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 5 回目の実施となる．以下，平成 23 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

前年まで教員用と事務局用に設問内容の異なる点検票を作成したが，今回はそれらを統合し同じ設問とした．

また, 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．

前回自己点検に用いた Moodle システム（Web 教材開発支援システム）はログイン手続きに戸惑う回答者が多かった．そこで今回は，キーワードなしに自分のアカウント認証によるログインだけで利用できる Web 上のアンケート方式を用いることにした．このページの URL を対象者にメールで通知し，回答者に同ページにアクセスして回答してもらうこととした．

実施期間は 2012 年 1 月 23 日から 2 月 10 日までとし，最終的に 2 月 21 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

常勤教員 204 人および非常勤（客員教員，研究員，系所属事務補佐を含む）163 人の合計 367 人の対象者のうち， 215 人（回収率 59%）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 135 人と事務補佐員等非常勤職員 43 人の合計 183 人の対象者のうち，172 人（回収率 94%）から回答を得ることができた．合計では 550 人のうち，387 人から回答を得て回収率は 70%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23年度自己点検票回収率とその内訳

教　　職　　員	合計	
教職員数※	550	
回収人数と回収率	387	70%

系	1系		2系		3系		4系		5系		総合教育院		センター		事務局	
教職員数※	62		43		60		47		44		17		94		183	
回収人数と回収率	41	66%	24	73%	31	52%	26	55%	25	57%	12	71%	56	60%	172	94%

※非常勤：特任教員，研究員，事務補佐員を含む

・昨年度との比較

図 1 は今回の結果を前回平成 22 年度の自己点検票回収率と比較したグラフである．回収率はほとんど今回の方が上回っていることが分かる．

前回低かった事務局の回収率が高くなった原因のひとつとして，研究室所属の非常勤職員を除く事務補佐を対象としたことにより通知が行き渡ったことと，平成 22 年 10 月から事務シンクライアント端末の利用が始まったことにより，アカウント管理などについてセキュリティ意識の向上が見られた．

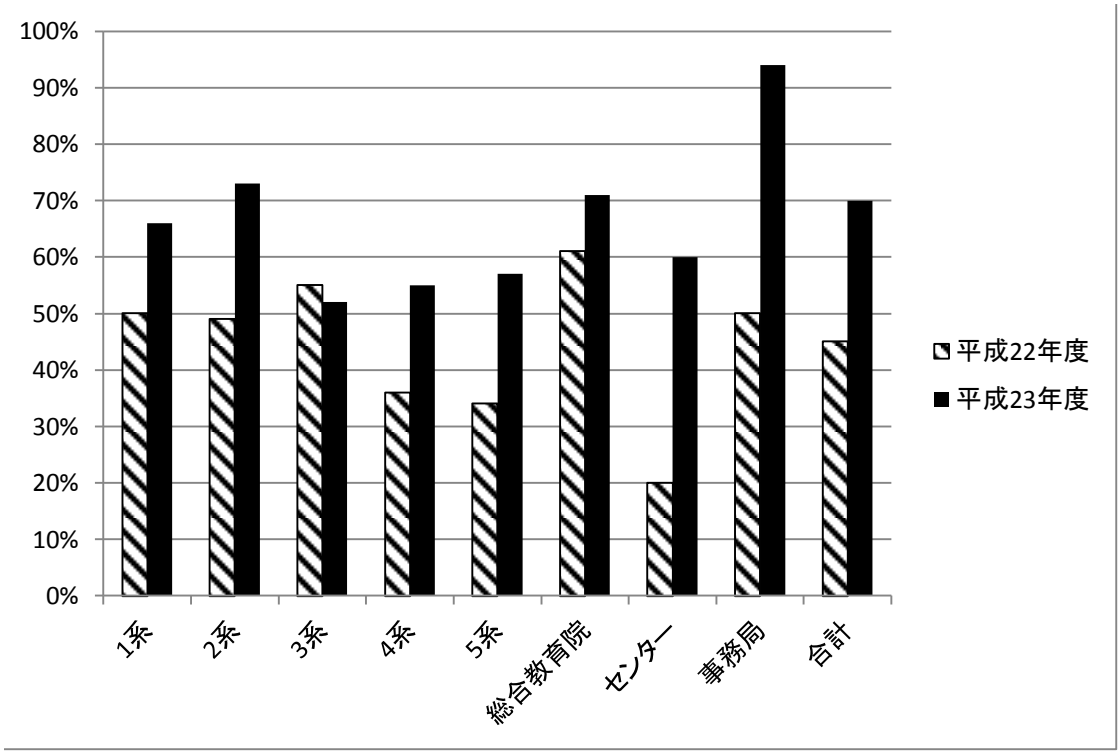

図 1.　自己点検票回収率

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. 90%以上が MicroSoft Windows 系で占められている.

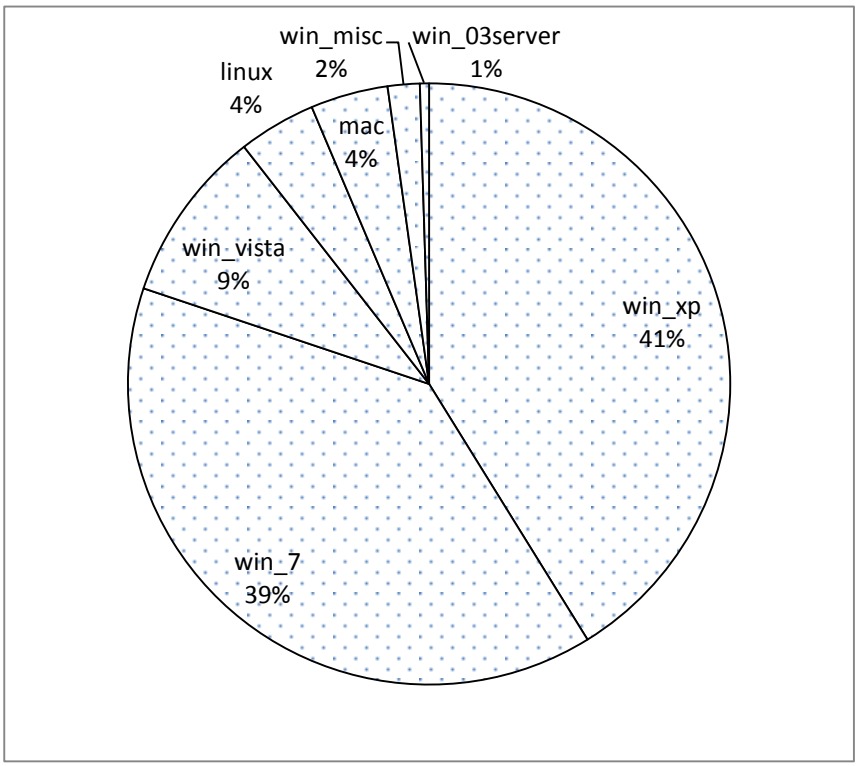

図2. 主に使用しているOSの割合

なお，平成 23 年度を含め，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（Q19～24）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23年度全体評価とその内訳

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	381	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	385	99%
Q4: 他人アカウントの不正利用の禁止	385	99%
Q5: 適正なパスワードの設定	383	99%
Q6: 退席時の端末パスワード・ロック	282	73%
Q7: ウィルス対策ソフトのインストール	374	97%
Q8: OS やその他ソフトのアップデート	375	97%
Q9: ソフトウェアの違法行為をしない	386	100%
Q10: 個人情報端末の盗難防止やデータ暗号化	340	88%
Q11: インシデント対応の認知	298	77%
※Q13: 卒業生（退職者）のアカウント管理	65	94%
Q14: 必要ないサービスデーモンを起動しない	69	100%
Q15: ファイアウォール管理	66	96%
Q16: コンテンツの定期的チェック	62	90%
Q17: サーバのログ情報の定期的チェック	47	68%

系	1系		2系		3系		4系		5系		総合教育院		センター		事務局	
設　問　概　要	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	40	98%	23	96%	31	100%	26	100%	25	100%	10	83%	56	100%	170	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	40	98%	24	100%	31	100%	26	100%	25	100%	12	100%	56	100%	171	99%
Q4: 他人アカウントの不正利用の禁止	40	98%	24	100%	31	100%	26	100%	25	100%	12	100%	56	100%	171	99%
Q5: 適正なパスワードの設定	41	100%	23	96%	31	100%	26	100%	25	100%	12	100%	54	96%	171	99%
Q6: 退席時の端末パスワード・ロック	37	90%	21	88%	23	74%	22	85%	20	80%	8	67%	47	84%	104	60%
Q7: ウィルス対策ソフトのインストール	40	98%	24	100%	28	90%	25	96%	25	100%	11	92%	53	95%	168	98%
Q8: OS やその他ソフトのアップデート	41	100%	24	100%	30	97%	25	96%	25	100%	11	92%	52	93%	167	97%
Q9: ソフトウェアの違法行為をしない	41	100%	24	100%	31	100%	26	100%	25	100%	12	100%	55	98%	172	100%
Q10: 個人情報端末の盗難防止やデータ暗号化	38	93%	20	83%	27	87%	18	69%	16	64%	9	75%	54	96%	158	92%
Q11: インシデント対応の認知	35	85%	20	83%	26	84%	23	88%	22	88%	10	83%	48	86%	114	66%
※Q13: 卒業生（退職者）のアカウント管理	10	100%	6	100%	14	100%	7	100%	3	75%	1	50%	7	100%	17	89%
Q14: 必要ないサービスデーモンを起動しない	10	100%	6	100%	14	100%	7	100%	4	100%	2	100%	7	100%	19	100%
Q15: ファイアウォール管理	10	100%	6	100%	14	100%	7	100%	3	75%	1	50%	7	100%	18	95%
Q16: コンテンツの定期的チェック	10	100%	5	83%	13	93%	6	86%	4	100%	1	50%	7	100%	16	84%
Q17: サーバのログ情報の定期的チェック	4	40%	5	83%	11	79%	5	71%	2	50%	2	100%	5	71%	13	68%

※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．Q14～Q17 はサーバ管理に関して前回より具体的で詳細な設問としたため比較できず，前回分を空白とした．「はい」の回答率のどちらもほとんど今回の方が上回っていることが分かる．

Q11 のインシデント対応手順の回答率が H22 年度より下がったのは事務職員が事務シンクライアント端末を使用することによりシステム上の事故を意識せずに利用できること，および移動の多い事務補佐員の一部に認識されていなかったことが原因になっている．

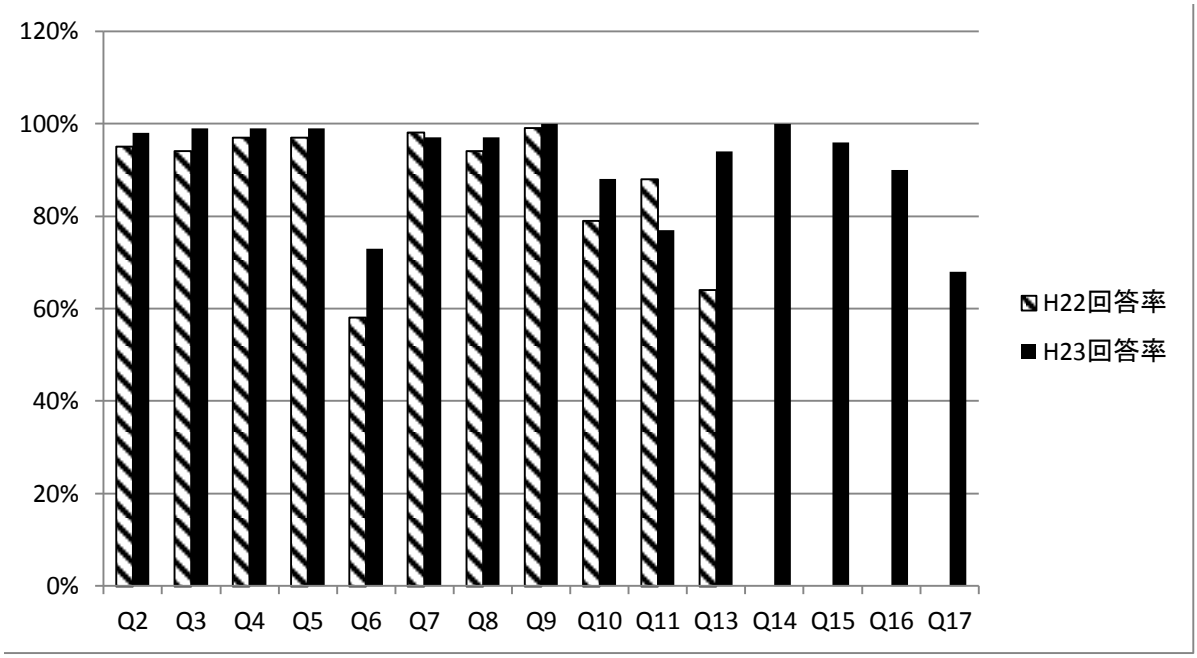

図 3.「はい」の回答率

【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．

なお，今回 Web アンケート方式を実施したことにより，昨年同様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，個別に催促状を送付するなどの対策を 2 度ほど行った．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 23 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
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 ： 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. 2010 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だけでも違法行為となりますのでご注意ください. 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 ・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
	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.
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
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
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のないサービス（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．