【報告】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
後藤 仁志，岡部 正幸，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おり，平成 19 年度から今回で 4 回目の実施となる．以下，今年度の評価結果と 4 年間の総合的な分析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 6 つの点に関する質問で構成され，「はい」と答えることで求められる回答になるように設定されている．

1. 自己，障害の報告を誰に何時するか，手続きの認知度を測ることと，有償コンテンツの不正コピーやファイル交換ソフトウェアの使用禁止を再確認する．
2. アカウント管理する上で具体的な項目をあげて注意を促す．
3. 電子メールおよびウェブ閲覧に関する注意事項を確認する．
4. 端末機器のセキュリティ対策について，ウィルス対策ソフトウェアの扱いやソフトウェアのインストールに関する注意事項を確認する．
5. 強化されたポートアクセス制限について，現状と今後の方針について確認する．
6. サーバ管理に関して，情報メディア基盤センターが提供しているホスティングサービスを認識してもらう．また，各研究室でサーバを管理している場合は，注意すべき点を指摘して確認してもらう．

なお，例年通り，自己点検票には設問以外に意見欄を設け，ネットワーク運用についての意見や質問，および各設問内容や回答方法に関する感想など記入できるようにした．また，別紙に示したように，教員用と事務局用に若干設問内容の異なる点検票を作成した．

昨年の自己点検実施後の意見を参考に，今回は，moodle システム（Web 教材開発支援システム）を用いて，上述の自己点検票を Web 上で回答できるように情報メディア基盤センターで自己点検回答ページを作成した．このページの URL と操作手順を対象者にメールで通知し，回答者自ら同ページにアクセスし，認証ログインした上で回答を入力した．実施期間は 2011 年 1 月 28 日から 2 月 10 日までとし，最終的に 2 月 21 日までの回答について，moodle システムの機能を用いて自動集計した．

集計結果を各系と事務局のネットワーク部員に送付し，自己評価をした．

【集計結果】

常勤教員 209 人および非常勤（客員教員や研究員）72 人の合計 281 人の対象者のうち，114 人（回答率 41%）からの回答を回収した．また，事務局の常勤職員 131 人と事務補佐員等非常勤職員 98 人の合計 229 人の対象者のうち，114 人（回答率 50%）から回答を得ることができた．

自己点検の集計結果と，各系と事務局のネットワーク部員による自己評価は，3 月 11 日の第 5 回ネットワーク部会にて報告し，ネットワークのセキュリティ運営に反映させる措置を行った．

情報セキュリティポリシー自己点検票の回答集計結果を別紙表 1 と 2 に示す．また，平成 22 年度を含め，これまでに実施した自己点検の結果は，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．

【今年度の全体評価】

良いと思われる点は，一般利用に関する設問（Q2～18）については，概ね満足できる回答が多く，特に，パスワード管理やファイル交換ソフトの禁止など，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関する関心が高いことは評価できる．

一方，悪いと思われる点は，Q15 にみられるように，端末の盗難防止措置やデータ暗号化に対する意識が低いように思われる．学内で盗難事件があったことを考えると，今後，少なくとも個人情報を扱う端末について盗難防止措置やデータの暗号化などの措置を検討する必要がある．

また，Q17 の本学が設置している防護壁（ファイアウォール）に関する質問や，Q23 の卒業生や退職者のアカウント管理の回答から，外部からのネットワークアクセスについてあまり注意が払われていないことがわかる．現在の所属者以外のアカウントはハッカーやクラッカーに狙われやすく，今後，管理者に強く注意喚起する必要性がある．

以上の点を踏まえた今後の取り組みとしては，研究室にある PC の盗難防止やデータ暗号化に対して，どのような措置が必要かを検討し，何らかの対応措置を実施したい．また，ネットワーク管理者に対して，アカウント管理だけでなく，定期的にログチェックを行うように意識を高める注意喚起していきたい．

今回，moodle システムによる Web 回答方式を実施した，これによって，これまでネットワーク部員の負担になっていた自己点検票の配付と回収，およびセンターでの集計作業が軽減されたが，逆に，教職員の回答率が大きく下がる結果となった．これは Moodle の使い勝手の悪さに起因すると思われるが，実際に印刷物として自己点検票が手元にないことで，回答に対する責任意識を低下させた可能性が高い．今後は，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検討していく必要がある

【4 年間の評価】

今年度の集計結果と合わせて，4 年間同じ内容の設問（Q2, 3, 5, 9-15, 18, Q20-24）に対する回答推移を，教員と事務局に分けて，総合的な分析を試みた.

・教員の回答推移

一般利用者向けの設問に対する 4 年間の「はい」の回答率の推移は次のように大別することができる（別紙図 1）.

A) 回答率が常に高いか上昇傾向にあり，高いセキュリティ意識を維持できている
B) 回答率は上昇傾向にあったが，ある程度の意識レベルで停滞している
C) 回答率に大きな増減が見られず，知る人ぞ知る状態にある
D) 回答率が下降傾向にあり，セキュリティ意識を高める施策が必要である

多くの設問，例えば，Q3（ファイル交換ソフトの禁止），Q5（適正なパスワード設定），Q9（ウィルス対策ソフト），Q10（OS 等のアップデート），Q13（ゲームや情報漏えいソフトの禁止），Q14（配布元未確認ソフトのインストール禁止）などが A)である．特に，Q2（インシデント対応と報告義務）は 4 年間高い回答率を維持している．これらは毎年実施している利用説明会において最も強調している項目でもあり，その効果が表れているといえるだろう.

B)に該当する設問には，Q11（商用ソフトのライセンス数把握）や Q15（盗難防止やデータ暗号化）などがある．これらは，以前は低い意識にあったが，この自己点検の取り組みを通して徐々に意識されるようになってきた．しかしながら，未だ十分なレベルには達しておらず，特に Q15 については，回答率 70%を未だ満たせていない．教職員の問題作成や成績管理などに関する危惧すべき状況にあると言って良い.

C)については，Q18（VPN サービスの認知）が該当し，80%の回答率である．自宅から学術雑誌の閲覧するためには VPN の利用が欠かせないが, その点で不便を感じている教員が少ないというのが現実かもしれない．今後，より認知度を高めることで，本学の研究活動を活性化することにつながる可能性がある.

D)に該当する Q12（退席時のパスワード・ロック）は，H20 年度までは 90%の回答率であったが，H21 年度に 75%まで急降下し，H22 年度でも低い回答率のままである．原因は Vista や 7 などの最近の Windows のデフォルト設定が変更になったためと考えられる．つまり，H20 年度以前もセキュリティ意識があったことによる回答ではなかったと思われる．設定方法を具体的に記載した文書を配布する必要があるかもしれない.

Q19 以降はサーバ管理者向けの設問であり，Q20 以降が 4 年間同じ内容だった．「はい」の回答率の 4 年間の推移を別紙図 2 に示した．年々回答率が上昇しているのは Q21（定期的バックアップの実施）のみであった．その他については，上記 B)に該当する Q22（利用者履歴等の定期的検査の実施），C)に該当する Q24（卒業生の外部アクセス管理）だけでなく，Q20（定期的サーバ運用状況の確認など）や Q23（卒業生のアカウント管理）など，サーバ管理上の必須の作業に対する意識が急激に低下している．今後は，共通サーバの利用者が今一つ広まらない点を改善し，研究室レベルでのサーバ管理を減らすような施策を高じる必要がある.

・事務局の回答推移

事務局向けの自己評価に関する 4 年間の回答推移について，別紙図 3 に示した.

事務職員に関する問題点の一つは，個別の設問に対する回答よりも自己点検票の回答回収率の低さにある．H19 年度の 76%を除けば，ここ 3 年間 で 50%に低下している．主な原因は非常勤職員にも自己点検を拡大したことにより，回答していない職員が増えたためである.

一方，回答した職員の各設問に対する「はい」の回答率は，概ね高く維持されているか，上昇傾向にあり，セキュリティに対する意識は十分に高いと言える．これは，職員の使う PC がシンクライアントに切り替わりつつあり，以前と異なる動作からセキュリティを意識せざるを得ないことが影響していると思われる．回答率が停滞している Q14（退席時のパスワード・ロック）についても，システムのグループポリシーを変更などの対応を今後検討する.

また，Q2（インシデント対応と報告義務）について，H22 年度の回答率が下がっている．これも自己点検を非常勤職員までに広げたことが原因であろう．今後，非常勤職員に対する情報セキュリティポリシーの徹底が課題となる.

【まとめ】

「情報セキュリティポリシー自己点検」の 4 年間の推移を検討した結果，全体として基本的な事項については広く認識されており，情報セキュリティ意識が向上しているといってよいだろう．ただし，設問によっては，設問自体の意味が分からない，あるいは勘違いしたまま回答している可能性も考えられ，特に，これまで自己点検を実施してこなかった非常勤職員の認識を高めていく必要がある.

今後は，本学のネットワークサービスについて，どんなサービスがあり，どんな利用ができるのか，また，どんな情報セキュリティ対策が必要かなどを周知し，分かりやすく且つセキュリティ意識向上効果を生む設問を検討しながら,「情報セキュリティポリシー自己点検」を実施していきたい.

以上です.

セキュリティーポリシー自己点検票　教員用

1 あなたの所属を選択してください。

2 インシデント発生時の対応について伺います.
ウイルス感染・Web ページ改ざん・その他サーバへの不正侵入などのインシデントを発見した場合には，ネットワーク接続を速やかに遮断し被害の拡大防止に努める，また対応後はインシデント報告書を情報メディア基盤センターに 提出しなければならないことを知っている.

3 有料のソフトウェアなどを不正にアップロードまたはダウンロードすると著作権の侵害となり訴訟の対象になります．本学ではファイル交換ソフトウェア(WinMX, Winny, Share, Napster, Wrapster, Gunutella, BitTorrent, Cabos など)の使用を禁止しています.
使用禁止を知っている.

4 他の利用者のアカウントを使用してはいけません．他人のアカウントを利用したことはない.

5 英語の小文字だけでなく，大文字・数字等を使ったパスワードを設定している.

6 電子メール及びウェブ閲覧について伺います． 電子メールを私的目的（研究・業務に必要のないメールマガジンへの登録等）で利用してはならないことを知っている.

7 ウェブサイト閲覧は，研究・業務上必要な範囲で閲覧するものであり，不審なサイト等の閲覧をしてはいけないことを知っている.

8 電子メールの利用及びウェブサイトの閲覧について，適正な利用のため，その利用状況についてモニタリング及び監査されることがあることを知っている.

9 モバイル PC を含めて端末機器（ネットワークに接続できるコンピュータ）について伺います.
Windows, Linux や Mac 等の OS にウィルス対策ソフトウェアなどを入れてセキュリティ対策をしている.

10 端末の OS およびソフトウェアのアップデートを適宜行っている.

11 Windows などの OS や商用ソフトウェアのライセンス数を把握している.

12 退席時に他人が使用できないようにパスワード等でロックしている.

13 端末でゲームや情報漏えいにつながるソフトウェアを利用していない.

14 配付元が確認できないソフトウェアをインストールしていない.

15 個人情報を扱っている端末について盗難防止措置やデータの暗号化を行っている.

16 USB メモリなどのネットワーク以外のメディアを介したウィルス感染に対して，使用前にウィルスチェックをするなどの対策をしている.

17 ネットワークのアクセス制限について伺います.
学内のネットワークは外部から発信された通信をファイアウォールにてデフォルトでブロックしていますが，申請をすれば解除できることを知っている.

18 接続を学内ネットワークに限定しているサーバであっても，VPN サービスを利用 すれば，学外からアクセス可能なことを知っている.

19 ○ 以下は研究室のサーバを管理している方に伺います．該当しない方は以上で設問終了です.
研究室のサーバ管理について伺います.ホスティングサーバ（共通サーバ）を利用している.

20 ○ 問題 20 にて「はい」の方は以上で設問終了です．「いいえ」の方は続けてください.
サーバ運用において，本来必要のないサービスが管理者が把握しないまま起動され，不正侵入の原因になることがあります．定期的にサーバの運用状況を確認し，利用許可のあるサービス以外は機能を無効にしている.

21 定期的にバックアップをとっている.

22 利用者の履歴などを定期的に検査している.

23 卒業生(退職者)のアカウント管理をしている.

24 卒業生(退職者)が外部から研究室のコンピュータを操作しているか把握している.

25 ご意見、ご要望などございましたら、ご記入ください.

セキュリティーポリシー自己点検票　事務局用

1 あなたの所属を選択してください。

2 インシデント発生時の対応について伺います.
ウイルス感染・Web ページ改ざん・その他サーバへの不正侵入などのインシデントを発見した場合には，ネットワーク接続を速やかに遮断し被害の拡大防止に努める，また対応後はインシデント報告書を情報メディア基盤センターに 提出しなければならないことを知っている.

3 有料のソフトウェアなどを不正にコピーすると訴訟になる場合があることを知っている.

4 有料のソフトウェアなどを不正にアップロードまたはダウンロードすると著作権の侵害となり訴訟の対象になります. 本学ではファイル交換ソフトウェア(WinMX, Winny, Share, Napster, Wrapster, Gunutella, BitTorrent, Cabos など)の使用を禁止しています.
使用禁止を知っている.

5 アカウント・パスワード管理について伺います.
自己パスワードは秘密としなければなりません.

6 「他の利用者のアカウントを使用してはならない. 」とありますが，他人のアカウントを利用したことはない.

7 「いかなる場合も他の利用者のパスワードを聞き出してはならない. 」とありますが，他人のパスワードを聞き出したことはない.

8 英単語だけでなく，数字・記号を使った強いパスワードを設定している.

9 電子メール及びウェブ閲覧について伺います.
電子メールを私的目的（研究・業務に必要のないメールマガジンへの登録等）で利用してはならないことを知っている.

10 ウェブサイト閲覧は，業務上必要な範囲で閲覧するものであり，不審なサイト等の閲覧をしてはいけないことを知っている.

11 電子メールの利用及びウェブサイトの閲覧について，適正な利用のため，その利用状況についてモニタリング及び監査されることがあることを知っている.

12 各自が業務で使用しているパソコンについて伺います.
ウイルス対策ソフトは導入されている.

13 端末の OS およびソフトウェアのアップデートを適宜行っている.

14 退席時に他人が使用できないようにパスワード等でロックしている.

15 配付元が確認できないソフトウェアをインストールしていない.

16 盗難防止措置等のセキュリティ対策をしている.

17 端末でゲームや情報漏えいにつながるソフトウェアを利用していない.

18 ネットワークのアクセス制限について伺います.
事務局は，外部からの攻撃を防御するため，ファイアーウォールの設定により外部からアクセスが出来ないようになっています.
VPN 接続サービスを使えば学外から事務局ホームページにアクセスができることを知っている.

19 VPN 接続サービスを利用している.

20 事務局セキュリティ対策基準について伺います.
事務局用にセキュリティ対策基準が策定されていることを知っている.

21 ご意見、ご要望などございましたら、ご記入ください.

表1　平成 22 年度　情報セキュリティポリシー自己点検票集計（教職・職員）

教　　員	合計	
教員数※	281	
「はい」の回答数と回答率	114	41%
設　問　概　要※※※	**回答数**	**回答率**
Q2: インシデン ト対応と報告義務の認知	110	96%
Q3: ファイル交換ソフトウェアの利用禁止	110	96%
Q4: 他人アカウントの不正利用の禁止	112	98%
Q5: 適正なパスワードの設定	112	98%
Q6: 電子メールの私的目的利用の禁止	107	94%
Q7: 不審サイト等の閲覧の禁止	114	100%
Q8: メールやウェブ等のアクセス監視の認知	104	91%
Q9: ウィルス対策ソフトのインストール	111	97%
Q10: OS やその他ソフトのアップデート	111	97%
Q11: OS や商用ソフトのライセンス数把握	99	87%
Q12: 退席時の端末パスワード・ロック	87	76%
Q13: ゲームや情報漏えいソフトの利用不可	112	98%
Q14: 配付元未確認ソフトのインストール	113	99%
Q15: 個人情報端末の盗難防止やデータ暗号化	77	68%
Q16: USB メモリ等の使用前ウィルスチェック対策	92	81%
Q17: ファイアウォールと解除依頼の認知	69	61%
Q18: VPN サービスの認知	93	82%
Q19: ホスティングサーバ（共通サーバ）の利用	31	60%
Q20: 定期的サーバ運用状況の確認など	16	73%
Q21: 定期的バックアップの実施	21	95%
Q22: 利用者履歴等の定期的検査の実施	18	82%
Q23: 卒業生（退職者）のアカウント管理	14	64%
Q24: 卒業生（退職者）の外部アクセスの管理	17	77%

職　　員	合計	
職員数※※	229	
「はい」の回答数と回答率	114	50%
設　問　概　要	**回答数**	**回答率**
Q2: インシデント対応と報告義務の認知	90	79%
Q3: 有料ソフトの不正コピー禁止	113	99%
Q4: ファイル交換ソフトウェアの利用禁止	105	92%
Q5: パスワードの守秘性の認知	117	103%
Q6: 他人アカウントの不正利用の禁止	109	96%
Q7: 他人パスワードの聞き出し禁止	114	100%
Q8: 適正なパスワードの設定	108	95%
Q9: 電子メールの私的目的利用の禁止	109	96%
Q10: 不審サイト等の閲覧の禁止	114	100%
Q11: メールやウェブ等のアクセス監視の認知	110	96%
Q12: ウィルス対策ソフトのインストール	112	98%
Q13: OS やその他ソフトのアップデート	103	90%
Q14: 退席時の端末パスワード・ロック	46	40%
Q15: 配付元未確認ソフトのインストール	113	99%
Q16: 盗難防止措置	103	90%
Q17: ゲームや情報漏えいソフトの利用不可	114	100%
Q18: VPN サービスの認知	57	50%
Q19: VPN サービスの利用	98	86%
Q20: 事務局用セキュリティ対策基準の認知	90	79%

※特任教員，研究員を含む
※※事務補佐員を含む
※※※Q19 以降はサーバ管理者への設問．Q19 はサーバ管理者の回答．
Q20 以降は研究室サーバ管理者の回答．

表2　平成 22 年度　教員向け情報セキュリティポリシー自己点検票集計（系・所属別）

系	1 系		2 系		3 系		4 系		5 系		総合教育院		センター	
教員数※	48		37		42		39		32		18		65	
「はい」の回答数と回答率	24	50%	18	49%	23	55%	14	36%	11	34%	11	61%	13	20%
設　問　概　要※※	数	率	数	率	数	率	数	率	数	率	数	率	数	率
Q2: インシデン ト対応と報告義務の認知	22	92%	18	100%	23	100%	14	100%	11	100%	10	91%	12	92%
Q3: ファイル交換ソフトウェアの利用禁止	24	100%	18	100%	21	91%	14	100%	10	91%	11	100%	12	92%
Q4: 他人アカウントの不正利用の禁止	24	100%	18	100%	22	96%	14	100%	11	100%	10	91%	13	100%
Q5: 適正なパスワードの設定	24	100%	18	100%	22	96%	14	100%	10	91%	11	100%	13	100%
Q6: 電子メールの私的目的利用の禁止	22	92%	18	100%	22	96%	13	93%	11	100%	8	73%	13	100%
Q7: 不審サイト等の閲覧の禁止	24	100%	18	100%	23	100%	14	100%	11	100%	11	100%	13	100%
Q8: メールやウェブ等のアクセス監視の認知	21	88%	16	89%	21	91%	14	100%	11	100%	8	73%	13	100%
Q9: ウィルス対策ソフトのインストール	24	100%	17	94%	22	96%	14	100%	11	100%	10	91%	13	100%
Q10: OS やその他ソフトのアップデート	24	100%	18	100%	21	91%	14	100%	11	100%	10	91%	13	100%
Q11: OS や商用ソフトのライセンス数把握	22	92%	16	89%	18	78%	13	93%	10	91%	9	82%	11	85%
Q12: 退席時の端末パスワード・ロック	21	88%	17	94%	16	70%	10	71%	7	64%	6	55%	10	77%
Q13: ゲームや情報漏えいソフトの利用不可	24	100%	18	100%	22	96%	14	100%	11	100%	10	91%	13	100%
Q14: 配付元未確認ソフトのインストール	24	100%	18	100%	23	100%	13	93%	11	100%	11	100%	13	100%
Q15: 個人情報端末の盗難防止やデータ暗号化	15	63%	15	83%	13	57%	10	71%	7	64%	6	55%	11	85%
Q16: USB メモリ等の使用前ウィルスチェック対策	20	83%	15	83%	16	70%	12	86%	10	91%	7	64%	12	92%
Q17: ファイアウォールと解除依頼の認知	14	58%	13	72%	16	70%	8	57%	6	55%	5	45%	7	54%
Q18: VPN サービスの認知	22	92%	13	72%	20	87%	14	100%	10	91%	6	55%	8	62%
Q19: ホスティングサーバ（共通サーバ）の利用	7	54%	4	57%	9	56%	4	57%	3	75%	1	50%	3	75%
Q20: 定期的サーバ運用状況の確認など	6	100%	2	67%	4	57%	3	100%	1	100%	0	0%	0	0%
Q21: 定期的バックアップの実施	5	83%	3	100%	7	100%	3	100%	1	100%	1	100%	1	100%
Q22: 利用者履歴等の定期的検査の実施	6	100%	3	100%	5	71%	2	67%	1	100%	1	100%	0	0%
Q23: 卒業生（退職者）のアカウント管理	4	67%	2	67%	6	86%	1	33%	1	100%	0	0%	0	0%
Q24: 卒業生（退職者）の外部アクセスの管理	6	100%	2	67%	6	86%	2	67%	1	100%	0	0%	0	0%

※特任教員，研究員を含む．　※※Q19 以降はサーバ管理者への設問．Q19 はサーバ管理者の回答．Q20 以降は研究室サーバ管理者の回答．

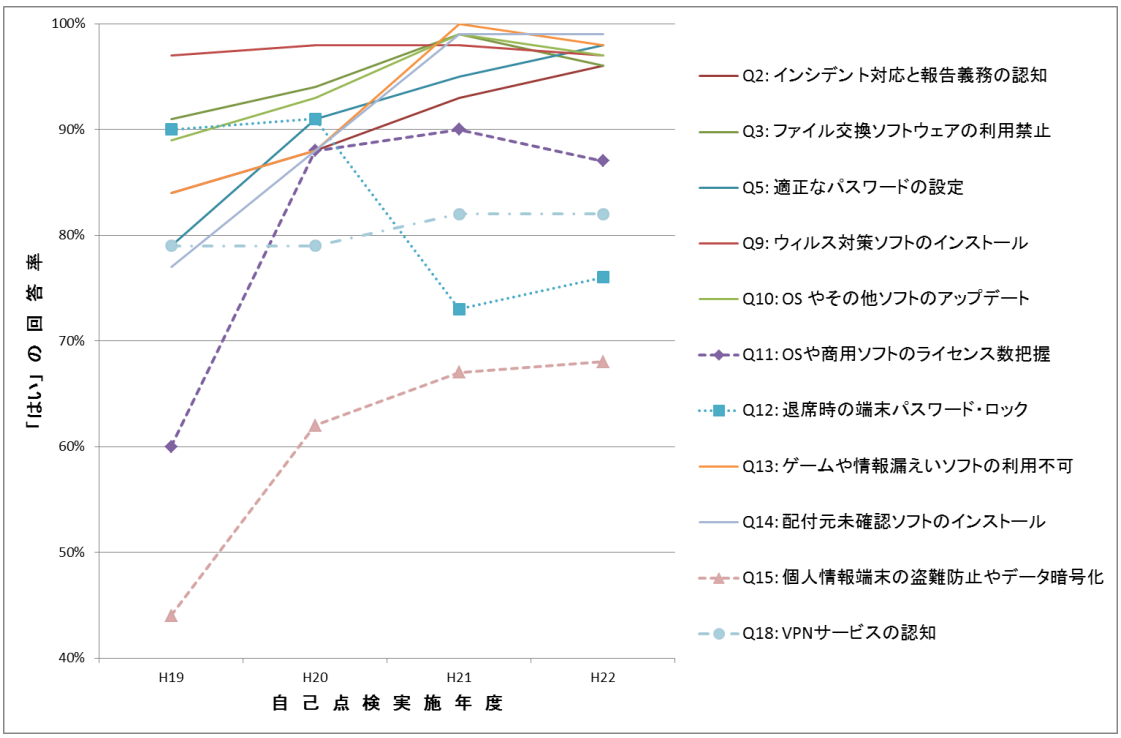

図１　４年間の自己点検票回答率の推移（教員用，一般向け）

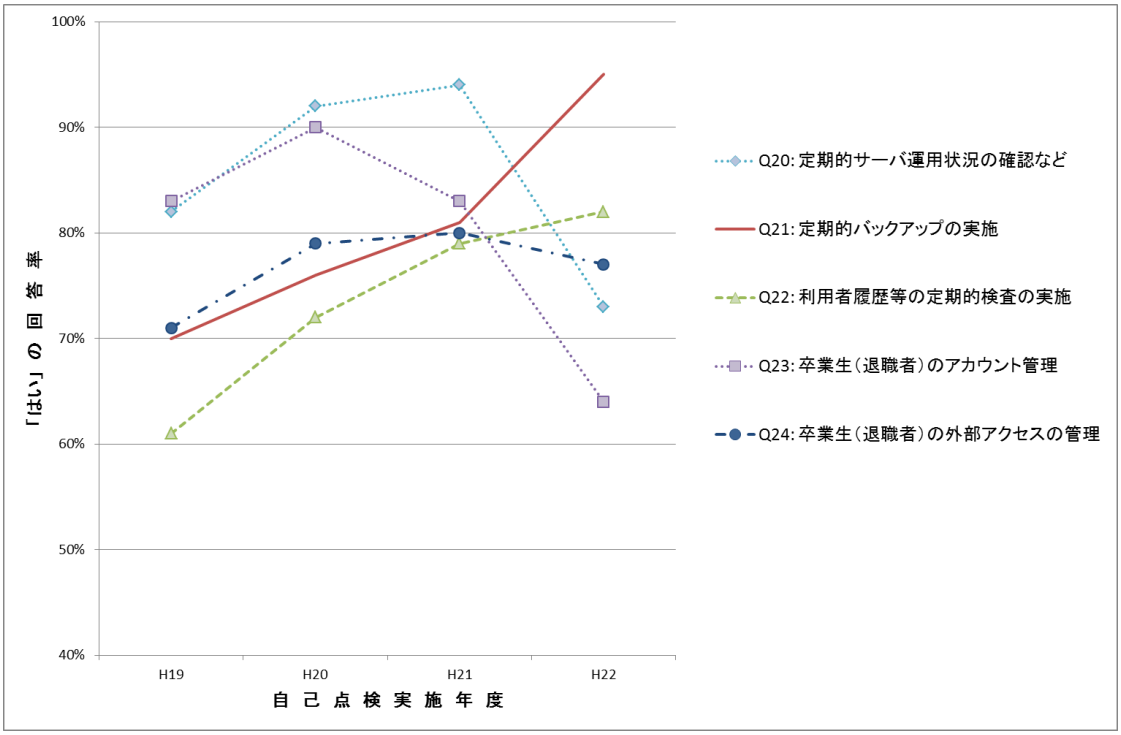

図２　４年間の自己点検票回答率の推移（教員用，管理者向け）

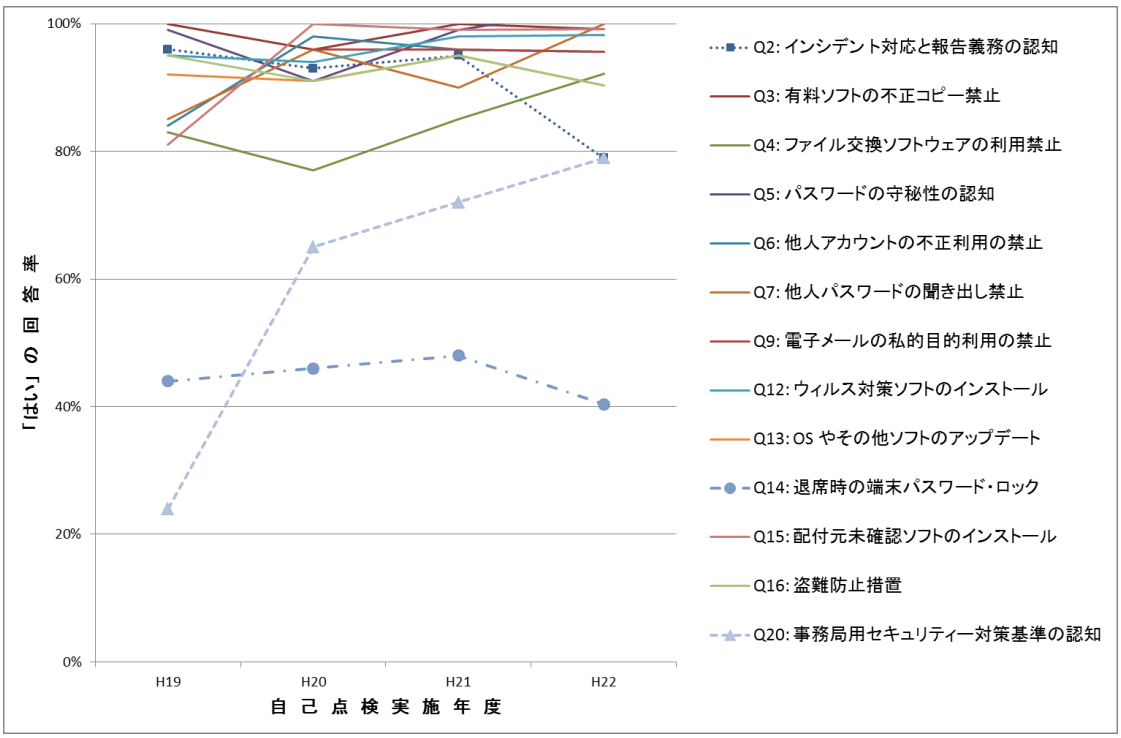

図３　４年間の自己点検票回答率の推移（職員用）