令和６年４月　［学生・学外共同研究者向け］

ネットワークを安全に利用するための
情報セキュリティ対策

★ ネットワークを利用するリスクについて

ネットワークに接続された現在のコンピュータは，あらゆる人々とつながることを可能とし，我々の情報通信環境は情報の量やコストの面で一昔前からは信じられないほど便利になりました。しかし，あらゆる人から情報をもらえるということは，あらゆる人が自分のコンピュータに接続し，大事な情報を盗んだり，情報を壊して使えなくしたりというリスクが潜んでいることに留意しておくことが必要です。

★ 情報セキュリティポリシーについて

学校や自治体，企業等，組織の中でどのようにして情報資産を守り，情報セキュリティを確保するかといったルールを明らかにして，構成員にそれを守ることを求めることが一般的になってきました。こういったルールは「情報セキュリティポリシー」と呼ばれています。

兵庫教育大学においても，情報セキュリティポリシーをはじめ，情報セキュリティ対策に関する各種規程等を整備しています。

兵庫教育大学の情報セキュリティポリシー及び情報セキュリティ対策に関する各種規程等は，CSIRT（情報セキュリティインシデント対応チーム）のWebページに掲載していますので，ご参照ください。

このリーフレットでは，ネットワークを安全に利用するために最低限守らなければならない事項をまとめています。

★ 情報セキュリティインシデントについて

情報セキュリティポリシーが定められていても，定められたルールを守らなければ，事故や事件が起きてしまいます。情報セキュリティを脅かす事故や事件のことを「情報セキュリティインシデント」と呼びます。

情報セキュリティインシデントを起こさないためには，まず「自分が起こす可能性がある」ということを意識することが重要です。これである程度は防ぐことができます。

しかし，たとえば，コンピュータウイルスが知らないうちに自分のコンピュータに侵入し，他人のコンピュータを攻撃した等，意識していても起きる場合があります。

★ ウイルス感染の疑いが発生した場合の対応

ウイルスに感染した場合又は感染したと疑われる場合は，更なる感染を未然に防止するため，直ちに当該機器をネットワークから分離するとともに，電源を切らずにそのままの状態にしておいてください。また，当該機器の責任者等に報告し，指示を仰いでください。報告したことによるペナルティはありません。

★ 情報セキュリティインシデントを知った場合の対応

情報セキュリティインシデントを発見した場合は，下記の情報セキュリティインシデント通報窓口に通報してください。

情報セキュリティインシデント通報窓口

CSIRT（情報セキュリティインシデント対応チーム）
Email　：csirt@hyogo-u.ac.jp
電　話：0795-44-2054又は2209
Webページ　https://www.hyogo-u.ac.jp/in/csirt/

ネットワークを安全に利用するために気をつけること

OSやソフトウェアは常に最新の状態にする

コンピュータは便利である一方，多くの弱点（脆弱性）を抱えています。多くのコンピュータウイルスは，OSやソフトウェアの脆弱性を利用して感染します。脆弱性を解消するためには，製造元から無料で配布されるセキュリティ更新プログラム（パッチ）を適用し，常に最新の状態を保つようにしてください。

ウイルス対策ソフトウェアを導入する

コンピュータウイルスに感染しないよう，ウイルス対策ソフトウェアを導入し，ウイルス対策ソフトウェア及び定義ファイルを常に最新の状態に保つようにしてください。

また，ダウンロードした時点ではウイルスが検出されなかったが，後に定義ファイルが更新され，ウイルスが検出される場合もあるので，定期的にウイルススキャンを実施してください。

パスワードは大切に管理する

他の者にパスワードを教えない，他の者のパスワードを使用しない，不注意でパスワードが他の者に知られてしまうことがないよう最大限の注意を払う，使い回しをしないなど，適切に管理してください。

また，パスワードを設定する際は，個人や組織の名前，識別コード，著名人の名前，キーボードの並び順を利用した文字列（qwerty）等は，容易に推測できるので，使用しないようにしてください。

不審なメールの添付ファイルは開かない

身に覚えがない不審な電子メールには，コンピュータウイルスが潜んでいる可能性があります。安易に添付ファイルを開いたり，リンク先のURLをクリックしないようにしてください。

偽のホームページへの誘導や不正なスクリプトの実行を未然に防ぐため，原則として，受信した電子メールはテキストとして表示させるようにしてください。

インターネットカフェやホテル等で重要な情報をやりとりしない

学外のインターネットカフェやホテル等に設置されている不特定多数の者が利用可能な端末又はWi-Fiを使用する場合は，入力内容を盗聴するソフトウェアが仕掛けられていたり，他人にパスワードやアカウントを盗み見されるおそれがあります。これらを利用して，学内の情報システムへアクセスしたり，重要な情報をやりとりしたりしないようにしてください。

不適切な情報を発信しない

各種権利侵害を伴う情報が発信された場合は，法律により罰せられるだけでなく，本学の社会的信用を失わせるおそれもあります。

本学ドメインからの情報発信だけに限らず，利用者が個人契約しているインターネット接続業者のウェブページや，X（旧Twitter）等のSNSから，個人として情報を発信する場合であっても，大学に籍を置く公人とみなされることが多いので，注意してください。