

県内でも個人情報流出のおそれ！

～脆弱性の放置に注意～

情報流出の被害にあわないように、システムの再点検を

県内企業のシステムが不正アクセスされ、個人情報が出た可能性があると発表がありました。他人事と考えずに、どの事業所、団体においても発生する可能性がある問題であると認識し、現状のシステムを過信せず、先手を打って対策しましょう。

◎Webサーバのバージョンを確認して、脆弱性の無いものに更新してください！

- 脆弱性があるとホームページが容易に改ざんされます。
- Webアプリケーションも同様に脆弱性の無いバージョンに更新してください。
- 定期的にホームページのメンテナンスを行ってください。
- データは暗号化して、改ざん・漏洩に備えましょう。

分からなかったら業者に確認

◎ ネットワークの設定を確認してください！

- 外部との通信や、外部と内部ネットワーク間の通信は必要最低限に設定しましょう。
- 定期的にログを確認し、不審な通信（内部から外部への通信も含む）が無いか確認しましょう。
- ウェブアプリケーションファイアウォール等を導入している場合は攻撃パターンを登録し、不正なリクエストを遮断しましょう。

◎ ID・パスワードの設定を確認しましょう！

- ID・パスワードを平文で保存しないようにしましょう。
- パスワードは英数字や記号等を組み合わせた複雑なもの以外許可しないようにしましょう。
- 二要素認証等の安全性を高める仕組みを導入しましょう。

◎ サービス利用者に対して周知してください！

- ID・パスワードの使いまわしを極力しないようにしましょう。
- OSやウイルス対策ソフト等は、最新の状態に保ちましょう。

◎ 他の犯罪への注意

流出した個人情報を基に、意図しないダイレクトメールが送られたり、振り込め詐欺の予兆電話等の不審な電話がかかってくる可能性もあります。不審なメール、電話に十分注意し、犯罪被害に遭わないよう注意してください。

システム保守を複数の会社が行っている場合は、漏れの無いように各社に確認しましょう。

<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 >