Ｆ－ＣＳＮＥＴ通信かわら版

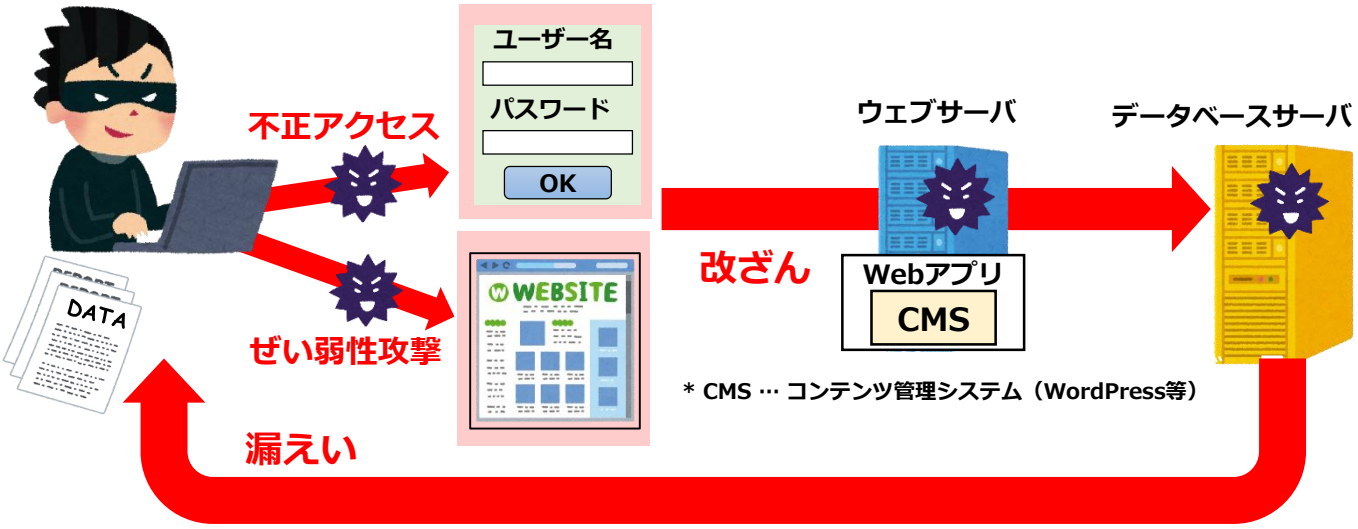
令和5年6月号

ウェブサイトが狙われています！

管理者用ID・パスワードの管理が適切に行われてなかったり、OSやソフトウェアのぜい弱性（セキュリティ上の欠陥）が放置されていると、不正アクセスやぜい弱性攻撃を受け、ウェブサイトを改ざんされ、ひいては情報窃取につながるおそれがあります。
今一度、自組織のウェブサイトの安全性を確認し、被害防止に努めましょう。

攻撃の一例

攻撃者は、窃取した管理者用ID・パスワードを悪用したり、OSやソフトウェアのぜい弱性を突いたりするなどして、ウェブサイトの改ざんや情報窃取を行っています。



＊ CMS … コンテンツ管理システム（WordPress等）

安全性向上のための対策

ウェブサイトを安全に運用するために、次に掲げる対策を講じましょう。

■管理者ID・パスワードの適切な管理

パスワードは強固に設定し、パスワードの使い回しを避けましょう。

■OSやソフトウェアのぜい弱性情報の確認、最新のパッチ等の適用

自組織で導入中のOSやぜい弱性情報について適宜確認し、最新のパッチ等を適用しましょう。

■WAF等のセキュリティ機能の活用

セキュリティ機能を確認し、不審な通信を遮断しましょう。

＊ WAF … Web Application Firewall

ＩＰＡ（独立行政法人情報処理推進機構）のウェブサイトにおいて「ECサイト構築・運用セキュリティガイドライン」が公開されていますので、ご活用ください。

https://www.ipa.go.jp/security/guide/vuln/guideforecsite.html

◆ 福岡県中小事業者サイバーセキュリティ支援ネットワーク（通称：F-CSNET）とは、県内中小事業者のサイバー犯罪被害の未然防止･拡大防止を目的として、県内の中小企業支援団体と公的機関で構築したネットワークです。

◆ 福岡県警察本部サイバー犯罪対策課では、最新のサイバー犯罪の手口や対策などをTwitterやホームページに掲載していますので、ぜひご覧ください。

【Twitter】 【HP】