サイバーセキュリティ対策通信

大阪府警察本部サイバーセキュリティ対策課

放置された脆弱性がターゲット！

全ての企業・団体が狙われています！



大量の個人情報が漏洩する事案が多発しています。
インターネットに公開されているシステムは特に攻撃の対象となりやすいため「いつ攻撃を受けてもおかしくない」という前提で対策を講じることが重要です。
脆弱性情報が公開されると、短期間で悪用される危険性があるので、計画的かつ迅速に対応することが求められます。

「脆弱性の適切な管理」の基本対策

対策１ OS・アプリ等のパッチを速やかに適用する

・ 脆弱性情報の公開後、短期間で悪用・攻撃が行われる危険があります。
・ インターネットに公開されていない内部サーバーも含めて計画的かつ迅速に修正プログラムを適用し、最新の状態を保ちましょう。

対策２ サポートが終了している製品・バージョンを利用しない

・ サポート終了製品は修正プログラムが提供されず、脆弱性が放置されます。
・ 製品のサポート期間を把握して、機器の更新を行いましょう。

対策３ 利用していないシステム・機能の停止・削除する

・ 放置されたシステムや機能は、攻撃者の侵入の足がかりとして悪用されます。
・ 不要なシステムや機能は速やかに停止・削除を行い、リスクを抑えましょう。

対策４ 定期的な脆弱性診断等を実施する

・ システムやネットワークに潜在するセキュリティ上の弱点を早期に把握することが不可欠です。
・ 定期的に脆弱性診断を実施し、安全性を客観的に確認しましょう。

対策５ 不要なポート・プロトコル・サービスを無効化する

・ 業務上不要なポートや通信プロトコルを解放したままにすると、不審な外部接続を許す原因となります。
・ 必要な通信のみを許可するようにしましょう。



サイバー攻撃による被害は、もはや情報システム部門だけの問題ではありません。
サイバーセキュリティ対策を経営課題と位置づけ、必要な投資や人的体制整備を含む対策の強化をお願いします。

その他サイバー犯罪対策に関する事は
大阪府警察のウェブサイトやXを確認ください

大阪府警察ウェブサイト

大阪府警察サイバーセキュリティ対策情報 X