H24 年度 情報セキュリティ自己点検アンケート

様

情報メディア基盤センター

日頃は，情報セキュリティ推進活動にご協力頂き誠にありがとうございます．このアンケー トは，情報セキュリティに関する重要事項を本学教職員に再確認してもらうことを目的としており，本学情報セキュリティポリシーの規定により毎年の実施が義務付けられています．

設問は全部で 12 個（サーバ管理者の場合は 17 個）あります．回答欄の下には質問の関連情報 を載せていますので，ご確認の上ご自分の端末環境について今一度再確認をお願い致します．

☆ 利用環境について

設問１：主に利用している OS についてお答え下さい（複数回答可）

- Windows : ☐ 8 ☐ 7 ☐ Vista ☐ XP ☐ 2012 Server ☐ 2008 Server ☐ 2003 Server ☐ その他
- MacOSX : ☐ 10.8 (Mountain Lion) ☐ 10.7 (Lion) ☐ 10.6 (Snow Leopard) ☐ 10.5 (Leopard) ☐ その他
- Linux : ☐ Ubuntu ☐ Redhat (CentOS) ☐ Debian ☐ その他

☆ ネットワーク利用について

設問２：研究教育・業務以外の目的で大学のネットワーク回線を利用していない

○ はい ○ いいえ

株取引・メルマガ登録・Web サイト運営など私用目的での利用は禁止されています．
設問 3：ファイル交換ソフト(P2P ソフト)を利用してデータのダウンロード・アップロードをしていない

○ はい ○ いいえ

ファイル交換ソフトには，Winny，Share，BitTorrent などがあります．2013 年 1 月 に施行された改正著作権法により，違法にアップロードされたデータをダウンロードす る行為に刑事罰が課せられることなりました．なお，本学ではデータの性質を問わ ず，ファイル交換ソフトの使用自体を禁止しています．学生にも周知徹底のほどよろしく お願い致します．

☆ アカウント・パスワード管理について

設問４：他者（同僚・学生など）とのアカウントの貸し借りをしていない

○ はい　○ いいえ

アカウントの貸し借りは厳禁です．一時的な貸し借りも同様です．
設問５：パスワード管理について，以下の項目をすべて守っている

- ユーザ ID と同じでない
- 生年月日，電話番号など個人情報から類推できるものでない
- 固有名詞や辞書に載っていそうな単純な単語を使っていない
- 大文字・小文字，数字・記号を混ぜたものにしている

○ はい　○ いいえ

パスワードはできるだけ短い期間で変更し，同じものを使い回すことはやめましょう．ま た，パスワードのメモ書き，自動入力設定などは行わないようにしましょう．パスワード 入力は見ない・見られないようにしましょう．
設問６：離席や退席で利用していた端末から離れる際は，スクリーンロックやログオフ 処理を行い他人に利用されないようにしている（自動設定を含む）

○ はい　○ いいえ

スクリーンロック機能がある場合は，自動設定にしておきましょう

☆ ウイルス・脆弱性対策について

設問７：利用するコンピュータにはすべてウイルス対策ソフトがインストールされている

○ はい　○ いいえ

情報メディア基盤センターでは，シマンテック社の ウイルス対策ソフト （Symantec Endpoint Security）を無償で配布していますので，必ずインストールしてください
設問８：利用している OS，ソフトウェアには常に最新のセキュリティ対策を施している

○ はい　○ いいえ

最近のOSのほとんどは自動アップデート機能を備えていますので，必ず設定をONにしてく ださい．また，ソフトウェアの重大な脆弱性が発見された場合は情報メディア基盤センター からもアナウンスしてますので迅速に対処してください．

☆ ライセンス管理について

設問９：ソフトウェアを違法にコピーしたり，違法コピーされたものを使用したりしていない

○ はい　○ いいえ

ソフトウェアに限らず，違法コピーは著作権法違反で罰せられる行為ですので絶対にやめ てください

☆ 情報漏えいについて

設問１０：成績情報，個人情報などの機密データにはパスワードロックや暗号化などの漏 えい対策を施している

○ はい ○ いいえ

機密情報は，管理専用端末の設置，アクセス権限の徹底，持ち出さない，万一盗難にあっ ても解読されないなどの対策を行うことが重要です．管理端末に一緒にインストールする ソフトウェアの脆弱性対策にも十分気をつけてください． ファイル交換ソフトのインストールなどは言うまでもなく厳禁です．

☆ インシデント対応について

設問１１：ウイルス感染，クラッキングなどの被害にあった場合の対応について知ってい る

○ はい ○ いいえ

ウイルス感染，クラッキングなどによって違法行為の踏み台にされていることが疑われる， または判明した場合には，感染ホストをネットワークから直ちに切り離し，感染ホストの 調査（必要であれば情報メディア基盤センターに協力を依頼）と警察などの外部機関への ログデータ提出に備え，ハードディスクなどを保管しておく必要があります． また， インシデント報告 を速やかに情報メディア基盤センターまで提出して頂く必要があります．

☆ サーバ管理について

設問１２：Web サーバ， ファイルサーバ，計算サーバなどを管理している．

○ はい ○ いいえ

設問１２で「いいえ」を選択された方は，以上になります． 右の送信ボタンを押してアンケートを終了してください

設問１２で「はい」を選択された方は，続けて以降の設問にお答え下さい

設問１３：サーバにアクセスできるアカウントを定期的（特に教職員の異動，学生の卒業 時期）に整理している

○ はい ○ いいえ

利用者の異動・卒業に伴い放置されたアカウントはクラッキングされやすいため，アカ ウントの確認・整理は定期的に行うようにしてください．

設問１４：サーバの運用に必要のないサービス（デーモン等）は起動させていない

○ はい ○ いいえ

必要のないサービスは管理・監視の目が届きにくくなるため起動させないようにしましょ う．逆に不正アクセスにより見知らぬサービスが立ち上げられていることもありますので，稼動しているサービスは定期的にチェックするよう心がけましょう．

設問１５：ルータまたはサーバ自身のファイアウォール機能により，サーバにアクセスで きるネットワーク， ポート等を適切に限定している

○ はい ○ いいえ

SSH サーバ，Web サーバを標的とした不正アクセスの試みは日常的に行われていますので，サーバにアクセス可能なネットワークの範囲を限定しておくことが効果的です．情報メディア基盤センターでは VPN サービスを提供していますので，学外からサーバに安全にアクセスしたい場合 などにご活用ください．

設問１６：サーバで管理しているコンテンツを定期的にチェックしている

○ はい ○ いいえ

機密データの紛失・盗難の可能性のほか，最近では特に 不正アクセスにより Web サーバのコンテンツが改ざんされる被害が多発しています．中に は，詐欺サイトを作成されるなど犯罪の手助けをしてしまうこともありますので定期的な チェックを心がけましょう．

設問１７：サーバのログ情報を定期的にチェックしている

○ はい ○ いいえ

ログ情報の中でも，ログイン履歴（特に遠隔ログイン）は不正アクセスの痕跡を見つける 手がかりとなりますので，定期的にチェックするようにしましょう．

設問は以上になります．記入が完了したら右の送信ボタンを押してください