TCSP Toyama Prefectural Police Cyber Security Personnel
サイバーセキュリティの置き薬
2020年 第18号

ドメイン名ハイジャックに注意しましょう！

国内で、ドメイン登録サービス内のアカウントに対する不正アクセスが発生しました。サービスの脆弱性を悪用したもので、ドメイン登録情報が不正に書き換えられて、メールの不正取得が行われたとのことです。

第三者が、何らかの方法でドメイン名を乗っ取る行為を、「ドメイン名ハイジャック」といいます。

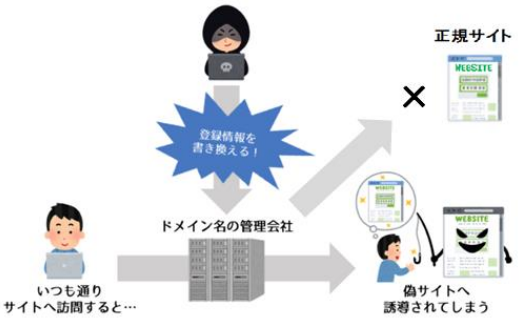
＜ドメイン名ハイジャックの手口＞

ドメイン名ハイジャックにはいくつかの手法があり、代表的なものとしては、

- レジストリに登録されている情報を不正に書き換える
- 権威 DNS サーバに不正なデータを登録させる
- キャッシュ DNS サーバに不正なデータをキャッシュさせる

の3つがあり、どれもドメイン名ハイジャックの方法として悪用されます。

手口としては、DNS サーバに登録されている Web サイトに関する情報を不正に書き換えることで、**特定のドメイン名にアクセスした時に、正規の Web サイトではなく、偽の Web サイトへと誘導する**、というものです。



＜対策＞ 自社ドメインの WHOIS 情報、DNS 情報は正しいか確認してください

- ○ 定期的にドメイン名の登録情報を WHOIS 等で確認する
- ○ 登録情報の変更申請に関するレジストラからの確認メールを見落とさないように注意する

万が一の際の素早い対応につなげてください。

引用元：○ サイバーセキュリティ.com
「URL:https://www.cybersecurity-jp.com/cyber-terrorism/31073」
○ JPNIC「URL:https://www.nic.ad.jp/ja/basics/terms/dom-hijack.html」