講座

Web広告

村山　哲治

Webマーケティングの実践にはセキュリティ対策も必要

■自社でも起こり得るサイトのハッキング

つい先日のこと，当社のクライアントをGoogleで検索してみると次のようなメッセージが検索結果に表示されているのを発見しました。

「このサイトは第三者によってハッキングされている可能性があります。」

このクライアントではＳＥＯ対策や自社サイトを媒体に広告を掲載していることもあり，すぐさまクライアントに連絡をしてその対応を行った結果，翌日にはその表示もされなくなり，ひとまず胸をなでおろしたということがありました。

今回は発見も早く，被害がなかったからよかったものの，閲覧ユーザーの情報が盗まれたり，ウイルスをまき散らすことになっていたらと思うとぞっとする出来事でした。

このサイトではGoogle Search Consoleを導入していたため，Googleよりハッキングの検知があった旨のメッセージがSearch Consoleにも届いていましたが，このような表示がされていることをリアルタイムに気づくことは難しいかもしれません。

このケースのように，ＳＥＯ対策やプロモーションに力を入れていても，サイト運用においてセキュリティ面での対応に問題があると，サイトへの流入が多ければ多いほどユーザーの信頼を落とすことになり，サイト戦略そのものが台無しになってしまいます。

こうした事例は対岸の火事ではなく，自社サイトでも発生する可能性は十分にあります。そこでサイトのハッキングの原因と対策について考えてみたいと思います。

■ハッキングされる原因とは

サイトがハッキングされるには何らかの原因があります。大きくは外部要因と内部要因とに分けられます。外部要因では，サイトを管理しているサーバーホスティング側のなんらかの脆弱性などをつかれてハッキングされるケースです。内部要因としては，パスワードの漏えい（ＦＴＰ・ＣＭＳ管理ログイン）やサイト管理者のＰＣがウイルス感染していたり，ＣＭＳ（WordPressなど）のバージョン更新や，同じくＣＭＳに後からインストールされたプラグインのバージョン更新などが滞っていたりすると，その脆弱性をついてハッキングされることがあります。当社のこのクライアントは，内部管理のパスワードが非常に分かりやすく，かつWordPressのバージョンアップもされていないという二つの問題がありました。ちなみに原因特定の一つの目安として，サーバーのログイン履歴から見知らぬＩＰが残っているかどうかで原因の切り分けが出来ます。もし，知らないＩＰの痕跡があればＦＴＰパスワード漏えいが考えられ，それが残っていない場合はＣＭＳからのハッキングが考えられます。

いずれにしても，パスワードの管理（複雑なものにする，定期的に変更する，運用部門で退職者が出たら変更するなど）やサーバーログのチェックはサイト運用タスクとして入

れていただきたい項目です。

■ハッキングされた場合の対応

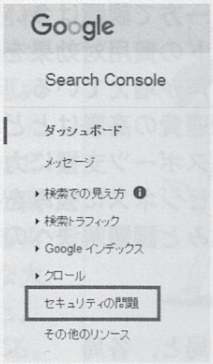
こうしたことはめったに起こることではないため，ハッキングが認められると多くの場合，動揺して早く何とかしようと，あれやこれやと自分の判断でやってしまいがちです。

しかし，それが被害の拡大などにつながることが多いため，落ち着いて正しい手順でその対応を行う必要があります。

対応の仕方としては，専門業者に任せるか自社で行うかのどちらかしかないのですが，専門業者が行うにしてもその対応手順は同じで，以下の流れで行います。

1．サイトの隔離
2．被害の確認
3．脆弱性の特定と対応
4．Google へ再審査リクエスト
5．事後対策

1．サイトの隔離



脆弱性対応の規模や範囲にもよりますが，長くても３日，通常は２日ほどかかると見ておかなければなりません。そのうえで，被害が拡大しないようサイトをメンテナンス表示にして閉鎖します。あわせて，運用関係者にはサーバーやサイトにアクセスしないようアナウンスするとともに社内のＰＣがウイルスに感染していないかを確認します。

2．被害の確認

Google Search Console を使用していれば「セキュリティの問題」という項目から内容を確認します。そしてサイトの改ざん内容を html のソースやリンク，ＣＭＳであればデータベースなどから不審なファイルやソースがないかを確認します。

3．脆弱性の特定と対応

改ざん内容やサーバーログより脆弱性の原因を特定し，新たに書き加えられたファイルやリンクの削除，ＣＭＳのバージョンアップ，パスワードの変更などの対応を行います。

4．Google へ再審査リクエスト

確認と対応を行い，サイトが以前の状態に戻ったことを確認し，Google の再審査ページからリクエストを送り，Google 側でそれが確認できれば検索エンジンでのアラーム表示が削除されます。

5．事後対策

まず対外的には，サイト閉鎖から再開に至った報告の告知。閉鎖していた時間や内容にもよりますが，あまり詳細に報告してもかえって不安を煽ることになりかねませんので，これに関してはサイト運用側の判断になると思います。

問題は今後の運用ルールに関する部分です。一度脆弱性が認められたサイトは再度ハッキングを試みられる可能性があります。そのため，社内のネットワーク環境の見直し（各自のＰＣ管理），パスワードやＣＭＳの運用ルール，セキュリティチェックの仕方などを明確に定め，関係者の中で共有し運用にあたる，といった流れになります。

当社のクライアントで発生した事案も「まさかうちが」「このくらいは大丈夫だろう」といった，やや緩い認識の中で運用されていたことで起こったことでした。とくにサイトの制作や運用で WordPress はある意味，世界標準として利用されているツールだけに攻撃の対象にもなりやすいことを認識し，まめにバージョンアップを行ったり，必要以上にプラグインを入れたりしないなどの対応は必要です。

どんなにＳＥＯや Web マーケティングで効果をあげていようとも，いったん自社サイトに警告メッセージが表示されてしまうと，サイト訪問者や売り上げ，ブランドイメージが一気にダウンするということにもなりかねません。Web マーケティングの実践には，セキュリティ対策も含めて考えるべきです。

（東京ドアーズ／人間力教育センター代表）