

情報セキュリティ対策のお願い(1)

ウイルス、マルウェア対策

- 工学部／工学研究科において多発しているセキュリティ事故と、その主な経路
 - P2Pソフトの利用(最多) → 次スライド
 - マルウェア感染
 - 信頼できないダウンロードサイト、メールリンクによる誘導
 - ID・パスワード盗用
 - 脆弱なパスワードの使用、フィッシングメール
- 自宅等、学外にてご利用のPCについても
 - OS、ソフトウェアの定期的なアップデート
 - ウイルス対策ソフトウェアの導入を行うことを強く勧めます。

※ウイルス対策ソフトウェアについては、一部のソフトウェア会社が家庭内・非商用での利用目的に限定した無料版を提供しています

情報セキュリティ対策のお願い(2)

著作権保護、P2Pファイル交換ソフトウェアについて

- 特別な理由がない限り、学内ネットワーク(KUINS)において P2Pファイル交換ソフトの利用は禁止されています。自宅でP2Pソフトウェアを起動したPCを、学内ネットワークに接続することで、規程違反に問われるケースが報告されています。
- 電子ジャーナルをはじめとする資料は個人利用の範疇で利用し、複製や再配布は行わないでください。
- 著作権を侵害していると思われるコンテンツ(いわゆる「海賊版」)を利用しないでください。学外でのPC利用においても、京都大学の構成員、並びに社会人として節度ある行動を願います。

情報セキュリティ対策のお願い(3)

e-Learning の受講

「京都大学情報セキュリティ e-Learning」を受講してください

- 大学が提供する
 - 教育用計算機システム
 - 電子ジャーナル、データベース
 - 電子メール
 - 受講方法
- 等を利用する上で、最低限知っておくべき内容です

<http://www.iimc.kyoto-u.ac.jp/ja/services/ismo/e-Learning/>

にアクセスしてください。

(情報環境機構のページからもたどれます)

ECS-ID により受講者の確認をします



左の2次元バーコード
を読み取ることも
アクセスできます。

**本日の受講を
推奨します。**

※未受講者の方は**大学ネットワーク接続に制限**がかけられる
場合があります。また**個別にご連絡**することがあります。

<http://www.iimc.kyoto-u.ac.jp/ja/services/ismo/e-Learning/>