

情報セキュリティミニガイド

2015年4月発行
第1版



改ざんされたWebサイトを閲覧した場合等、利用中のPCにウイルス感染の恐れがある時は、ウイルスキヤッチも実施して下さい。

報告事項

- ・インシデントが発生した機器のIPアドレス
- ・インシデントの内容 (URL, キヤッチ画面像等)
- ・発見日時 (日本時間)
- ・報告者の氏名, 連絡先

全学セキュリティ窓口

所属部局の窓口

全学セキュリティインシデントが発生した可能性のある場合は、速やかに下記窓口のどちらかへ連絡をお願いします。

緊急対応フロー

セキュリティ関連連絡先

◆所属部局の窓口 (各自記入して下さい)

部署
TEL
MAIL

◆全学セキュリティ窓口

企画・情報部情報基盤課セキュリティ対策掛

i-s-office@iimc.kyoto-u.ac.jp

http://www.iimc.kyoto-u.ac.jp/ja/services/ismo/

TEL:075-753-7490

上記メールアドレスと
情報セキュリティのWebページにアクセスできます



http://www.iimc.kyoto-u.ac.jp

京都大学では情報セキュリティeラーニングの受講が全構成員に義務付けられています。毎年コンテツツを見直していますので、毎年度受講してください。

情報セキュリティe-Learning

来ていますか？

スマホも同様に対策が必要です

◆アカウント、パスワードを適切に管理する

パスワードは**使い回さず、8文字以上で推測されないもの**の設定が必須

◆OSやソフトウェアは常に最新にする

◆ウイルス対策ソフトを導入し最新状態で確実に動作させる

◆URLのクリック、メールの添付ファイルの開封は慎重に行う

◆情報資産を定められた目的以外に使用しない

※ KUNINS-IIにおいて、部署長名で届出た場合は
例外的に利用できます。

使用できないソフトの例
BitTorrent(ビットレント),
Xunlei(迅雷), Winny(ウィニー),
Share(シェアー), Edonkey(エドナキー), WinMX(ウィンエムエックス)などP2P型ファイル自動公開送信機能をもつもの

P2Pファイル交換ソフトはインターネットを通じてファイルを不特定多数で共有するソフトウェアです。著作権侵害やウイルス感染の恐れが高い等の問題があり、学内ネットワークの使用は禁止※です。

P2Pファイル交換ソフトは
使用禁止

対策をおろそかにすると…

* 機密情報や個人情報が流出してしまう

* Webサイトが改ざんされてしまう

* 京都大学や部局の信用が失墜する

* 不正送金で金銭的被害にあう

* 知らない間に攻撃に加担し加害者になってしまう

このような被害を出さないためには、皆さん**一人ひとりの意識と日々の行動が重要**です。

詳細は、情報環境機構のサイト
http://www.iimc.kyoto-u.ac.jp
の「情報セキュリティ」ページをご覧ください。本小冊子「セキュリティ関連連絡先」の二次元/バーコードも利用できます。

本学の活動に必要な不可欠な情報資産の円滑な運用と保護に取り組みため「京都大学における情報セキュリティの基本方針」をはじめとする様々な規程等を策定しています。概要はこの冊子で案内の情報セキュリティe-Learning受講を通して習得できます。

本学のセキュリティポリシー