

公開サイトの脆弱性に注意！

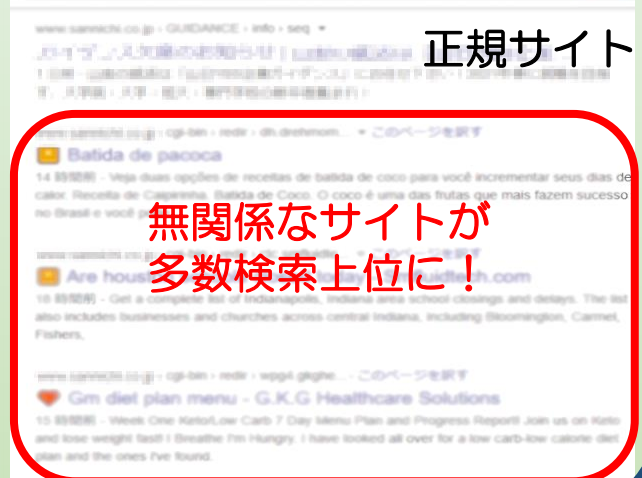
県内企業の公開サイトで脆弱性が発見されたり、サイトを改ざんされる事案が発生しています。いずれも利用者を悪意あるサイトへの誘導を図るものです。現時点で利用者の被害は確認されていないものの、公開サイトを運営する企業にあっては、注意が必要です。

事例1：オープンリダイレクトの脆弱性

例えば脆弱性のあるサイトへのリンクを細工して掲示板等に掲載したり、メール配信することにより、リンクをクリックした利用者が悪意あるサイトに転送されてしまう脆弱性です。

偽サイトへの誘導や、Web検索で表示順位を上げるためのSEOポイズニングと呼ばれる手口に利用されます。

脆弱性が発見されたサイトを
ドメイン名で検索した結果



事例2：サイト改ざん

WordPressと呼ばれるシステムで作られたサイトで、WordPressの脆弱性を突かれ、正規サイトのURLでアクセスすると、詐欺サイトに転送されるように改ざんされた事案です。

サイトの利用者が詐欺サイトに誘導されるとともに、Web検索でサイトの正規ドメイン名を検索すると、ECサイトを装った偽の商品情報ページが多数ヒットする状態になっていました。

改ざんされたサイトを



- 公開コンテンツの適切な設定（公開範囲等）
- サイト構築に使用しているソフトウェアバージョン等の適切な管理
- 定期的なコンテンツの改ざんチェック等の対策をお願いします！