平成29年度
情報セキュリティ意識調査

回答まとめ（2018.3）

実施日：2018/2/9～3/7

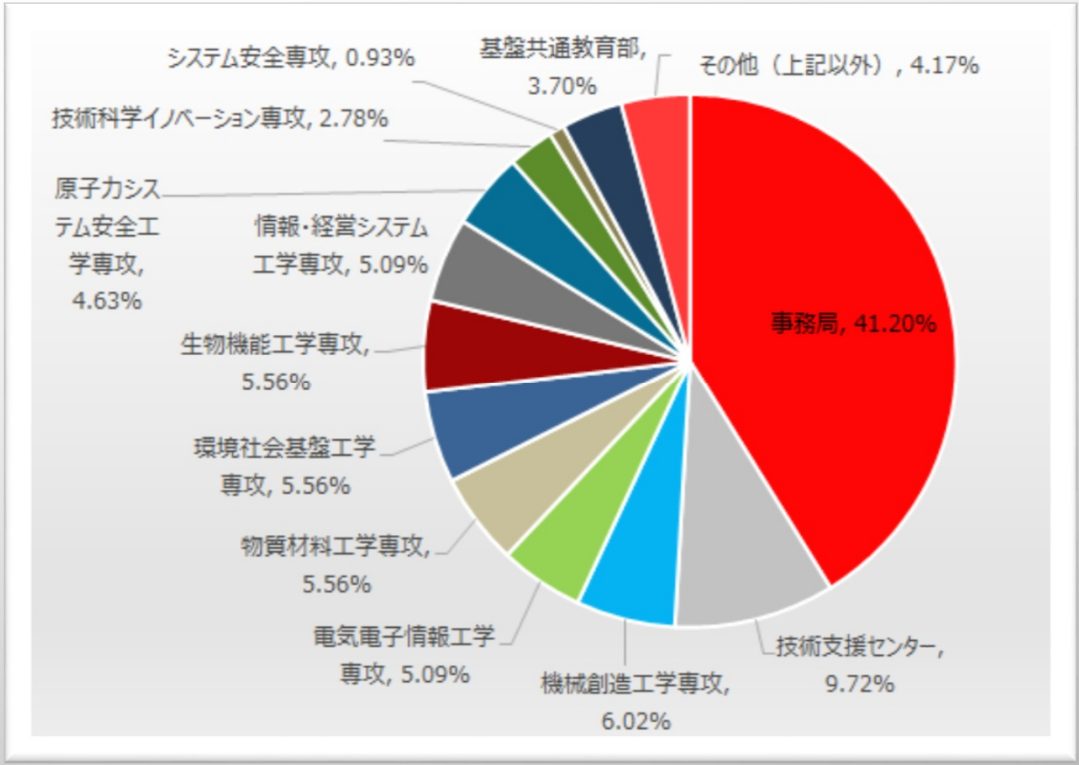
回答数：216人　回答割合40.7%

（役職員数　2/28現在：531人）

（※学生、非常勤講師除く）

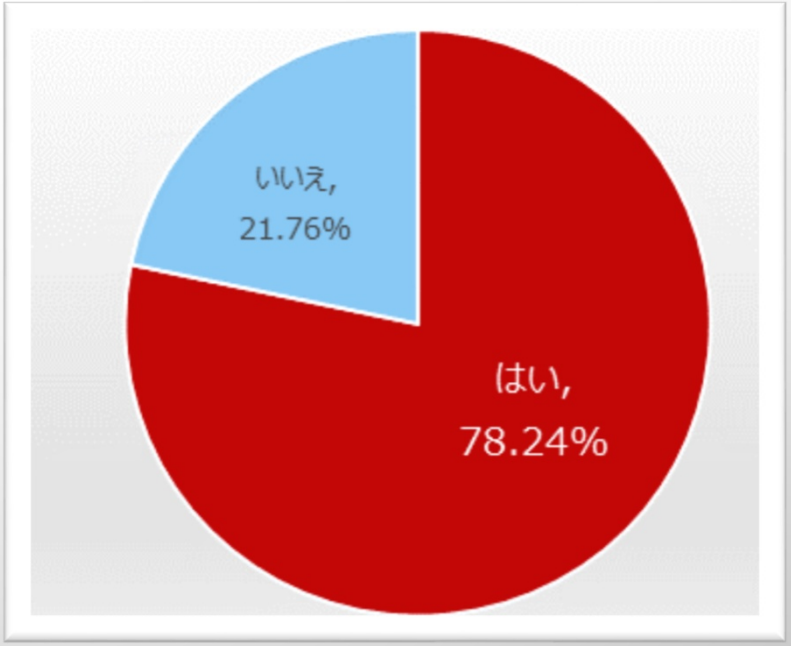
■ 所属を選択してください。

Answer Choices	Responses	
事務局	41.20%	89
技術支援センター	9.72%	21
機械創造工学専攻	6.02%	13
電気電子情報工学専攻	5.09%	11
物質材料工学専攻	5.56%	12
環境社会基盤工学専攻	5.56%	12
生物機能工学専攻	5.56%	12
情報・経営システム工学専攻	5.09%	11
原子力システム安全工学専攻	4.63%	10
技術科学イノベーション専攻	2.78%	6
システム安全専攻	0.93%	2
基盤共通教育部	3.70%	8
その他（上記以外）	4.17%	9
	Answered	**216**
	Skipped	**0**



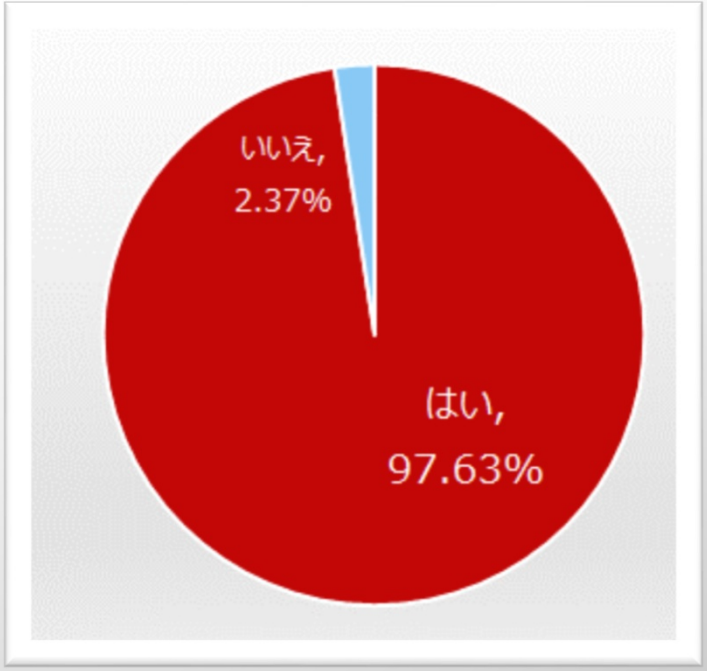
■「長岡技術科学大学　情報セキュリティ管理運用の手引」を読んだことがありますか？

Answer Choices	Responses	
はい	78.24%	169
いいえ	21.76%	47
	Answered	**216**
	Skipped	**0**



■ パスワードは、充分な複雑さ（長さや文字の種類）を設定していますか？

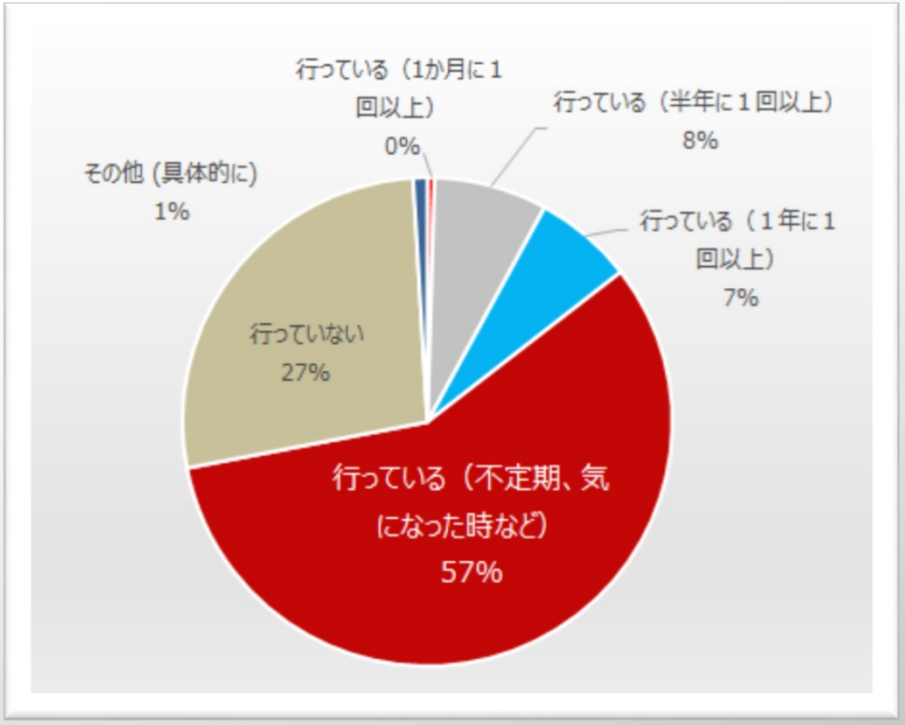
Answer Choices	Responses	
はい	94.91%	205
いいえ	5.09%	11
	Answered	**216**
	Skipped	**0**



※【数字＋アルファベットの大文字／小文字】で8桁のパスワードを構成した場合、約218兆どおりの組合せとなります。最低でもこの位の強度を保つように日頃から注意しましょう。

■ パスワードは定期的に変更していますか？

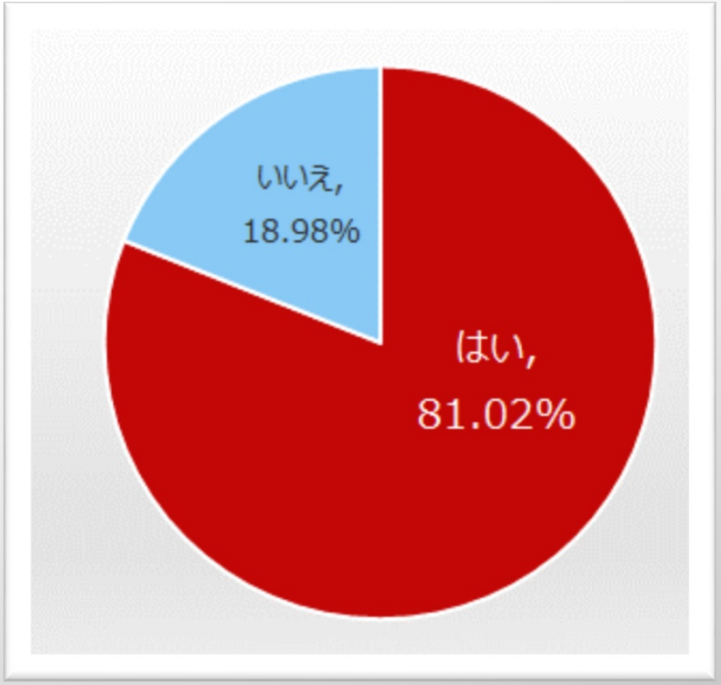
Answer Choices	Responses	
行っている（1か月に１回以上）	0.47%	1
行っている（半年に１回以上）	7.48%	16
行っている（１年に１回以上）	6.54%	14
行っている（不定期、気になった時など）	57.48%	123
行っていない	27.10%	58
その他（具体的に）	0.93%	2
	Answered	**214**
	Skipped	**2**



2018年3月に総務省から「パスワードの定期的な変更は不要」である旨の注意喚起が行われました。定期的に変更することでパスワードの作り方がパターン化することや、フレーズの使い回しをすることが問題であるとのことです。
定期的な変更よりは、サービスごとに固有のパスワードを設定し、かつ、一定の強度を持った内容（文字数や文字種を増やす）で設定することを心掛けましょう。

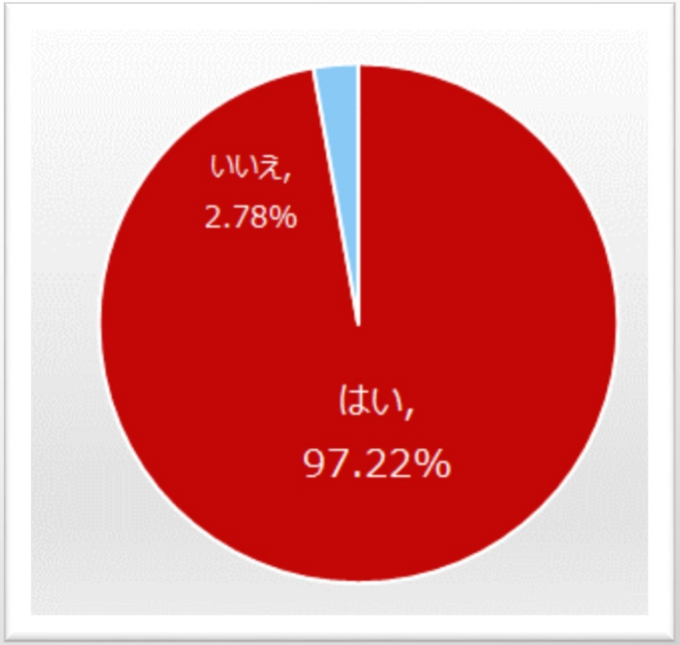
■ 利用サイト毎にパスワードを使い分けていますか？

Answer Choice:	Responses	
はい	81.02%	175
いいえ	18.98%	41
	Answered	**216**
	Skipped	**0**



■ パスワードは、第三者の目に触れないよう管理していますか？

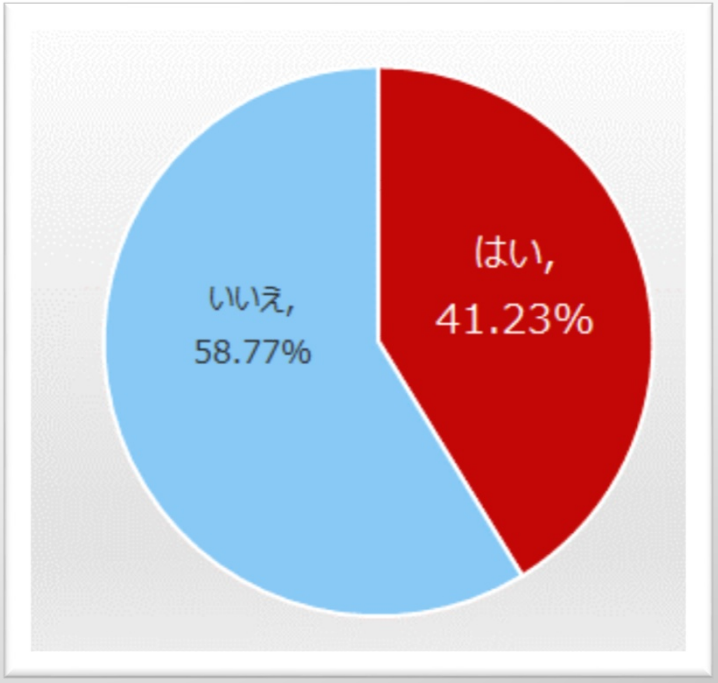
Answer Choice	Responses	
はい	97.22%	210
いいえ	2.78%	6
	Answered	**216**
	Skipped	**0**



※デスク周り、引き出し等にメモを貼ることはやめましょう。

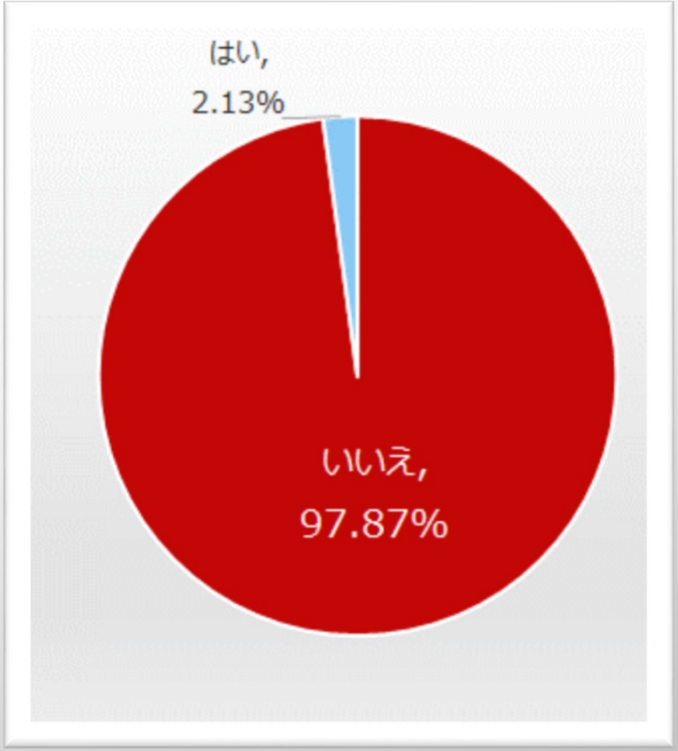
■ 業務の必要上、業務に関係する情報（非電子化情報も含む）を学外へ持ち出したことがありますか？

Answer Choice:	Responses	
はい	41.23%	87
いいえ	58.77%	124
	Answered	**211**
	Skipped	**5**



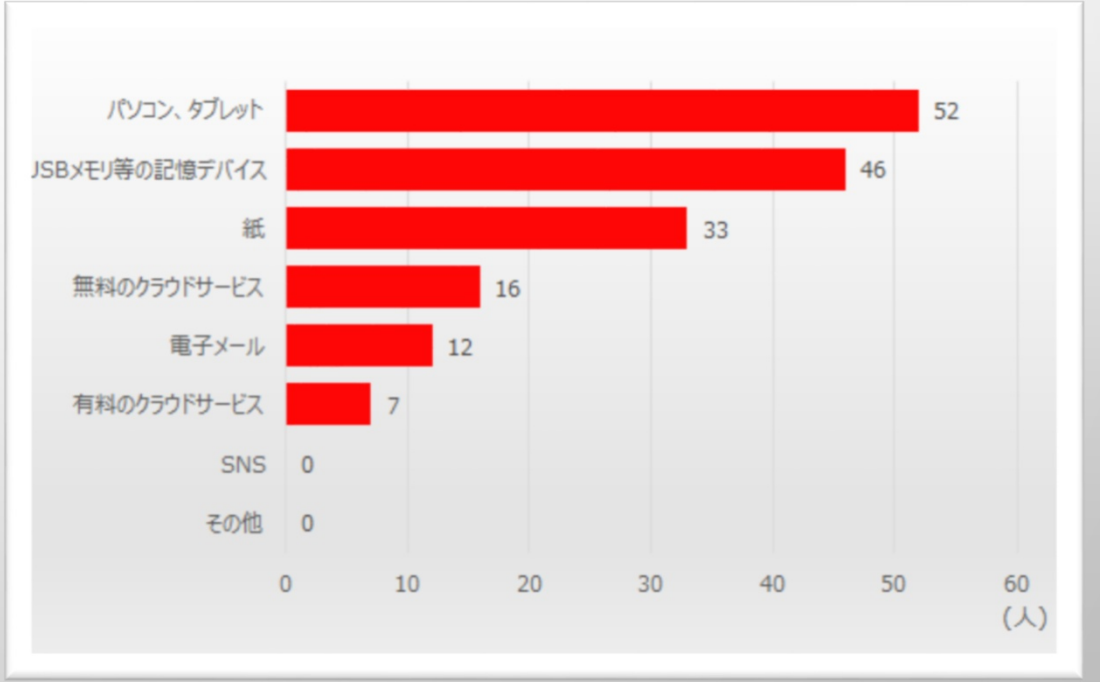
■ 前問（Q.8）で「はい（持ち出したことがある）」と答えた人のみ回答してください。外部に持ち出した情報を紛失したことがありますか？

Answer Choices	Responses	
いいえ	97.87%	92
はい	2.13%	2
「はい」の場合は具体的な内容を記載してください。		2
	Answered	**94**
	Skipped	**122**



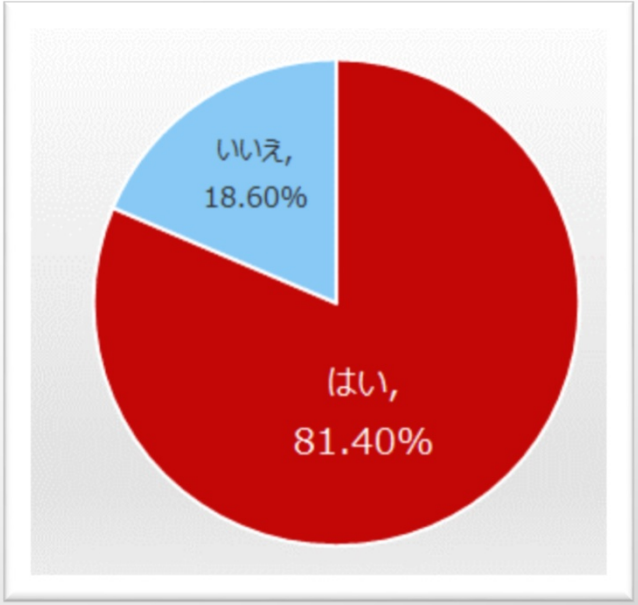
■ Q.8で「はい（持ち出したことがある）」と答えた人のみ回答してください（複数回答可）。持ち出した情報の媒体・方法は何ですか？

Answer Choices	Responses	
パソコン、タブレット	60.47%	52
USBメモリ等の記憶デバイス	53.49%	46
紙	38.37%	33
無料のクラウドサービス（オンラインストレージ、Gmail フリー版などのwebメールも含みます）	18.60%	16
電子メール（プロバイダと契約をして利用しているアカウントが対象です）	13.95%	12
有料のクラウドサービス（オンラインストレージ、Gmail ビジネス版などのwebメールも含みます）	8.14%	7
SNS	0.00%	0
その他	0.00%	0
その他（具体的に）		1
	Answered	**86**
	Skipped	**130**



■ 前問（Q.8）で「はい（持ち出したことがある）」と答えた人のみ回答してください。持ち出した情報は、暗号化等の適切なセキュリティ対策を行いましたか？

Answer Choices	Responses	
はい	81.40%	70
いいえ	18.60%	16
	Answered	**86**
	Skipped	**10**



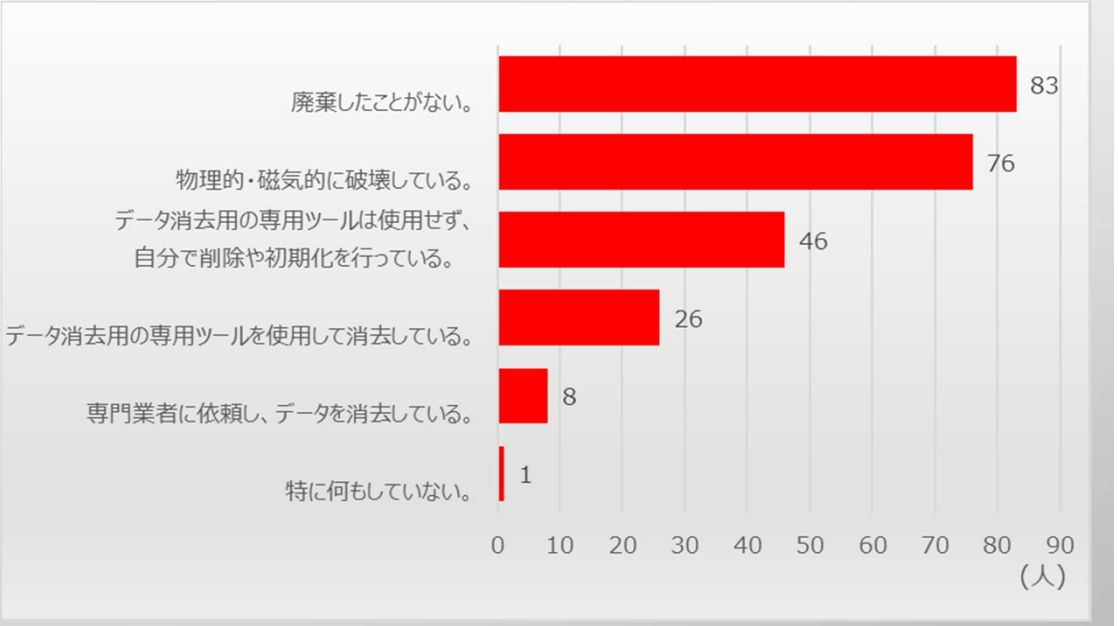
Answer Choices	Responses	
デバイスの起動・使用自体にパスワードを設定している	59.30%	51
データ自体を暗号化（パスワード付き）している	30.23%	26
データへのアクセスにパスワードを設定している	24.42%	21
データにアクセスする通信を暗号化している	11.63%	10
データ・資料を入れるバッグ等に施錠している	3.49%	3
上記以外の場合、具体的な方法を記入してください	5.81%	5
	Answered	**86**
	Skipped	**130**

具体的な方法

- ドライブやフォルダをキーファイルによって暗号化している
- データの暗号化（EFS 機能の利用）
- 自身の研究内容なので紛失しても問題ない
- 個人情報については基本的に持ち出さないことにしている
- 記憶デバイスは財布などに入れ管理している。

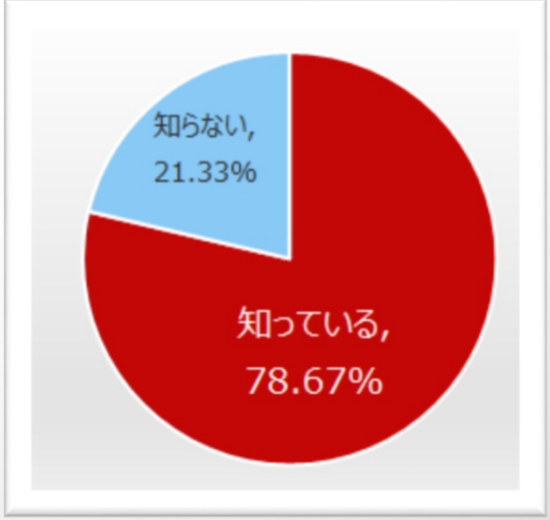
■ PC,記憶デバイス等を廃棄する場合は、記録されているデータを『完全に消去』していますか（複数回答可）？

Answer Choices	Responses	
廃棄したことがない。	40.10%	83
物理的・磁気的に破壊している。	36.71%	76
データ消去用の専用ツールは使用せず、自分で削除や初期化を行っている。	22.22%	46
データ消去用の専用ツールを使用して消去している。	12.56%	26
専門業者に依頼し、データを消去している。	3.86%	8
特に何もしていない。	0.48%	1
上記以外の方法で行っている場合は、具体例を記入してください。		0
	Answered	**207**
	Skipped	**9**



■ 情報セキュリティインシデントに直面した場合の連絡先を知っていますか？

Answer Choice	Responses	
知っている	78.67%	166
知らない	21.33%	45
	Answered	**211**
	Skipped	**5**



「知っている」回答者が選択した連絡先(複数回答)

Answer Choices	Responses	
学術情報課　情報システム係	49.29%	104
情報処理センター	26.54%	56
各部門の情報セキュリティ専門部会員	23.70%	50
総務課　総務係	7.11%	15
具体的な部署名を記入してください	1.42%	3
	Answered	**211**
	Skipped	**5**

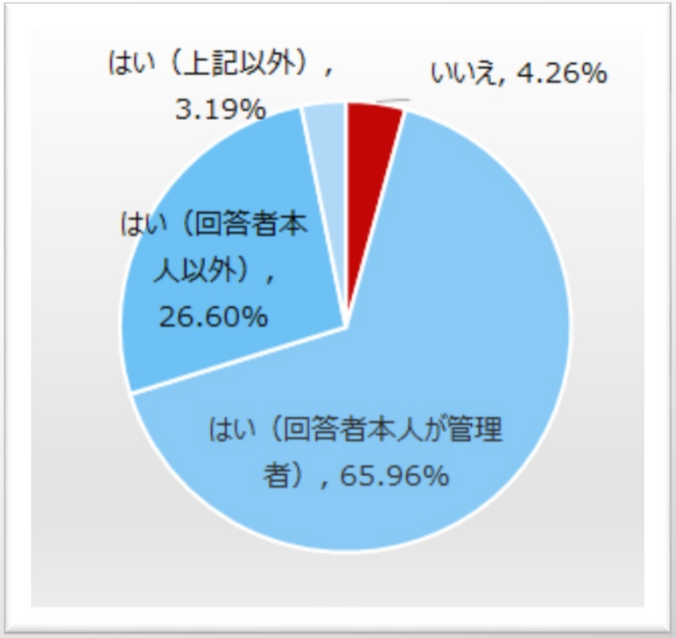
正しい連絡先は、以下のいずれかとなります。

- 学術情報課情報システム係
- 情報処理センター
- 最寄りの情報セキュリティ専門部会員

具体的な部署名：情報セキュリティ専門部会（CSIRT部門）、事務局情報システム係、まずは課内のパソコンリーダー，情報セキュリティー専門部会員（機械専攻担当）

■ 研究室等に設置してあるPCの管理者を設定していますか？

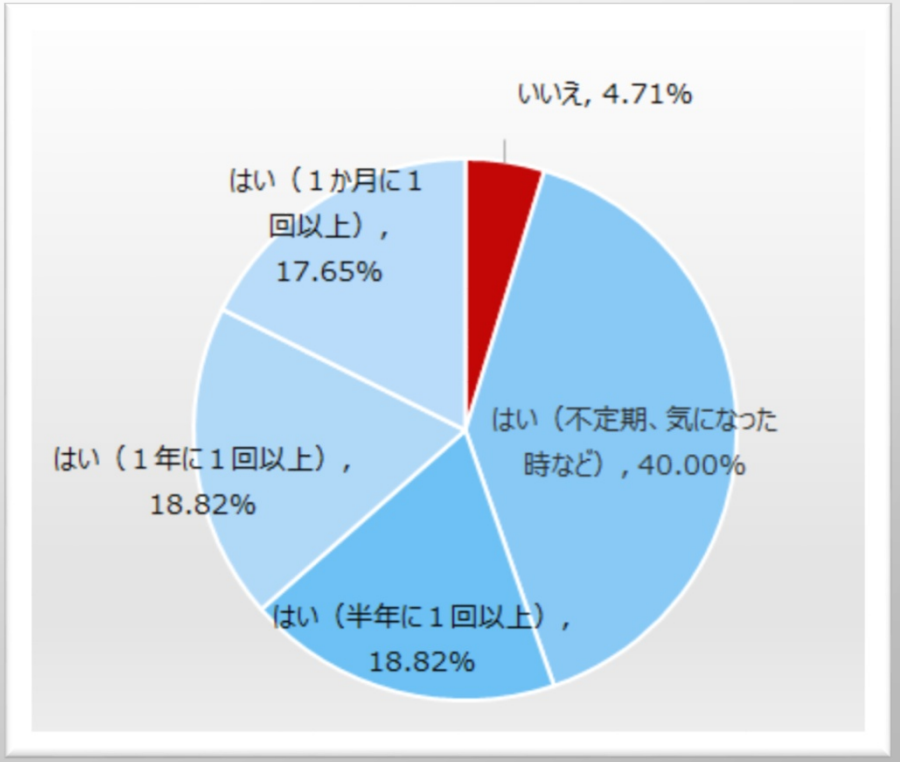
Answer Choices	Responses	
はい（回答者本人が管理者）	65.96%	62
はい （回答者本人以外で研究室や専攻内の教職員）	26.60%	25
はい（上記以外） 具体的な管理者を記入してください	3.19%	3
いいえ	4.26%	4
	Answered	**94**
	Skipped	**122**



具体的な管理者：技術職員、施設課職員、各機器利用の学生

■ 研究室等に設置してあるPCや無線LANルータの管理・使用状況（OSのアップデート、ウェブへの公開状況、CMSツールの管理、セキュリティ対策ソフトの更新状況、用途外プログラムのインストール状況等）を定期的に確認していますか？（管理者を回答者本人以外に設定している場合は、これらの報告を定期的に受けていますか？）

Answer Choices	Responses	
はい（不定期、気になった時など）	40.00%	34
はい（半年に１回以上）	18.82%	16
はい（１年に１回以上）	18.82%	16
はい（１か月に１回以上）	17.65%	15
いいえ	4.71%	4
その他 (具体的に)	0.00%	0
	Answered	**85**
	Skipped	**131**



■ まとめ

研究室等で管理している学外公開サーバに対する管理状況の緊急自己点検（2017年1月実施）の内容を受け、今年度は学外公開を行っているセキュアードサーバ（一部）に対して、外部機関によるセキュリティ監査を実施いたしました。幸いにも重大な脆弱性は検出されませんでしたが、一部のサーバにおいてクロスサイトスクリプティングの脆弱性、内部情報を含んでいると思われるコンテンツの学外公開等の脆弱性が検出されました。本学には100台以上の学外公開サーバがありますので、これらのサーバに対して引き続き計画的にセキュリティ監査を行っていきます。サーバ等のデバイス管理については、昨年度と大きな変化はありませんでしたが、頻度や強度はまだ向上できる余地はあります。

今年度の調査で目立った点としましては、パスワードを強化している方が、前年度比7ptの上昇となっています。パスワードに関連した事項として、今期は総務省等から「パスワードの定期的な変更は不要」との注意喚起が行われ、大きな転換期となりました。今まで推奨されていた定期的な変更は、パスワードの作り方のパターン化やフレーズの使い回しを助長するため、かえって安全性の低下を招くとのことです。この観点からも、パスワードの強度が全体的に上がっていることはとても良いことです。

次にデータを持ち出す際の取扱いについて、暗号化など適切な方法で対応する方が昨年度比6.4ptの上昇となっています。万が一のことを考え、多くの教職員の意識が向上していると思われます。

三点目としては、インシデント等の発生時に連絡する窓口を正しく理解されている方が、前年度比26.5ptも上昇しました。今は防ぐだけでなく、実際に起こってしまうことを想定し、対処することが求められています。「連絡先」はその一歩目ですので、広く理解いただけていることは、その後の対応をスムースにする効果があると考えられます。

情報セキュリティに関しまして、引き続き御協力をよろしくお願いいたします。

学内専用　情報セキュリティのページ：http://www.nagaokaut.ac.jp/j/gakunai/security/security-top.html