

セキュリティポリシー自己点検票 教員用

- 1 あなたの所属を選択してください。
- 2 インシデント発生時の対応について伺います。
ウイルス感染・Web ページ改ざん・その他サーバへの不正侵入などのインシデントを発見した場合には、ネットワーク接続を速やかに遮断し被害の拡大防止に努める、また対応後はインシデント報告書を情報メディア基盤センターに提出しなければならないことを知っている。
- 3 有料のソフトウェアなどを不正にアップロードまたはダウンロードすると著作権の侵害となり訴訟の対象になります。本学ではファイル交換ソフトウェア (WinMX, Winny, Share, Napster, Wrapster, Gunutella, BitTorrent, Cabos など) の使用を禁止しています。
使用禁止を知っている。
- 4 他の利用者のアカウントを使用してはいけません。他人のアカウントを利用したことはない。
- 5 英語の小文字だけでなく、大文字・数字等を使ったパスワードを設定している。
- 6 電子メール及びウェブ閲覧について伺います。電子メールを私的目的 (研究・業務に必要なのないメールマガジンへの登録等) で利用してはならないことを知っている。
- 7 ウェブサイト閲覧は、研究・業務上必要な範囲で閲覧するものであり、不審なサイト等の閲覧をしてはいけないことを知っている。
- 8 電子メールの利用及びウェブサイトの閲覧について、適正な利用のため、その利用状況についてモニタリング及び監査されることがあることを知っている。
- 9 モバイル PC を含めて端末機器 (ネットワークに接続できるコンピュータ) について伺います。
Windows, Linux や Mac 等の OS にウイルス対策ソフトウェアなどを入れてセキュリティ対策をしている。
- 10 端末の OS およびソフトウェアのアップデートを適宜行っている。
- 11 Windows などの OS や商用ソフトウェアのライセンス数を把握している。
- 12 退席時に他人が使用できないようにパスワード等でロックしている。
- 13 端末でゲームや情報漏えいにつながるソフトウェアを利用していない。
- 14 配付元が確認できないソフトウェアをインストールしていない。
- 15 個人情報扱っている端末について盗難防止措置やデータの暗号化を行っている。
- 16 USB メモリなどのネットワーク以外のメディアを介したウイルス感染に対して、使用前にウイルスチェックをするなどの対策をしている。
- 17 ネットワークのアクセス制限について伺います。
学内のネットワークは外部から発信された通信をファイアウォールにてデフォルトでブロックしていますが、申請をすれば解除できることを知っている。
- 18 接続を学内ネットワークに限定しているサーバであっても、VPN サービスを利用すれば、学外からアクセス可能なことを知っている。
- 19 ○ 以下は研究室のサーバを管理している方に伺います。該当しない方は以上で設問終了です。
研究室のサーバ管理について伺います。ホスティングサーバ (共通サーバ) を利用している。
- 20 ○ 問題 20 にて「はい」の方は以上で設問終了です。「いいえ」の方は続けてください。
サーバ運用において、本来必要のないサービスが管理者が把握しないまま起動され、不正侵入の原因になることがあります。定期的にサーバの運用状況を確認し、利用許可のあるサービス以外は機能を無効にしている。
- 21 定期的にバックアップをとっている。
- 22 利用者の履歴などを定期的に検査している。
- 23 卒業生 (退職者) のアカウント管理をしている。
- 24 卒業生 (退職者) が外部から研究室のコンピュータを操作しているか把握している。
- 25 ご意見、ご要望などございましたら、ご記入ください。