企業のホームページが狙われています！

あなたの会社のホームページで、管理者ログイン用のＵＲＬやＩＤ・パスワードを、面倒だからと言って、初期状態のままで運用したりしていませんか？

危険です！

“設定の不備”をついた攻撃による被害が発生中です！

例：ｗｏｒｄｐｒｅｓｓを使って作成されたホームページへの不正アクセス被害（イメージ）

攻撃者は、初期状態のままで運用されていた管理者用ログイン画面のＵＲＬやＩＤ等を推測して不正アクセスを行い、管理者権限を取得します。

この管理者権限を使って、ホームページの改ざんや、データベースに保管されている顧客情報等の機密情報を窃取します。

例に挙げたwordpressは簡単にホームページが作成・管理ができるソフトウエアで、広く使われていることから、初期設定のままだとログイン用のURLやID等を攻撃者に容易に推測されてしまいます。

対策

管理者権限用の初期設定（URL・ID・パスワード等）を推測されにくいものに変更する。

その他サイバー犯罪対策に関する事は、大阪府警ホームページをご確認ください。

企業・組織等に向けたサイバーセキュリティ講演も実施中！

https://www.soumu.go.jp/main\_sosiki/cybersecurity/telework/