群馬県警察 Gunma.Pref.Police
部外用

サイバーセキュリティ対策通信 令和元年度 第２号

サイト改ざんによるクレジットカード情報流出に注意

～国内で被害が増加しています～

情報流出の被害にあわないように、システムの再点検を

ネットショッピングシステムの決済画面を改ざんして、クレジットカード情報を盗む手口（フォームジャッキング）による被害が県内でも確認されています。現状のシステムを過信せず、今一度、対策ができているか確認をしましょう。

最初に Check!

○ 既に、「改ざん」が行われていないか確認しましょう。
- 購入画面等に、不審なJavaScriptが設置されていないか、クレジットカード入力画面が不正なURLになっていないか、あるいは、いつもと違う画面が表示されていないか確認しましょう。

○ FTP、SSH等のログを確認し、不審なアクセスが無いか確認しましょう。

管理画面のセキュリティ対策 Check!　分からなかったら業者に確認

○ 管理画面のURLが推測されやすいものになってないか確認しましょう。
- 管理画面のURLは、初期URLではなく、自社にしか分からないものに変更しましょう。

○ 管理画面へのアクセス制限を行いましょう。
- 管理画面は、必ず英数字や記号を組み合わせた推測されにくいパスワードを設定しましょう。
- 部外者がアクセスできないようIPアドレスを制限しましょう。

サーバのセキュリティ対策 Check!　分からなかったら業者に確認

○ Webアプリケーションを利用する場合は、更新プログラム（パッチ）の適用及び適切なアクセス権限を設定しましょう。
- 特に、非公開とするべきフォルダ（ディレクトリ）は、利用者から閲覧できないよう適切にアクセス権限を設定しましょう。

○ 改ざん検知サービスを利用しましょう。
サーバ管理会社によっては、改ざんを検知するサービスを提供している場合があるので利用を検討しましょう。

情報流出が確認された場合 Check!　警察にも相談しましょう

○ 被害拡大防止のため、直ちにサービス停止を検討しましょう。
○ 業者に相談し、必要なログ等の保全や被害状況の調査を行いましょう。

導入したままメンテナンスを行っていないネットショッピングシステムには、ぜい弱性が発見されているものも見受けられます。サーバ管理会社や保守業者に確認して、確実にメンテナンスを行うようにしましょう。

＜群馬県警察本部警務課サイバーセキュリティ対策係 TEL027-243-0110 ＞