群馬県警察
Gunma Prefectural Police

サイバーポリスニュース

Webサイトを開設している事業者のみなさん

不正アクセスによるサイト改ざんに注意！

～システムの脆弱性を見直しましょう～

被害に遭わないように、システムの再点検を！

Webシステムに対する不正アクセスにより、サイト改ざんや個人情報流出等の被害に遭う可能性があります。アクセス制限や簡単なパスワードを設定するなど、Webシステムの脆弱性を放置している場合は、特に注意が必要です。現状のシステムを過信せずに、再点検を行いましょう。

◎既に「改ざん」が行われていないか確認しましょう。

- 会員入力画面や購入画面等に、不審なJavaScriptが設置されていないか、入力画面が不正なURLになっていないか、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。
- Webサーバ、FTP、SSH等のログを確認し、不審なアクセスがないか確認しましょう。

◎ 管理画面のセキュリティ対策

- 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、管理者等、特定の者にしか分からないよう複雑なものに変更しましょう。
- 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。
- 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。

危険な例）ID:manager　Pass:1111、ID:admin　Pass:1234等

◎ サーバのセキュリティ対策

- 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。
- 改ざん検知、ぜい弱性診断サービスなどを活用し、サーバのセキュリティを高めましょう。

◎ 情報流出が確認された場合

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Webシステムは、被害に遭うリスクが高くなります。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。

＜群馬県警察本部生活安全部サイバー犯罪対策課　TEL027-243-0110 ＞