サイバー犯罪の「踏み台」にされないために

ウェブサイトの脆弱性や運用管理の不備を悪用され、情報漏えいやウェブサイトを改ざんされるなどの被害が発生しています。
改ざんされたウェブサイトは、偽サイトへの「踏み台」にされるなど、様々な犯罪に悪用されています。
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

犯罪者

脆弱性を突いた攻撃、
不正アクセス、
マルウェア感染などで改ざん

偽サイト作成

サイト改ざん

攻撃者が作成した偽サイト
(http://×××.xyz)

代金を騙し取られる**偽ショッピングサイト**や個人情報やクレジットカード情報等を盗まれる**フィッシングサイト**などによる被害が発生。

リダイレクト（転送）

踏み台に改ざんされてしまったサイト
(http://●●●.com)

検索エンジンから踏み台サイトを経由して、偽サイトへ**自動的に転送**（リダイレクト）される。

⚠ 検索結果に表示されたURLと一致しない

被害者

検索エンジンからキーワード検索。

検索上位に踏み台サイトが表示されるように設定されている。
（表向きは、改ざんされたサイトのURLが表示される）

- **OS**や**ソフトウェア**を**常に最新の状態**にしておく
- **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**管理用アカウントの管理**を徹底する
- ウェブサーバーの**ログを保管**し、定期的に確認する

埼玉県警察本部サイバー対策課