青い森のサイバーセキュリティ

令和４年７月
青森県警察本部
サイバー犯罪対策課

ＥＣサイトの改ざん・利用者被害の防止を

◎正規のＥＣサイトが改ざんされ、利用者の情報が盗み取られる被害！

一般企業の正規のECサイト(※1)を改ざんし、不正なスクリプトを設置することで、当該サイトを利用した利用者の情報を盗み取るという手口が確認されています。

これは「Webスキミング」と呼ばれる手口の一種で、利用者が通常の商品購入手続き等を行った際に、その間に入力されたクレジットカード情報等の個人情報を盗み取るものです。

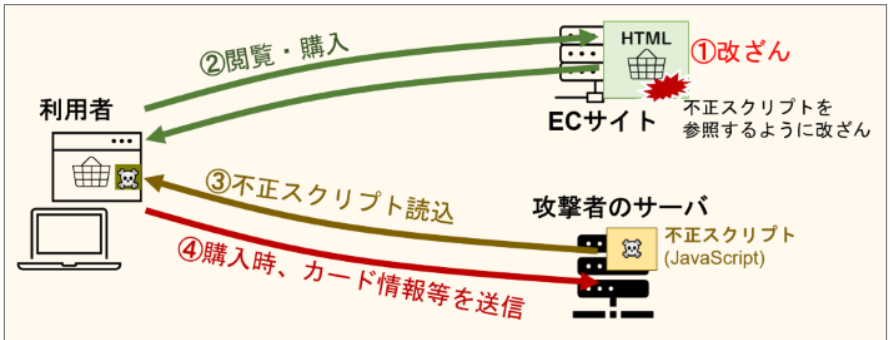

図　クレジットカード情報等を盗み取るまでの流れ

◎被害を防ぐためにサイト管理の強化を！

ECサイトの改ざん被害を防ぎ、事業と顧客を守るため、次の項目について確認・検討しましょう。

1　被害の未然防止

（1）サイトの管理者用アカウント不正利用の防止

⇒　推測されにくいパスワード、多要素認証に変更

⇒　管理画面へのアクセス制限を設定

（2）コンテンツ管理システム(CMS)やOS等の脆弱性の解消

⇒　ソフトウェアアップデートのこまめな適用

2　運用状況の監視

（1）不審なコンテンツ変更・管理者ログイン状況の監視

⇒　監視ツールの導入、アラートのメール通知

（2）WAF(※2)による通信監視

3　事業継続体制の確保

データバックアップの適時取得と迅速なサイト復旧方法の確立

※1:Electoric Commerce（エレクトリック　コマース=電子商取引）の略
※2:Web Application Firewall（ウェブアプリケーション　ファイアウォール=Web通信攻撃監視システム）の略
出典:一般財団法人日本サイバー犯罪対策センター，“ECサイト改ざんによるクレジットカード情報窃取について“，
https://www.jc3.or.jp/threats/topics/article-442.html