第5章　情 報 セ キ ュ リ テ ィ

ネットワークに接続された情報機器は，管理方法が適切でなければ，悪意を持った者やウィルスなどによる攻撃を受け，情報漏えいや情報の破壊・改ざんなどの被害を受ける可能性がある。情報機器を用いれば情報の発信が容易に行えるため，使用方法が適切でなければ，自分に被害が及ぶだけでなく，他の人に迷惑をかける恐れがある。他人への加害行為としては例えば以下に示すようなものがある。

- 著作権，著作隣接権，肖像権などの侵害
- 他人の個人情報の無断公開
- 名誉毀損，誹謗中傷
- 不正アクセス
- ダイレクトメールやチェーンメールの発信
- ウィルスやワームの感染拡大

情報機器を管理する者は，悪意のある者による不正アクセスや情報改ざん・漏えいを防ぐ措置を全ての情報機器に対して講じておかなければならない。ネットワークに接続された情報機器は踏み台として第三者への攻撃に利用される可能性があるため，普段使用していない装置であっても十分なセキュリティ対策を施す必要がある。万が一被害にあった場合はその被害を最小限に抑えるため迅速に適切な処置を行う必要がある。また，情報を発信する際は他人の権利を侵害したり不快感を与えたりしないよう十分注意する必要がある。

神戸大学内の情報機器は教育研究や事務処理のために設置されているので，一般には問題のない行為であっても，営利目的などの本来の目的から外れる使用は原則禁止されている。以下では，神戸大学工学部における情報機器の管理・使用法に関して説明する。

１．基本方針

神戸大学における情報機器の管理運営・使用法に関する基本方針は「神戸大学情報セキュリティポリシー」（以下「セキュリティポリシー」と記す）に示されている。「セキュリティポリシー」には用語の定義も示されているので，本章における専門用語の用法は「セキュリティポリシー」に準ずるものとする。

情報機器の利用については「学内ネットワーク及びサーバの利用に関するガイドライン」，「クライアント機器の設置及び利用ガイドライン」，「インターネット上のサービス利用に関するガイドライン」などに，情報機器の管理については「サーバ機器管理ガイドライン」，「ネットワーク機器の管理に関するガイドライン」などに定められている。これらの文書および以降に「」付きで示された題目の文書は神戸大学情報基盤センターホームページの『コンテンツ』内にある『情報セキュリティポリシー』というページ[1)]より入手可能である。詳細な情報が必要な場合はこれらを適宜参照のこと。

２．情報機器の利用

学内の情報機器を利用する際は以下の点に注意すること。

（１）システム管理者が定める利用規定に従うこと。

（２）利用に際し利用申請が必要な場合は予め提出しておくこと。

（３）個人所有の機器を学内ネットワークに接続する際はネットワーク管理者の許可を得る必要がある。適切なセキュリティ対策が施されていない機器は接続してはならない。

（４）以下の行為は禁止されている。

a. 犯罪行為に結び付く恐れのある行為
- ・法律に抵触する行為
- ・著作権の侵害行為（ソフトウェア，印刷物，他のホームページなどの無断転載，改変）
- ・著作隣接権の侵害行為（演奏，翻訳などの無断転載，改変）
- ・肖像権の侵害行為
- ・猥褻な文章・画像の公開
- ・不正アクセス

b. 公序良俗・社会的公正さに反すること
- ・他人の誹謗中傷
- ・他人の情報や受信メールの無断公開
- ・他人を不快にする情報の公開
- ・不特定多数へのダイレクトメール
- ・営利目的での利用や社会通念上認められる範囲を逸脱した私的利用

（５）パスワードに関しては以下の点に注意すること。

a. 自己のパスワードは他人には秘密にする。

b. 他人のパスワードを聞き出してはならない。

c. 管理者から変更の要請があった場合は速やかに対応しなければならない。

d. パスワードに関する問合せにはいかなる場合も応じてはいけない。

（６）利用資格のないサーバ機器を利用することは厳につつしむこと。

（７）インターネット上のサービスを利用する際には以下の点に注意すること。

a. インターネットに流出した情報の取り消しはできないことを認識し，取り扱う情報の取捨選択及び利用は慎重に行うこと。

b. 利用するサービスの提供側による情報の二次利用についての有無を規約等で確認し，特に秘密保持が必要な情報に対して利用する場合は，問題がないか確認すること。

c. 些細な情報であっても組み合わせることで個人情報が特定されプライバシーが侵害される恐れがあるので発信する内容には注意すること。

３．情報機器の設置・管理

研究室などでは，自分が利用するパソコン等の情報機器を自らが設置・管理しなければならないことがある。その際に注意すべき事項を以下に示す。

（１）許可した者以外が利用できないような対策を施すこと。入室が制限された場所への設置，パスワードや IC カードによる電子的認証など。

（2）利用者には「学内ネットワーク及びサーバの利用に関するガイドライン」を提示し，遵守するよう指導する。

（3）クライアント機器をネットワークに接続する際は以下に従うこと。

a. 事前にネットワーク管理者に申請し，IP アドレスを取得する。

b. パソコン等にはセキュリティ対策を施す。特に Windows の場合は「クライアント機器の設置及び利用ガイドライン」別紙「Windows パソコンをネットワークに接続する場合の手順」に従って最新パッチを導入する。

c. P2P ソフトウェア（Winny，Torrent 等を代表するインターネットを介して不特定多数のコンピュータの間でファイルを共有するソフト）などの違法行為に繋がる恐れのあるソフトウェアはインストールしない。

（4）ルータ，スイッチ，ハブなどのネットワーク機器を設置する際は，特定ユーザ以外が利用できないように注意する。詳細については「ネットワーク機器の管理に関するガイドライン」参照のこと。

（5）無線通信を利用したネットワーク機器(無線 LAN ルータ,無線 LAN アクセスポイント 等)を設置利用する場合は，パスワード保護や MAC アドレスフィルタリング等によるセキュリティ対策を施して，特定ユーザ以外が利用できないように留意する。特に学外の集合住宅に近接しているエリアでは，学外の人物に学内ネットワークを利用されないように注意が必要である。

（6）サーバ機器を設置する場合は，通常のセキュリティ対策を行うのは当然だが，アクセスログの蓄積・管理なども行う必要がある。管理の詳細については「サーバ機器管理ガイドライン」を参照のこと。対外サーバの設置については「対外公開サーバ設置基準」参照のこと。

（7）情報セキュリティに関する事故，情報システムの不審な動作，公開情報の改ざん，システム上の障害及び重大と思われる誤動作を発見した場合は直ちに報告しなければならない。具体的な手順は「インシデント対応手順」に従うこと。

4．学外の Web サーバを公式の Web サーバとして使用する場合

本学における公式の Web サーバ（部局が管理するものも含む）を学外のレンタルサーバ等に置く場合あるいはそれと同等のことを行う場合は，情報セキュリティ委員会に申請が必要である。コンテンツへのセキュリティ対策，インシデント発生・運用時の管理，外部業者との契約の基準については,「本学における情報システム等を学外におく場合等に係る取扱い」を参照すること。

参考文献

1）http://www.istc.kobe-u.ac.jp/Documents/Security/SecurityPolicy/

2）神戸大学：神戸大学情報セキュリティポリシー

3）神戸大学：学内ネットワーク及びサーバの利用に関するガイドライン

4）神戸大学：クライアント機器の設置及び利用ガイドライン（別紙「Windows パソコンをネットワークに接続する場合の手順」を含む）

5）神戸大学：インターネット上のサービス利用に関するガイドライン

６）神戸大学：サーバ機器管理ガイドライン
７）神戸大学：ネットワーク機器の管理に関するガイドライン
８）神戸大学：対外公開サーバ設置基準
９）神戸大学：インシデント対応手順
１０）神戸大学：本学における情報システム等を学外におく場合等に係る取扱い