



サイバー攻撃への備え

インターネットが、国民生活や社会経済活動に不可欠な社会基盤として定着する中で、我が国の政府機関、民間企業等に対するサイバー攻撃が発生しています。特に、社会機能を麻痺させる電子的攻撃であるサイバーテロや情報通信技術を用いた諜報活動であるサイバーインテリジェンスの脅威は、国の治安や安全保障に影響を及ぼすおそれのある問題となっています。

警察では、「東京オリンピック・パラリンピック競技大会」、「ラグビーワールドカップ2019」を控え、サイバー攻撃対策を推進しています。

サイバーテロ・サイバーインテリジェンスの手口

- 攻撃対象のコンピューターに不正に侵入
- 不正プログラムに感染させ、管理者の意図しない動作を命令

【主な手口】

- ・標的型メール攻撃 (不正プログラムを添付したメールを送りつけ感染させる)
- ・水飲み場型攻撃 (ウェブサイトを開覧したPCに不正プログラムを自動的に感染させる)



サイバー攻撃への備え

- ① セキュリティ環境の整備の推進 (アップデートや設定変更等)
- ② 見知らぬメール等は、安易に開かず送信元を確認
- ③ 社員等教育の取組推進

サイバー攻撃かなと思ったら警察へ通報を！

- ① パソコンが不審な動作をしている
- ② ホームページが閲覧できない
- ③ ホームページの内容が改ざんされている

早岐警察署 0956-39-0110

