# 技術的・物理的セキュリティ

## 【　技術的セキュリティ（安全管理措置）】

技術的対策としては、ネットワークインフラセキュリティ、アプリケーションセキュリティ、不正アクセス対策などが含まれます。
ここでは、学校の業務の中でも、特に身近な問題として感じられる項目を挙げています。

### 1　コンピューターウィルス対策

ネットワークに接続された環境下では、たった１台のコンピューターのウィルス対策を怠るだけで、ネットワーク全体にウィルスが蔓延し、大きな損害を与える可能性があります。

A　予防対策

1）PC 使用者へのセキュリティ教育とセキュリティ体制を整える。
・ウィルスの感染を未然に防ぐため、従業員の基礎的知識が必要。感染を防ぐ為に必要な手順を整え、教育を行う。また、感染してしまった場合の手順なども整えておく。

2）ウィルスやワームの傾向、感染方法、症状などに関しての、最新情報を常に入手し、把握する。

3）システムの管理
・管理対象コンピューターの、パターンファイルの更新、適用状況、ウィルスチェックの状況などを的確に管理する。
・ウィルス感染の場合も考慮し、データのバックアップとリストア体制の整備を行う。

4）ワクチンソフト導入
・インターネット接続ポイント、ネットワークの境界
・各サーバー
・各クライアント PC

B　ウィルスの感染経路

・電子メールの添付ファイル
・電子メールの HTML スクリプト
・ウェブサイトの閲覧
・ネットワークのファイル共有
・マクロプログラムの実行

C　感染した場合

・感染コンピューターをネットワークから、隔離する。
・ワクチンソフトなどにより、ウィルスチェックと駆除を行う。
**＊専門家への依頼をお勧めします。**

D　感染による症状例

・他のウィルス、システムへの侵入経路（バックドア）が作成される。
・システムが改竄される。
・コンピューター内のファイル、パスワードなどを、メール添付ファイルとして送信する。
・アドレス帳のアドレスに対して、メールを（大量に・ランダムに）送信する。
・特定サイトへ Dos 攻撃をする。
・一定期間後、または直ぐに、データの破壊、ハードディスクのフォーマット、起動不能 BIOS の書き換えなどの破壊を行う。

E　その他、スパイウェア、ウィニー（ファイル交換ソフト）について

スパイウェアは、コンピューター内部からインターネットに対して情報を送り出すソフトウェアで、ＰＣ内に存在していることや、動作していることに気付かない場合が多い。全てが悪質なものとは限りませんが、明らかに情報を盗む目的のものもあります。
・スパイウェアを除去するソフトウェアの導入

ウィニー（Winny） などのファイル交換ソフトを利用したウィルスにより、学校の個人情報や機密情報の漏えいにつながる。
・学校で使用するＰＣにファイル交換ソフトが無断でインストールされないこと。
・ファイル交換ソフトのインストールされた個人所有のＰＣに、学校の個人情報データなどが保存されないよう、徹底管理する。

## 2　システム対策

1）アクセス制御（データ・システム）
- ネットワーク境界での通信の制御（ファイアーウォール）
- OS、アプリケーションで行うホスト上でのアクセス制御
- データへのアクセスをする従業員数を最小化する（不必要な従業員がデータにアクセスできないようにする）。
- アクセス権限を最小化する。
- データを格納したシステムの同時利用者数・利用時間の制限

2）アカウント・パスワード管理（＊下記参考）
- パスワードの他に、指紋、静脈などの生体認証もある。
- アカウントにより、従業員の一人として結び付けられるようにする。データにログインした場合、記録によって従業員を特定できる。
- データへのアクセスが正当な権限、従業員本人であることを確認する。

3）ログの管理
- 問題が発生した場合には、重要な情報源となる。
- ログの収集、ログの分析・監査、ログの保管。

4）バックアップ・リストア
- 安全を確認できるバックアップファイル。

（フルバックアップ）・・・・システムすべてのファイルをバックアップする。
（増分バックアップ）・・・・前回から更新されたファイルのみ。
- インシデント発生、パッチ適用時の障害発生などの場合、システムを元の状態に戻す。

5）性能監視・セキュリティ監視
- システムのトラフィック、性能の監視によりインシデントの早期検地
- 侵入検知システム（IDS）による監視

6）セキュリティホール対策
ソフトウェアバグのみではなく、システムの脆弱性となる、さまざまな種類のセキュリティホール対策

7）パッチ管理
パッチ管理システムの導入などにより管理する。

## 3　データ移送（運搬、郵送、宅配便等）・送信時の対策（暗号化）

・移送時における紛失・盗難が生じた際の対策（媒体に保管されている個人データの暗号化など）

・盗聴される可能性のあるネットワーク（インターネットや無線ＬＡＮ等）で個人データを送信（本人及び従業者による入力やアクセス、メールに添付してファイルを送信する等を含むデータの転送等）する際の、個人データの暗号化

| |
|---|
| 【安全なパスワードの作成条件】 |
| ・名前などの個人情報からは推測できないこと |
| ・英単語などをそのまま使用していないこと |
| ・アルファベットと数字が混在していること |
| ・適切な長さの文字列であること |
| 【危険なパスワード】 |
| ・自分や家族の名前、ペットの名前 |
| ・電話番号や郵便番号、生年月日など、他人から類推しやすい情報 |
| ・従業員コード |
| ・辞書に載っているような一般的な英単語 |
| ・“aaaaa”など、同じ文字の繰り返し |
| ・ユーザー名と同じ文字列 |
| ・短かすぎる文字列 |

## 【　物理的セキュリティ（安全管理措置）】

「経済産業省　ガイドライン」では、物理的安全管理措置として、下記の通り述べています。学校でも十分、留意、応用できる内容となっております。

『物理的安全管理措置とは、入退館（室）の管理、
個人データの盗難の防止等の措置をいう。』

＜物理的安全管理措置として講じなければならない事項＞

1　入退館（室）管理の実施
2　盗難等の防止
3　機器・装置等の物理的な保護

＜各項目について講じることが望まれる事項＞

1　入退館（室）管理を実施する上で望まれる事項

・個人データを取り扱う業務上の、入退館（室）管理を実施している物理的に保護された室内での実施
・個人データを取り扱う情報システム等の、入退館（室）管理を実施している物理的に保護された室内等への設置

2　盗難等を防止する上で望まれる事項

・離席時の個人データを記した書類、媒体、携帯可能なコンピュータ等の机上等への放置の禁止
・離席時のパスワード付きスクリーンセイバ等の起動
・個人データを含む媒体の施錠保管
・氏名、住所、メールアドレス等を記載した個人データとそれ以外の個人データの分離保管
・個人データを取り扱う情報システムの操作マニュアルの机上等への放置の禁止

3　機器・装置等を物理的に保護する上で望まれる事項

・個人データを取り扱う機器・装置等の、安全管理上の脅威（例えば、盗難、破壊、破損）や環境上の脅威（例えば、漏水、火災、停電）からの物理的な保護

＊　PC 本体の盗難、持ち出しを防止する、ケーブルロック（鍵付きのケーブルで PC を机などに固定する）や、セキュリティ機能を備えた機器の利用などは、リスクの低減につながります。