学部１～３年生用

東京都市大学　情報セキュリティポリシー　「セキュリティ対策チェックシート」

2013 年 4 月 1 日施行　情報基盤センターSC 作成

情報セキュリティポリシーとは、本学の情報システムや情報資産を守るための取り決めです。このポリシーを導入する背景には、主に増加するサイバー攻撃や情報流失が挙げられます。懸念事項を防止するために各自、情報セキュリティ意識を向上させ、実践できるよう、ポリシーが制定・導入されることになりました。なおポリシーは、第 1 部から第 3 部までの 3 部構成でまとめられています。ポリシーの内容は以下の Web ページをご覧下さい。

http://www.itc.tcu.ac.jp/iss/

対策のポイントは 3 つです。

・技術的対策は、暗号化や不審メール対策などの様々な情報技術を駆使して行う対策です。
・物理的対策は、情報資産を安全に保管するなどで、紛失や損失から守るための対策です。
・人的対策は、構成員に情報セキュリティセキュリティの重要性を理解してもらい、ルールを守って貰えるようにするための対策です。

皆さんに情報セキュリティセキュリティの重要性を理解し、対策ができているか？確認チェックを行いましょう！

1　物理的対策

（1） 情報機器及び記憶媒体の紛失・盗難対策（*情報機器及び記憶媒体は以下を示します*）

※記憶媒体・・・CD、DVD、MO、フロッピーディスク、USB メモリ、HDD 等
※情報機器・・・サーバー、ノート PC、デスクトップ PC、タブレット端末、スマートフォン等

確認チェック☑しましょう！

その場から離れる際には、**置き忘れ**がないか確認します。	□
情報機器が出入り自由な場所に設置されている場合は、安易に**持ち出されない**ように対策します。	□
席や教室から一時的に離れる場合は、記憶媒体をその場に**放置**しないようにします。	□
情報機器を持参する場合は、盗難に合わないよう**身につけておく**か、**目の届く場所で使用**します。	□

（2）情報機器及び記憶媒体の持ち出し対策（*機密・重要情報が入った情報機器及び記憶媒体は、極力持ち出しを控えましょう！*）

関係者以外が機密・重要情報の入った情報機器及び記憶媒体のファイルやフォルダなどを開けないよう、**暗号化やパスワードの設定**をします。	□
第三者が使用できるような環境（インターネットカフェなど）で機密・重要情報を閲覧した、使用しないように**心掛け**ます。	□

（3）情報機器及び記憶媒体の廃棄及び譲渡

機密情報・重要情報が入った情報機器及び記憶媒体を廃棄、もしくは譲渡する際には、**保存情報を読み出しできない状態**にします。	□
機器に入っている記憶媒体(ディスク)の**残存情報の有無を確認**します。	□
記憶媒体(ディスクや USB 等)を破棄する場合は、完全に消去するソフトを使用しファイル復元ソフト等で復旧されないようする方法、または**物理的に破壊して**から処分するなどの対策を行います。	□

（4）情報機器及び記憶媒体の持ち込み

情報機器及び記憶媒体を学内へ持ち込む場合は、**ウイルス対策ソフトを導入**し、情報セキュリティ対策を講じます。 特に、拾得や譲渡により入手した情報機器及び記憶媒体については、ウィルス感染などの危険性を最大限に考慮します。	□

2　人的対策

（1）各自の役割や責任の理解と実践

情報セキュリティのために、**各自が果たすべき役割と責任**について理解し、実践します。 特に、取引業者などの学外者に対しても、情報セキュリティポリシーを説明の上、遵守を求め、必要に応じて、秘密保持に関する取り決めを行います。	□

（2）セキュリティ事故・障害時の対応と報告

情報セキュリティに関する事故・障害及び公開情報の改ざん等を発見した場合には、当該学科 ISS 管理者あるいは ISS 担当者に**報告**します。	□

（3）卒業時の対応

卒業や退学をする場合は、本学の資産である情報機器やソフトウェアライセンス、重要情報・機密情報などを所持している場合には、**返却、廃棄**し、外部へ持ち出さないようにします。	□

3　技術的対策

（1）各自の役割や責任の理解と実践

・自己の**パスワードは秘密**です。 ・十分なセキュリティを維持できるよう、自己のパスワードの設定及び変更に配慮します。 ・全学認証システムのパスワードは、毎年所定の期間内(今年は 4~6 月)に **1 回以上のパスワード変更**を行うことが義務付けられていますので変更します。　(変更をしないと、パスワードが無効となり、認証されなくなりますので注意してください)	□

（2）無線 LAN 暗号鍵の管理

無線 LAN 基地局(アクセスポイント)は、不正アクセスおよびネットワークの情報を傍受されて悪用されないよう、使用する構成員は、無線 LAN 暗号鍵を秘密扱いとし、**他人に教えない**ようにします。 なお、情報基盤センターが管理する無線 LAN 基地局を利用する場合は、「無線 LAN 利用申請」をしてください。	□

（3）メールの誤送信・情報流出対策

メールの誤送信をしないように、**送信時には最大限配慮**を行います。	□
機密情報、重要情報の添付ファイルについては、**パスワードを施す**などの情報流出対策を講じます。	□

（4）ライセンス管理

ライセンス保持者は、契約の内容を遵守しライセンスを適切に管理します	□

（5）ネットワーク接続機器のウィルス対策

本学のネットワークに接続する情報機器は**ウィルス対策ソフトを導入**し、OS・アプリケーションのセキュリティアップデートを行うなどのセキュリティ対策を講じます。 ウィルス対策が不可能な機器については、情報基盤センターに相談するなどして、個別に**可能な範囲**で対策を行います。	□

（6）ファイル共有ソフトの使用禁止

情報の漏えい防止およびウィルス対策として、以下の行為は原則**禁止**されています。 ・違法なファイル交換などを目的とするファイル共有ソフトを、本学のパソコン等にインストールしての使用 ・ファイル共有ソフトをインストールしたパソコン等を学内に持ち込む行為	□

（7）無線 LAN 基地局の適正管理

他人に情報を傍受されて悪用されたり、無断で無線 LAN 基地局を使用されないよう、無線の暗号規格として WPA・WPA2 を使用します。	□

（8）公開するウェブページの適正運用

本学に関連する内容のウェブページやブログ、ソーシャルメディアなどの書き込みを公開する場合は、学内外（設置場所）に関係なく、本学の「コンテンツ倫理綱領」を遵守し、学外サーバーについては、そのサービスを提供する組織の利用規則も併せて遵守します。	□