情報システムを利用するユーザのための基準とガイドライン

2003年 10月 30日 情報システム会議 制定

1. 情報システム利用の全般的規定

・関西学院（以下、「本学」という。）の設置・管理するすべてのコンピュータおよびネッワーク等の情報システムは、本学の教育・学習・研究・事務業務、もしくは、本学で認められたプロジェクトや業務を行うために利用されるものとする。本学は、教職員および学生の諸活動にとって、これらの設備の重要性を認め、情報システム設備へのアクセスを限定、または拡張する権利を有する。
　なお、このガイドラインに言う「システム管理者」とは、「情報セキュリティ基本ポリシー」に於ける「情報セキュリティ管理者」と同義に扱う。

・情報システムを利用する者（以下、「ユーザ」という。）は、「情報システムの利用に関する規定」に従い、適切な利用を行う責任があり、システム管理者によって示された利用条件を守らなければならない。

・本学の情報システムを商業利用、または本学と関連のない活動に使用してはならない。

・本学は、ユーザの情報や資料の機密性を守る努力をするとともに、教職員にも情報や資料の機密性を守るよう指導を行う。

・本学は、常に、情報システムからの情報の損失を防ぐよう努力する。また、情報システムおよびデータに関するプライバシー・セキュリティ・保全性の確保についても努力する。ただし、最善の努力にもかかわらず、情報の損失やデータの遺漏があった場合、本学は、ユーザに対する責任を負わない。情報システムからの情報・データの損失を防ぐため、ユーザは様々な合理的手段を講じなければならない。

・万が一、情報システムから情報が損失し、それがユーザの適正な管理を超えた理由によるものであった場合には、情報システム部門は、その情報の復元を援助する。

・ユーザは、情報システムの利用により特許を侵害したり、著作権に違反するような行為を行ってはならない。

・万が一、ユーザが特許の侵害や著作権違反を行い、それにより、本学に対して、法的行動、主張や要求が行われた場合、当該ユーザはそれを補償しなければならない。

・ユーザは、本学に在籍しなくなった場合(退職・卒業など)、自己のデータが通知なく本学の情報システムから削除されることを認識しているものとする。

・本学は、全ユーザの情報システムの利用について、下記の権利を有する。
　全ユーザの情報システム利用について、制限もしくは規制する権利
　ユーザにとって害となるような情報・データやシステムを、コピー、削除、もしくは変更する権利
　不正または不適切な利用から情報システムとユーザを守るため、ユーザへの通知の有無に関らず、前記の処置を行う権利

・本学は、情報システムを定期的にチェックし、監視する権利および情報システムを保護するために必要な措置を講ずる権利を有する。

・本学は情報システムの完全性およびセキュリティを保護するために緊急の措置をとる権利を有する。これには、プログラム・ジョブ等を終了させることや、ユーザアカウント名やパスワードを一時的に変

更すること等が含まれる。この緊急措置は本学がさらなる措置をとる権利を放棄するものではない。

・ユーザは、関連する法律、「ネットワーク利用倫理規程」（以下、「倫理規程」という。）等の本学の規程、情報セキュリティポリシー（含 基準とガイドライン）に従って情報システムを利用するものとし、これらに違反する利用を不正利用とする。情報セキュリティ統括責任者は、不正利用の疑いがあると認めた場合、倫理規程に基づき必要な調査を行い、違反者に対する相当の措置を提言できるものとする。この不正利用には、ユーザの以下の行為を含むものとする。

情報システムに対して故意に物理的ダメージを与えた場合
不正に得た機密情報を保持していた場合
情報システム部門によるサービスを故意に妨害した場合
他者のアカウント（利用 ID）・パスワードを取得・使用する、もしくは取得を試みた場合
設備を不正に利用した場合

2. 情報システムの利用に関する規定

(1) はじめに

情報システムの利用に関し、ここに規定することは、いかなる共有資源を利用する場合にも適用される常識的なものである。

(2) 適切な利用

本学の情報システムの適切な利用とは、本学の教育・学習・研究・事務業務、もしくは、本学で認められたプロジェクトや業務のための利用を意味する。

(3) ユーザの義務

本学の情報システムのユーザは以下の義務を負うものとする。

1) セキュリティ
・データ・個人情報・パスワード、機密データの保護
・コンピュータのファイルセキュリティ機能の最大限の利用
・パスワードのつけ方に注意すること、また定期的に変更すること
・事務データへのアクセス、事務データの使用を管理するためのセキュリティポリシーや手続きに従うこと

2) 機密性
・他のユーザのプライバシーを尊重すること
・故意に他のユーザまたは大学の所有するファイル、パスワードに関する情報の検索、コピー、修正などをしてはならない
・システム管理者および本人の許可なく、他人の ID でシステムを利用してはならない
・教職員や学生の個人的なデータを漏洩してはならない

3) 他のユーザの権利を尊重すること

4) 著作権やプログラム、データのライセンスなど法的保護を尊重すること

5) 電子メール・ネットニュース・WWW などの意図された使用法を尊重すること
たとえば、偽メール、他者に脅威となったり嫌がらせとなったりするようなメール、システムの効率の障害となるようなチェーンメール、利益目的の宣伝メール等を送信しないこと。

6) 情報システムの完全性を尊重すること

たとえば、システムに侵入する、システムのソフトやデータにダメージを与える、システムを変更してしまうようなプログラムやトランザクション・データを開発したり使用したりしないこと。なお、システム、ネットワーク、データに変更を加える場合には、システム管理スタッフの指示の下に行わなければならない。

7) 本学の情報セキュリティポリシー、もしくは利用規程等に違反した、または重大な違反の恐れのある情報があれば、それを報告すること。

(4) 特定の活動についての規定

特定の活動を以下に示す。ユーザは法令、規程等を遵守し、不適切な利用・行為を行ってはならない。

1) 不法な活動

一般的に、法令に違反するような情報を本学の情報システムに保存する、もしくは、本学の設備を使用してそのような情報にアクセスすることは不適切な使用である。

2) 規制ハードウェア・ソフトウェア

ユーザは、本学の情報セキュリティポリシーに違反したり、ライセンス違反や契約違反になるようなプログラムや情報を所有したり、他者に与えたり、情報システムにインストールしたり、実行したりしてはならない。

情報システムへのモニタリングデバイスの接続は不適切な利用である。これには、データ、パケット、その他の情報をモニタリングする目的で電子機器を接続することが含まれる。システム管理者がモニタリングする場合を除き、研究等の目的でこのようなハードウェアを使用したい場合には、情報セキュリティ統括責任者の許可を得る必要がある。

3) 複写と著作権

ユーザは著作権法および関連法令を遵守しなければならない。

本学の情報システムの大半のソフトウェアは、本学もしくは第三者が所有しており、ライセンスや契約による合意とともに著作権法やその他の法律によって保護されている。ユーザはソフトウェアの使用と再配布ライセンスの条件を尊重し、遵守しなければならない。これには、プログラムやデータのコピー・再販売の禁止、教育以外の目的、営利目的での利用の禁止なども含まれる。

4) 嫌がらせ(ハラスメント)行為

本学はセクシャルハラスメントを禁じている。本学の情報システムを、セクシャルハラスメントだけでなく、他者を侮辱する、中傷する、嫌がらせをするなどのために使用してはならない。以下はその例である。

・意図的にコンピュータで猥褻な言葉、写真またはその他を送信する、肉体的な害を相手やその家族に与えるなどと脅迫すること
・他者を悩ませる、嫌がらせる、邪魔をすることを目的に、正当な理由がないのに意図的に接触し、相手が止めて欲しいと望むようなことをすること
・他者の教育、研究、事務等の成果物を、コンピュータを使用して故意に破壊したりすること
・コンピュータを使用して故意に他者のプライバシーや学問等を侵害すること、また脅迫して他者のプライバシーを侵害すること

また、誰もがアクセスできる場所に人の感情を害するような資料をおくことを禁ずる。インターネット上などでは、本学の構成員が「人の感情を害するようなものである」と判断するような資料がある。例えば、露骨な性的な画像などがそれである。本学は、今のところ、そのような資料を取得することを制限はしていないが、誰もがアクセスできる場所にそのような資料をおくことは不適切だと考える。誰もがアクセスできる場所とは、誰もが使うことができるコンピュータのスクリー

ンやプリンタ、ファイルサーバ、WWW サーバを指すが、これらに限られるわけではない。

5）資源の浪費

情報システムに対して、故意にその機能に障害を与えるような行為、また正規ユーザによるアクセスを拒否する行為は不適切な利用である。

「資源の浪費」には、チェーンレターを送ること、故意に大量に不必要な印刷をすること、故意に多くのディスクスペースを使用すること、故意にネットワークに重い負荷をかけることなど、システムに対する悪戯や情報システムの円滑な運用を損なうような行為が含まれるが、これだけに限らない。

6）ゲーム

本学の情報システムを利用して、ゲームを行ってはならない。研究・教育上の理由からゲームが必要な場合は、許可を得なければならない。

7）商用利用

本学の情報システムを利用した営利を目的とする商行為は禁止されている。以下のために情報システムを利用することは不適切な利用である。

・商業利益を得るための利用、また第三者を商業的に有利にさせるような行為
・本学に関連のない活動
・本学の目的やサービスに関連しない、商用目的の広告活動

8）個人所有のパソコン（ＰＣ）の利用

ユーザは、個人所有のＰＣ等に保存されている本学の情報に関しても、その安全と完全性の確保について義務を負う。これには、定期的にディスクのバックアップを取ること、その機械への物理的なアクセス、およびネットワークを経由してのアクセスを管理すること、ウィルス対策ソフトをインストールし使用することなどが含まれる。ユーザは、自分のＰＣに、他のコンピュータ資源にアクセスするためのパスワードなどの情報を保存しないのが望ましい。また、ユーザは、原則として本学の情報システム利用のためのパスワードや他の機密性のあるデータ、情報を自分のＰＣやフロッピー、ＣＤなどのメディアに保存してはならない。

9）個人的なビジネスのための利用

本学の情報システムを、報酬を得られるような個人的な外部の仕事や本学に関係のない組織の利益のために使用してはならない。ただし、本学の規程・制度に則り行う場合は、この限りでない。

10）ローカルシステムに関する追加の規定

本学の情報システムは、多くの“システム”から構成されている。たとえば、教育研究システム、事務システム、研究室毎のシステムなどがあげられる。それぞれのシステム毎にシステム利用に関する規則や規制を設けている。また、それぞれのシステムにそのポリシーおよび運用に責任を持つ情報セキュリティ管理者を置くこととしている。ユーザはこれらの人々に協力するとともに、本学とローカルシステムそれぞれのポリシーを守らなければならない。ローカルポリシーは本学のポリシーよりも規制が厳しい場合もある。これは本学のセキュリティポリシーが最低限の基準であるということである。

11）本学ネットワークへの接続

キャンパスのほとんどの建物がキャンパスネットワークに含まれている。本学の情報システムの完全性を保つために、キャンパスネットワークへの接続は、申請により許可された者にのみ許されている。ユーザは既存のユーザ接続ポイントにのみ適切な機器を取り付けることができる。ネットワーク接続の追加、ネットワークの再配置などの要望は、情報システム室で受け付ける。

12）外部サービスの利用

本学が接続している外部のネットワーク通信サービスや事務システム・サービスは、それぞれ利用基準を定めている。それぞれの基準を遵守することはユーザ個人の責任である。ユーザが外部のネットワークポリシー等に違反した場合、本学はそのユーザを保護することはできない。

13）印刷

ユーザは、本学の情報を印刷する際には、情報の安全性と機密性を確保する義務を負う。

3. 電子メールの利用に関する規定

(1) 前文

本学の電子メールシステムは、教育・研究・業務のために利用されることを目的としている。電子メールシステムは、本学の規則やポリシー、それに関連する法令に基づいて管理されている。

(2) 適切な利用とユーザの責任

ユーザは自分の送るメッセージの内容、宛先、管理についての個人の責任をはっきりと認識しなければならない。特に以下の点に留意する必要がある。

・本学の構成員に害を及ぼすような情報を含んでいないこと
・わかりやすい丁寧なものであること
・本学のポリシーに沿ったものであること
・プライバシーと機密性について他人の権利を守ったものであること
・猥褻なもの、人の感情を害するようなもの、人を中傷するような内容を含んでいないこと
・本学の利益に反する目的のために使用されるようなことがないこと
・正確で、適切な、参考となる署名を含んでいること
・不必要にシステムに負荷をかけないものであること
・商業目的に使用しないこと

(3) データのバックアップ

システム管理者はシステムの障害に対応するためにデータのバックアップ作業を行うが、重要なデータに関しては、各自がフロッピーなどのメディアにバックアップを行うべきである。

(4) 機密保持と安全性

ユーザは、電子メールシステムの機密保持と安全性について、以下のことを認識・理解した上で利用する。

・電子メールは必ずしも安全・確実なものではない
・本学のコンピュータとネットワークは本学が管理する設備であり、本学は、保存されている情報の内容について、必要な場合には調査を行うことがある
・個人的な機密資料は本学の設備を通して送信しないことを推奨する
・ユーザは自分のパスワードの完全性を確保し、本学のパスワードセキュリティポリシーを遵守しなければならない
・機密性のある資料は、慎重を期する場合、暗号化されない限り電子メールを通して送信すべきでない。機密資料の転送は、必要のある場合にのみ、作成者の許可を得た上で行うべきである
・電子メールは即時性・到達性を保障されたものではなく、場合によっては相手方にメールが届くまでに数日、数週間かかることがあること
・メールの受信者が受け取ったメッセージや転送されたメッセージ、添付されたメッセージを削除しない限り、システム上からメッセージは削除されないこと

・電子メールはファックスやメモと同様に改ざんされる可能性がある。メッセージの内容が疑わしい場合、ユーザは、必要により電話等の別の手段を利用してその真偽を確かめるべきである

(5) 損害等の補填

ユーザの不適切な使用によって生じた重大な損失や損害について、本学は当該ユーザに損害等に対する補填を求めることがある。

(6) 保証の限度

本学は、最善の努力をもって電子メールシステムの正常な運用にあたる。それにも拘わらず、ユーザのファイル、メッセージ、データの不達、あるいは不適切な利用等の結果これらが失われた場合については、本学は責任を負わず、それらのデータ等の保証も行わない。

4. パスワードの管理に関する規定

(1) パスワード管理

パスワードの管理については以下のとおりとする。

・パスワードは記憶するものとする。書き留めてはならない
・パスワードは個人のものであり、決して他人と共有してはならない
・パスワードは３ヶ月から６ヶ月に一度程度変更すべきである。万が一他人に知られた可能性がある場合は、すぐに変更しなければならない

(2) パスワード管理業務

パスワードの管理業務は以下のとおりとする。

・システム管理者は、パスワードクラッキングソフト等を利用し、定期的に脆弱なパスワードを調査することができる
・新しいパスワードや変更後のパスワードは、写真の添付された身分証明書・学生証等で本人確認を行った上で手渡すことを原則とする。決して電話や電子メールで伝えてはならない

(3) パスワードの構成

パスワードには、他人が推測もしくはクラッキングしにくいものを設定しなければならない。

・６文字以上のパスワードを使用すること
・たとえば、配偶者や子供、もしくは、ペットなど、自分に近い何かの名前をパスワードにしないこと。好きな作家や食べ物も同様である
・決して自分のＩＤや名前と同じにしてはならない
・ニックネームなどの自分を連想させるような単語を使用しないこと
・辞書にある単語をそのまま使用しないこと
・数字と文字を両方含んだパスワードを使用すること
・すばやく正確にタイプでき、小文字だけでなく大文字を含むものを使用すること

5. ＰＣ教室・施設の利用に関する規定

(1) 前文

ＰＣ教室・ＰＣ利用施設（以下、「ＰＣ教室」という。）は、教育、学習、研究、関連する諸活動のためにのみ提供されている。ＰＣ教室とは、大学の授業・自習用に用意されたＰＣ設置の教室や、図書館に設置されたＰＣ利用スペースなどを指す。ＰＣ教室は、学内的に限られた資源であり、他者と共有しなければならないものである。ＰＣ教室の利用に際し、ユーザは、「情報システムの利用に関する規定」等、このガイドラインに規定する事項を遵守し、効率的、倫理的に正当な利用を心掛けなければならない。ＰＣ教室での不適切な行為は、利用停止もしくはその他の措置の理由になることがある。

⑵ 利用ＩＤの管理

利用ＩＤは本学の構成員に対して、個人が利用するものとして本学から与えられるものであり、以下の事項を遵守しなければならない。

・利用ＩＤを家族や友達と共有してはならない。また、他人にパスワードを教えてはならない
・パスワードの管理については、「パスワードの管理に関する規定」に基づいて、個人で管理しなければならない
・他人の利用ＩＤを使用してはならない。故意でなく、本来アクセスが認められていない情報へのアクセスができた場合は、直ちに担当者に届け出なければならない
・他人のパスワードを見つけようと試みたり、認可されていないユーザＩＤを使って他人のアカウントにアクセスしてはならない

⑶ 学生証等の携帯

ＰＣ教室等を利用する際は、常に学生証等本学の身分を証明するものを携帯し、担当者の指示があれば提示しなければならない。適切な身分証明書を持たない者に対しては、ＰＣ教室等への入室を拒否する場合がある。

⑷ 適切なネットワークの利用

インターネットを利用する際は、ネットワークのエチケット（ネチケット）、ガイドラインを守らなければならない。また、ネットワーク資源を無駄に使ってはならない。
ネチケットは、よいマナーと常識に基づいて作られている。以下はそのいくつかである。

・電子メールをいつも確認する
・可能な限り電子メールはテキストの１画面にとどめる
・電子メールに大きな添付ファイルをつけて送らない
・人を不快にさせるような言葉を使わない
・インターネット上の他のユーザに対し、礼儀をわきまえる

⑸ 不法な活動の禁止

適切な認証やライセンスなしにソフトウェアをダウンロード、コピーしてはならない。
いかなるシステムに対してでも故意にウィルスを入れることやその他のハッキングをすることは違法である。

人を不快にさせるような、猥褻なもの、いやがらせのためのもの、他人を中傷するようなもの、他人のファイルやプログラムにダメージを与えるようなものを送信すること、また、あらゆる関連する法律に違反することは行ってはならない。

⑹ 教室でのエチケット

・ＰＣ教室は飲食禁止、禁煙である
・過度の騒音を立ててはならない
・ＰＣの台数は限られており、譲り合って利用すること
・ＰＣ教室担当者や他のユーザに対して礼儀を守ること
・ゲームをしてはならない
・情報部門のスタッフや教室運用担当者の指示を守ること
・ＰＣ内蔵のスピーカーは利用しない。学習・研究上の理由から必要な場合には、ヘッドフォンを利用すること
・その他、他のユーザの迷惑になるような行為はしてはならない

6. インターネット利用条件・基準に関する規定

(1) 範囲

インターネット経由で手に入れることのできる新たな資源、新たなサービス、相互接続は、新たなチャンスをもたらすと同時に新たなリスクをもたらす。このリスクに対し、ここでは、本学のインターネットセキュリティに関する正規のポリシーを規定する。これは、本学の情報システムを利用する教職員、学生、契約者、臨時に雇用された者等、全構成員に適用される。

(2) 情報の伝達

1) ダウンロード

本学以外のところからインターネットを経由してソフトウェアをダウンロードする場合は、いかなる場合であっても、ウィルス検知ソフトを使用しなければならない。ソフトウェアの提供者が信頼できない場合は、ダウンロードしたソフトは、ネットワークに接続されていないスタンドアローンのＰＣ等でまずテストしなければならない。これは、そのソフトウェアがウィルスやワーム、トロイの木馬等を含んでいた場合、被害を該当機器のみにとどめるためである。

2) 疑わしい情報

インターネットを通じて得たすべての情報は、他の（インターネットでない）情報で確認できない限り、疑わしいと判断すべきである。インターネット上では品質管理が行われておらず、多くの情報がすでに遅れたものであったり、不正確なものであったりするからである。

3) 連絡・接触

極端に言えば、インターネットを通じての連絡は、適切な方法で、その連絡の正当性を確認した上でない限り、本学からの情報であると信用できない場合がある。

4) 情報のセキュリティ

インターネット上では、盗聴やメッセージの妨害が、容易に頻繁に行われていると認識すべきである。したがって、本学の機密に類する重要な情報については、認可された方法であらかじめ暗号化されていない限り、インターネットを経由して送信してはならない。クレジットカードの番号、ログインのためのパスワードをはじめ、大学のシステムにアクセスできる他のパラメータについてもクリアテキストでインターネット上に送信してはならない。また、本学がインターネット上に認証を必要とするサービスを提供する場合、必ず、暗号化された通信手段を用いなければならない。

(3) ソフトウェアのセキュリティ

本学のコンピュータのソフトウェア、関連書類、その他の同種の内部情報は、本学が理事長、もしくは情報セキュリティ統括責任者の名前において特別に許可しない限り、どのような目的のためであっても、本学以外の第三者に販売したり移動させたりしてはならない。

(4) 個人的なセキュリティ

1) プライバシー

本学の情報システムやインターネットを使用しているユーザは、自分の通信が第三者に見られないように自動的に守られている、と思ってはならない。ユーザは個人に関する情報についても、暗号化されない限り、インターネットを経由して送信してはならない。情報の機密に関して疑問等がある場合は、システム管理者や情報システム室、情報メディア教育センターなどの関係部署に連絡を取り、解決することとする。

2) 調査する権利と守秘義務

本学のシステム管理者は、必要な場合には、予告なしに本学のコンピュータ内に保存されている電子メール、個人的なファイル、その他の情報を調査することができるものとする。また、電子メールやホームページ閲覧のログを保存し、調査することも同様である。

ただし､調査は必要最小限にとどめることとし､担当者はプライバシーの保護に努めるとともに、

職務上知り得たことを他に漏らしてはならない。

3) 公の発言

インターネット上の掲示板等を通じて、ユーザ（特に教職員）が本学との関係を言及する場合には、その意見が個人の意見であり、必ずしも本学の意見ではないということを明示しなければならない。

ユーザはインターネットを通じて、本学の関係者や本学の公のイメージに悪影響を与えるような内部情報を公開してはならない。

インターネット上のホームページ、メーリングリスト、公のニュースグループ、また関連する公の掲示板に対してコメントをする場合は、その内容に十分注意しなければならない。

4) アクセス制限

公開目的の WWW サーバを除き、本学のコンピュータにインターネットを通じて接続することを希望するすべてのユーザは、本学内のネットワークに接続する前に認証を受けなければならない。

情報セキュリティ統括責任者の事前の承認がない限り、教職員は、本学に属さないユーザが、本学のシステム・ネットワーク・情報へのアクセスを可能にするようなモデムの設置や、インターネット等外部とのネットワーク接続などを行ってはならない。

5) セキュリティ上の問題の警告

以下の事態が生じた場合には、ユーザは情報システム室に通知しなければならない。

・本学の機密情報が失われた、もしくは認められていない第三者に開示された場合、またはそれが疑われるとき

・本学の情報システムが、認められていない方法で使用されたとき、またはそれが疑われるとき

・パスワードやその他のアクセス制限のメカニズムが失われた、盗まれた、開示された場合、またはそれが疑われる場合

・ファイルが見つからない、頻繁にシステムがダウンする、メッセージが誤送されるなど、システムが異常な動きをしているとき

ユーザは本学や、他のインターネット上のサイトのコンピュータセキュリティの仕組みを調べようと試みてはならない。一般的に、このような場合には警報システムが作動する。この行為はハッキング行為であり、当該ユーザは、場合によっては刑事訴追される可能性がある。

情報セキュリティ統括責任者から、あらかじめ書面による認可を受けていない限り、ハッキングツールを含むファイルやその他の疑わしい資料の所持は、ハッキング活動の明確な証拠と位置づけられることがある。

7. 補則

本ガイドラインは、学内外の状況により必要に応じて見直しを行い、変更するものとする。

（備考）

1) 本ガイドラインは 2003 年　10 月　1 日から適用する。

以　上