安全を維持するなど行うべきことも少なくなりません。ウェブサイト運営者としての役割・責任をしっかり認識した上で、安全なウェブサイトを運営していってください。」

「わかった！ウェブサイト利用者に安心して利用してもらえるよう頑張るよ。」
「でも、今日くらいはウェブサイトの完成を祝わないとね。ということで祝杯をあげよう！」

「ふふふ、そうでしたね。遅くなりましたが、ウェブサイトの完成おめでとうございます。」

■参考文献

「本資料では、ウェブサイトを運営する上での基本的な脅威と責任について触れてきました。」
「この他にも、IPA では、ウェブサイトを運営する上で必要な情報をまとめた資料やウェブサイトを数多く公開しています。」
「以下に何点かご紹介させていただきますので本資料と併せてご確認いただき、是非ウェブサイト運営にお役立てください。」

・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/files/000044736.pdf
ウェブサイト運営者がどのように脆弱性に対処すればよいかを解説した資料です。
具体例なども交え、本資料の内容よりも詳細に対応方法などを紹介しています。

・知っていますか？脆弱性
https://www.ipa.go.jp/security/vuln/vuln_contents/index.html
ウェブサイトにおける代表的な脆弱性について、わかりやすくアニメーションで解説しています。

・安全なウェブサイトの作り方
https://www.ipa.go.jp/security/vuln/websecurity.html
ウェブサイトを構築する上で、作りこんでしまいがちな脆弱性とその対処方法を解説しています。

・情報セキュリティ対策支援サイト
https://security-shien.ipa.go.jp/
中小企業における情報セキュリティ対策の水準向上の支援を目的としたウェブサイトです。
情報セキュリティ対策の状況を診断できる「5 分でできる！自社診断」などのサービスをご利用いただけます。

・対策のしおり
https://www.ipa.go.jp/security/antivirus/shiori.html
情報セキュリティ対策について何をすれば良いか分からないという企業や組織に向けて、項目ごとに対策方法を記載したしおりをまとめたものです。

IPA 独立行政法人 情報処理推進機構
Information-technology Promotion Agency, Japan

〒113-6591 東京都文京区本駒込2丁目28番8号
（文京グリーンコートセンターオフィス16階）
URL http://www.ipa.go.jp/security/