山梨県警察サイバー犯罪対策課からのお知らせ

御社の ウェブサイト 改ざんされていませんか？

どうやったら改ざんされていることが分かるの？

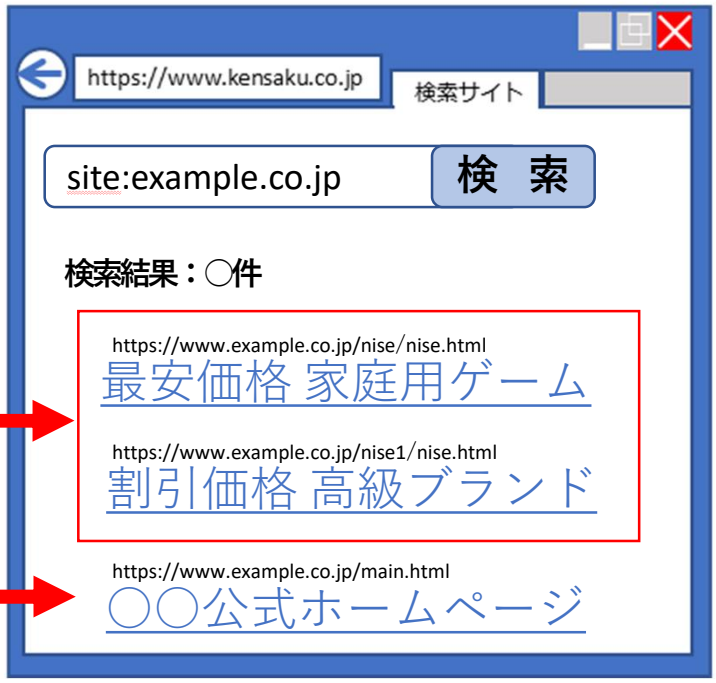
自社ウェブサイトを検索してみましょう！

①検索サイトで
『site:（自社ドメイン）』
と入力して検索！（www等のサーバ名は不要です。）

【例】自社のウェブサイトが「www.example.co.jp」の場合、「site: example.co.jp」と入力してください。

②検索結果に自社ドメインを使用した見覚えのないページが表示されたら、改ざん（不正にファイルを蔵置）されています！

自社公式ウェブサイト



改ざんされていた場合はすぐに対策を！

自社の担当者等に連絡の上、不正なページの削除、ぜい弱性の修正等の対策を行ってください。

また、アクセスログ等を保存の上、最寄りの警察署又は山梨県警察本部のサイバー犯罪相談窓口に通報・相談してください。

山梨県警察本部のサイバー犯罪相談窓口はこちら⇒

https://www.pref.yamanashi.jp/police/formmail/uketuke.html

山梨サイバーセキュリティ通信

令和５年－⑧
山梨県警察本部

ＤＤｏＳ攻撃の踏み台対策

ＤＤｏＳ攻撃とは

- 攻撃者が**不正に操作した多数のパソコン**（ボット）などから攻撃目標（Webサーバなど）に**一斉に大量のデータを送付**し、**処理機能を停止**（閲覧できなくなるなど）させる**攻撃**

ＤＤｏＳ攻撃の手口

- 攻撃者は事前にコントロール可能となっているＩｏＴ機器（ネットワーク上の防犯カメラなど）やルータ、パソコン（総称して**ボットネット**）などに対して、Ｃ２サーバから**一斉に指令を送り**（ボットネットを**踏み台**にして）攻撃目標に**大量にデータを送付**します。
- **踏み台にされる原因**は、**マルウェアに感染**することや**認証情報**（ＩＤ、ＰＡＳＳＷＯＲＤ）が**盗まれて利用**される、**機器の脆弱性を利用**されることなど
- **ボットネットを貸し出して、金儲け**をしている**サイバー攻撃集団も存在**し、知らぬ間に**金儲けに利用されている**ことも

ＩｏＴ専用マルウェア『Ｍｉｒａｉ』

- **ＩｏＴ機器**などに感染して**ボットネットの一部**とする**マルウェア**
- 『Ｍｉｒａｉ』に感染しても通常どおりＩｏＴ機器は使用可能であるなど、**潜伏性が高い**マルウェア
- ソースコード（マルウェアを作成するための文字列）が公開されており、**亜種が多数存在**する
- 再起動をすると駆除される場合もあるが、脆弱性が改善されていなかったり、認証情報が盗まれていた場合は、**すぐに再感染**する

ＤＤｏＳ攻撃の踏み台にされないためには

- ☑ **認証情報**（ＩＤ、ＰＡＳＳＷＯＲＤ）を**初期値**から**複雑な物**に変更
- ☑ 使っていないＩｏＴ機器は**電源をオフ**にし、**ネットワークから隔離**
- ☑ ＩｏＴ機器の**フォームウェア**を**定期的にアップデート**
- ☑ ＩｏＴ機器の**自動アップデート機能**を利用
- ☑ サポートが終了した**古いＩｏＴ機器**はフォームウェアのアップデートができず、**脆弱性が改善されない**ため、**買替えを検討**