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

【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 7 回目の実施となる．以下，平成 25 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る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，機関外の研究者が利用している場合の対策とオープンリゾルバについての質問を 5 問追加した．

実施期間 2014 年 2 月 21 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 390 人（常勤）のうち，223 人（回収率 57%）から回答を得ることができた．情報セキュリティポリシー自己点検票の回収人数と回収率を表 1 に示す．

表1. 平成25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	41	41	38	35	24	10	60	141	390人
回数人数	17	14	21	14	11	5	34	107	223人
回収率	41%	35%	75%	40%	46%	50%	57%	76%	57%

・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．95%が MicroSoft

Windows 系で占められている．

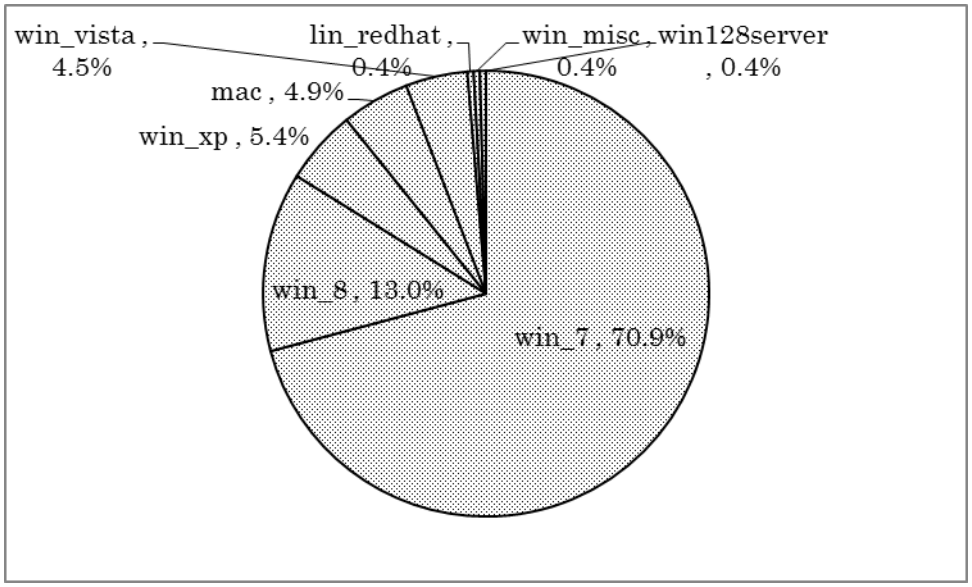

図 1．主に使用している OS の割合

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．

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．また，サーバ管理者向けの設問（Q13～Q23）では，サーバのコンテンツとログのチェックを定期的に行っていることが評価できる．

表2　平成25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	220	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	221	99%
Q4: 他人アカウントの不正利用の禁止	222	100%
Q5: 適正なパスワードの設定	221	99%
Q6: 退席時の端末パスワード・ロック	175	78%
Q7: ウィルス対策ソフトのインストール	217	97%
Q8: OS やその他ソフトのアップデート	220	99%
Q9: ソフトウェアの違法行為をしない	223	100%
Q10: 個人情報端末の盗難防止やデータ暗号化	206	92%
Q11: インシデント対応の認知	186	83%
※Q13: 卒業生（退職者）のアカウント管理	39	91%
Q14: 必要ないサービスデーモンを起動しない	43	100%
Q15: ファイアウォール管理	40	93%
Q16: コンテンツの定期的チェック	40	93%
Q17: サーバのログ情報の定期的チェック	33	77%
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	5	12%
Q19: 不正アクセスへの対策を行っている	13	30%
Q20: DNSサーバを運用している	13	30%
Q21: オープンリゾルバは何か知っている	13	30%
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	9	21%
Q23: オープンリゾルバ対策をしている	5	12%

※Q13以降はサーバ管理者(43名)への設問. (分母43)

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	16	94%	14	100%	21	100%	14	100%	11	100%	5	100%	34	100%	105	98%
Q3	16	94%	14	100%	21	100%	14	100%	11	100%	4	80%	34	100%	107	100%
Q4	16	94%	14	100%	20	95%	14	100%	11	100%	5	100%	34	100%	107	100%
Q5	17	100%	14	100%	20	95%	14	100%	11	100%	4	80%	34	100%	107	100%
Q6	15	88%	13	93%	19	90%	13	93%	11	100%	2	40%	33	97%	69	64%
Q7	17	100%	14	100%	18	86%	14	100%	11	100%	4	80%	33	97%	105	98%
Q8	17	100%	14	100%	21	100%	14	100%	11	100%	4	80%	34	100%	105	98%
Q9	17	100%	14	100%	21	100%	14	100%	11	100%	5	100%	34	100%	107	100%
Q10	13	76%	14	100%	20	95%	14	100%	8	73%	4	80%	33	97%	100	93%
Q11	16	94%	12	86%	18	86%	14	100%	10	91%	4	80%	32	94%	79	74%
Q13	8	100%	5	100%	8	100%	2	100%	2	100%	1	50%	7	100%	6	67%
Q14	8	100%	5	100%	8	100%	2	100%	2	100%	2	100%	7	100%	9	100%
Q15	8	100%	4	80%	8	100%	2	100%	2	100%	1	50%	7	100%	8	89%
Q16	8	100%	5	100%	8	100%	2	100%	2	100%	1	50%	7	100%	7	78%
Q17	5	63%	5	100%	7	88%	2	100%	2	100%	1	50%	6	86%	5	56%
Q18	1	13%	1	20%	2	25%	0	0%	0	0%	1	50%	0	0%	0	0%
Q19	2	25%	2	40%	3	38%	0	0%	0	0%	1	50%	0	0%	5	56%
Q20	1	13%	2	40%	2	25%	2	100%	0	0%	1	50%	1	14%	4	44%
Q21	2	25%	2	40%	2	25%	2	100%	0	0%	1	50%	1	14%	3	33%
Q22	1	13%	2	40%	2	25%	0	0%	0	0%	1	50%	0	0%	3	33%
Q23	0	0%	2	40%	1	13%	0	0%	0	0%	1	50%	0	0%	1	11%

※Q13以降はサーバ管理者への設問.

・3 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 3 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，先に述べたように Q10 の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は良い傾向である．ただし， Q13 と Q15 のアカウントおよびサーバファイアウォール管理について「はい」の回答率が若干下がっている．これらはクラッキング被害に直結事項であるため，注意を促していきたい.

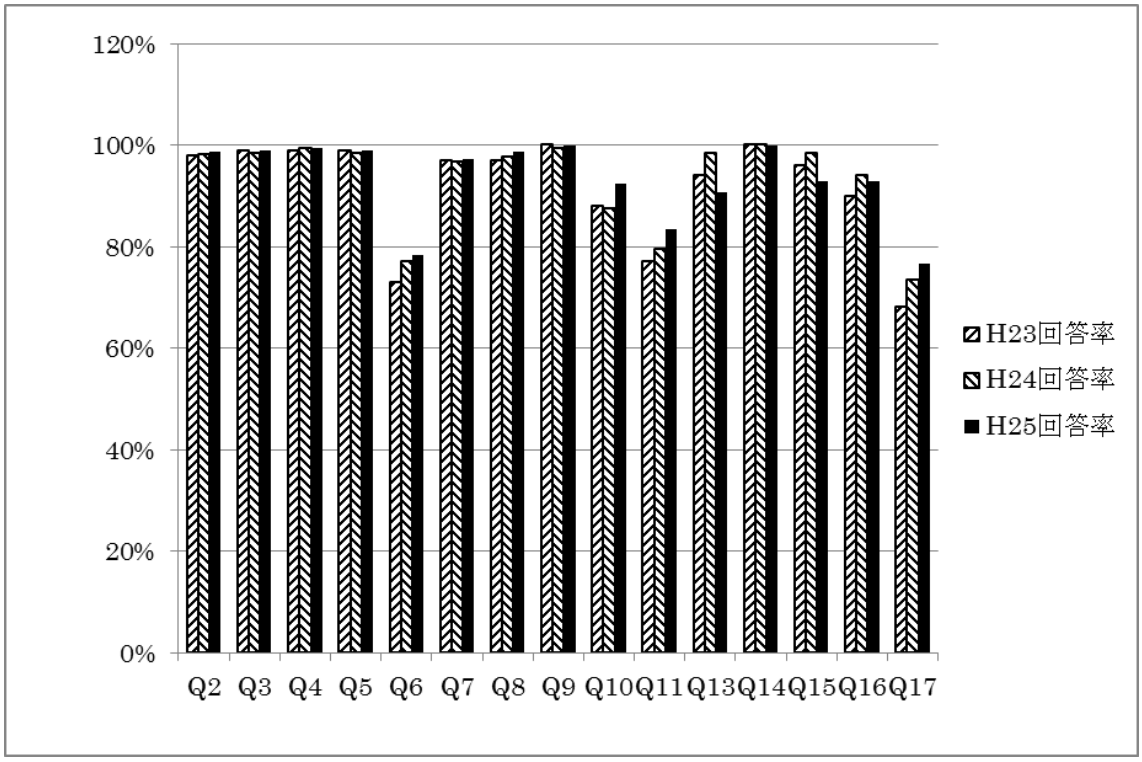

図 2.「はい」の回答率

【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 25 年度情報セキュリティーポリシー自己点検票

☆ 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：□ 10.9（Marvericks） □ 10.8（Mountain Lion） □ 10.7（Lion） □ 10.6（Snow Leopard） □ 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 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，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：計算サーバなど，機関外の研究者がログインして作業を行うサーバを管理している
○ はい ○ いいえ
該当する場合は，次の設問１９についてもお答えください.
設問１９：管理しているサーバを機関外の研究者も利用している場合，不正アクセスへの対策を行っている
○ はい ○ いいえ
接続可能な IP アドレスを限定する，VPN 経由で接続してもらうなどの対策を行ってください.
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