# 情報セキュリティ対策の注意点

関東管区警察局茨城県情報通信部情報技術解析課

| 対策項目 | 注意点 |
|---|---|
| コンピュータウィルス対策 | 1　新しいコンピュータウィルスによる被害が毎日報告されています。コンピュータウィルス対策ソフトを導入するだけではなく、常に最新のコンピュータウィルスに対応できるようパターンファイルを更新して下さい。<br>2　プロバイダがウィルス対策機能を提供している場合は、パソコンにコンピュータウィルスメールが着信する前に削除されますのでコンピュータウィルスの感染を未然に防ぐことが出来ます。機能の詳細については加入しているプロバイダの相談窓口に問い合わせ下さい。<br>3　パソコンのアドレス帳に登録されているメールアドレスにコンピュータウィルスメールを送るものがあります。知らず知らずコンピュータウィルスに感染している場合もあります。知人や取引先からのメールであっても、必ずコンピュータウィルス対策ソフトでチェックした後メールを開くようにしてください。<br>4　コンピュータウィルスについての情報はコンピュータウィルス対策ソフトを製造している業者や警察庁情報セキュリティポータルサイト@police(http://www.cyberpolice.jp)で情報を公開していますので参考として下さい。 |
| 情報漏洩対策 | 1　車両を離れたわずかな間に、車内にあったパソコン(顧客情報の入ったもの)が盗まれた事例があります。パソコンやフロッピーディスク等を外部に持ち出す場合は、盗難に注意してください。<br>2　インターネットファイル共有ソフトによりパソコン内の情報が漏れたり、インターネットファイル共有ソフトの機能を利用したコンピュータウィルスにより、作成中のファイルが画像として配信された事例があります。重要情報が保存されたパソコンにはインターネットファイル共有ソフトを絶対にインストールしないで下さい。<br>3　パソコンを使用中に席を離れる場合、利用権限のない者が重要情報にアクセスすることを防ぐため、解除する際にパスワードの入力が必要な機能を用いて画面をロックして下さい。 |
| フィッシング詐欺 | 1　銀行や信販会社を装って口座番号や暗証番号を入力させるフィッシング詐欺が日本国内でも発生しています。銀行や信販会社からの不審なメール等について問い合わせる場合は、直接銀行や信販会社に問い合わせて下さい。<br>2　フィッシング詐欺についての情報は警察庁情報セキュリティポータルサイト@police(http//www.cyberpolice.jp)で公開していますので参考としてください。 |
| 不正アクセス対策 | 1　無線 LAN を無断使用し、インターネットオークション詐欺を行っていた事例があります。無線 LAN を使用する場合は、不正利用や防ぐため、必ず暗号機能やパスワード機能を有効にしてください。<br>2　ネットカフェでオンラインバンキングを利用した際、文字記録ソフトにより暗証番号が記録され、第三者に大金が引き出された事例があります。ネットカフェでは暗証番号などの個人情報を入力しないでください。<br>3　長い間同じパスワードを使用していると推測される可能性がありますので、パスワードは定期的に変更しましょう。 |
| サイバーテロ対策 | 1　重要データを保管しているコンピュータに対するサービス停止やホームページの改竄に備え、関係者や関係部門に連絡や手続きができるように確認しておきましょう。<br>2　サイバーテロ対策について警察庁情報セキュリティポータルサイト@police(http//www.cyberpolice.jp)で公開していますので参考としてください。 |