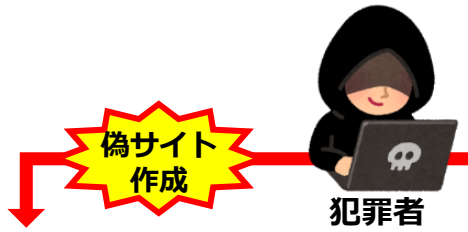
自社のサイトが詐欺サイトの「踏み台」に！？

ウェブサイトを改ざんされると、詐欺サイトへの「踏み台」にされる等、様々な犯罪に悪用されてしまいます。ウェブサイト管理者の方は、サイトを改ざんされないための対策が必要です。

ウェブサイトを「踏み台」利用する手口の例



攻撃者が作成した詐欺サイト
(https://✕▲.xyz)

踏み台に改ざんされたサイト
(https://●●●.com)

偽ショッピングサイトやフィッシングサイトなどに転送される被害が発生。

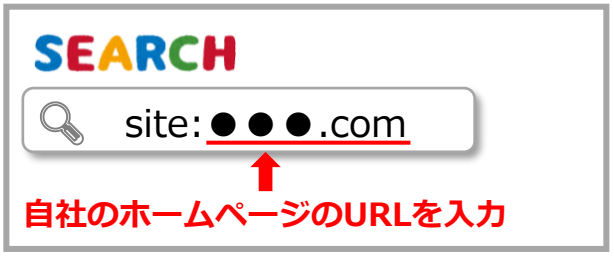
検索エンジンから踏み台サイトを経由して、**詐欺サイトへ自動的に転送（リダイレクト）**されてしまう。

自社のサイトが改ざんされていないか、手軽に確認ができます！

大手検索サイトの検索バーに、

site:（自社のホームページのURL）

と入力して検索実行。



日頃の対策

- OSやソフトウェアを常に最新の状態に保つ
- 管理者のＩＤ・パスワードを適切に管理
- セキュリティソフトを導入し、常に最新の状態にしておく
- ウェブサーバーのログを保管し、定期的に確認する

改ざんされてしまったら…

- 被害に遭ったサーバ、ネットワーク機器等の調査
- ウェブアプリケーションやＣＭＳ等をアップデートし、脆弱性を塞ぐ
- 攻撃者からアクセスされた可能性があるパソコン、サーバ、ネットワーク機器等のパスワードを変更
- 直ちにサービスを停止し、アクセスログ等の証拠保全をする
- 警察に通報・相談する

埼玉県警察 サイバーセキュリティレポート R6.7
サイバー局サイバー対策課