



サイバーセキュリティの置き薬

2020年
第4号

CMSのぜい弱性・設定を再点検！

最近、CMS(コンテンツ・マネージメント・システム)のぜい弱性を悪用して、ホームページを改ざんする事案が多数発生しています。

既知のぜい弱性を突いた攻撃による手口です。利用するCMSが最新のバージョンに更新されているか等を確認してください。

サイト改ざんの手口

- ① CMSのぜい弱性を悪用して、不正プログラムがアップロードされる。
- ② アクセス権限が制限されていないフォルダ内のファイルが改ざんされる。

対策

1. CMSは最新のバージョンを利用する

2. フォルダのアクセス権限を適切に設定する

現在確認されているホームページ改ざんでは、CMSのぜい弱性が悪用されたこと及びフォルダのアクセス権限が適切に制限されていなかったことが原因です。

今一度、被害にあわないためにも、上記2点について、再確認をお願いします。



《情報提供(通報)をお願いします》

今後、東京オリンピック・パラリンピック競技大会に向けて、国内の企業を狙ったホームページ改ざんの発生が懸念されます。ホームページ改ざん等のサイバー犯罪を確認した際は、警察まで情報提供(通報)をお願いします。

【富山県警察サイバー犯罪対策課 076-441-2211】

2月1日～3月18日は「サイバーセキュリティ月間」です。
“サイバーセキュリティは全員参加”