

# 平成19年度情報セキュリティ現状調査報告書

セキュリティ対策専門委員会

平成20年3月

## 1. 調査の概要と回収状況

### (1) 調査期間

平成19年4月2日(月) ～ 平成19年4月27日(金)

### (2) 調査方法

インターネット上の学内限定アンケート

### (3) 調査対象

学内のパソコンを使用している職員(各種学内予算で購入したパソコンについて回答)

### (4) 調査目的

弘前大学情報セキュリティポリシーに基づき、ポリシーの評価及び見直しを行う。

### (5) 回収状況

大学全体として445名の回答が寄せられ、回答者全員がすべての調査項目に対して回答されていたため、有効回答者数を445名とした。なお、総合情報処理センターの研究用メールシステムの登録ユーザー(学生を除く)は1,953名なので、回収率は22.8%であった。本調査にご回答頂いた方の所属を表1にまとめた。

表1. 回答者の所属

部局等名	回答者数
人文学部	38
教育学部	46
医学研究科	44
保健学研究科	65
理工学研究科	47
農学生命科学部	29
医学部附属病院	76
その他の附属施設	22
事務局	78
合計	445

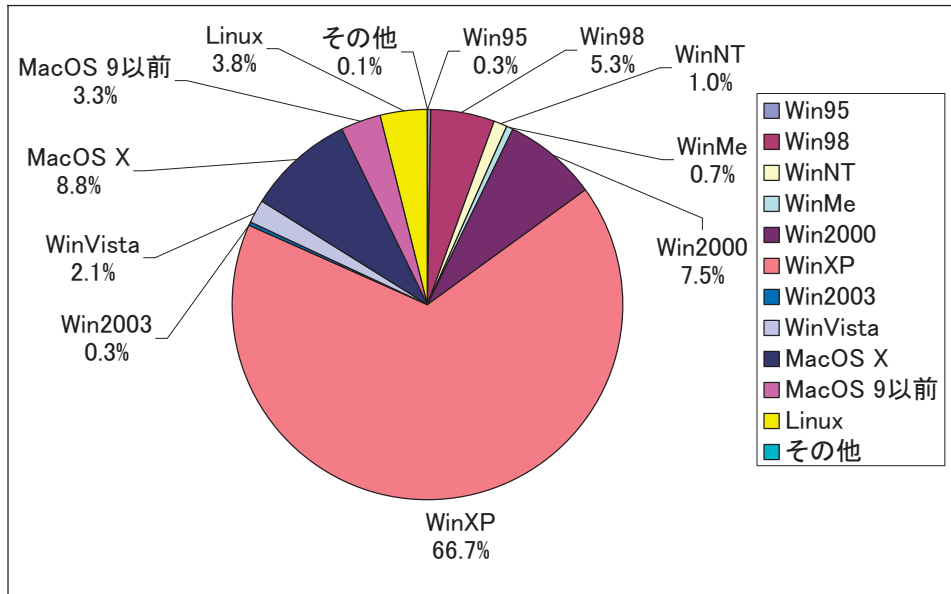
## 2. 調査項目毎の調査結果

問1. 使用しているOS毎のパソコンの台数について記入してください。

回答者が現在使用しているOSについて、回答のあった計968台の端末に関するデータが得られ、その集計結果を図I-1にまとめた。813台(84.0%)がWindowsを使用しており、特にWindows XPを半数以上の646台(66.7%)で使用している結果となった。一方で、OSのサポート期間が終了しているWindows 95, Windows 98, Windows NT, Windows Meの端末は計71台(7.3%)使用している現状がある。これらのOSはセキュリティ上の不具合を解消するためのセキュリティパッチの配布が行われない。サポート期間の終了されたOSの使用は常にセキュリティ上の危険に晒され

ている状態であると伺われる。(n=968, 図 I-1)

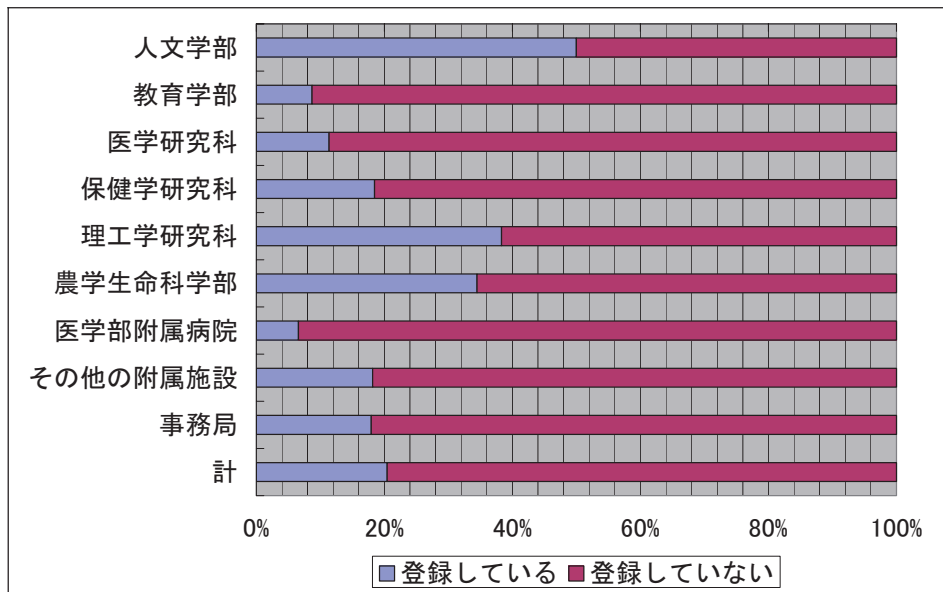
図 I-1. 使用している OS の状況 (n=968)



問 2-1. 情報セキュリティポリシーに定める最重要限定情報及び非公開情報を情報管理台帳に登録していますか。

情報セキュリティポリシー（以下、「ポリシー」という。）に定める最重要限定情報及び非公開情報（以下、「重要情報」という。）の取り扱いについて、情報管理台帳に登録している回答者は 91 名（20.4%）と少なかった。部局別の登録状況では、人文学部 50.0%、理工学研究科 38.3%と比較的高いものの、一方で附属病院 6.6%、教育学部 8.7%、医学研究科 11.4%と低く、ポリシー上に定める情報の取り扱い方法の理解に差があることが推測される。(n=445, 図 II-1)

図 II-1. 情報管理台帳への登録状況 (n=445)

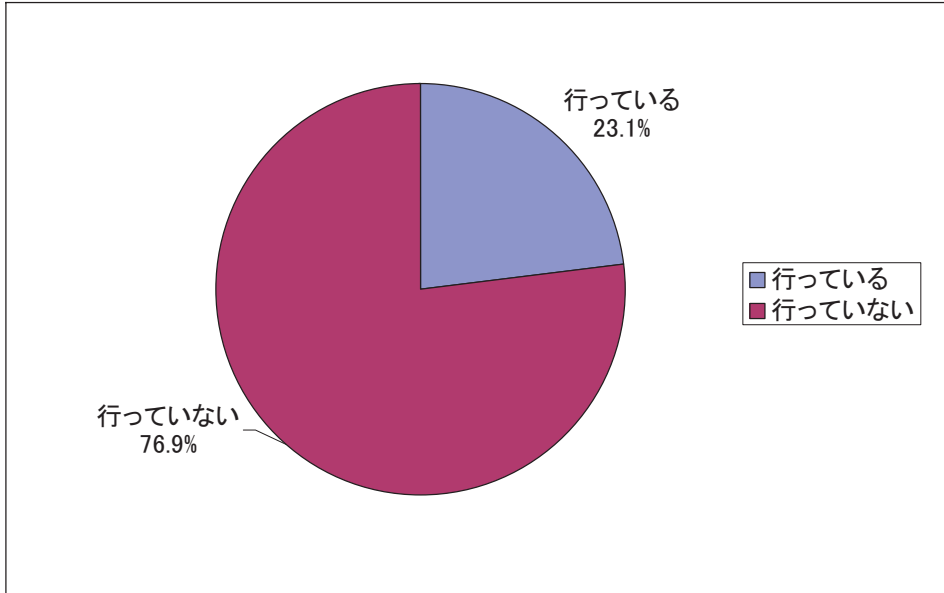


問 2-2. 最重要限定情報及び非公開情報に対して、データの暗号化を行っていますか。

情報管理台帳に登録している回答者のうち、ポリシーに定めるデータの暗号化を行っているのが

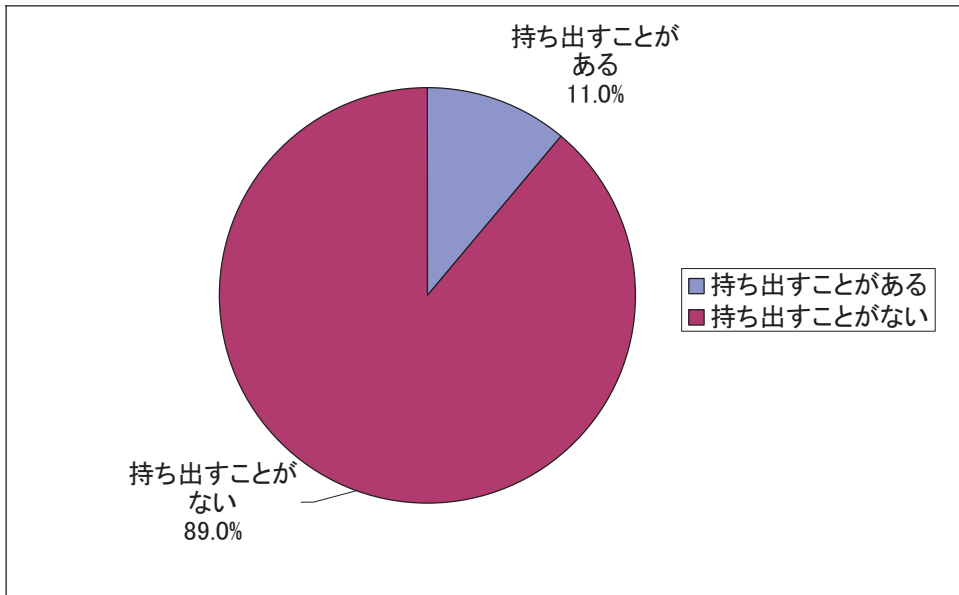
21名(23.1%)とポリシーに定める重要情報を扱っているにも関わらず、そのセキュリティ対策が不十分であることが明らかとなった。(n=91, 図Ⅱ-2)

図Ⅱ-2. 情報の暗号化状況 (n=91)



問2-3. 記録媒体に最重要限定情報及び非公開情報を保存し、学外に持ち出すことがありますか。情報管理台帳に登録している回答者のうち、記録媒体を学外に持ち出すことがあるのは10名(11.0%)と少ないが、記録媒体を学外で紛失しないよう、その取扱には特に注意が必要である。(n=91, 図Ⅱ-3)

図Ⅱ-3. 情報の学外への持ち出し状況 (n=91)

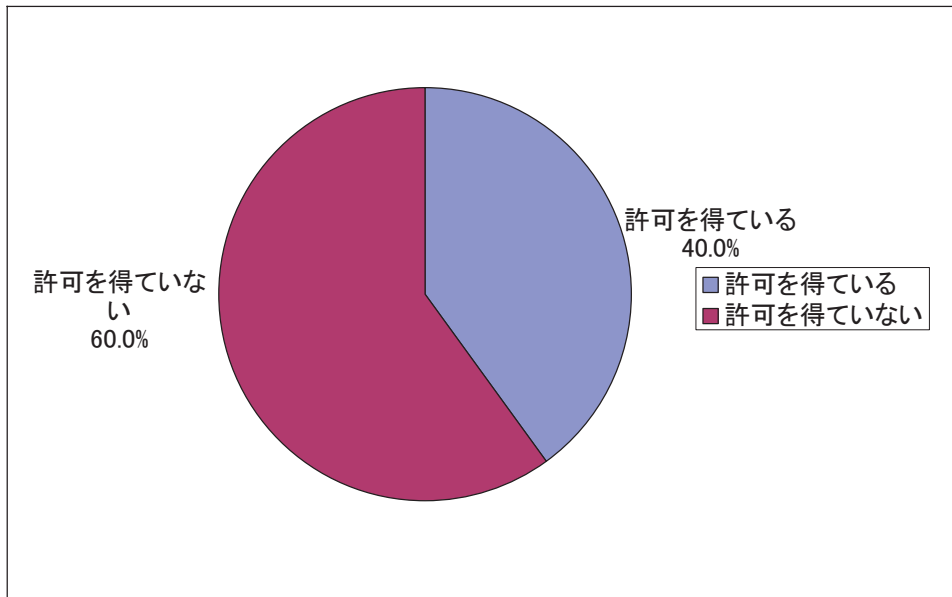


問2-4. 最重要限定情報及び非公開情報を学外へ持ち出す場合、事前に申請書を提出し部局情報セキュリティ管理者の許可を得ていますか。

データを学外に持ち出すことがある回答者のうち、ポリシーに定める部局情報セキュリティ管理者の許可を得ているのは4名(40.0%)と低い結果となり、ポリシーが浸透していないことが伺われ

る。(n=10, 図Ⅱ-4)

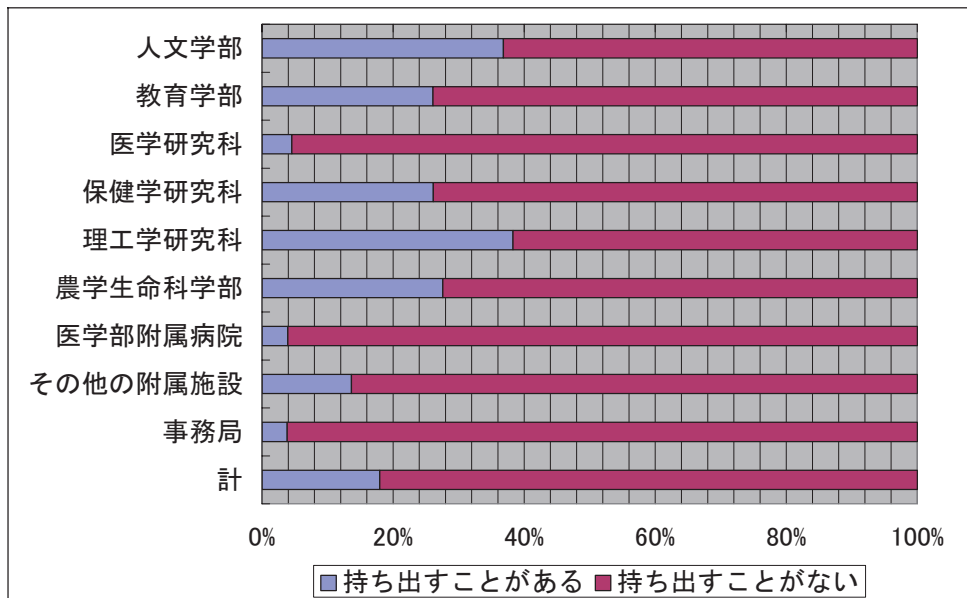
図Ⅱ-4. 情報持ち出し申請状況



問3-1. パソコンを学外に持ち出すことはありますか。

パソコンの学外への持ち出しについて、持ち出すことがある回答者は80名(18.0%)も存在しており、パソコンを学外で紛失しないようその取扱には特に注意が必要である。部局別の持ち出し状況では理工学部38.3%, 人文学部36.8%と高いものの、一方で事務局3.8%, 医学部附属病院3.9%, 医学研究科4.5%と低く、パソコンを学外に持ち出す意識に差が見られた。(n=445, 図Ⅲ-1)

図Ⅲ-1. パソコンの持ち出し状況 (n=445)

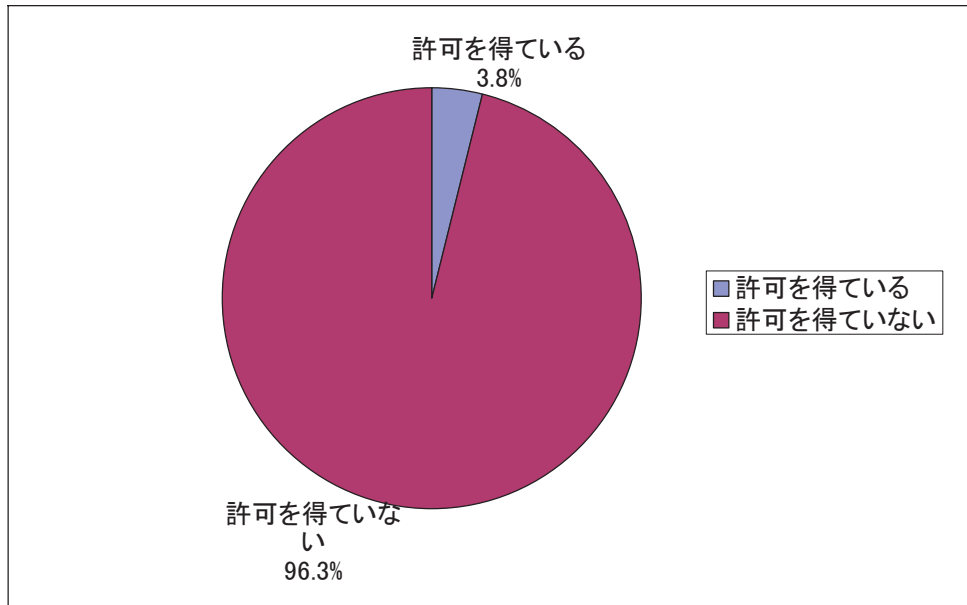


問3-2. パソコンを学外に持ち出す必要がある場合、事前に申請書を提出し部局情報セキュリティ管理者の許可を得ていますか。

パソコンを学外に持ち出すことがある回答者のうち、ポリシーに定める部局情報セキュリティ管理者の許可を得ているのは3名(3.8%)と非常に低く、ポリシーが浸透していないことが伺われる。

(n=80, 図III-2)

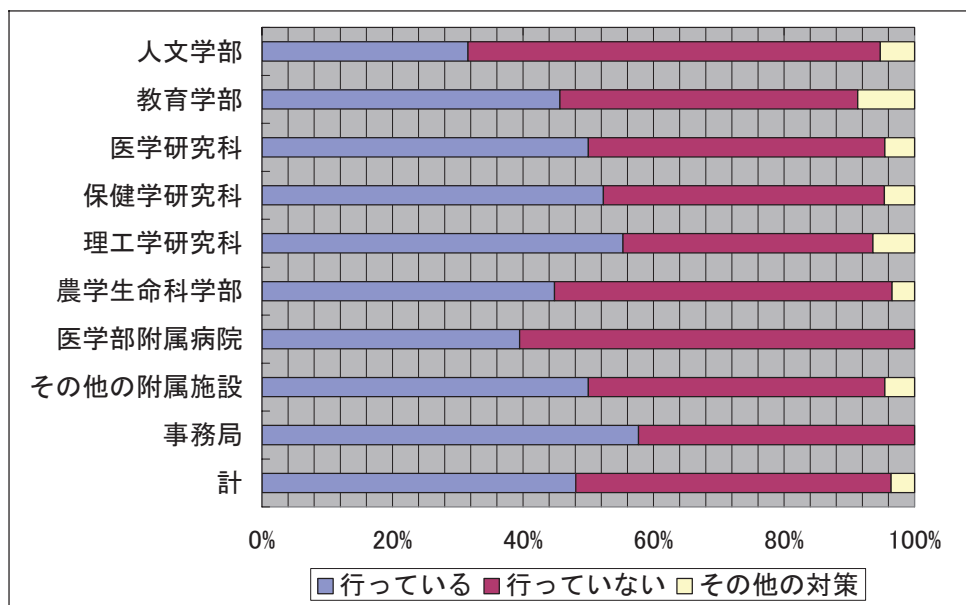
図III-2. パソコンの持ち出し申請状況 (n=80)



問4. パソコンを第三者に盗み見られたり，許可なく変更されたりしないように，パソコンの操作ロックを行っていますか。

パソコンを第三者に盗み見られたり，許可なく変更されたりしないように，パソコンの操作ロック及びその他の対策を行っている回答者は併せて 230 名 (51.7%) とまだ半数のものの，他のセキュリティ対策に比べ，遵守されていることがわかった。部局間では，特に大きな差は見られなかった。(n=445, 図IV-1)

図IV-1. パソコンの不正利用対策状況 (n=445)

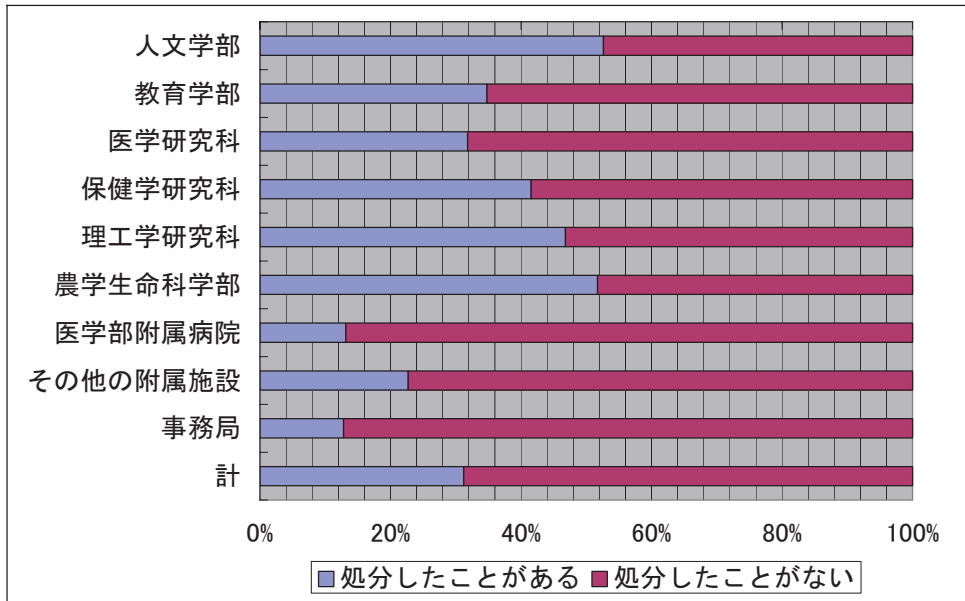


問5-1. パソコンまたは記録媒体を処分したことはありますか。

パソコン及び記録媒体の処分をしたことがある回答者は 139 名 (31.2%) となった。部局別の処分状況では人文学部 52.6%，農学生命科学部 51.7%と高く，事務局 12.8%，医学部附属病院 13.2%

と低い処分状況であった。部局によっては個人で処分せずにまとめて処分する方法をとっている部局もあり、個人で処分を行った意識が低いことが原因と伺われる。(n=445, 図V-1)

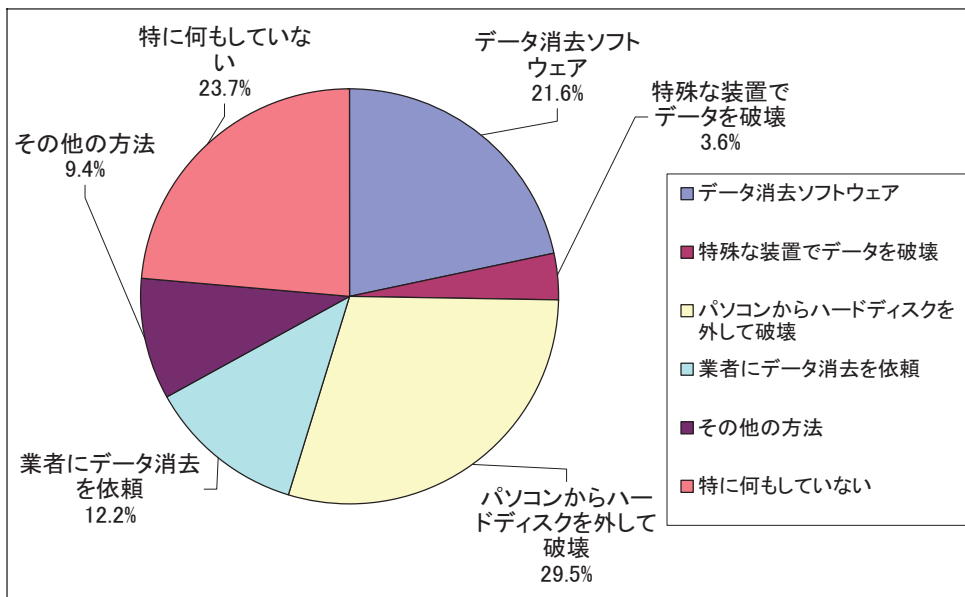
図V-1. パソコン及び記録媒体の処分状況 (n=445)



問5-2. パソコンまたは記録媒体を処分する際に、どのような方法でデータを消去または破壊しデータが復元できない状態にしていますか。

処分をしたことがある回答者のうち、ポリシーで定める処分方法(データ消去ソフトウェア、特殊な装置でデータを破壊、パソコンからハードディスクを外して破壊及び業者にデータ消去を依頼)で処分をしているのは93名(66.9%)と半数以上を占め、比較的遵守されている。一方で、特に何もせずそのままパソコン及び記録媒体を処分しているのが33名(23.7%)も存在し、情報漏えいの危険性が伺われる。通常パソコンの操作においてファイルの削除等を行っただけでは、データが消去されたわけではなく、データを復元することが可能であるため、注意してほしい。(n=139, 図V-2)

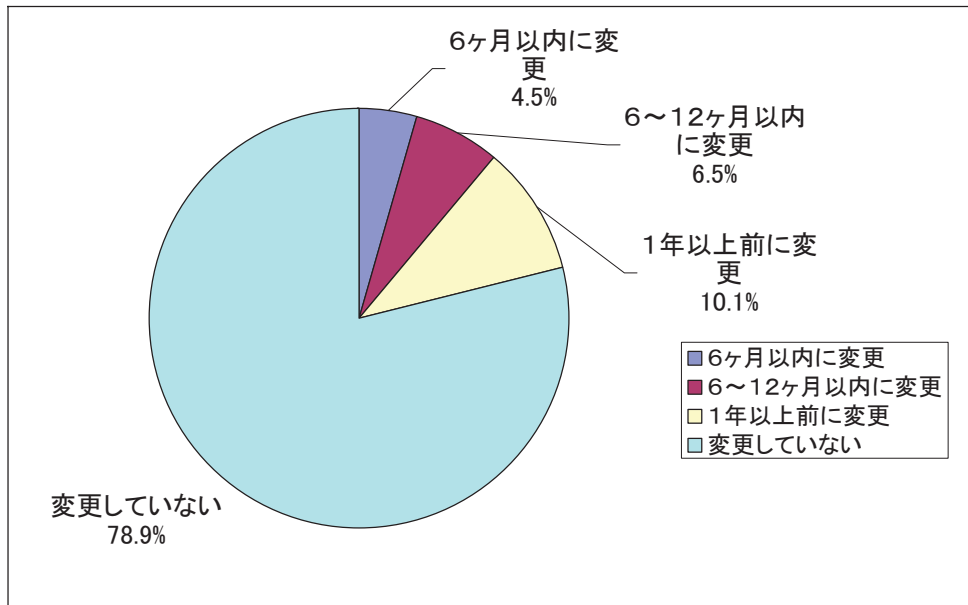
図V-2. パソコン及び記録媒体の処分方法 (n=139)



問6. 情報システムのパスワードを定期的に変更していますか。

ポリシーで定める情報システムのパスワードを6ヶ月以内に変更している回答者は20名(4.5%)と非常に少なく、また初期に設定したパスワードは、そのまま使わないことと定められているにも関わらず、351名(78.9%)の回答者がID取得後一度も変更したことが無い状況であった。パスワードについては、推測されにくいパスワードを設定すること及び定期的に変更することにより、情報セキュリティが高まるため、この状態では不正にパスワードを取得される可能性が高いことが伺われる。(n=445, 図VI-1)

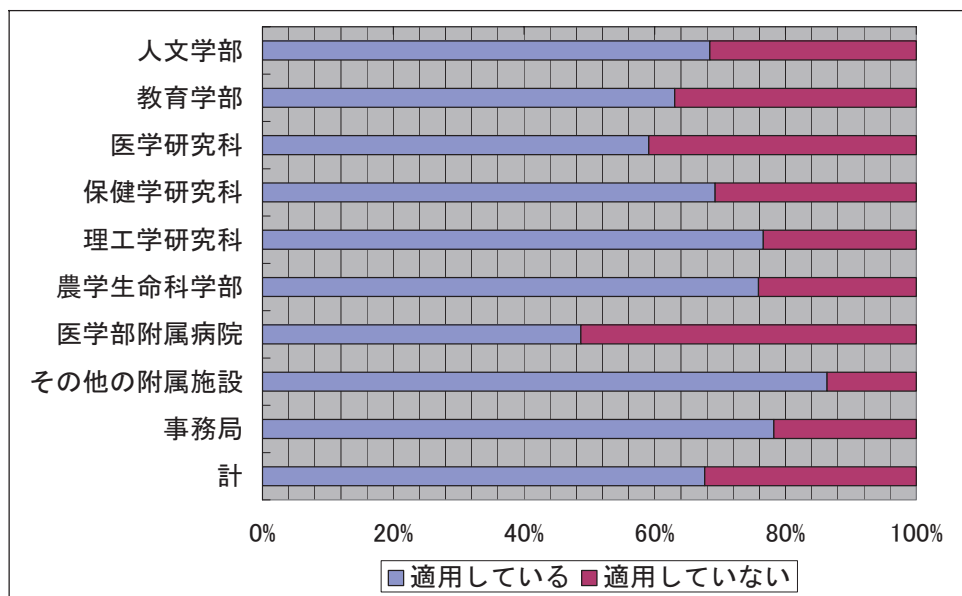
図VI-1. パスワードの変更状況 (n=445)



問7. OS または導入しているソフトウェアのサポートの期間が終了していない場合、配布されるセキュリティパッチを常に導入していますか。

ポリシーで定める OS 及び導入しているソフトウェアの配布されるセキュリティパッチの適用をしている回答者は301名(67.6%)となった。部局別の適用状況では、医学部附属病院のみ48.7%とやや低い、ほとんどの部局が高い状況である。サポート期間が終了しセキュリティ上問題があるOSを使用している現状(問1参照)もあり、サポート期間にあるOS及び導入しているソフトウェアを使用している回答者については、高い割合でセキュリティパッチを適用していると推測できる。(n=445, 図VII-1)

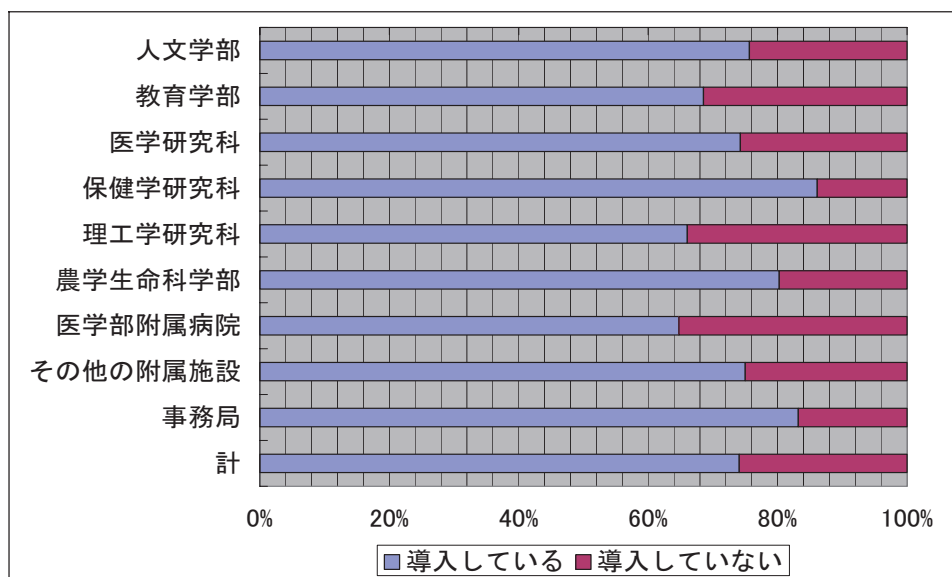
図Ⅶ－１．セキュリティパッチの適用状況 (n=445)



問8. ウィルス対策ソフトウェアを導入している OS 毎のパソコンの台数について記入してください。

ポリシーに定めるコンピュータウィルスに対する必要な措置として、ウィルス対策ソフトを導入しているパソコンは 717 台 (74.1%) となった。部局別の導入状況では、保健学研究科 86.1%、事務局 83.2%と比較的高いものの、一方で医学部附属病院 64.8%、理工学研究科 66.0%とやや低く、全体的にはウィルス対策への意識はやや高いが、実際年間数件のウィルス被害が発生している現実から導入率を高める必要がある。(n=968, 図Ⅷ－１)

図Ⅷ－１．ウィルス対策ソフト導入状況 (n=968)



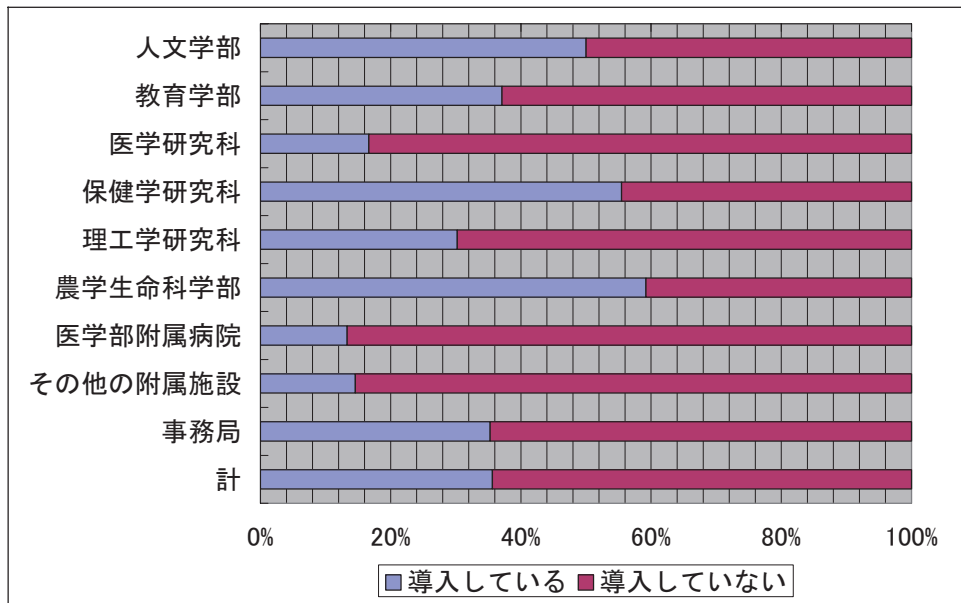
問9. スパイウェアを除去するソフトウェアを導入している OS 毎のパソコンの台数について記入してください。

パソコンの操作履歴や保存されている情報を、外部へ流出させるスパイウェアに対する措置として、スパイウェア対策ソフトを導入しているパソコンは 345 台 (35.6%) となった。部局別の導入状況では、農学生命科学部 59.2%、保健学研究科 55.5%、人文学部 50.0%と比較的高いものの、一方で



医学部附属病院 13.3%, 医学研究科 16.7%と大変低い状況であった。スパイウェアの存在について、まだまだ知られていない状況が推測される。(n=968, 図IX-1)

図IX-1. スパイウェア対策ソフト導入状況 (n=968)



## まとめ

本調査は、ポリシーが平成17年8月30日の運用から1年半経過し、運用開始から初めて行った調査であり、ポリシーの運用状況を把握し、ポリシーの評価及び見直しを行うための調査であった。ポリシーを遵守する上で守るべき基本的な事項を各調査項目として設定し、本調査を行い、445名の有効回答が寄せられ(回収率は22.8%)、総計968台の端末についてのデータが得られた。

各調査項目の結果全体から伺えるのは、各部局に差は見られるものの、ポリシーの遵守状況が低いと判断せざるを得ない結果となった。この結果により、ポリシーの存在が充分浸透していないことが考えられる。また、回収率が低いことから情報セキュリティに関する意識が低いことが推測される。

情報セキュリティ対策で一番重要なことは、職員・学生一人一人が情報セキュリティへの意識を高めることである。NPO法人日本ネットワークセキュリティ協会の調査によると2006年の個人情報漏えいの公表件数は993件で、前年の1,032件に対して96%と前年と同規模の件数であった。その原因は、「紛失・置忘れ」、「盗難」、「誤操作」、「管理ミス」と人為的なミスが多く、全体の70%を超えている。コンピュータウィルスが原因であれば、ウィルス対策ソフト等の技術的な対策も可能であるが、人為的な原因となると技術的な対策だけでは難しく、個人一人一人が情報セキュリティへの意識を高め、不注意な行為を減らす努力が必要となってくる。

今後は、ポリシーを広く学内に周知し、理解を求める必要がある。その具体的な対策として、ポリシーの説明会等を開催すること、情報セキュリティに対する意識の啓発を行うため、引き続き情報セキュリティセミナーの開催をすること及び情報セキュリティに関する知識や情報を発信するホームページを作成することが考えられる。

ポリシーを広く学内に周知し、ポリシーへの理解を深めることで、情報セキュリティへの意識が高まり、ポリシーの遵守状況が向上することを期待する。そのことが本学の情報セキュリティを確保す

る近道であると考え。なお、本調査は今後も1年に1回、実施していく予定である。次回の調査時には、ぜひ多くの職員に参加していただき、今回以上のポリシーの遵守状況が見られることを期待している。

## 参考資料 1

### 調 査 項 目

問1. 使用しているOS(※)毎のパソコンの台数について記入してください。

問2-1. 情報セキュリティポリシーに定める最重要限定情報及び非公開情報を情報管理台帳に登録していますか。

(問2-1で「登録している」を選んだ方は回答してください)

問2-2. 最重要限定情報及び非公開情報に対して、データの暗号化(※)を行っていますか。

問2-3. 記録媒体(※)に最重要限定情報及び非公開情報を保存し、学外に持ち出すことがありますか。

(問2-3で「持ち出すことがある」を選んだ方は回答してください)

問2-4. 最重要限定情報及び非公開情報を学外へ持ち出す場合、事前に申請書を提出し部局情報セキュリティ管理者の許可を得ていますか。

問3-1. パソコンを学外に持ち出すことはありますか。

(問3-1で「持ち出すことがある」を選んだ方は回答してください)

問3-2. パソコンを学外に持ち出す必要がある場合、事前に申請書を提出し部局情報セキュリティ管理者の許可を得ていますか。

問4. パソコンを第三者に盗み見られたり、許可なく変更されたりしないように、パソコンの操作ロック(※)を行っていますか。

問5-1. パソコンまたは記録媒体を処分したことはありますか。

(問5-1で「処分したことがある」を選んだ方は回答してください)

問5-2. パソコンまたは記録媒体を処分する際に、どのような方法でデータを消去または破壊しデータが復元できない状態にしていますか。

問6. 情報システムのパスワード(※)を定期的に変更していますか。

問7. OSまたは導入しているソフトウェアのサポート(※)の期間が終了していない場合、配布されるセキュリティパッチ(※)を常に導入していますか。

問8. ウィルス対策ソフトウェア(※)を導入しているOS毎のパソコンの台数について記入してください。

問9. スパイウェアを除去するソフトウェア(※)を導入しているOS毎のパソコンの台数について記入してください。

※用語説明

・OS

Windows や MacOS などのコンピュータシステム全体を管理するソフトウェア

・暗号化

データを第三者に盗み見られたり、許可なく変更されたりされないよう、専用のソフトウェアなどを用いてデータを変換すること。

・記録媒体

フロッピーディスクや CD-ROM 等のデータを記録するもの

・パソコンの操作ロック

「ユーザパスワードによるロック」、「USB 機器によるロック」などの、OS やソフトウェア等の機能を用いて、パソコンの操作をできなくすること

・情報システムのパスワード

総合情報処理センターのシステム利用申請書により取得したパスワード及び学部等のシステム利用で所得したパスワードなど

・サポート

メーカーが自社の製品を購入した顧客に対し、不具合の対応や使い方のアドバイスなどを行うこと

・セキュリティパッチ

不具合を修正するためのプログラム

・コンピュータウイルス

他人のコンピュータに勝手に入り込んで悪さをするプログラム

・ウイルス対策ソフトウェア

「ウイルスバスター」、「アンチウイルス」などのコンピュータウイルス等を検出及び除去するソフトウェア

・スパイウェア

パソコンを使っている人の行動や個人情報などを収集し、得られたデータを作成元に送られるソフトウェア

・スパイウェアを除去するソフトウェア

「AD-AWARE」、「スパイボット」などのスパイウェアを検出及び除去するソフトウェア

## 参考資料 2

## 単純集計表

問 1. 使用している OS 毎のパソコンの台数について記入してください。(回答端末数 968)

	Win95	Win98	WinNT	WinMe	Win 2000	WinXP	Win 2003	Win Vista	MacOS X	MacOS 9以前	Linux	その他	合計
回答者数	3	51	10	7	73	646	3	20	85	32	37	1	968
構成比 (%)	0.3	5.3	1.0	0.7	7.5	66.7	0.3	2.1	8.8	3.3	3.8	0.1	100.0

問 2-1. 情報セキュリティポリシーに定める最重要限定情報及び非公開情報を情報管理台帳に登録していますか。(回答者数 445)

	登録している	登録していない	合計
回答者数	91	354	445
構成比 (%)	20.4	79.6	100.0

問 2-2. 最重要限定情報及び非公開情報に対して、データの暗号化を行っていますか。(回答者数 91)

	行っている	行っていない	合計
回答者数	21	70	91
構成比 (%)	23.1	76.9	100.0

問 2-3. 記録媒体に最重要限定情報及び非公開情報を保存し、学外に持ち出すことがありますか。(回答者数 91)

	持ち出すことがある	持ち出すことがない	合計
回答者数	10	81	91
構成比 (%)	11.0	89.0	100.0

問 2-4. 最重要限定情報及び非公開情報を学外へ持ち出す場合、事前に申請書を提出し部局情報セキュリティ管理者の許可を得ていますか。(回答者数 10)

	許可を得ている	許可を得ていない	合計
回答者数	4	6	10
構成比 (%)	40.0	60.0	100.0

問3-1. パソコンを学外に持ち出すことはありますか。(回答者数 445)

	持ち出すことがある	持ち出すことがない	合計
回答者数	80	365	445
構成比 (%)	18.0	82.0	100.0

問3-2. パソコンを学外に持ち出す必要がある場合、事前に申請書を提出し部局情報セキュリティ管理者の許可を得ていますか。(回答者数 80)

	許可を得ている	許可を得ていない	合計
回答者数	3	77	80
構成比 (%)	3.8	96.3	100.0

問4. パソコンを第三者に盗み見られたり、許可なく変更されたりしないように、パソコンの操作ロックを行っていますか。(回答者数 445)

	行っている	行っていない	その他のセキュリティ対策を行っている	合計
回答者数	214	215	16	445
構成比 (%)	48.1	48.3	3.6	100.0

問5-1. パソコンまたは記録媒体を処分したことはありますか。(回答者数 445)

	処分したことがある	処分したことがない	合計
回答者数	139	306	445
構成比 (%)	31.2	68.8	100.0

問5-2. パソコンまたは記録媒体を処分する際に、どのような方法でデータを消去または破壊しデータが復元できない状態にしていますか。(回答者数 139)

	データ消去ソフトウェアを使用	特殊な装置でハードディスクのデータを電氣的、磁氣的に破壊	コンピュータからハードディスクを取り外して物理的に破壊	専門の業者にデータ消去を依頼	特に何もせず、処分している	その他の方法で処分している	合計
回答者数	30	5	41	17	33	13	139
構成比 (%)	21.6	3.6	29.5	12.2	23.7	9.4	100.0

問6. 情報システムのパスワードを定期的に変更していますか。(回答者数 445)

	6ヶ月以内に変更	6～12ヶ月以内に変更	1年以上前に変更	変更していない	合計
回答者数	20	29	45	351	445
構成比 (%)	4.5	6.5	10.1	78.9	100.0

問7. OS または導入しているソフトウェアのサポートの期間が終了していない場合、配布されるセキュリティパッチを常に導入していますか。(回答者数 445)

	適用している	適用していない	合計
回答者数	301	144	445
構成比 (%)	67.6	32.4	100.0

問8. ウィルス対策ソフトウェアを導入している OS 毎のパソコンの台数について記入してください。(回答端末数 968)

	Win95	Win98	WinNT	WinMe	Win 2000	WinXP	Win 2003	Win Vista	MacOS X	MacOS 9以前	Linux	その他	合計
回答者数	0	15	4	2	62	557	2	17	42	15	1	0	717
構成比 (%)	0.0	2.1	0.6	0.3	8.6	77.7	0.3	2.4	5.9	2.1	0.1	0.0	100.0
導入率 (%)	0.0	29.4	40.0	28.6	84.9	86.2	66.7	85.0	49.4	46.9	2.7	0.0	74.1

問9. スパイウェアを除去するソフトウェアを導入している OS 毎のパソコンの台数について記入してください。(回答端末数 968)

	Win95	Win98	WinNT	WinMe	Win 2000	WinXP	Win 2003	Win Vista	MacOS X	MacOS 9以前	Linux	その他	合計
回答者数	0	7	0	0	17	289	1	12	17	2	0	0	345
構成比 (%)	0.0	2.0	0.0	0.0	4.9	83.8	0.3	3.5	4.9	0.6	0.0	0.0	100.0
導入率 (%)	0.0	13.7	0.0	0.0	23.3	44.7	33.3	60.0	20.0	6.3	0.0	0.0	35.6