エキスパート活動　課題A「アクセス制御と不正アクセス」

□事例から考えよう！　※右の資料を参考に考えよう

＜事例A＞

(1)学校の課題提出フォルダは、どのようなアクセス制御になっていたと考えられるかまとめてみよう。

(2)アクセス制御がない場合、どのような問題が発生するのかまとめてみよう。

(3)アクセス制御は、どのような場面で活用されているのか調べてみよう。

＜事例B＞

(1)この事例において、問題となる行為は何かまとめてみよう。

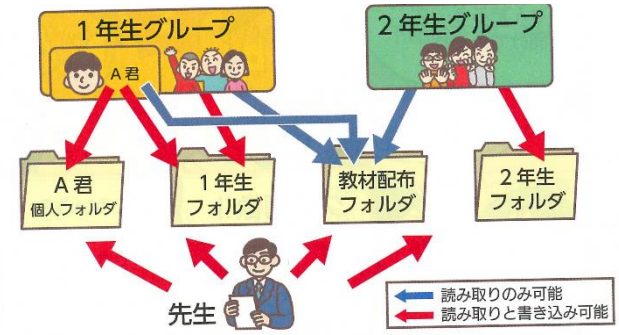
(2)不正アクセス行為をした場合、どのような罰則があるのか調べてみよう。

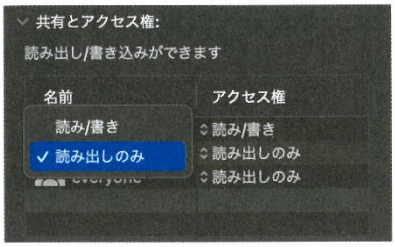
(3)不正アクセスに関する事件は、実際にどのようなものがあるのか調べてみよう。

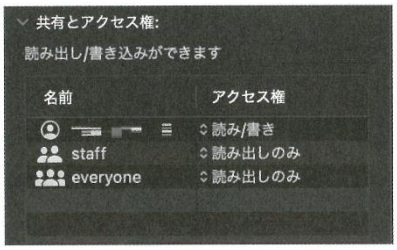
□アクセス制御

大切な情報を複数人のユーザで扱う場合には、閲覧、編集、削除などは、アクセスが認められたユーザのみができるようにする。これをアクセス制御という。これにより、悪意のある人物やケアレスミスによる情報漏えい、改ざん、データの紛失などを防ぐことができる。なお、管理者ユーザ（Administrator）など限られたアカウントは、すべての権限が許可されている。この状態をフルコントロールという。

例えば、学校のファイルサーバでは、下の図(左側)のようにアクセス制御されていることが多い。また、コンピュータでの設定画面は下の図(右側)のようなものがある。







□不正アクセス禁止法

正式名称は「不正アクセス行為の禁止などに関する法律」である。アクセスを許可されていない人が、無断で他人のアカウントを使用する「なりすまし行為」や、コンピュータなどの脆弱性と呼ばれる、設計上の不具合やミスが原因の弱点を突いて侵入する「侵入行為」は、不正アクセス行為となる。

この法律では、禁止事項が成立した場合、以下の罪によって罰せられる。

禁止事項	罪名
不正なアクセス	不正アクセス罪
不正なパスワードの取得	不正取得罪
他人への第三者の ID やパスワードの提供	不正助長罪
不正取得された ID やパスワードなどを保管する行為	不正保管罪
ユーザをだまして ID やパスワードを入力させる行為（フィッシング行為）	不正入力要求罪

□不正アクセスへの対策

不正アクセスを防ぐために、以下の対策をしよう。

①安全なパスワードを設定し、正しく管理する

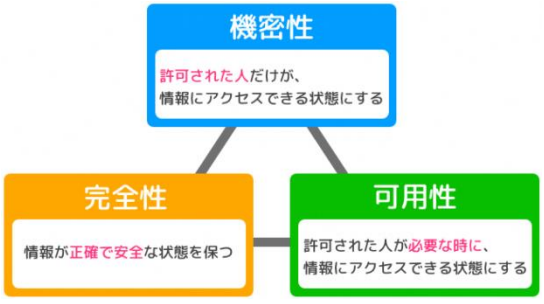
②多要素認証を導入する

③常にウイルス定義ファイルや OS などを最新の状態に保つ

また、OS にはファイアウォールの機能があり、コンピュータ本体の不正侵入を防止する。ファイアウォールは、インターネットと内部のネットワークの間に設置する装置やソフトウェアの総称であり、各種サーバにより構成する。外部からの不正アクセスを防止するだけでなく、内部から外部へのアクセス制限を行うこともできる。ただし、ファイアウォールがあれば絶対に安全というわけではない。

□情報セキュリティ３要素（CIA：Confidentiality Integrity Availability）

大切な情報を安全に管理するうえでは、情報セキュリティが欠かせない。情報セキュリティには、三つの要素（機密性、完全性、可用性）がある。



エキスパート活動　課題Ｂ　「フィルタリング」

□事例から考えよう！　※右の資料を参考に考えよう

＜事例１＞

(１)フィルタリング機能でブロックされる内容には、どのようなものがあるのか調べてみよう。

(2)フィルタリング機能を使用しない場合、どのような問題が発生するのか考えてみよう。

(3)フィルタリング機能は、どのようなところで実際に使われているのか調べてみよう。

＜事例2＞

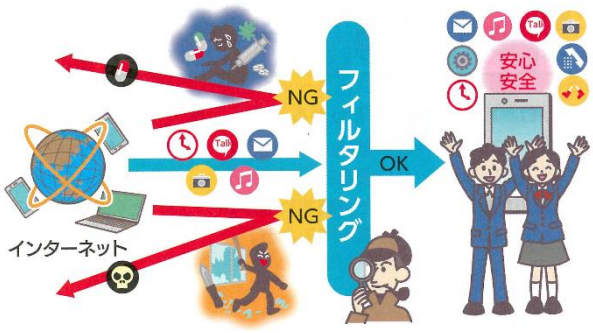
(１)不快な内容のメッセージを防ぐには、どうすればよいのか調べてみよう。

(2)SNS には、どのようなフィルタリング機能があるのか調べてみよう。

(3)自分自身がSNSを使用するとき、どのようなフィルタリング機能を設定すればよいのか考えてみよう。

□フィルタリング機能の必要性

フィルタリング機能があると、自由にインターネットを見られなかったり、アプリが自由に使えなかったりして、不便に思うことがある。一方で、インターネットの世界は、何か問題が起きた場合、その痕跡を二度と消すことができないリスクがある。フィルタリングは、未成年者を危険なサイトやアプリなどから守るために必要不可欠なものである。



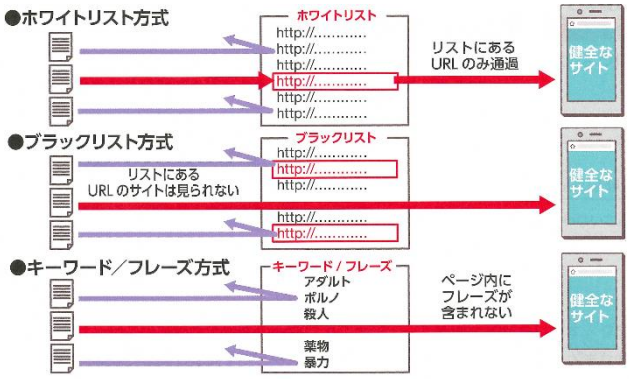
フィルタリングには、年齢などに合わせて制限の項目が変更できるものもある。どのくらいの段階のフィルタリングを設定するのか、保護者と十分に相談し、活用しよう。

フィルタリング対象となる項目には、成人向けコンテンツ、犯罪・暴力に関する内容、不正 IT 技術に関する内容がある。また、YouTube などの動画配信サイトでは、成人向けのコンテンツを含む可能性がある動画を制限する機能も存在している。

□フィルタリングの方式

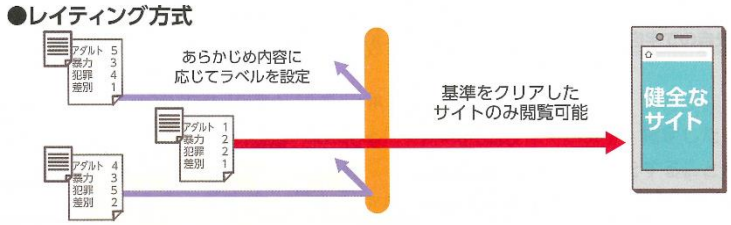
フィルタリングの方式には、いくつかの種類が存在する。フィルタリングソフトウェアの種類や設定で、下記の方式によりフィルタリングされる。（表または左の図）

方式	説明
ホワイトリスト方式	登録された安全な Web サイトのみ閲覧できる方式。
ブラックリスト方式	登録された有害な Web サイトの閲覧を制限できる方式。
キーワード／フレーズ方式	登録された有害なキーワードやフレーズが含まれる Web ページの閲覧を制限できる方式。



□レイティング方式

インターネット上の各 Web サイトに対してあらかじめ一定の規準で格付け（レイティング）を行い、基準をクリアしたサイトの閲覧が可能になるようにしたフィルタリングの方式。



□メールのフィルタリング設定

メールの受信にもフィルタリングがある。設定には、以下のようないくつかの方法がある。

- 特定のメールアドレスのみ受信、または、拒否
- 指定したドメイン名（メールアドレスの「@」以降の部分）のメールのみ受信、または、拒否
- 特定の危険な URL が含まれたメールを拒否
- 自動判定による迷惑メール拒否

迷惑メールを受信せず、必要なメールのみ受信できるよう、フィルタリングの設定を調整しよう。

□「青少年が安全に安心してインターネットを利用できる環境の整備などに関する法律」について

平成 30 年2月 1 日の「青少年が安全に安心してインターネットを利用できる環境の整備などに関する法律」の法改正で、18 歳未満の青少年が携帯電話の契約、機種変更をする際には、フィルタリングの設定が法律で義務化された。しかし、フィルタリングが設定されていてもフィルタリングの方式により、閲覧できる情報が異なるため、フィルタリングを過信せず、安全で正しい利用ができるように心がけよう。

エキスパート活動　課題 C　「無線 LAN と暗号化」

□事例から考えよう！　※右の資料を参考に考えよう

＜事例 A＞

(1)無線 LAN ルータの初期設定には、どのような方法があるのか調べてみよう。

(2)簡単接続の機能を使わない場合は、どのようにして接続すればよいのか調べてみよう。

(3)無線 LAN ルータのセキュリティの種類には、どのようなものがあるのか調べてみよう。

＜事例 B＞

(1)この事例の公衆無線 LAN は、なぜセキュリティが低いのか考えてみよう。

(2)セキュリティの低い公衆無線 LAN を使用すると、どのような問題が発生するのか考えてみよう。

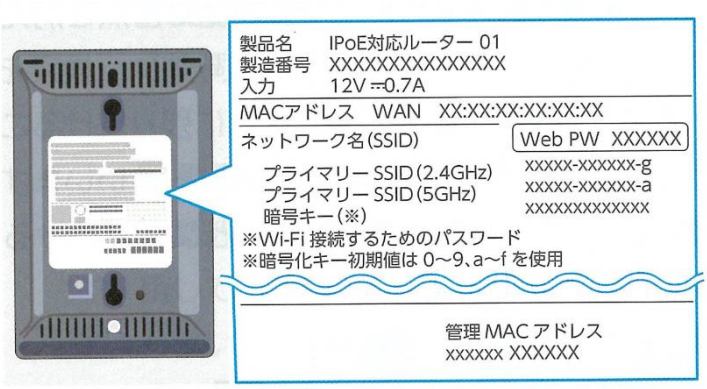
(3)公衆無線 LAN に接続する際には、何に気を付けるとよいのか話し合ってみよう。

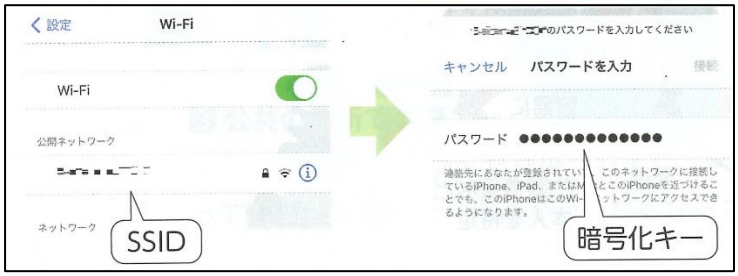
□SSID と暗号化キー、ステルス化

簡単設定などの機能を使わずに無線 LAN に接続するには、SSID と暗号化キーの設定が必要である。SSID はネットワークの名前である。また、暗号化キーは無線 LAN ルータの暗号を解読するための鍵となる。SSID と暗号化キーを確認するためには、無線 LAN ルータ本体の設定画面から確認するか、無線 LAN ルータの裏側に記載されたシールで確認を行う。セキュリティ上、暗号化キーは、購入時に設定されているものから変更することが望ましい。(右上の図)

無線 LAN に接続する際は、端末の設定画面で、使用したいネットワークの SSID を選択し、暗号化キーを入力することで接続できる。(右の図)

無線 LAN に接続できる機器で無線 LAN に接続する場合、電波の届く範囲にある無線 LAN の SSID が一覧で表示されます。外部の人に無断で無線 LAN を設定されないようにするために、SSID を見えないようにすることができます（ステルス化)。(右の図)



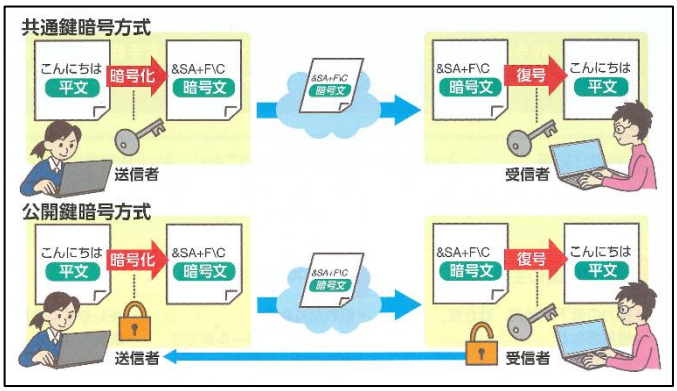


□インターネットで使われる二つの暗号化方式

暗号化されていない状態のデータのことを「平文(ひらぶん)」と呼び、第三者が平文を読み取れない状態にすることを「暗号化」という。また、暗号化されたデータをもとの平文に戻すことを「復号」という。

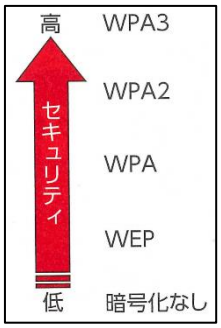
インターネットで使われる暗号化の方式は、共通鍵暗号方式と公開鍵暗号方式が一般的に使われている。それぞれどのような暗号化の方式なのか、特徴を整理しておこう。(右の表と下の図)

共通鍵暗号方式	公開鍵暗号方式
送信者と受信者が同じ鍵である共通鍵を使い、暗号化と復号を行う暗号方式。処理速度は公開鍵暗号方式より速いが、共通鍵を安全な方法で共有しなければならない。	受信者がインターネット上に公開鍵を公開して、送信者はその公開鍵を使用して暗号化する方式。受信者は、秘密鍵を使用して平文に復号する。共通鍵暗号方式と比べ処理速度が遅いが、秘密鍵をインターネット上で共有する必要はない。



□無線 LAN のセキュリティ

無線 LAN には、いくつかのセキュリティの強度が存在している。暗号化の強度が高い WPA3、WPA2 を設定するとよい。



□暗号化と公衆無線 LAN の盗聴

公衆無線 LAN では、暗号化が行われていなかったり、暗号化のレベルが低かったりするものがある。しっかりと暗号化が行われていないと、通信途中で通信内容を盗み見られる可能性があり、さまざまな犯罪につながる可能性がある。暗号化が行われていない、または、暗号化の強度が低い公衆無線 LAN は使わないようにしよう。