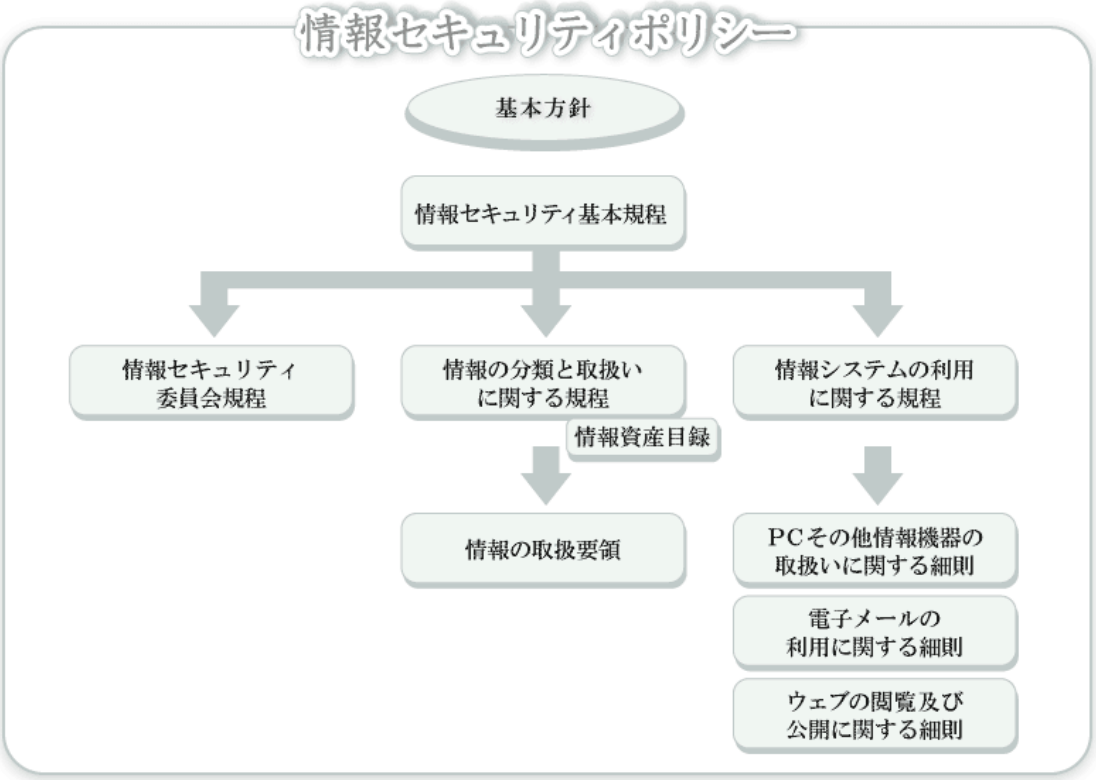
学生のみなさんへ

守ろう！
情報セキュリティ

～情報セキュリティポリシーが制定されました～

PCやスマホ、インターネットの利用が日常生活の一部となっている現在、情報漏えいをはじめとする情報セキュリティリスクは、とても身近なものとなっています。インターネットを通じて情報が漏えいしてしまうケースや、情報が満載のUSBメモリを失くしてしまうケース、スマホを落としてしまうというケースもありますね。たとえばサークル活動に関わる個人情報などを、パスワード設定をしていないノートPCに保存したりしていませんか？情報セキュリティ事故は、あなただけでなく身近な友人の情報を危険に晒し、場合によっては、あなたの所属する団体・グループの活動に支障が出ることにもなりかねません。

東京経済大学では、情報資産を情報セキュリティ侵害から守り、適切に管理していくために「情報セキュリティポリシー」を定めています。情報セキュリティポリシーは、次のような構成になっています。



全文は、情報システム課のサイト（http://www.tku.ac.jp/iss/）で学内公開していますので、是非ご一読ください。

このパンフレットでは、「情報セキュリティポリシー」の中から、学生の皆さんに特に注意していただきたい点をピックアップして解説しています。あなたの情報セキュリティリスクはどの程度なのか点検してください。そして、あなたの情報をしっかり守っていきましょう。

チェックしてみよう！

- ☐ TKU－NETのIDを他人に貸していませんか？ ☞ P.4
- ☐ パスワードを、定期的に変更していますか？
- ☐ パスワードに、電話番号や生年月日を使用していませんか？
- ☐ ネットカフェなどで、ポータル等のサービスを利用していませんか？ ☞ P.5
- ☐ 学内のPCでパソコンにログインしたまま、席を離れていませんか？ ☞ P.6
- ☐ ノートPC、スマホやケータイ、パスワード設定をしていますか？
- ☐ USB メモリに大事なデータを保存して持ち運んでいませんか？
- ☐ 自分が管理するPCにウィルス対策ソフトを導入していますか？ ☞ P.7
- ☐ ウィルス定義ファイルは最新になっていますか？
- ☐ OSやアプリケーションソフトのアップデート、していますか？
- ☐ スマホにもセキュリティ対策していますか？
- ☐ 機密性の高い情報をメールで送っていませんか？ ☞ P.8
- ☐ 不審なメールを無防備に開封していませんか？
- ☐ To、Cc、Bcc　正しく使い分けていますか？
- ☐ 電子メールの書き方、送り方のマナー、知っていますか？ ☞ P.9
- ☐ ウェブサイト上のバナー広告やリンクを無防備にクリックしていませんか？ ☞ P.10
- ☐ ウェブサイトからダウンロードしたファイルを、無防備に実行していませんか？
- ☐ ブログや Twitter に、不用意に個人情報や公序良俗に反することなどを書き込んでいませんか？ ☞ P.11
- ☐ コピペでブログ、発信していませんか？

TKU－NETのID・パスワードは、情報を守る鍵

TKU－NETのIDは、本学の情報サービスや情報環境を利用するための入り口の鍵であり、そこに保存される情報を守るための鍵です。本学の情報サービスや情報環境は、本学学生の教育・研究のために提供されるものであり、TKU－NETのIDを持つ本学学生及び本学関係者のみが利用できるものです。ID・パスワードは、適切に管理しましょう。

☑ TKU－NETのIDを他人に貸していませんか？

TKU－NETのIDを他人に貸せば、当然ながら、ファイルサーバー上に保存されているあなたのファイルや、TKUポータルで参照できる成績情報等が、参照されたり改ざんされたりする危険性があります。また、他人があなたのIDを使って、何らかの問題を起こした場合には、あなたの責任も問われることになります。

ID、パスワードの貸し借りは厳禁です。

☑ パスワードを、定期的に変更していますか？

万一、パスワードが盗み見やハッキング等により、盗まれてしまった場合でも定期的にパスワードを変更していれば、そのIDを不正に使われ続けることを防ぐことができます。3ヶ月に1度程度は、パスワードを変更しましょう。また、パスワードを、目につきやすい所にメモして貼っておくようなことはやめましょう。

☑ パスワードに、電話番号や生年月日を使用していませんか？

推測されやすいパスワードは、パスワードが盗用される要因となります。
パスワードを盗まれにくいものとするために、次の点を守ってください。

・半角英字と数字を混在させる。
・新旧同じパスワードにしない。
・氏名、生年月日、電話番号等推測されやすい文字列を使用しない。

ネットカフェなどで、ポータル等のサービスを利用していませんか？

ネットカフェ等不特定多数の人が利用するPCは、悪意のあるプログラムが仕掛けられている可能性があり、ID、パスワードを盗まれる危険性があります。このような場所で、ID、パスワードの入力が必要な情報サービスを利用することは避けましょう。口座番号等、悪用される恐れのある情報を送受信することも避けた方が安全です。

TKU－NETパスワードルール
◆使用できる文字は、半角英数です。
◆ユーザIDを含めることはできません。
◆文字数は、6文字以上15文字以内。
◆英字は大文字と小文字を区別します。
◆新旧同じパスワードにはできません。

強力なパスワードとは･･･

（microsoft のサイトより抜粋）
★少なくとも8文字以上のもの
★ユーザ名、本名、企業名を含まないもの。
★単語をそのまま使用していないもの。
★前のパスワードと大幅に異なるもの。
★4つのカテゴリの文字（英大文字、英小文字
数字、記号）を全て含むもの。

大事な情報、置き忘れに注意！

PC教室には、USBメモリが挿入されたまま置き忘れられていることがしばしばあります。学生課にも大量の忘れ物USBメモリが届いています。

大事な情報の置き忘れ、紛失、盗難には、充分注意してください。

あわせて、万一紛失してしまった場合にそこに保存されている情報が漏れることのないように、パスワードの設定や情報の暗号化を心がけましょう。

万一、サークル住所録等の個人情報など悪用される恐れがある情報を保存したUSBメモリやPC等を紛失した場合は、学生課に届け出てください。

☑ 学内のPCでパソコンにログインしたまま、席を離れていませんか？

少しの間でも、PCを離れる時は、ログオフまたはシャットダウンしてください。

☑ ノートPC、スマホやケータイ、パスワード設定をしていますか？

ノートPC、スマホ、携帯電話には、写真やメールなど、多くの情報が入っていますね。これらの機器は紛失の危険も多く、また、数分放置した間に悪用される危険も多いものです。万一の紛失や盗難に備えて、パスワード設定、スクリーンロックの設定等をしてあなたの情報を守りましょう。

☑ USB メモリに大事なデータを保存して持ち運んでいませんか？

USB メモリは、紛失・置き忘れが多い記憶媒体です。紛失・置き忘れに充分注意するとともに、大事な情報、悪用されたくない情報を保存する場合には、万一に備えて、パスワードの設定、情報の暗号化をしておきましょう。

パスワードの設定や、情報の暗号化については、USB メモリに付属のマニュアル等を参照してください。

コンピュータウィルスから、情報を守ろう！

コンピュータウィルスは、あなたのコンピュータに侵入し、コンピュータの動作に異常を起こしたり、情報を盗んだり、ファイルを破壊したりする不正プログラムです。感染経路は、メールの添付ファイル、USBメモリ、インターネットからダウンロードしたファイル、時には、インターネット上でクリックしただけで感染することもあります。また、あなたのコンピュータが被害にあうだけでなく、ネットワーク上に被害を撒き散らしてしまうこともあります。

自宅やサークル等で自分が管理するPCには、必ずウィルス対策を行いましょう。

また、最近では、スマホを狙ったウィルスが急増しており、スマホ用のウィルス対策ソフトもリリースされています。スマホにもPCと同様のウィルス対策が必要です。

☑ 自分が管理するPCにウィルス対策ソフトを導入していますか？

☑ ウィルス定義ファイルは最新になっていますか？

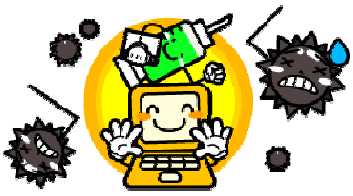
PC購入時に、ウィルス対策ソフトを導入しただけでは、安心できません。ウィルス定義ファイルが常に最新の状態になっていることが肝心です。また、ウィルス対策ソフトが有効期限切れになっていないかにも注意しましょう。

ウィルス対策ソフトが常に最新の状態で機能していることを確認しましょう。

☑ OSやアプリケーションソフトのアップデート、していますか？

OSやアプリケーションソフトに対する更新プログラムが定期的に出されており、これを導入することにより、セキュリティが強化されます。

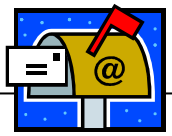
定期的にアップデートを実行しましょう。



☑ スマホにもセキュリティ対策していますか？

スマホにも、PCと同様のセキュリティ対策が必要です。ウィルス対策ソフトを導入する、アップデートを行う、信頼できるところからアプリケーションを導入する、等の対策を行いましょう。

電子メール利用の心得



電子メールは、今日では、必要不可欠なコミュニケーションツールですね。しかし、電子メールを安全に活用するには、いくつか心得ておくべきことがあります。

確認してみましょう。

機密性の高い情報をメールで送っていませんか？

電子メールは、機密性が高いものではありません。郵便にたとえるならば、封書ではなくハガキと考えてください。銀行口座の情報や暗証番号などをメールで連絡するのは避けましょう。機密性の高い情報をどうしてもメールで送る必要がある場合には、メール本文に書くのではなく、ファイルを作成し、そのファイルを暗号化・パスワード付与して添付ファイルとして送りましょう。その際、そのパスワードは、そのメール以外の方法で、漏えいに充分注意して、伝えましょう。

不審なメールを無防備に開封していませんか？

ウィルスの感染経路は、いくつかありますが、電子メールの添付ファイルと、HTML メールは最も一般的なものの1つです。場合によっては、メールを開封しただけでウィルス感染してしまうこともあります。

覚えの無い不審なメールは開封せずに削除しましょう。

To、Cc、Bcc　正しく使い分けていますか？

To は、メールの宛先、Cc（CarbonCopy）と Bcc（BlindCarbonCopy）は、宛先ではないけれども参考として同じメールを送信する場合に使います。Cc と Bcc の違いは、Bcc で指定されたメールアドレスは他の受信者には伝わらないことです。

お互いにメールアドレスを知っている人達に送るのであれば、To または Cc を使用すればよいのですが、面識の無い人達に一斉にメールを送る場合には、宛先は Bcc で指定しましょう。To や Cc では、メールアドレス情報の漏えいになり、さらに場合によっては、プライバシーの漏えいになることもあります。注意しましょう。

電子メールの書き方、送り方のマナー、知っていますか？

安全に、快適に電子メールを利用するために、電子メールを書く時、送る時のマナーがあります。確認してみましょう。

◆半角カタカナや機種依存文字は使わない。

ローマ数字や①、㏍、㈱等は、機種依存文字といって、PCの環境によって表示されないことがあります。また、半角カタカナも文字化けの原因になりますので、使用しないようにしましょう。

◆原則として、テキスト形式で送りましょう。

リッチテキスト（HTML）形式のメールは、受信側の環境によっては正しく表示されないことがあります。また、ウィルス混入の危険性もあり、HTML 形式のメールを禁止している会社等もあります。友人間のメールであればリッチテキスト形式でも良いのですが、会社等に送る場合は、テキスト形式で送るのが原則です。

◆添付ファイルのサイズに注意しましょう。

受信できるメールのサイズは、サーバーで制限がかけられていることが一般的です。スムーズな送受信のためにも、1MB 程度までを目途にしましょう。

◆件名は具体的に

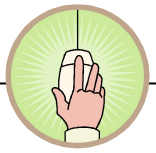
件名は、メール内容を端的、具体的に表すものにしましょう。

「こんにちは」「お願い」等の件名は迷惑メールと判断され、届かないこともあります。

◆チェーンメールは、やめましょう。

「不幸の手紙」のように他の人への転送を要請するメールをチェーンメールといいます。チェーンメールは、ネットワークに高負荷をかける迷惑行為です。発信しないのはもちろん、受信しても転送するのはやめましょう。

ウェブサイトに潜む危険



ウェブサイトは情報収集や情報交換の場としても、ショッピングの場としても、大変便利なものです。しかし、そこには多くの危険が潜んでいます。ウェブサイトに潜む危険をきちんと把握して、安全に活用しましょう。

ウェブサイト上のバナー広告やリンクを無防備にクリックしていませんか？

インターネット上には、不正なソフトウェアをダウンロードさせることを目的としたリンクや、不正なサイトへの誘導を狙ったリンクが多数存在します。また、バナー広告には、有害なサイトやウィルスダウンロードサイトへのリンクが設定されていることもあります。

無防備にバナー広告やリンクをクリックすることは、危険ですのでやめましょう。

ウェブサイトからダウンロードしたファイルを、無防備に実行していませんか？

インターネットから入手できるファイルには、危険なものが多数存在しています。不必要なファイルのダウンロードは、やめましょう。何らかの目的でファイルをダウンロードした場合は、それを開く前に、不正プログラムの有無を必ず確認しましょう。（不正プログラムが含まれていた場合は、直ちに削除しましょう。）また、電子署名等により、配布元の組織が適切な組織であるかどうかを確認しましょう。

ブログや Twitter などに、不用意に個人情報や公序良俗に反することなどを書き込んでいませんか？

学外のウェブサイトの掲示板やブログに書き込みを行う場合、書き込む内容が情報漏えいにあたらないか、またプライバシーや著作権の侵害にあたらないか充分に注意しましょう。

自分の個人情報を書き込む場合、そのサイトが信用できるものであるか、きちんと確認しましょう。また、重要な情報を書き込む場合、SSL/TLS 通信が利用されているか（URL が、https:で始まっているかどうか）も確認しましょう。

最近、Twitter 上にアルバイト先で職務上知ったことなどを安易につぶやいてしまうトラブルが報道されています。インターネット上のつぶやきは、全世界に向かって叫んでいるのと等しいことを自覚して、つぶやく前に、その内容が適切であるか、充分に確認しましょう。

コピペでブログ、発信していませんか？

ニュース記事、雑誌の表紙、写真、アニメキャラクターなどの著作物は、著作権法によって保護されており、無断コピーは、著作権法違反になります。Webサイトで見つけた記事や写真などを安易にコピペして自分のサイトやブログに掲載するのは、（明らかに著作権フリーを謳っているものを除き）、違法行為です。

「コピペでレポート」も、著作権法に抵触します。他人の著作物を自身のレポートに「引用」することは認められていますが、「引用」には①引用部分を明確にすること、②レポート本文と引用部分の主従関係が明確であること、③出典を明示すること等の要件があり、これらを満たさないものは違法行為です。

コピペをする時には、それが著作権侵害にあたらないか、必ずチェックしましょう。

情報セキュリティパンフレット
「守ろう！情報セキュリティ」

2011 年 12 月発行
編集・発行　東京経済大学　情報セキュリティ委員会
事務局　東京経済大学学務部情報システム課