# F－CSNET通信かわら版

令和5年5月号

## ウェブサイト改ざんに注意！

自組織のウェブサイトが改ざんされると、業務運営に支障が生じるだけでなく、サイバー攻撃の踏み台に悪用されるなど、多方面に悪影響が及ぶ可能性があります。
下記の方法で、自組織のウェブサイトの安全性の有無について確認してみましょう。

## ウェブサイトの確認方法

① 検索ブラウザの検索バー、またはアドレスバーに、「site:自組織のドメイン」を入力して検索します。

例：自組織のウェブサイトのURLが「https://www.example.co.jp」の場合、「site:example.co.jp」と入力します。

② その結果、自組織ドメインを使用した**見覚えのないページ**が確認された場合は、**「改ざん」**されています（不正なファイルが蔵置された可能性もあります）。

※　改ざんされたページを放置したままだと、サイトを訪問したユーザーがウイルスに感染する危険性があります。


## ウェブサイトが改ざんされた場合の措置

ウェブサイトの改ざんが確認された場合は、速やかに自組織のシステム担当者に連絡し、**「不正なページの削除」「改変されたページの修正」「ウェブサーバーの脆弱性の修正」**等を行ってください。
また、ウェブサーバーのアクセスログ等を保存のうえ、**最寄りの警察署**に通報・相談してください。

◆　福岡県中小事業者サイバーセキュリティ支援ネットワーク（通称：F-CSNET）とは、県内中小事業者のサイバー犯罪被害の未然防止・拡大防止を目的として、県内の中小企業支援団体と公的機関で構築したネットワークです。

◆　福岡県警察本部サイバー犯罪対策課では、最新のサイバー犯罪の手口や対策などをTwitterやホームページに掲載していますので、ぜひご覧ください。

【Twitter】　【HP】