

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 後藤 仁志

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6回目の実施となる。以下、平成24年度の評価結果について前年度との比較を含めて報告する。

【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・遵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。設問を章末表3に示す。

実施期間は2013年3月4日から3月15日までとし、最終的に3月31日まで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

常勤206人および非常勤（客員教員，研究員，系所属事務補佐を含む）205人，合計411人の対象者のうち，205人（回収率50%）から回答を得ることができた。また，事務局については，常勤職員133人と事務補佐員等非常勤職員69人の合計202人の対象者のうち，130人（回収率64%）から回答を得ることができた。全体では613人のうち，335人から回答を得て回収率は55%となった。

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 24 年度自己点検票回収率とその内訳

教職員	合計
教職員数	613 人
回収人数	335 人
回収率	55%

系	1系	2系	3系	4系	5系	総合教育院	各センタ	事務局
教職員数	61	55	53	52	45	18	127	202
回数人数	31	24	44	28	21	8	49	130
回収率	51%	44%	83%	54%	47%	44%	39%	64%

・ 昨年度との比較

図 1 は今回の結果を前回平成 23 年度の自己点検票回収率と比較したグラフである。

回収期間が短かったこと、および事務局では平成 25 年 3 月に事務補佐員の異動が多かったため、回収率が低くなってしまった。しかし、昨年度回収率の低かった 3 系では、系会議等において、「自己評価に回答することはネットワーク利用者の責務であること」、「新入生には、情報倫理テストの修了をもってアカウントを発行するという厳しい対応をとっていること」などについて周知徹底することにより高い回収率となった。次回からは、こうしたネットワーク利用に関してさらなる意識向上に努めて回収率を高くしていく。

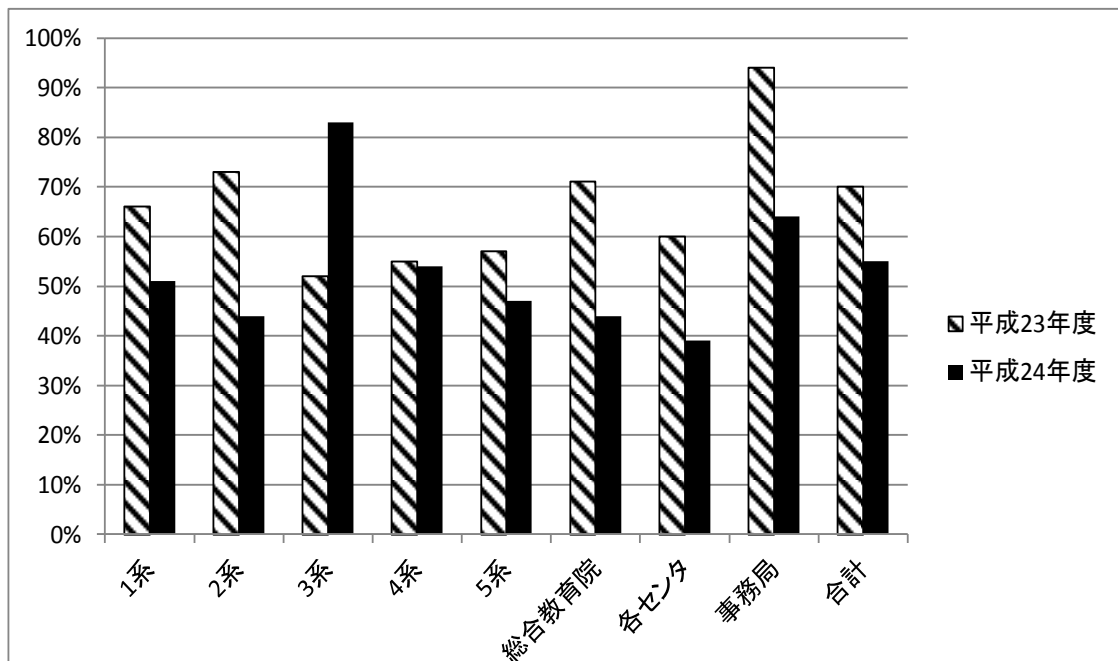


図 1. 自己点検票回収率

また、図 2 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。81%が Microsoft

Windows 系で占められている。

なお、MicroSoft によると Windows XP/Office 2003/Internet Explorer 6 はいずれも 2014 年 4 月 9 日に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り、セキュリティ上問題となる。OS, Office, ブラウザ自体をアップデートしてもらうようアナウンスしていく必要がある。

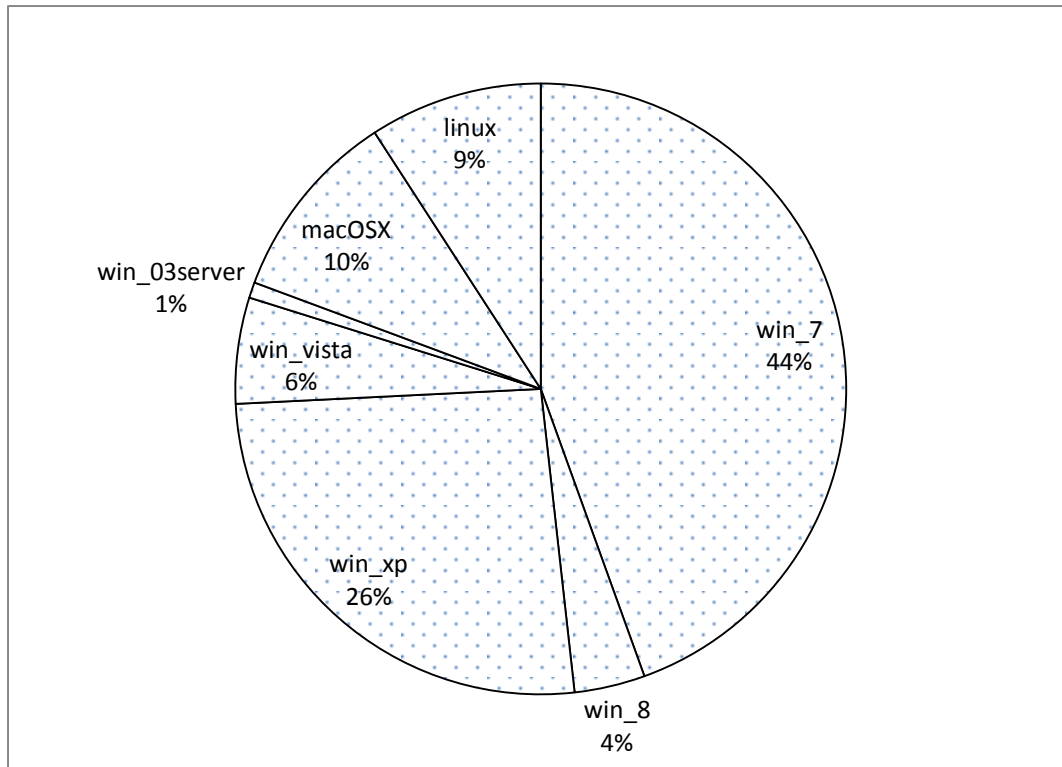


図 2. 主に使用している OS の割合

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 (Q13~17) では、定期的バックアップに対する関心が高いことは評価できる。

一方、Q17 のサーバログのチェックについては手が行き届いていない状況であることが分かった。

表2 平成24年度全体評価とその内訳

教 職 員 設 問 概 要	合 計	
	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	329	98%
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	330	99%
Q4: 他人アカウントの不正利用の禁止	333	99%
Q5: 適正なパスワードの設定	330	99%
Q6: 退席時の端末パスワード・ロック	258	77%
Q7: ウィルス対策ソフトのインストール	324	97%
Q8: OS やその他ソフトのアップデート	327	98%
Q9: ソフトウェアの違法行為をしない	333	99%
Q10: 個人情報端末の盗難防止やデータ暗号化	293	87%
Q11: インシデント対応の認知	266	79%
※Q13: 卒業生(退職者)のアカウント管理	67	99%
Q14: 必要ないサービスデーモンを起動しない	68	100%
Q15: ファイアウォール管理	67	99%
Q16: コンテンツの定期的チェック	64	94%
Q17: サーバのログ情報の定期的チェック	50	74%

設 問 概 要	系		1系		2系		3系		4系		5系		総合教育院		センター		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	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	30	97%	24	100%	43	98%	28	100%	21	100%	8	100%	49	100%	126	97%		
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	29	94%	24	100%	44	100%	28	100%	21	100%	8	100%	49	100%	127	98%		
Q4: 他人アカウントの不正利用の禁止	30	97%	24	100%	44	100%	28	100%	21	100%	8	100%	49	100%	129	99%		
Q5: 適正なパスワードの設定	30	97%	24	100%	44	100%	28	100%	20	95%	8	100%	49	100%	127	98%		
Q6: 退席時の端末パスワード・ロック	26	84%	22	92%	35	80%	23	82%	15	71%	4	50%	45	92%	88	68%		
Q7: ウィルス対策ソフトのインストール	29	94%	24	100%	42	95%	28	100%	21	100%	8	100%	47	96%	125	96%		
Q8: OS やその他ソフトのアップデート	29	94%	24	100%	42	95%	28	100%	21	100%	8	100%	49	100%	126	97%		
Q9: ソフトウェアの違法行為をしない	30	97%	24	100%	44	100%	28	100%	21	100%	8	100%	49	100%	129	99%		
Q10: 個人情報端末の盗難防止やデータ暗号化	27	87%	24	100%	38	86%	25	89%	15	71%	4	50%	48	98%	112	86%		
Q11: インシデント対応の認知	8	100%	21	88%	37	84%	24	86%	16	76%	8	100%	45	92%	88	68%		
※Q13: 卒業生(退職者)のアカウント管理	8	100%	6	100%	18	100%	5	100%	4	100%	2	67%	7	100%	17	100%		
Q14: 必要ないサービスデーモンを起動しない	8	100%	6	100%	18	100%	5	100%	4	100%	3	100%	7	100%	17	100%		
Q15: ファイアウォール管理	8	100%	6	100%	18	100%	5	100%	4	100%	2	67%	7	100%	17	100%		
Q16: コンテンツの定期的チェック	8	100%	6	100%	17	94%	4	80%	4	100%	2	67%	7	100%	16	94%		
Q17: サーバのログ情報の定期的チェック	6	75%	6	100%	13	72%	3	60%	4	100%	2	67%	4	57%	12	71%		

※Q13以降はサーバ管理者への設問.

・ 昨年度との比較

図3は同じ項目の設問ごとに「はい」と答えた率について前回と比較したグラフである。「はい」の回答率はほぼ同じか今回の方が上回っていることが分かる。特に Q6, Q13, Q16, Q17 が上がったのは良好である。

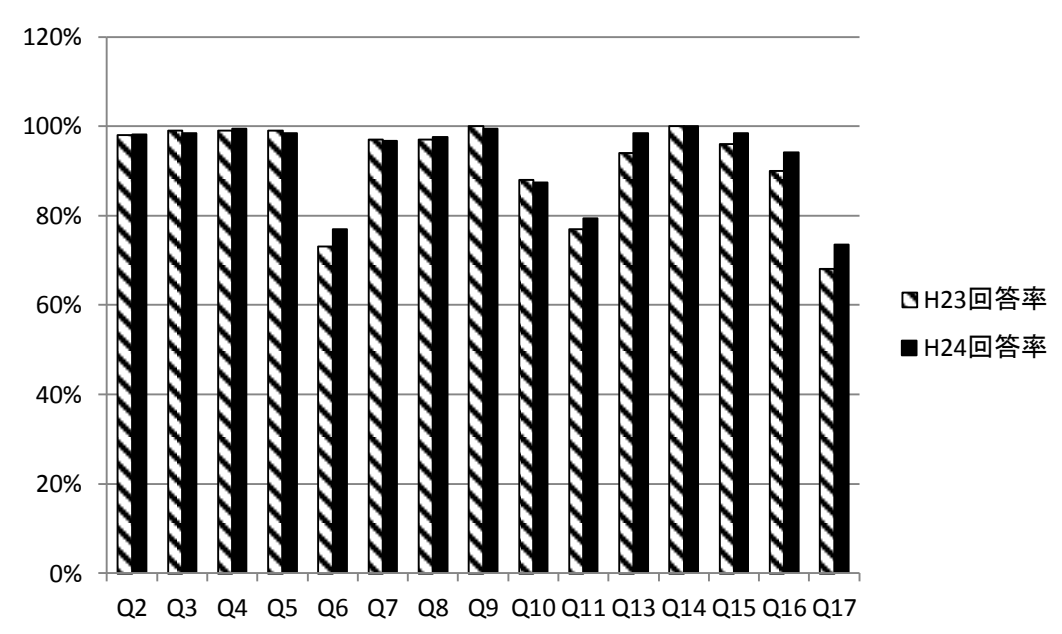


図 3. 「はい」 の回答率

【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、サーバのログチェック作業に要する手間を軽減する方法について検討する必要がある。

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。期限までに Web 回答のない分については、催促をメールにて送付する対策を行った。それでも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。

表 3. 平成 24 年度情報セキュリティポリシー自己点検票

☆	利用環境について
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) <ul style="list-style-type: none"> ・Windows : 7 Vista XP 2008 Server 2003 Server その他 ・MacOSX : 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
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 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。
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 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になりました. 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
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 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.
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 <ul style="list-style-type: none"> ・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き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ない 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 入力は見えない・見られないようにしましょう.
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) 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
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 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
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 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
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 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

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
	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．管理端末と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
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
	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
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．
	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ください
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
	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．
14	サーバの運用に必要なサービス（デーモン等）は起動させていない
	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．
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
	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．
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
	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．
17	サーバのログ情報を定期的にチェックしている
	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．