セキュリティ・チェックリスト解説　【5～10分】

セキュリティ全般について

□　１　児童生徒の写真や作品は，本人と保護者の同意を得た上で利用している。

　児童生徒の個人情報の管理は大切です。学校新聞やWebページに顔写真や児童生徒の作品を掲載する際など，その扱いに注意する必要があります。

□　２　仕事に関係のないWebページは見ていない。

　悪意のあるWebページを閲覧しただけで，悪意のあるプログラムを実行される危険性があります。そのような被害に遭わないためにも，仕事上必要でないWebページの閲覧は避けるようにしましょう。

□　３　学校のコンピュータに無断でソフトウェアをインストールしていない。

　Webページでダウンロードしたり，外から持ち込んだりしたソフトウェアは，安全性の検証ができていないことがあります。どうしてもそのソフトウェアが必要な場合，ネットワークから切り離した環境で動作確認をし，管理者の許可を得てから使用するようにしましょう。

□　４　機密情報は電子メールで送っていない。

　電子メールは複数のサーバーを経由して相手先に届くため，他人が情報を入手してしまう危険性があります。また，メールは一般的に暗号化もされていません。
　機密情報を電子メールで送信することは，避けるようにしましょう。

□　５　機密情報を含む紙や記録媒体は，適切な方法で廃棄や削除をしている。

　何気なく捨てているゴミの中にも，個人情報が含まれていることがあります。機密情報を含む紙は，情報が漏えいしないようにシュレッダーなどで処分しましょう。また，記録媒体については，データを完全消去するソフトウェアなどを利用して，情報が漏えいしないようにしましょう。

□　6 コンピュータのユーザーＩＤやパスワードは，他人に知られないよう管理している。

ユーザーIDとパスワードは，その人を識別する重要な情報です。これらの情報が他人の目に付きやすいところにあると，なりすまし（他人のIDやパスワードを盗み，その人のふりをしてネットワーク上で活動すること）をされるなど，大きな問題を引き起こす危険性があります。IDとパスワードは暗記するか，自分しか分からないところに記録しておくようにしましょう。

□　7 電子メールを誤送信しないように注意している。

電子メールは，一旦送信すると取り消すことができません。宛先は手入力か，アドレス帳をクリックして選ぶ形で入力しますが，必ず送信前に正しいアドレスであることを確認するようにしましょう。
また，メーリングリストから送られてきたメールについて，単純に「返信」した場合，そのメーリングリスト加入者全員に情報が届くので注意が必要です。

□　8 離席時や帰宅時にコンピュータを不正操作されないための対策をしている。

ちょっと席を離れた間に，作業の内容を盗み見されたり，勝手にコンピュータを操作されたりすることがないよう，コンピュータにパスワードロックをかけるなどの対策を施すようにしましょう。

□　9 コピーやプリンタの出力用紙は，直ちに回収している。

離れた場所にあるプリンタに出力した書類は，ついつい取りに行くのを忘れることがあります。多数の人の目に触れる場所に，各種の情報資産をさらすことがないように心がけましょう。

□　10 帰宅時には机上を片付けている。

紛失や盗難を防ぐためにも，帰宅時には机上を片付け，機密文書については，鍵のかかるところに保管するようにしましょう。

□　11 ファイル共有ソフトは，自宅のコンピュータにもインストールしていない。

ファイル共有ソフトを通じた情報漏えいは社会問題化しており，政府等による共有ソフト自体の不使用の呼びかけがなされています。

ＵＳＢメモリ等でデータを持ち出す際について

□　12 データを持ち出す際，決められた必要な手続きを知っている。

　データを持ち出すことで，情報漏えいの危険性が高まります。しかし，仕事上どうしてもデータを持ち出さなければならないこともあります。その際に，学校でどのような手続きが必要なのか，日頃から確認しておきましょう。

□　13 ＵＳＢメモリなどを持ち出す時には，常に携行している。

　持ち出したデータは，盗難に遭ったり，紛失したりしないようにするためにも，常に携行するようにしましょう。

□　14 持ち出したデータは，パスワードが設定されているか暗号化されている。

　万一，持ち出したＵＳＢメモリ等を紛失した場合，大切なデータが簡単に漏えいしないようにするためにも，データを暗号化し，パスワードを入力しないと読み取りができない状態で保存しておきましょう。

□　15 ウイルス対策ソフトを自宅のコンピュータにもインストールしている。

　コンピュータウイルスは，インターネットや電子メール，ＵＳＢメモリ等，いろいろな経路で侵入してきます。データを持ち帰り，使用する際には自宅のコンピュータにも，必ずウイルス対策ソフトをインストールするようにしましょう。

□　16 ウイルス対策ソフトは，定期的に更新し，最新の状態にしている。

　日々，新しいコンピュータウィルスが出現しています。それに対応するためにも，ウイルス対策ソフトは定期的に更新し，新しいコンピュータウイルスの侵入を防ぐようにしましょう。

□　17 ＯＳ(Windows等)やソフトウェアは定期的に更新し，最新の状態にしている。

　コンピュータウイルスは，ＯＳやソフトウェアのプログラムのセキュリティホール（脆弱性）につけ込み，コンピュータに被害をもたらします。定期的にＯＳやソフトウェアを更新し，脆弱性に対処するようにしましょう。

□　18 自宅で使用したデータは，自宅のコンピュータから必ず消去している。

　自宅のコンピュータにデータをコピーして作業した場合，そのファイルを必ず完全に消去して，データの漏えい・拡散を防ぐようにしましょう。