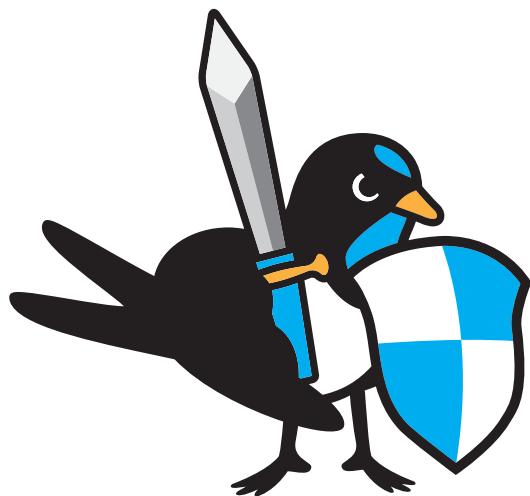


情報倫理とセキュリティ のためのガイド



東京工業大学
Tokyo Institute of Technology

情報倫理とセキュリティのためのクイックガイド

一目で分かる注意点をまとめてみました。情報倫理とセキュリティに関してより詳しい内容は、本篇を読むようにして下さい。分かりやすいQ&Aもまとめてあります。

【倫理的・法的規則上の注意】

メール、インターネットサイトの閲覧	詐欺やハラスメントに注意しましょう 情報の発信元送信先を確認しましょう
SNSやブログの利用	SNSは全世界に見られることに気がつきましょう
個人情報・プライバシー・人格権の保護	自分と他人のプライバシーも守りましょう
研究者の倫理	学生も研究に係わる者として高い倫理をもちましょう
情報と知的財産の保護	とくに著作権侵害に注意しましょう
ソフトウェアの利用	ライセンスが必要です
法律の遵守	処罰が科せられる場合もあります
教職員	就業規則上の責任があります

【セキュリティ上の注意】

モバイル機器の利用	紛失・情報漏えいに注意しましょう
バックアップ・セキュリティアップデート	定期的に最新のものにしましょう
パスワード管理・ハッキング対策	パスワードを常に安全なものにしましょう
共有設定・ネットワーク管理	アクセス管理を徹底しましょう
障害・不正アクセス・情報漏えい時の対応	迅速にシステム管理者と担当部署へ連絡しましょう

情報倫理とセキュリティ のためのガイド

情報は、社会で流通してはじめて大きな意味を持ちます。特にコンピュータとそれをつなぐインターネットを流れる情報は、膨大で高速に伝達され、その影響は瞬時に地球規模に広がる可能性があります。そのような情報の取扱いには、社会を円滑に発展させるために考えられたさまざまな制約があります。

このガイドは、社会において守るべき情報の取扱いに関する規則や心掛けについて、本学の学生および職員を対象として平易にまとめたものです。

上手に情報やインターネットを活用して、生活を実り多いものとするために、これらの守るべきことにいつも注意を払い、事故を起こさない、事故にまきこまれないように、心掛けましょう。










前半は倫理的・法的規則篇、後半はセキュリティ篇に分かれ、具体的な問題例とその対応についてのQ&Aもあります。目次には、みなさんが利用しているコンピュータ、ネットワーク別に関連する項目が分かるように、以下のマークを付けてあります。











目次

情報倫理とセキュリティのためのガイド

05 倫理的・法的規則篇

- 05 メール、インターネットサイトの閲覧 
- 06 SNS やブログの利用 
- 06 個人情報・プライバシー・人格権の保護 
- 07 研究者の倫理 
- 08 情報と知的財産の保護 
- 09 ソフトウェアライセンス 
- 10 そのほかの法律の遵守 
- 11 就業規則関係一主に教職員 
- 11 問題が発生したとき 

12 セキュリティ篇

- 12 モバイル機器の利用 
- 12 バックアップ 
- 12 ウィルス対策 
- 13 セキュリティアップデート 
- 14 パスワード管理・ハッキング対策 
- 15 共有設定・ネットワークの管理 
- 15 障害時の対応 
- 15 不正アクセス・情報漏えい 

16 Q&A 篇

- 16 私物コンピュータの大学ネットワークへの接続
- 16 大学ポータルサービスへの接続
- 16 大学のソフトウェアの私物コンピュータへのインストール
- 17 文献検索
- 17 データベースのダウンロード
- 17 アップデートソフトのコピー
- 18 論文の公開
- 18 研究状況の公開
- 18 コンピュータやネットの目的外使用
- 19 事実を述べるのも中傷？
- 19 どこまでが個人間のやりとりか
- 19 コピープロテクト
- 20 プログラムの複数人による利用
- 20 電子書籍等の複数人による利用
- 20 コンピュータへの侵入・破壊行為
- 21 不正侵入の防止
- 21 インターネット上の自分の名誉を害する書き込み

22 関係ホームページ等



倫理的・法的規則篇

インターネットを通じて自由に情報発信ができるようになった分だけ、倫理的な考え方や法律等を守ることも求められるようになっていきます。



メール、インターネットサイトの閲覧



インターネット上の情報交換では、意識せずに犯罪行為や違法行為を行ってしまうことが少なくありません。違法薬物の取引、賭博行為、ネズミ講あるいは詐欺行為等、刑事罰を伴う違法行為です。好奇心や巧妙な勧誘により、スマートフォンからでもこれらの違法行為に簡単に加担してしまう危険があるので、加害者にはならないように十分に注意して下さい。メールを通じて借金の返済やアダルトサイト等の利用料金を請求されるといった詐欺事件があとをたちません。詐欺の被害に遭っても、お金が戻ってくることはほとんどありません。詐欺の被害に遭わないように十分に注意して下さい。

メールアドレスを公開することは、詐欺に遭遇する機会を増やすことになる点にも配慮して下さい。スパムメールの送付先に登録され、見たくもないメールの処理に時間を奪われることにもなるので、注意して下さい。

インターネットのサイトを閲覧しているだけでも被害に遭遇する可能性があります。URLをよく確かめずにアクセスすると、本物のサイトに似せた偽サイトに誘導されることがあります。これは、アクセスした人のIDやパスワード等の大切な情報を盗み取るためのフィッシングサイトと呼ばれ広く見られます。サイトにアクセスする時はURLを確かめて、サイトにSSL証明がない(httpsで始まらないURL)等、怪しいと思ったら、情報を入力しないようにしましょう。

セクハラのように相手が嫌がることをしてはいけません。自分が好きなことであっても相手にとってはとても嫌なことかもしれません。相手の気持ちを考えた情報交換を心掛けるようにしましょう。

メールでは、普通の会話と違い、感情がエスカレートしがちです。自制心が強く求められます。怒っている時には決してメールを送信せず、冷静になってから考え直すことも必要です。

カルトやテロに関連する組織等の勧誘もメール等を使って行われる場合があります。十分に注意をしてください。

SNSやブログの利用



ミニブログ(Twitter, LINE, Google+), SNS(GREE, Mobage, Facebook)*等の利用にも注意が必要です。個人で開設するホームページやこれらのミニブログ等の利用は、個人の自己発現の方法として重要であり、表現の自由として保護も受けます。大学では現在のところ、個人でこれらを利用することについて特別な制限をしていません。

しかし、ブログやSNSで発信する情報には、利用者の生活に密接な情報が多く含まれます。そのため、思いもよらずに自分の個人情報が公開されることがあります。また、発信した情報によっては、閲覧した人から予想もしない反応をされ、ひどい場合には、いわゆる炎上する場合があります。

これらの便利なサービスを利用する場合は、以下のようなことに注意を払ってください。また、SNSを利用する場合には、個人情報公開される初期設定になっていることも多いので、必ず最初に設定を確認しましょう。

- ・ SNS は、プライベートな場ではない。
- ・ SNS は、他人を非難する場ではない。
- ・ SNS は、自分の行いを懺悔する場ではない。
- ・ SNS での発言は、取り消せないものと考えよう。
- ・ SNS 上の情報は、いずれ流出するものと考えよう。
- ・ SNS での発言の匿名性は、いずれ破られるものと考えよう。
- ・ SNS の利用者には、善人のふりをした悪人もいることを忘れない。
- ・ SNS での不用意な発言は、激しい批判にさらされることもあることを覚悟しよう。

*各社のサービス等の登録商標です。

個人情報・プライバシー・人格権の保護



インターネットは、ホームページ、ブログ、メール等のサービスを通して、一個人の持っている情報を広く世界に公開・伝達することを可能としました。色々と情報発信してみたいと思うのは自然なことです。しかし、危険な面があることを十分承知して下さい。



自分の個人情報：個人を特定する情報を公開することは危険です。例えば氏名、住所、電話番号、生年月日を知られてしまうと、他人がこの情報をもとに悪意を持った『なりすまし行為』をする可能性があります。

懸賞金やプレゼントがもらえるアンケート等に答えることで、個人情報が第三者に漏洩する危険があります。

スマートフォンで撮影した写真には GPS の位置情報等が付加されます。自宅等の位置情報は個人情報の一種といえます。自宅で撮影した写真等をブログに投稿する場合には、位置情報が付加されないように注意しましょう。友人等の自宅で撮影する場合も注意しましょう。ストーカー被害や窃盗被害のきっかけになる危険性もあります。

自分から情報を提供しなくても、無料でアクセスできる WiFi 等でメール等のやりとりはすべて第三者に丸見えになってしまいます。

他人の個人情報：他人のプライバシーや他人の人権を侵害しないように、常に意識しなければいけません。

自分の情報を扱う以上に、他人の情報の取り扱いには注意が必要です。他人の個人情報を承諾なしに公開してしまうこと等ないように注意して下さい。

他人のメールを盗み見るような事を絶対にしてはいけません。例えば、サーバ管理をしている立場の人は、メールの送受信履歴に触れる機会があるかもしれません。誰が誰と送受信しているかということはプライバシーの問題になり得ます。

SNS、YouTube やニコニコ動画等の動画投稿サイトに動画を投稿する場合にも、他人を撮影したものを無断で投稿すると、肖像権という人格権の侵害が問題になる場合があるので注意が必要です。

研究者の倫理



学生も研究活動を担う一員として、研究者の倫理を守るようにしなければなりません。

レポートや論文作成でのコピーが話題になります。剽窃や盗用というと重大さがわかりやすいかも知れません。レポートや論文作成で、他人の文書や写真図表等を適切に引用せずに切り貼りし、利用することは、剽窃や盗用となります。著作権の問題になるばかりではなく、研究者の倫理にも反します。

インターネット上のコンテンツを引用元を示さずに利用する行為は、仮に著作権の侵害にならない場合でも、研究者の倫理として行ってはなりません。また、広めた方が良さそうな内容であったとしても、辞書風に書かれた内容でも、必ずしも真実とは限りません。必ず、引

用元を確認して、確かな内容のものを引用しなければいけません。

研究に関するデータは、研究結果の正当性を確かめるための重要な情報です。データを意図的に変更することを、データの改ざんとよびます。データを改ざんすることは研究そのものを否定することとなり、研究者の倫理に反します。決して行ってはなりません。

また、他人の個人情報等を取り扱う研究に携わる場合には、個人情報の保護が十分になされるようにしなければなりません。

このほかにも、大学では武器や危険物の製造にも利用できる技術情報に接することがあるかもしれません。例えば、安易に3Dプリンタのデータや製造工程等を部外者に教えたり、インターネットで公開するようなことも慎みましょう。

情報と知的財産の保護



文字、写真、音楽は創作物としてできあがったときから、著作物として法的に保護されます。紙の印刷物ばかりでなく、インターネットやCD等の電子的情報も、著作物として保護されます。他人に著作権のある情報は、原則として、無断に利用することはできません。利用には、条件がついていることが多いので注意が必要です。特に、電子的情報はコピーや送信が容易に行えるので、他人の著作権を侵さないように十分注意して下さい。SNS、ファイル共有システム、無料動画サイト等を利用する場合にも当てはまります。

許可なく複製や使用が許されるのは、例えば次のような場合に限られています。

- ・私的使用のための複製
- ・一定の条件で行う複製（図書館等での複製）
- ・出典を明らかにし、自己の記述が主であるような引用（倫理的・法的規則篇：研究者の倫理も見て下さい。）
- ・営業を妨げない範囲での教育目的での複製、あるいは試験問題としての複製
- ・バックアップのためのプログラムの複製（ダウンロード版ではこのような複製も禁止されている場合があります。）
- ・非営利目的での上演（大学の学園祭での上演については、上映用のビデオ・コンテンツ提供会社との業務使用契約や、音楽の著作物の権利処理が別途必要となることがあります。）
- ・時事事件の報道のための利用等

なお、コピープロテクション等の技術的保護手段を回避して複製することは禁止されています。

著作物に関する法的規則について少し詳しくみてみましょう。

二次的著作権：著作物そのもの以外に、編集された著作物、データベースとして集積された著作物には、二次的な著作権が発生します。電子的に公開されているものでも、自動ダウンロードプログラム等を利用して、大量のファイルを一括してダウンロードすることが、利用規約で禁止されている場合がほとんどですので、注意して下さい。

著作隣接権：著作者の権利以外に、その実演家、レコード作製者、放送事業者には、著作隣接権が与えられますので、この権利も侵さないようにすることが求められます。なお、電波以外に有線放送事業者も放送事業者と認められています。

送信可能化権：インターネットの情報を複製、あるいは再頒布することにも注意して下さい。他人の著作物をインターネットで公開するときには、その人から（自動公衆通信における送信可能化権の）許諾も必要です。無料動画サイト等に投稿する場合にもあてはまります。

著作者人格権：複製権や上演権等の財産権以外に、著作者人格権と呼ばれる著作物の同一性保持、氏名表示や公表に関する権利が保護されていますので、勝手に著作物の内容を変更して、それを原著作者の著作物として公表すること等は許されません。

動画・音の商標：動画・音の商標が法律で認められるようになりました。これらの他人の商標に含まれる音や動画を無断で、インターネット上で使用することは商標法にも違反し、許されません。

ファイルの自動共有：P2P等ファイルを自動で共有するソフトウェアは、他人の著作物が無断で共有されていたりするため、知的財産権を侵害する事件に巻き込まれやすいといえます。また、P2Pソフトウェアをインストールしているコンピュータから、大切な個人情報や企業の秘密情報が流出する事件等もたびたび報道されています。そのため、P2Pソフトウェアは大学のネットワークでは利用が禁止されています。

ソフトウェアライセンス



ソフトウェアは一般にライセンス契約（使用許諾契約の形）で取引されますが、その使用許諾契約により、勝手に複数のコンピュータにインストールして使用することは禁じられてい

ます。そのような行為を頼まれても、たとえそれが、指導教員や上司であったとしても、きっぱりと断りましょう。

複数のコンピュータで使用が必要な場合には、必要数の追加的なライセンス契約を結ぶようにしましょう。

大学では、研究や業務で使用するソフトウェアについて包括契約を結んでいるものがあります。

そのほかの法律の遵守



法律の規定ならびにその趣旨を守り、以下の行為はやめましょう。

- ・他人のアカウントやパスワード等を隠れて調べたり、プログラムに潜むセキュリティホールをついて、保護されている情報にアクセスすること。
- ・他人の管理するコンピュータへ接続された端末やインターネットを経由して侵入したり、保存されている情報を取得あるいは、削除・改変すること。（不正アクセス禁止等に関する法律）
- ・コンピュータウイルス等を作成したりすること。（刑法の不正指令電磁的記録に関する罪）
- ・他人が不快に感じる無意味な電子メール（スパムメール）を送信したり、自分が受信したスパムメールを他人に転送すること。
- ・インターネット上のサービスに対して、大量の要求を送ることによって、サービスの機能不全を起こさせること。（刑法の業務妨害，業務で行うと，特定電子メールの送信の適正化等に関する法律）
- ・ホームページの投稿フォームやブログ等に犯罪的な行為の予告を書き込むこと。（刑法の業務妨害，脅迫）
- ・いやがらせ目的で研究室の共同 PC や情報に暗号をかけてパスワードを教えないこと。
- ・執拗にメールを送りつけないこと。（ストーカー行為等の規制等に関する法律）
- ・性的な画像の取扱い。（児童ポルノに係る行為の規制及び処罰ならびに児童保護に関する法律，私事性的画像記録の提供等による被害の防止に関する法律（リベンジポルノ防止法））
- ・企業や商品の商標を無断でホームページに使用すること。（商標法）
- ・企業の顧客情報・技術情報等を不正に取得すること。（不正競争防止法）
- ・収集した個人情報を収集時に約束した利用目的以外に利用すること。（個人情報保護法，研究者倫理）
- ・共同研究の成果で秘密にされているものを，共同研究者の承諾を得ずにインターネット上で公開したり第三者に教えること。（著作者人格権，研究者倫理）



具体的な行為が違法か、公序良俗に反するか否かといったことは、最終的には司法の判断が必要になる場合があります。例えば、他人が違法行為を行っていても何もとがめられていないからといって、自らもその行為を行って良いということは絶対にありません。自らの行動を自ら正当化してはいけません。また、他人から疑いを持たれるような行為も慎みましょう。『李下に冠を正さず』で自らの行動を律して下さい。

就業規則関係---主に教職員のみ



国立大学法人東京工業大学の職員の服務については、就業規則で規定されています。職員には、これまでの国家公務員の時と同様に、以下の義務等があります。

- ・職務に専念する義務
- ・法令、大学の規則、職務上の命令に従う義務
- ・職務上知ることのできた秘密を守る義務
- ・大学の信用を傷つける行為や不名誉となる行為の禁止
- ・大学の規律と秩序を乱すことの禁止

例えば、勤務時間中にパソコンで私的な処理を行ったり、大学の秘密が含まれたファイルを他に転送したり、インターネット上の掲示板に業務と関係のない内容の書き込みを行ったりすることは、就業規則に違反することとなります。これらの義務等に違反した場合、懲戒解雇、停職、減給、戒告の懲戒処分、または訓告、嚴重注意、注意の対象となることがあります。研究や仕事を一緒にしている相手に、執拗に過度の負担や要求をするメールを送ることも、いわゆるパワーハラスメントにあたる場合もあります。また、指導学生等へのメールが同様にアカデミックハラスメントにあたる場合があります。

問題が起きたとき



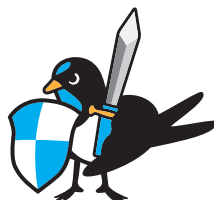
具体的な問題が発生したときは、情報倫理委員会にお知らせ下さい。

【情報倫理委員会連絡先】

メールアドレス：cce@jim.titech.ac.jp

セキュリティ篇

倫理的・法的な事項を遵守すると同時に、他者からの攻撃やコンピュータの故障に備えて、各自のデータだけでなく他人のデータを守るためにも、セキュリティ対策には万全を期す必要があります。セキュリティに関して最低限心がけるべき事項を挙げますので、コンピュータを利用する際には十分に注意して下さい。



モバイル機器の利用



スマートフォンやタブレット、ノート PC 等モバイル機器を使って、メールのやりとりや文書の作成等を行うのが普通になっています。しかし、大事な内容のメールやデータが保存された機器を紛失すると、個人情報や機密情報が漏えいする危険があり、また悪用される可能性があります。大学のアカウントのメールを他のアカウントに転送設定している場合にも注意が必要です。機密情報等をモバイル機器でやりとりしないように注意するとともに、万一紛失した場合でも不正なアクセスがされないようにパスワードを設定する等十分に注意しましょう。

バックアップ



ユーザ各自のデータは貴重な個人の財産です。定期的に自らの責任でバックアップを取るよう心掛けましょう。定期的にデータのバックアップを取ってあれば、万が一 OS の再インストール等の必要に迫られても、各自の貴重なデータは保全されます。ただし、バックアップメディアには寿命があり、またそれが読める環境も技術の急速な進展により失われてしまうことがあります。その点に十分に留意して、短期的なバックアップと、長期的なバックアップについては、それぞれ最適な方法をとる必要があります。秘密でないデータについては、外部の信頼できるアーカイブサービスを利用することも選択肢の一つです。

ウィルス対策



PC でもスマートフォン等のモバイル機器でもウィルスによる被害が発生しています。ウィルスは、場合によってはデータを破壊することもあるので、なめてかかっては大変に危険です。さらに厄介なことに、自分では気付かないうちに、ネットワークを通じて次々と感染し、

友達のデータまで破壊してしまうこともあるのです。ウィルスに対しては、次のことに十分に注意して下さい。

- ・各自の PC には、ウィルスチェッカーをインストールするようにして下さい。
- ・定期的にアップデートを行ってパターンファイルを更新するよう習慣付けて下さい。

日々の細かな気遣いと習慣が、いざというときに被害から我が身を守ってくれます。

ウィルスチェッカーとて万全ではありません。定期的にパターンファイルを更新していたとしても、新種のウィルスが発生した直後は感染の危険性があることに注意して下さい。また、特定の機関や個人を狙った、標的型攻撃も増えつつあります。不審なメールや添付ファイル、不審なウェブサイトへのリンク等を開くと PC が感染するような仕組みが組み込まれています。したがって

- ・差出人が不明なメールは開けない。差出人に直接確認する。
- ・差出人が知合いであっても、内容が不自然なメールに添付されたファイルは開けない。

「少しでもおかしいな」と思ったらメール等は不用意に開かない、を徹底しましょう。

ウィルスの中には、ホームページを閲覧することで感染するものもあります。興味本位にいかがわしいホームページを閲覧すること等は慎みましょう。

信用できないフリーソフト等を不必要にインストールすることは慎みましょう。スパイウェアと呼ばれる、インストールした PC 内の重要な個人情報や、PC での操作履歴をこっそり外部へ報告するプログラムを、インストールと同時に埋め込まれることがあります。

セキュリティアップデート



各自の PC にインストールされている OS やアプリケーションソフトのセキュリティアップデートは、必ず行うようにしましょう。面倒だからとのんびり構えていると、いざというときに、大火傷をすることになります。PC を起動する際に、セキュリティアップデートの必要がないかどうかを確認する習慣を身に付けましょう。

ソフトウェアメーカーによるサポートが終了した OS を使用するのには、セキュリティアップデートもできなくなるので、新しい OS に入れ換える等必要な準備をすすめましょう。

パスワード管理・ハッキング対策



パスワードは情報システムを利用する際の鍵のようなものです。これが漏洩してしまうと、利用権のない第三者に無断で情報システムが利用されてしまいます。これは家の鍵を盗まれて泥棒に入られてしまうようなものです。パスワード管理に関しては、以下のことに注意しましょう。

- ・友人であっても、パスワードを他人に教えないようにしましょう。また、パスワードを書き留めたメモをディスプレイに貼り付けるのは、パスワードを教えているのと同じです。自分だけしか分からないように管理しましょう。
- ・パスワードは十分に長いものを利用し、他人が容易に推測できるような簡単なものを使うことは避けましょう。
- ・連続する数字、同一文字の繰り返しをパスワードにするのはやめましょう。
- ・あたかも本当の管理者のごとく装い、システム更新後のテストのため等と称して本物そっくりの偽物のサイトにログインさせ、パスワードを盗む、いわゆるフィッシングと呼ばれる手口が横行しています。いかなるシステム管理者もこのような要求をすることはありませんので、このようなメールに騙されないよう十分注意して下さい。

コンピュータ以外のプリンタ複合機、ネットワークカメラ等のネットワーク機器についても注意が必要です。これらの機器でもパスワードの設定ができます。パスワードを設定しなかったり、パスワードを購入時のままにしておくと、第三者がインターネットからこれらの機器にアクセスして、情報が漏えいする危険性があります。必ず、適切なパスワードを設定する等の対策を取るようになって下さい。

SNS、フリーメール、クラウドサービス等が相互に結びついてインターネットの便利な環境ができあがっています。このことは逆に、ハッキングを試みる者からは、私たちがインターネット上に重要な情報のいろいろな手がかりを公開している危険性も意味しています。ひとつのサービスのIDやパスワードを他のサービスと共用していたりすると、ひとつひとつの情報を組み合わせて、重要なメールアドレスのパスワード等が探り当てられる可能性があります。このような危険を避けるためにも、パスワードの設定、IDやパスワードの共用を避けるように注意が必要です。

クラウドサービスにもいろいろなものがあります。個人や大学の大切な情報を外部の、特に、無料のクラウドサービスにアップロードすることはやめましょう。クラウドサービスは急に使えなくなることがあります。活動に支障がないよう対策を採っておきましょう。

共有設定やネットワークの管理



PCの共有はなるべく避けましょう。個人情報や機密情報の漏えいの危険があります。家族や友人との間でもいけません。

IDやパスワードの共有は決して行わないで下さい。パスワードの使い回し（他のサービスで使っているもしくは使っていたパスワードを再利用する等）も止めましょう。

IDやパスワードを共有しなくても、Googleログイン等といったクラウドサービス等で、一回のログインでメールからファイルの保存等さまざまなサービスが受けられる場合、ブラウザを閉じてサービスへのログイン状態が続いていて、他の人が自由にアクセスできる状態になっている場合があります。これらのサービスでの作業が終了したときには、必ず、ログオフ（サインアウト）するように心掛けて下さい。

共有ファイル設定には十分に注意を払って、不必要にファイルを共有にしておかないよう気を付けましょう。特に、新しくファイルやフォルダを作成したときには、その共有設定がどうなっているか、確認する必要があります。ファイヤウォールは、ルータ等でも設定可能ですが、個人のコンピュータにおいても設定可能となっています。外部からのアクセスに対するポートは、必要のない限り、できるだけ閉じておく習慣を付けましょう。

障害時の対応



意図的に情報システムや情報資産への破壊行為を行うことは論外ですが、操作ミス等、意図しない行為や悪意はなくとも興味本位の行為が、結果的に情報システムの障害や他人の情報資産へ損害を与えることがあり得ることに注意して下さい。万が一、そのような事態になった場合、決して隠したりせずに、即座にシステム管理者に連絡し、被害が拡大しないように努めて下さい。

不正アクセス、情報漏えいが発生した場合



不正アクセスや情報漏えい（セキュリティンシデント）が発生した場合には、個人で対応することは困難です。所属部局や研究室のシステム管理者に連絡するとともに、全学のセキュリティ担当部署である東工大CERTに連絡を取って下さい。

【東工大CERT連絡先】

メールアドレス：contact@cert.titech.ac.jp

Q&A 篇



情報倫理とセキュリティにまつわる身近な疑問にお答えします。

Q. 私物コンピュータの大学ネットワークへの接続

自分のパソコンを大学のネットワークに接続して良いでしょうか。もし許可されているとしたら、どのような点に注意したら良いですか。

A. 研究室のネットワーク管理者の指示に従ってください。なお、学内の食堂等の公共エリアには無線LANが設置され、学生等が自分のパソコンをネットに接続できます。パソコンを接続するとき、自分のパソコンにウイルスが感染していないかどうか、くれぐれも注意して下さい。本学もいくつかのウイルスの被害に遭っていますが、ある事例ではその感染源は学生の接続したパソコンでした。共有設定やファイヤウォールの設定にも注意を払って下さい。

Q. 大学のポータルサービスに接続するにはどうして面倒な手順が必要なのですか。

A. ポータルへのアクセスには、IDパスワードとマトリックス認証が設けられています。これは外部からの不正なアクセスを防止するために設けられています。面倒でも、2段階認証、証明書を使うことに慣れて下さい。

Q. 大学のソフトウェアの私物コンピュータへのインストール

研究室で購入したソフトウェアを自分のパソコンにインストールしても良いのでしょうか。

A. これは、そのソフトウェアのライセンス契約と大学の財産の使用目的の観点から考える必要があります。ライセンス契約に従っている限りライセンス上の問題はありますが、これは研究室で購入したものですから研究室の業務に関連した目的にのみ用いることは、他の物品の場合と同じです。

私的目的への流用を疑われる恐れがあるので、私物のコンピュータへのインストールはやめましょう。

Q. 文献検索

他大学の知り合いから、本学で利用可能なデータベースや電子ジャーナルを使用した文献検索を頼まれたのですが、やっても良いのでしょうか。

A. データベースや電子ジャーナルは、本学がライセンス契約を結んで利用しており、利用者の範囲は本学に所属する教員・学生等に限定されています。個人の学術研究・教育目的以外の目的で利用することや、検索結果を他人に提供することは契約違反です。こうした行為が判明した場合、提供元から本学全体の利用が停止されますので、絶対に行わないで下さい。

Q. データベースのダウンロード

データベースや学術雑誌のサイトからデータや文献をダウンロードするときにはどのような点に注意したら良いですか。

A. 過去に何度も、本学の教員・学生が大量の文献をダウンロードしたため、提供元から本学全体の利用が停止された事例がありました。教育・研究上、大量のダウンロードを行う場合は、提供元の承諾が必要です。大量ダウンロードが必要な場合は、附属図書館に問い合わせして下さい。

Q. アップデートソフトのコピー

ウイルスに感染したパソコンを大学のネットワークに接続したことによる被害が出ました。そこで、例えば、セキュリティアップデートをしていなかったり、最新のウイルス定義をしていないパソコンは、繋いではいけない、というような規則を考えました。ところが、もしも訪問者が来たとき、その人のパソコンを繋げられないのでは不便です。また、パソコンをネットワークに繋げなければセキュリティアップデートやウイルス定義の更新もできません。そこで、ある程度安心できる状態にするためのCDを作ろうかと思いますが、それを行っても良いのでしょうか。

A. アップデートがされているか不確かな場合には、訪問者のパソコンを大学のネットワークにつなげるのではなく、大学の管理されたパソコンにデータを移して訪問者が使用できるようにする等の方法を考えましょう。

Q. 論文の公開

研究会等での発表論文を自分のホームページに載せても良いでしょうか。

A. 研究会等での発表論文や、国際会議や論文誌に投稿した論文を、投稿時点で自分のホームページに載せることは通常行っていることです。しかし、学会によっては、論文の著作権は著者のものでも、論文を学会誌以外で公開することを制限しているところもあります。特に採録後については、学会と相談してその規定に従って下さい。
(東工大のT2R2の運用指針も参考にして下さい。)

Q. 研究状況の公開

自分の研究の進行状況をインターネットで公開しても良いでしょうか。

A. あなたの研究と想着いても、その研究自体が先生の指示に基づいていたり、同僚のアイデアや未発表の研究成果に助けられていたりしている場合があります。あなたが自分の研究の進行状況をインターネットで公開することによって、公開を望んでない先生や同僚のアイデアを公開してしまうことになりかねません。また、あなたのインターネットでの公開を見て、見ず知らずの他人があなたより早くその内容を論文にまとめて発表してしまうことがあります。その結果、あなたの研究の成果であることを証明することは難しくなります。したがって、自分の研究の進行状況をインターネット等公開の場に載せることには、慎重な対処が必要です。学生の場合は、指導教員と相談すると良いでしょう。

Q. コンピュータやネットワークの利用（目的外使用禁止）

大学改革等の問題点等がネットワーク上で議論されており、ネットワークを通して、問題点を指摘したりしました。私のような行為は処罰の対象でしょうか。

A. この行為は、直接的な研究教育活動ではありません。しかし大学人として大学の将来を考える重要な行為の一つです。一方コンピュータやネットワークは広く一般的な情報インフラの一部となっており、大学業務を支えています。その意味ではあまり問題は無いと思われませんが、論点は、この行為が業務時間内に行う行為として適正であるかどうかという点にありその判断によります。

Q. 事実を述べるのも中傷になる？

私は、友人の知られたくない事実を、メーリングリストやブログで皆に知らせてしまいました。私は友人を中傷する気はなく、単に事実を述べただけだと思っていましたが、友人は、そのことを許せないようです。

A. 嘘の噂等を流すのはいけないことは、皆知っていると思いますが、事実を述べても中傷になる場合があります。むしろ実際の中傷には、そのようなケースが多いのではないのでしょうか。事実を述べても名誉毀損や人格権の侵害にあたる場合がありますので十分に注意しましょう。

Q. どこまでが個人間のやりとりか

私のメールに対して友人は、かなり強い反論を他の友人にも CC して私に返送して来ました。私だけへの返信ならば、個人間の意見のやり取りということで、問題ないと思いますが、その返信を勝手にメーリングリストにも CC しても良いのでしょうか。

A. これはある意味で、公の場で個人を強く批判したことになる可能性があります。名誉毀損と思われることがあるので、相手のメールを参照や添付する場合は、必ずあらかじめ承諾を得ましょう。

Q. コピープロテクト

CD や DVD の複製防止機能（コピーコントロール）をソフトを使って解除して複製することは著作権の侵害にあたりますか。

A. 著作権法 30 条 1 項は、個人的にまたは家庭内その他これに準ずる限られた範囲内において使用することを目的とするときは、使用者に著作物を複製することを認めています（私的使用のための複製）。しかし、技術的保護手段を回避することで複製可能となったものをその事実を知りながら複製した場合には、私的使用のための複製にあたらぬとしています（同項 2 号）。

このケースでは、ソフトを使用することで複製防止機能が解除できることを知りながらこれを使用し、複製しているわけですから、私的使用のための複製とは認められず、著作権（複製権）の侵害にあたります。

Q. クライアント／サーバ・システムの利用によるプログラムの複数人利用

学内のクライアント／サーバ・システムにおいて、サーバに1つのプログラムを保存し、クライアントがそれを一時的に引き出して使用するようにしたいのですが、法的にどのような注意が必要ですか。

A. サーバにコピーした1つのプログラムの複製権の許諾だけでなく、プログラムの著作権者から送信可能化権の許諾を受けることが必要となります。このような使用についても許諾を必要とするライセンス契約が多くみられます。

Q. サーバ上に置かれた電子書籍等の複数人利用

学内のイントラネット・システムで、サーバにプログラムではない電子書籍等の著作物、例えば1つの電子百科辞典を保存し、多数のクライアントで使用する場合の注意事項にはどのようなものがあるのでしょうか。

A. ハードディスクにコピーが許諾された電子百科辞典であっても、多数のクライアントでの使用を制限しているものもあります。
これとは別に、自分でスキャナを利用して書籍を電子化するいわゆる自炊が問題になる場合があります。

Q. コンピュータへの侵入・破壊行為

コンピュータへの侵入や破壊行為にはどのようなものがあるのでしょうか。

A. みなさんも「ウィルス」、「ワーム」、「トロイの木馬」等という言葉をよく聞くとと思います。マルウェアとも呼ばれ、コンピュータから個人情報不正取得されたり、システムの不正確操作が行われる可能性があります。また、大量のアクセスを集中させてウェブサーバーの機能を停止させる攻撃もあります。
さまざまな種類のものが新しく現れるので、最新のセキュリティ対策を心がける必要があります。

Q. 不正侵入の防止
不正侵入を阻止するためにはどのような点に注意したら良いでしょうか。

A. Windows 等の複雑かつ大規模な OS には、セキュリティホール（ソフトの欠陥とみなしてもよい）が存在し、クラッカーはそこを狙って侵入してきます。すでに見つかったセキュリティホールに関しては、ソフトウェアメーカーから「プログラムを直すプログラム」が公開されていますので、自分で修正することを心掛けて下さい。このような作業を普通「パッチを当てる」といいます。また、自分のコンピュータをきちんとした「ファイヤウォール」が設置されているサイトに接続すると同時に自分のコンピュータにもファイヤウォールを導入することも重要です。その他、ウィルスチェックプログラムを用いて、常時ウィルスのチェックを怠らないことも重要です。

Q. インターネット上の自分の名誉を害する書き込み
ブログに自分の名誉を害する書き込みがされていますどうすればよいでしょうか。

A. ブログの管理運営者（プロバイダ等）に削除を依頼することができます。本人自身では対応することが困難な場合も多いです。人権侵害や名誉毀損として法務局や警察等に相談して手助けを求めることもできます。沢山の書き込みがある場合、検索エンジンに検索表示されないような対応も可能ですが、手続も複雑です。弁護士等の専門家の協力も必要になります。だれに相談して良いか分からない場合には、法テラス（日本司法支援センター）に相談することができます。

【法テラスのホームページ】

<http://www.houterasu.or.jp/index.html>

関係ホームページ等

【東京工業大学情報倫理委員会（情報倫理とセキュリティのためのガイド）】

<http://www.titech.ac.jp/rinri/>

【東京工業大学情報システム緊急対応チーム】

<http://cert.titech.ac.jp/>

【東京工業大学情報倫理ポリシー】

http://www.jyoho.jim.titech.ac.jp/kik_sui/security/policy_1.pdf

【東京工業大学情報セキュリティポリシー】

http://www.jyoho.jim.titech.ac.jp/kik_sui/security/policy_2.pdf

【情報セキュリティインシデント発生時の報告について】

http://www.jyoho.jim.titech.ac.jp/kik_sui/security/index.html#higai

情報セキュリティインシデント発生時には、文部科学省国立大学法人支援課に報告を行っていますので、確認事項リストを記入のうえ、研究推進部情報基盤課情報企画グループ (kib.kik@jim.titech.ac.jp)までご連絡をお願いします。確認事項リストについては、全ての項目を埋めるまで報告を行わないのではなく、判っている状況を第一報として迅速に報告ください。

情報倫理専門委員会 WG

委員長 金子 宏直 准教授
副委員長 脇田 建 准教授
石川 謙 准教授
櫻井 実 教授
伊東 利哉 教授
山口 雅浩 教授
渡辺 治 教授
横田 治夫 教授
友石 正彦 教授
飯田 勝吉 准教授
松浦 知史 准教授
佐藤 礼子 准教授
戦 暁梅 准教授
秋友 豊香 広報・社会連携課長
田中 昇 教務課長
松原 康夫 情報基盤課長

(順不同)

(事務担当) 情報基盤課 小寺 孝志、森谷 寛

情報倫理とセキュリティのためのガイド

発行年月（初版） 平成 17 年 4 月 1 日
（第 2 版）平成 28 年 4 月 1 日

企画編集 情報倫理専門委員会 WG

発 行 東京工業大学