令和４年９月発行

Kagawa Cyber Security Information

香川県サイバーセキュリティ連絡ネットワーク通信Vol.79

Ｗｅｂサイトの改ざん対策について

改ざんの手口

XSS、CSRF、ゼロデイ攻撃など、
様々な攻撃手口がある！

①　脆弱性攻撃による改ざん

OS、Webサーバなどの脆弱性を利用し、直接コンテンツの改ざんを行う方法と、バックドア（外部通信可能な状態）を設置して遠隔操作で改ざんする方法があります。

②　管理用アカウントの乗っ取りによる改ざん

不正アクセス等により、管理用アカウントを乗っ取る方法で、正規のWebサイト操作方法により改ざんが行われるため被害に気が付きにくい特徴があります。

影響・被害

攻撃者の目的によって、Web改ざんによる被害も異なる。

- 攻撃は、ウイルス感染以外に、いたずらや自己主張を目的に行われることもあります。
- 利用者は、改ざんされたサイトへのアクセスを通じて別の不正サイトへ誘導され、不正なプログラムに感染してしまうことがあります。
- 自社のWebサイトが改ざんされることで、管理責任を問われたり、企業評価の低下につながるおそれがあります。

対策・予防

（ユーザの対策）

- ○ OSやソフトウェアを最新のバージョンにしましょう。
- ○ ウイルス対策ソフトを導入しましょう。
- ○ 信頼できないWebサイトにアクセスしないようにしましょう。

（管理者の対策）

- ○ パスワードを使いまわすことなく、Webサーバ管理用アカウントの管理を徹底しましょう。
- ○ ネットワーク機器をアップデートしましょう。
- ○ 不正サイトへの誘導を目的とした攻撃メール等は開かないように注意しましょう。

Webサイトは、企業にとって重要なビジネスツールであり、現代社会でWebサイトなくして事業は成り立たなくなっています。

そんなWebサイトが改ざんされることで、自社だけでなく、利用者や他の企業にも悪影響を及ぼしてしまう可能性があります。

また、管理者だけ対策を講じるのではなく、利用者も万全のセキュリティ対策を講じることが大切です！

香川県警察本部生活環境課　サイバー犯罪対策室　　TEL：０８７－８３３－０１１０