サイバーセキュリティ パートナーシップだより

R5-12

注意！

自社のウェブサイトが改ざんされるかも！？
～サイトのぜい弱性対処、できていますか～

近年、企業・団体のウェブサイトが改ざんされる事案が多数確認されており、もしも改ざんされれば、業務に様々な支障が生じる可能性があります。

「ウェブサイトは第三者から不正アクセスされるかもしれない」という危機意識を持つとともに、適宜、サイトのぜい弱性対処や適切なアカウント管理を行い、ウェブサイト改ざん被害を未然に防ぎましょう。

ウェブサイトが改ざんされたらどうなるの？

- 悪質サイト（偽ショッピングサイトやフィッシングサイト）への踏み台にされる
- 企業情報を改ざんされる
- サイトにマルウェア等を埋め込まれ、アクセスしたユーザーがウイルス感染する
- 復旧するために時間・費用を要する

等のおそれがあります。

不正アクセスされる原因は？

- ウェブサイトのぜい弱性（セキュリティ上の欠陥）を突かれる
- 管理者アカウント情報が推測されやすい簡単なものである

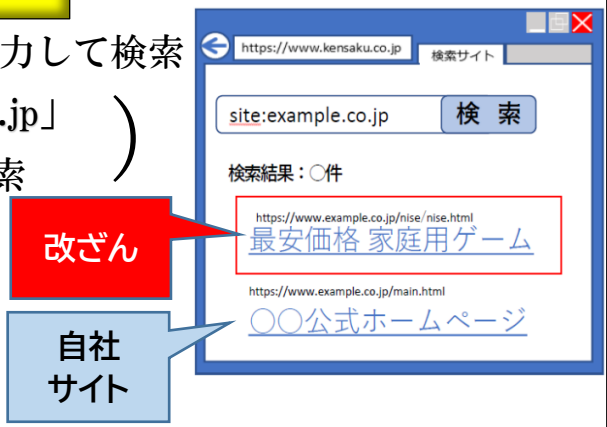
ことが主な原因と考えられます。

まずは自社サイトのチェックから！！

① 検索サイトで「site:自社ドメイン」と入力して検索

（※ 自社サイトURLが「www.example.co.jp」であれば、「site: example.co.jp」で検索）

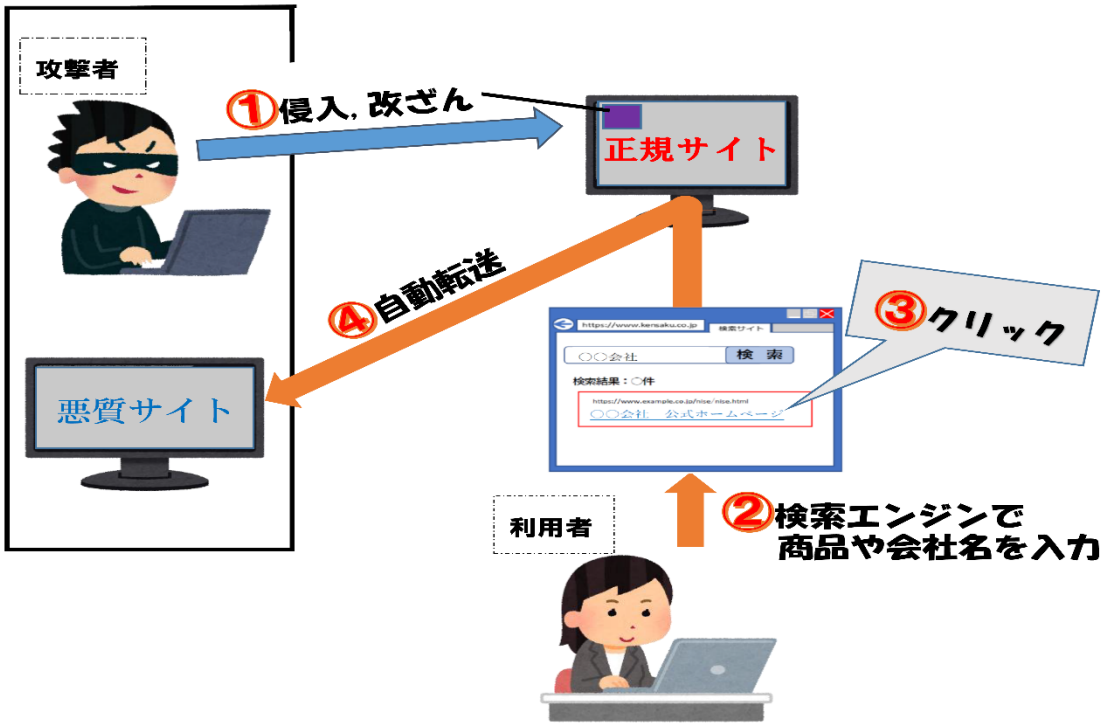
② 検索結果に自社ドメインを使用した見覚えのないページが表示されたら、**改ざん**（自社サイトのサーバ内に、不正にファイルを蔵置）されている



ウェブサイト改ざんの一例：悪質サイトへの誘導

攻撃者はウェブサイトに不正アクセスし、ウェブサイト内の改ざんを行い、当該サイトにアクセスした一般利用者を悪質サイトに誘導（自動転送：リダイレクト）させ、金銭や個人情報を得ようとします。

～誘導の流れ～



改ざんを防ぐために実施すべき対策

- ☑ ウェブサーバのソフトウェアや周辺機器のバージョンを確認し、最新にアップデートする
- ☑ 管理者パスワードを複雑にしたり、多要素認証機能を導入する

もしもウェブサイトが改ざんされたら

早急に自社の担当者に連絡し、不正なページの削除、ぜい弱性を修正する等、すぐに対策を行いましょう。

また、被害サイトに関係する各種記録（アクセスログやログイン履歴）を確認の上、警察へ通報、相談をお願いします。

山口県警察本部サイバー犯罪相談窓口
TEL　０８３－９２２－８９８３

県警ホームページにて広報資料や動画を公開中です。
（詳しくはQRコード参照）