情報セキュリティのポイント

まずはここから。被害者にも加害者にもならないために。

附属総合情報センター

Point 1 安直なパスワードは絶対厳禁！

1．自分の名前、誕生日、車のナンバーなど、周囲の人たちが容易に知ることができる文字列を使用しない。
2．大文字、小文字、数字、記号のすべてを使って最低８桁以上（10 桁以上が推奨）にする。
3．定期的に変更する。
4．他人には絶対に教えない（パスワードを聞いてくる人は間違いなく悪人です。）。
5．パスワードはアナログ管理（手帳など）とし、何のパスワードかは自分だけがわかるように記載しておく。絶対にパソコン内に記録しない。

Point 2 セキュリティ対策ソフトは絶対必需品と心得よ！

1．学内ネットワークに接続する際は、必ず学内統一ウイルス対策ソフトの導入を行うこと。
2．最近のマルウェア（ウィルス等）は、パソコンのユーザーに気づかれないように作られたものが主流。セキュリティ対策ソフトなしで発見することはほぼ不可能。
3．セキュリティ対策ソフトのウィルスパターンファイルはほぼ毎日更新されるので、常に最新の状態にしておくこと。
4．動作が急に遅くなった、ディスクやモデム等のアクセスランプが勝手に点滅するなど異常な兆候があったら、まずは LAN 接続を切断して、信頼できる詳しい人に相談を。

Point 3 ソフトウェアのアップデートをサボるのは自殺行為！

1．OS（Windows など）やアプリケーション（Word、Excel、Power Point、その他多数）には、「脆弱性」と呼ばれる安全性の弱い部分（セキュリティホール）があり、それを悪用した攻撃が日常的に行われています。
2．マイクロソフト社などソフトウェアのメーカーが公開する「修正プログラム」（セキュリティパッチ）は必ず適用すること。
3．OS を含め主要なソフトウェアの多くは、デフォルト（初期設定）で「自動更新」する設定になっているはずですが、何かの間違いで OFF になっていないか今一度確認を。

Point 4 トラブル発生時の最後の砦はバックアップ！

1．ウィルス等によるデータの破壊やランサムウェアによるデータの暗号化のみならず突然のパソコンの故障など、データを失うリスクは常にあることを意識すること。
2．バックアップ媒体は、外付けハードディスク、DVD、USB メモリーなどがあるが、それぞれの媒体の寿命や書き込み速度などの特性に応じた自分なりのバックアッププランを実行すること。
3．USB メモリーはコンパクトで便利な反面、壊れやすく、また「落とした・なくした・盗まれた」といったトラブルが最も多い媒体であることを理解した上で使用すること（USB メモリーの場合は二重のバックアップをしておくのが安全。）。

Point 5 電子メールを安全に使うための常識とマナーを身につけよ！

1．多くのメーラー（Outlook など）の初期設定は HTML メールだが、HTML にはプログラムが埋め込めるためセキュリティ的にはとてもリスクが高い。特に必要がある場合を除き、送受信ともに TEXT メールに変更すること（ビジネスの世界では TEXT メールが常識。）。
【注】攻撃メールを受信した場合、TEXT メールの場合は、メールを開いても、添付ファイルや本文中のリンクに触れない限り感染するリスクはほとんどないが、HTML メールの場合は、メールを開いた途端に感染させるプログラムを実行されるリスクが高い。

2．メールアドレス（＝個人情報）漏えい事故のほとんどが、TO、CC、BCC の使い方の間違いが原因。正しい使い分けを覚えて実践すること。

Point 6 秘密を護る。添付ファイルを護る！

1．Microsoft の Word、Excel、Power Point にはデータ暗号化機能があるので、機密性の高い情報を添付ファイルで送る場合はこれらの機能を有効に活用すること。
2．簡便な方法としては、zip 形式の圧縮ファイルへのパスワード設定（フリーウェアの Lhaplus などが多く使用されている。）もよく行われている。
3．重要な内容を含むメールを送る際には、本文には重要な内容は記載せず、暗号化した添付ファイル内に記載するのがより安全。
4．添付ファイルを開くためのパスワードは、電話連絡、あらかじめ当事者間で決めておくなどの方法とし、パスワードをメールで送ることはしない。

Point 7 その機器やデータの持ち込み・持ち出しは本当に大丈夫？

1．パソコンなどの機器やデータの持ち込み・持ち出しには、常に紛失・盗難やウィルス感染の拡大といったリスクが伴います。安全性が十分に確保できるか、また本当に持ち込み・持ち出しが必要かを十分に検討すること。
2．近年の個人情報への国民の意識の高まりや、頻繁に発生する情報漏えい事故などを背景に、多くの企業や組織では、持ち込み・持ち出しを制限したりルールを設けたりしています。自分が行おうとしている持ち込み・持ち出しが許されるのかについて確認を。
3．明確なルール等を設けていない組織等でも、持ち込み・持ち出しを行う場合は、上司・指導者等に確認を。

Point 8 漏えいが絶対に許されない３つの情報

患者情報

例え患者さんの氏名を出さなくとも、関係者であれば、誰に関する情報なのかが特定されてしまう場合があります。このような情報の漏えいは病院の信頼を大きく失墜させてしまいます。

業務上知り得た秘密

医療従事者は、患者さんの医療情報だけでなく、時として家族関係や就学状況その他の個人情報を知ってしまうことがあります。このような情報についても絶対に漏えいしてはいけません。

企業（組織）秘密

研究開発情報、取引関係や内部事情など、どこの企業や組織でも外部に漏れると都合が悪かったり、損失を被るような情報があります。組織に属する以上は、このような情報を漏らしてはいけません。

SNS が危ない！間違ってもこれらの情報を投稿してはいけない！

お問い合わせ・ご相談は
附属総合情報センター 総務・システム係 へ
（基礎医学研究棟 図書館２階の奥に事務室があります。）
内線：22390　or　e-mail：icccj@sapmed.ac.jp
Web サイト：　https://infonavi.sapmed.ac.jp/jpn/