コンピュータウイルス対策に関する基準とガイドライン

2002 年 3 月 27 日 情報ｼｽﾃﾑ会議 制定

1. 目的

学院内に設置されているサーバ・コンピュータ等について、コンピュータウイルス及びワーム等(以下、ウイルス)による被害を予防し、また、被害を拡大しないための対応策を定める。

2. ウイルス予防のための遵守事項と役割

1) ユーザが遵守すべき事項

見知らぬ相手から届いたメールには十分注意すること。
実行形式の添付ファイルに感染するウイルスは、システムの破壊を行うなど、悪質なものが多いので、不用意に実行・クリックしないこと。
ウイルス対策ソフトをインストールすること。また、パターンファイルは定期的に最新のものに更新すること。
ウイルスチェックを行わないまま、ダウンロードしたファイルを実行したり、メールの添付ファイルを開かないこと。
万が一のコンピュータウイルス被害に備えるため、データのバックアップを行うこと。
ファイルサーバ上のファイル及びメールの添付ファイルがウイルスに感染していた場合、システムの安全性を確保するために情報セキュリティ管理者によってウイルスの駆除、削除が行われることがある、また、その場合に連絡なくファイルが削除される場合があることを認識すること。
ウイルスの感染を発見した場合、各情報セキュリティ管理者に速やかに報告すること。

2) コンピュータ等の機器管理者が遵守すべき事項

「ユーザが遵守すべき事項」すべて
本学院のネットワークに接続するコンピュータには、ウイルス対策ソフトをインストールすること
パターンファイルを最新の状態に保つようにすること
（1 週間に 1 度はパターンファイルの更新を行うこと)
ウイルスの感染が発見された場合、当該コンピュータ等をネットワークから切断し(LAN ケーブルを抜くこと)、情報セキュリティ管理者に連絡すること。

3) 情報セキュリティ管理者の遵守すべき事項と役割

管理するサーバ等に対して、適切なウイルス対策を施さなければならない。
管理するコンピュータ等に対して、適切なウイルス対策を施さなければならない。
管理するシステム（個人データを保持するためのファイルサーバを含む）に対して、適宜ウイルスチェックを行い、感染が発見された場合、ファイルの所有者に知らせることなくウイルスの駆除、削除を行う。その結果、ファイルを削除することもある。

4) 情報セキュリティ総括部署の役割

情報セキュリティ総括部署は、学内のコンピュータへのウイルスの感染を防止するように努める。
情報セキュリティ総括部署は、コンピュータウイルス対策の必要性についての啓発活動に努めなければならない。
メールサーバやプロキシサーバなどのコンピュータウイルス進入経路となりやすいところに、コンピュータウイルス検知・削除機能を持たせる。また、その設置・管理を行う。
各部局等で利用するコンピュータのウイルス対策ソフトのライセンス管理を行う。

3. ウイルス発見時の対応

1）情報セキュリティ管理者

情報セキュリティ管理者は、ウイルス感染の報告を受けた場合、以下の対応を行う。

当該コンピュータ等のネットワークからの切断を行う。

発見されたウイルスの種類・感染方法等を確認する。

感染経路の確認、及び、当該コンピュータ等からの二次被害がないか確認を行う。

二次被害の可能性が考えられる場合、情報セキュリティ総括部署と相談の上、二次被害の可能のある者に連絡を行う。

当該コンピュータ等にインストールされているウイルス対策ソフトのバージョンとパターンファイルのバージョンを確認する。

所定のフォームを用いて、情報セキュリティ総括部署へ報告を行う。

2）情報セキュリティ総括部署の遵守すべき事項

情報セキュリティ総括部署は、必要に応じて、IPA などの機関にウイルス感染の報告を行う。

（備考）

1）本ガイドラインは 2002 年 4 月 1 日から適用する。
2）本ガイドラインは 2003 年 4 月 1 日から変更・適用する。
3）本ガイドラインは 2020 年 4 月 1 日から変更・適用する。
4）本ガイドラインは 2021 年 4 月 1 日から変更・適用する。

以　上