情報セキュリティポリシー自己点検・自己評価結果について

情報メディア基盤センター　ネットワーク部
部長　小林　良太郎
助教　岡部　正幸
助手　久松　住子
技術専門職員　小西　和孝

【はじめに】

「情報セキュリティポリシー自己点検」は，全教職員を対象にセキュリティ対策の実施状況を調査し，ネットワーク利用時に注意すべきことを確認するために，毎年実施している．この自己点検と集計結果に対する自己評価は，本学の情報セキュリティポリシーにおいて全ネットワーク利用者に義務付けられており，平成 19 年度から今回で 8 回目の実施となる．以下，平成 26 年度の評価結果について報告する．

【方法】

情報セキュリティポリシー自己点検票はネットワーク部会で検討したものを用いた．点検票の各設問は大きく分けて次の 7 つの点に関する質問で構成され，「はい」と答えることで回答者が点検項目を理解・尊守していることが確認できるように設定されている．

1. ネットワークの利用目的および本学におけるファイル交換ソフト使用禁止の確認
2. アカウント・パスワード管理における注意点の確認
3. ウイルス対策および OS・ソフトウェアアップデートの確認
4. ライセンス管理に関して，ソフトウェアの違法コピーに関する注意
5. 情報漏えいに関する注意
6. インシデント発生時の対応手順の確認
7. サーバ管理における注意事項の確認

昨年度同様，自己点検票の設問の下段に，設問に関連した注意事項を簡単な文章にして載せており，回答者が回答しながら，同時に注意事項を確認することができるようにした．設問を章末付録に示す．

前回に引き続き，Windows XP/Office 2003/Internet Explorer 6 はいずれも 2014 年 4 月 9 日に Microsoft 社のサポート期間が終了し，セキュリティパッチの提供が無くなったことを設問中の説明文に付して注意喚起を行った．

なお，今回はサーバ管理の設問に，SSH サーバの運用について質問を 2 問追加した．

実施期間 2015 年 2 月 20 日から 3 月 20 日に得られた回答について，システムにより自動作成されたエクセルデータを用いて集計した．集計結果は各センターおよび事務局のネットワーク部員に送付し，それぞれの所属についての自己評価を依頼した．

【集計結果】

・回収率について

教職員 344 人（常勤）および事務補佐員 147 人，研究員 49 人合計 540 人のうち，369 人から回答を得ることができた（回収率 68%）．これは昨年度の回収率 57%より 11%増となっており，情報セキュリティポリシーに対する意識の向上が見られた．自己点検票の回収人数と回収率を表 1 に示す．

表 1．平成 26 年度自己点検票回収率とその内訳

	機械工学系	電気･電子情報工学系	情報･知能工学系	環境･生命工学系	建築･都市システム学系	総合教育院	センター等	事務局	合計
教職員数	53	51	51	42	34	12	94	203	540
回収人数	29	48	34	26	17	6	58	151	369
回収率	55%	94%	67%	62%	50%	50%	62%	74%	68%

・主に利用している OS

図 1 に設問 1 の「主に利用している OS」の種類とその割合を示した．Mac と Linux 利用が増加し， Microsoft Windows 系は昨年度(95%)より減って 80%になっている．

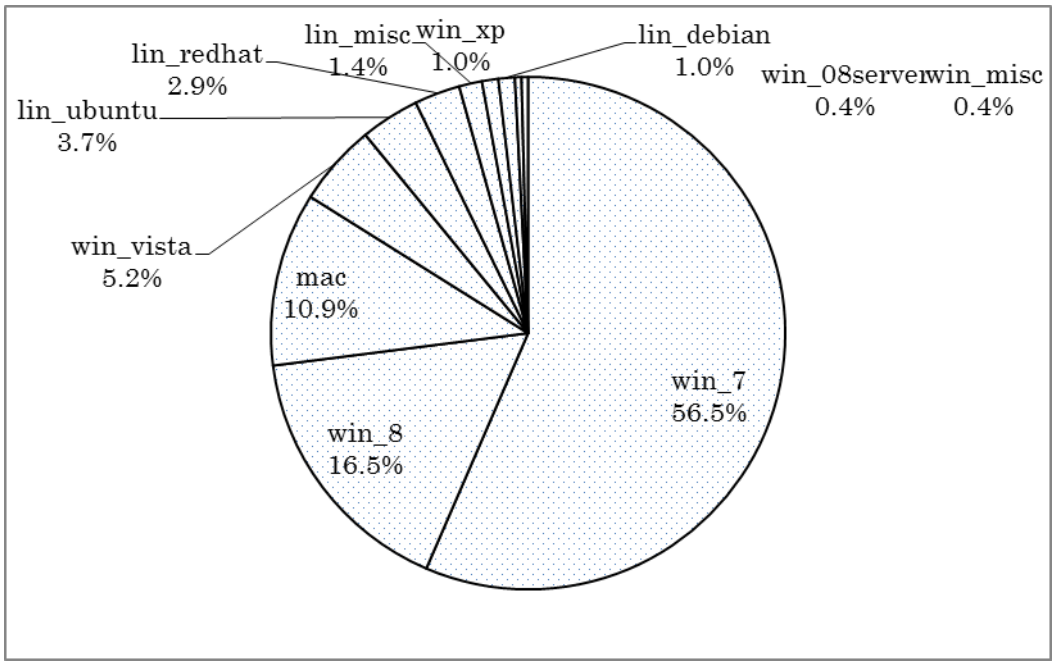

図 1. 主に使用している OS の割合

なお，これまでに実施した自己点検集計結果および自己評価は，情報メディア基盤センターの「ネットワーク利用」のページ（http://imc.tut.ac.jp/network/）に掲載している．

【評価】

・「はい」の回答率について

回答者数と「はい」の回答率について全体評価とその内訳を表 2 に示す．一般利用に関する設問（Q2～Q11）については，概ね満足できる回答が多く，特に，OS アップデート，ウイルス対策，パスワード管理などの基本セキュリティ対策が十分に行われている．更に機密データの漏えい対策に対する意識が向上していることが挙げられる．また，違法ソフトウェアの禁止など，個人のセキュリティに対する意識が高く維持されていることが確認できた．サーバ管理者向けの設問（Q13～Q25）では，サーバのコンテンツとログ管理に対する意識の向上が確認できた．近年問題となっている DNS サーバのオープンリゾルバ問題については，まだ知らない人も多いことが確認できたため，今回のアンケートを機に問題意識の向上を図っていきたい．

表 2　平成 26 年度全体集計結果と内訳

教　職　員	合計	
設　問　概　要	回答数	回答率
Q2: 研究教育・業務の目的でネットワーク利用をしている	365	99%
Q3: ファイル交換ソフトウェアのダウンロードおよび利用禁止	365	99%
Q4: 他人アカウントの不正利用の禁止	368	100%
Q5: 適正なパスワードの設定	367	99%
Q6: 退席時の端末パスワード・ロック	326	88%
Q7: ウィルス対策ソフトのインストール	368	100%
Q8: OS やその他ソフトのアップデート	369	100%
Q9: ソフトウェアの違法行為をしない	369	100%
Q10: 個人情報端末の盗難防止やデータ暗号化	348	94%
Q11: インシデント対応の認知	313	85%
Q12: サーバを管理している	58	16%
※Q13: 卒業生（退職者）のアカウント管理	55	95%
Q14: 必要ないサービスデーモンを起動しない	57	98%
Q15: ファイアウォール管理	55	95%
Q16: コンテンツの定期的チェック	54	93%
Q17: サーバのログ情報の定期的チェック	47	81%
Q18: 機関外の研究者がログインするサーバを管理している	45	78%
Q19: 不正アクセスへの対策を行っている	47	81%
Q20: DNS サーバを運用している	22	38%
Q21: オープンリゾルバは何か知っている	24	41%
Q22: オープンリゾルバを使った DNS amp 攻撃について知っている	23	40%
Q23: オープンリゾルバ対策をしている	23	40%
Q24: SSH サーバを運用している	26	45%
Q25:SSH 総当たり攻撃への対策を行っている	26	45%

※Q13 以降サーバー管理者 58 名への設問.（分母 58）

はいの回答率	機械工学系		電気･電子情報工学系		情報･知能工学系		環境･生命工学系		建築･都市システム学系		総合教育院		センター等		事務局	
	回答数	回答率	回答数	回答率	回答数	回答率	回答数	回答率	回答数	回答率	回答数	回答率	回答数	回答率	回答数	回答率
Q2	28	97%	47	98%	34	100%	26	100%	17	100%	5	83%	57	61%	151	100%
Q3	29	100%	47	98%	34	100%	26	100%	17	100%	5	83%	57	61%	150	99%
Q4	28	97%	48	100%	34	100%	26	100%	17	100%	6	100%	58	62%	151	100%
Q5	29	100%	47	98%	33	97%	26	100%	17	100%	6	100%	58	62%	151	100%
Q6	26	90%	45	94%	30	88%	25	96%	15	88%	5	83%	56	60%	124	82%
Q7	29	100%	48	100%	34	100%	26	100%	17	100%	6	100%	58	62%	150	99%
Q8	29	100%	48	100%	34	100%	26	100%	17	100%	6	100%	58	62%	151	100%
Q9	29	100%	48	100%	34	100%	26	100%	17	100%	6	100%	58	62%	151	100%
Q10	27	93%	45	94%	31	91%	25	96%	15	88%	6	100%	56	60%	143	95%
Q11	27	93%	40	83%	30	88%	25	96%	15	88%	6	100%	56	60%	114	75%
Q12	5	17%	8	17%	15	44%	4	15%	4	24%	1	17%	9	10%	12	8%
Q13	5	100%	8	100%	14	93%	4	100%	3	75%	1	100%	9	100%	11	92%
Q14	5	100%	8	100%	15	100%	4	100%	4	100%	1	100%	9	100%	11	92%
Q15	5	100%	8	100%	15	100%	4	100%	4	100%	1	100%	9	100%	9	75%
Q16	5	100%	8	100%	15	100%	2	50%	3	75%	1	100%	9	100%	11	92%
Q17	5	100%	6	75%	14	93%	2	50%	3	75%	1	100%	8	89%	8	67%
Q18	5	100%	7	88%	12	80%	2	50%	3	75%	1	100%	7	78%	8	67%
Q19	5	100%	6	75%	10	67%	4	100%	3	75%	1	100%	9	100%	9	75%
Q20	1	20%	2	25%	6	40%	2	50%	0	0%	0	0%	5	56%	6	50%
Q21	2	40%	2	25%	6	40%	2	50%	0	0%	0	0%	6	67%	6	50%
Q22	2	40%	1	13%	6	40%	2	50%	0	0%	0	0%	6	67%	6	50%
Q23	2	40%	2	25%	5	33%	2	50%	0	0%	0	0%	6	67%	6	50%
Q24	2	40%	5	63%	10	67%	2	50%	1	25%	0	0%	4	44%	2	17%
Q25	2	40%	5	63%	9	60%	2	50%	1	25%	0	0%	4	44%	3	25%

※Q13 以降はサーバ管理者への設問.

・4 年間の比較

図 2 は同じ項目の設問ごとに「はい」と答えた率について 4 年間の結果を比較したグラフである．「はい」の回答率に大きな変化は特に見られないが，H26 年度は H25 年度を Q14 以外すべて上回った．サーバ管理者には不要なデーモンを起動させないよう注意喚起をしていきたい．

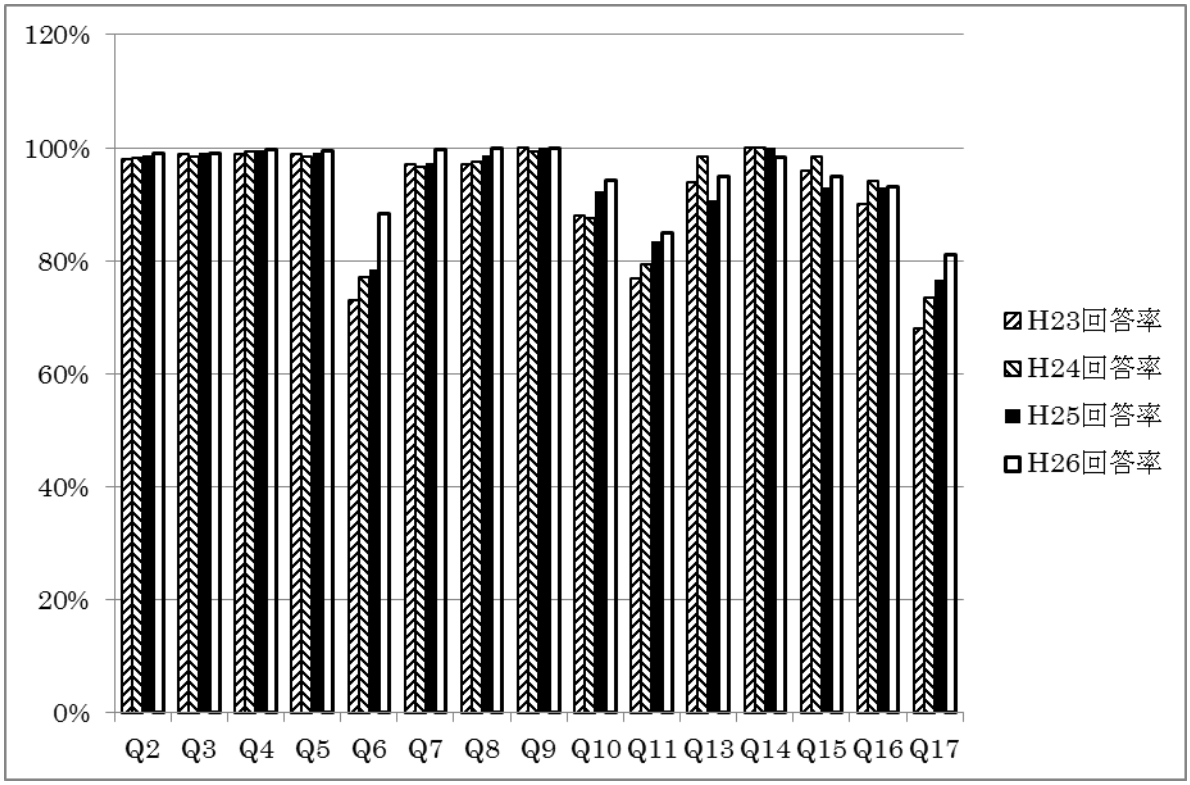

図 2.「はい」の回答率

【まとめ】

以上の点を踏まえた今後の取り組みとしては，基本的なセキュリティ管理を維持しつつ，インシデント発生を予防する更なる対策について検討，周知していく必要がある．またサーバ管理者に対して，アカウントやファイアウォール管理などのクラッキング対策を行うよう注意を促していきたい．なお，昨年同様 Web 形式のアンケート方式を実施することにより，ネットワーク部員の負担を軽減できた．回答のない対象者に今後どのように対応していくか検討する必要がある．

【付録】平成 26 年度情報セキュリティーポリシー自己点検票

H26 年度 情報セキュリティ自己点検アンケート

豊橋技術科学大学 天伯太郎 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 25 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 : ☐ 10.10 (Yosemite) ☐ 10.9 (Marvericks) ☐ 10.8 (Mountain Lion) ☐ 10.7 (Lion) ☐ その他
- Linux : ☐ Ubuntu ☐ Redhat (CentOS) ☐ Debian ☐ その他

Windows XP は，2014 年 4 月 9 日に製品サポートが終了しています．まだお使いの場合は，Windows 7, 8 などへ速やかに移行してください．

☆ 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 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，DNS 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18：本学の IP アドレス（133.15.x.x）を利用している人の中には，学外に所属している人が含まれているのを知っている

○ はい ○ いいえ

共同研究者，e-Learning 受講者などが該当します．

設問19：学内向け資料などへのアクセスを IP アドレスだけでなく，ユーザ認証によって制限している

○ はい ○ いいえ

設問18にありますように，IP アドレスによるフィルタでは不十分な可能性もありますので，ユーザ認証によるアクセス制限を行って頂きますようお願い致します．

設問20：DNS サーバを運用している

○ はい ○ いいえ

該当する場合は，次の設問21，22，23についてもお答えください．

設問21：オープンリゾルバとは何か知っている

○ はい ○ いいえ
オープンリゾルバとは，外部の不特定の IP アドレスからの再帰的な問い合わせを許可している DNS サーバのことです．
詳しくは，以下のサイトをご覧ください．
https://www.jpcert.or.jp/pr/2013/pr130002.html
設問22：オープンリゾルバを使った DNS amp 攻撃について知っている
○ はい ○ いいえ
DNS amp とは，多数のコンピュータから一斉に大量のデータを送りつけて対象を麻痺させる DDoS 攻撃の一種です．
詳しくは，以下のサイトをご覧ください．
https://www.jpcert.or.jp/at/2013/at130022.html
設問23：管理している DNS サーバはオープンリゾルバ対策がなされている
○ はい ○ いいえ
問い合わせを受け付ける IP アドレスを学内に制限するなどの対策を行ってください．
詳しくは，以下のサイトをご覧ください．
http://jprs.jp/tech/notice/2006-03-29-dns-cache-server.html
設問24：SSH サーバを運用している
○ はい ○ いいえ
該当する場合は，次の設問25についてもお答えください．
設問25：SSH 総当たり攻撃への対策を行っている
○ はい ○ いいえ
SSH 総当たり攻撃への対策について詳しくは，以下のセンターホームページをご覧ください．
https://imc.tut.ac.jp/wiki/Network/FAQ
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