「テロ対策パートナーシップ和歌山」通信【第5号】

令和元年８月２０日

テロ対策パートナーシップ

和　歌　山　事　務　局

サイバー攻撃の脅威と対策について

平素より、テロの未然防止に向けた取り組みへのご理解とご協力ありがとうございます。今回は、サイバー攻撃による被害の未然防止に向け、最近のサイバー攻撃の主な手口とその対策について紹介します。

○　情　　勢

近年、国内外において政府機関等に対するサイバー攻撃が続発しています。重要インフラの基幹システムを機能不全に陥れ、社会の機能を麻痺させるサイバーテロや、情報通信技術を用いた諜報活動の脅威は、国の治安、安全保障及び危機管理に影響を及ぼしかねない問題となっています。

このようなサイバー攻撃は、民間事業者や個人のパソコンやネットワークを経由（踏み台として利用）してなされることがあるため、セキュリティの強化を心掛ける必要があります。

○　サイバー攻撃の主な手口

◇　標的型メール攻撃

業務に関連した正当なものであるかのように装い、市販のウイルス対策ソフトでは検知できない不正プログラムを添付した電子メール（標的型メール）を送信し、受信者のコンピュータを不正プログラムに感染させ、情報の窃取を図るもの

◇　ＤＤｏＳ攻撃

特定のコンピュータに、複数のコンピュータから一斉に大量のデータを送信して負荷をかけるなどして、そのコンピュータによるサービスの提供を不可能にするもの

◇　水飲み場型攻撃

対象組織の職員が頻繁に閲覧するウェブサイトを改ざんし、当該サイトを閲覧したコンピュータに不正プログラムを自動的に感染させるもの

○　サイバー攻撃への対策

◇　ウイルス対策ソフトを導入し、常に更新しましょう
◇　ＯＳ・ソフトウェアを常に更新しましょう
◇　ＩＤ・パスワード管理を適切にしましょう
◇　定期的にバックアップを取りましょう
◇　設定や認証方法を見直しましょう
◇　手口を知り、対策方法を学びましょう
◇　クリック・タップ前に、相手が本人か確認しましょう
◇　セキュリティポリシーの策定、対応マニュアルの作成、体制の構築、セキュリティ訓練・職員への教養を行いましょう〔発生することを前提に対応を〕