平成30年度
情報セキュリティ意識調査

回答まとめ（2019.4）

実施日：2019/2/22～3/15

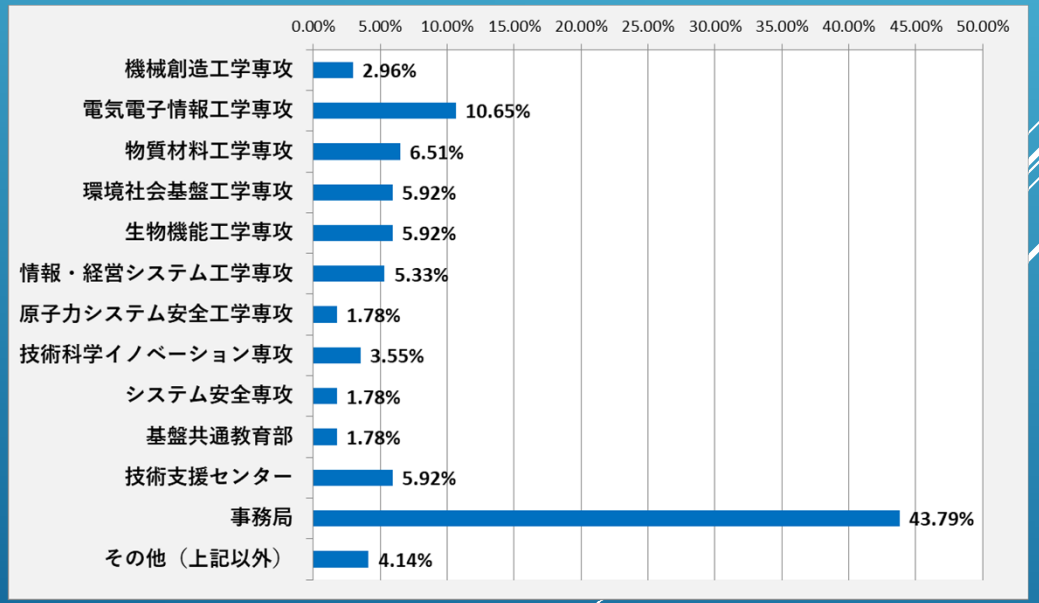
回答数：169人　**回答割合**32.82%

（役職員数　2019/2/28**現在：**515**人）**

（※監事、学生、非常勤講師、休職者除く）

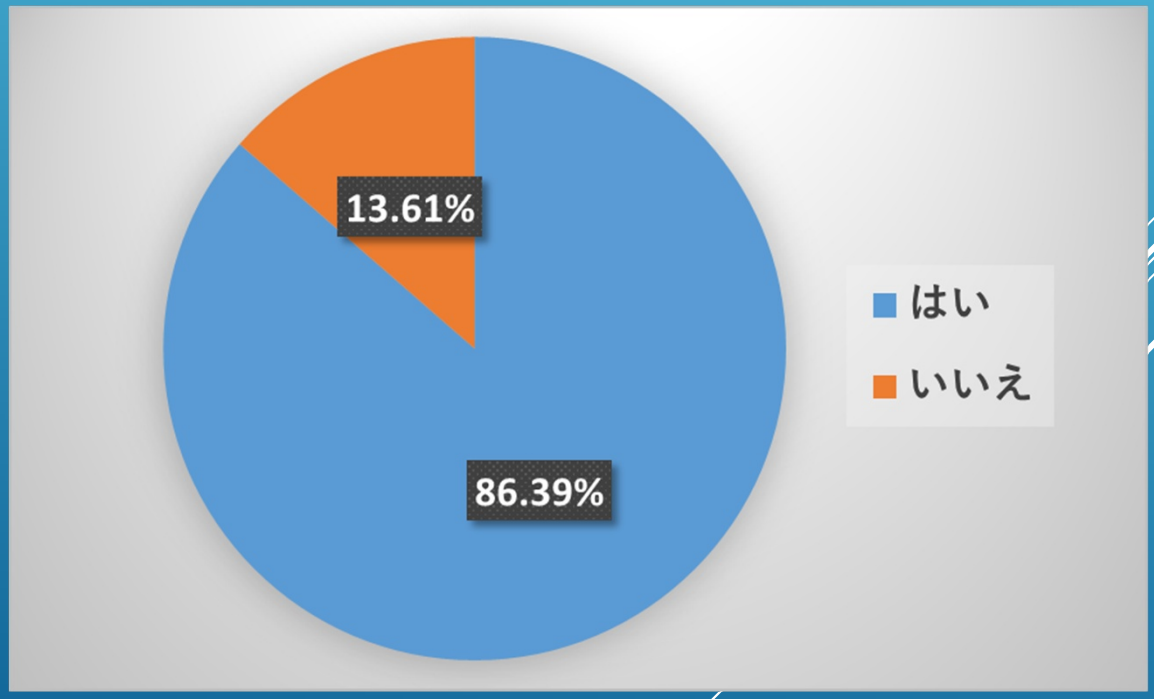
■ 所属を選択してください。

所属	回答率	回答数
機械創造工学専攻	2.96%	5
電気電子情報工学専攻	10.65%	18
物質材料工学専攻	6.51%	11
環境社会基盤工学専攻	5.92%	10
生物機能工学専攻	5.92%	10
情報・経営システム工学専攻	5.33%	9
原子力システム安全工学専攻	1.78%	3
技術科学イノベーション専攻	3.55%	6
システム安全専攻	1.78%	3
基盤共通教育部	1.78%	3
技術支援センター	5.92%	10
事務局	43.79%	74
その他（上記以外）	4.14%	7
合計	100.00%	169



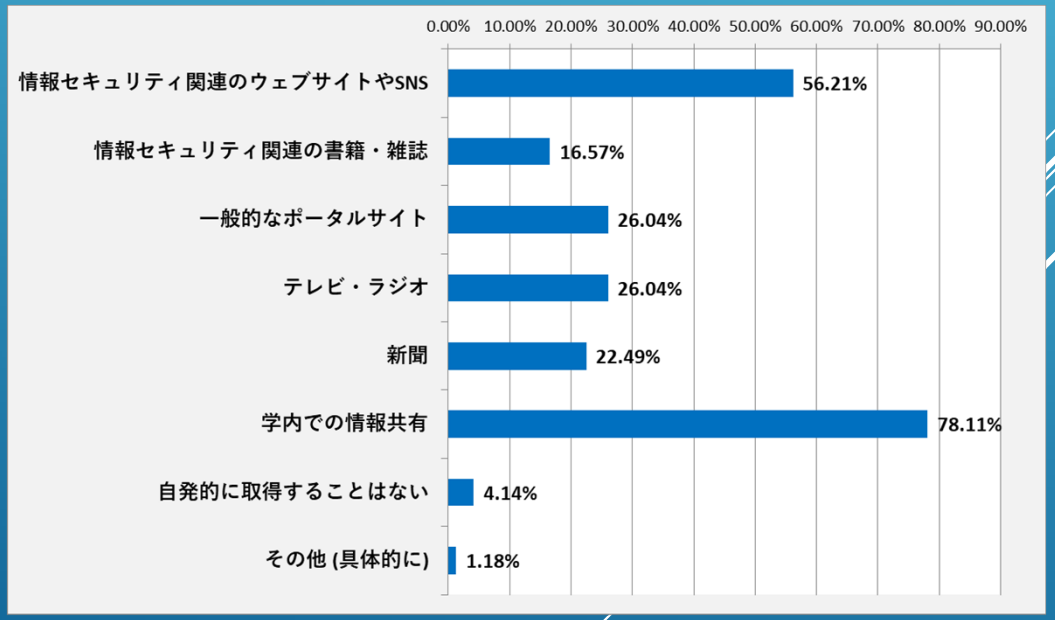
■「長岡技術科学大学　情報セキュリティ管理運用の取扱い」を読んだことがありますか？

回答	回答率	回答数
はい	86.39%	146
いいえ	13.61%	23
合計	100.00%	169



■ 情報セキュリティに関する知識や情報は主にどのように取得していますか？（複数選択可）

回答	延べ回答率	延べ回答数
情報セキュリティ関連のウェブサイトやSNS	56.21%	95
情報セキュリティ関連の書籍・雑誌	16.57%	28
一般的なポータルサイト	26.04%	44
テレビ・ラジオ	26.04%	44
新聞	22.49%	38
学内での情報共有	78.11%	132
自発的に取得することはない	4.14%	7
その他 (具体的に)	1.18%	2
合計（延べ）	100.00%	169

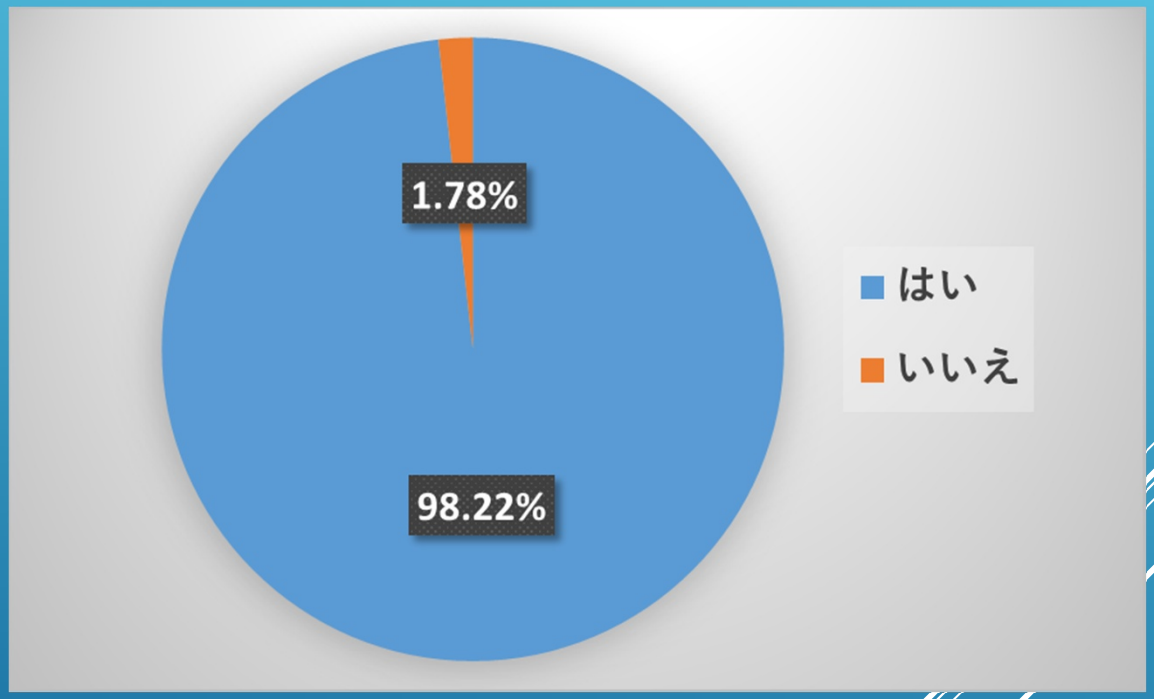


その他（具体的な方法）

- twitterでの収集、外部組織からのメイルでのお知らせなどデータの暗号化（EFS 機能の利用）
- Facebookにおける情報セキュリティ関連を専門とする「友達」からの情報

■ 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？

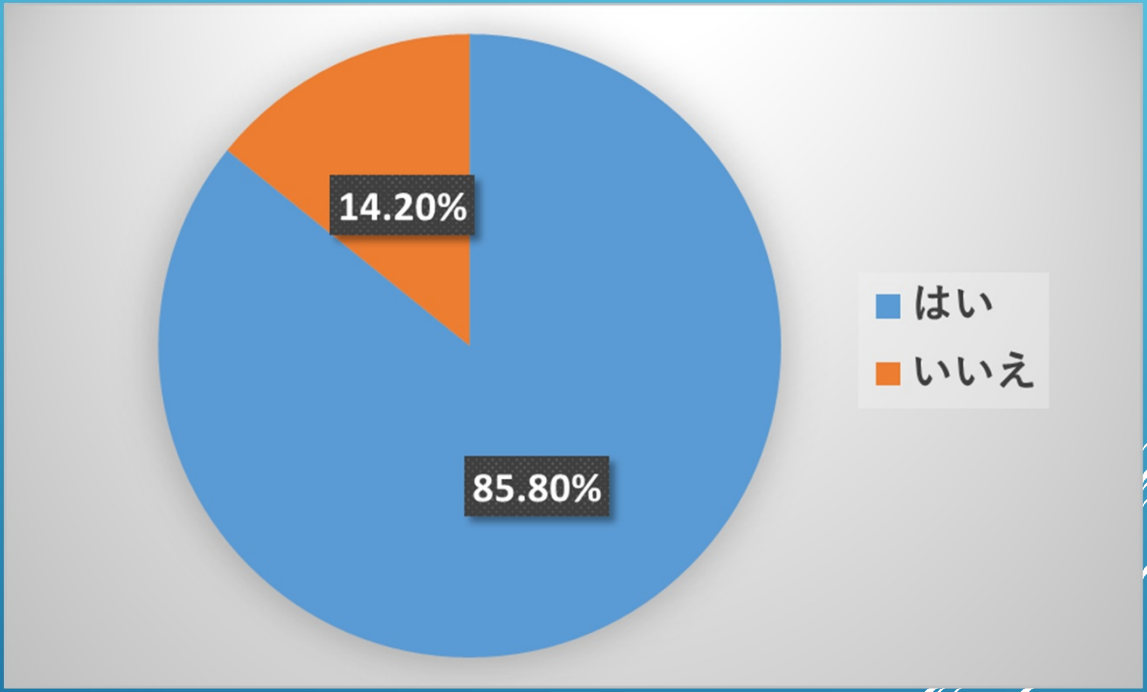
回答	回答率	回答数
はい	98.22%	166
いいえ	1.78%	3
合計	100.00%	169



※【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。

■ 利用サイト毎にパスワードを使い分けていますか？

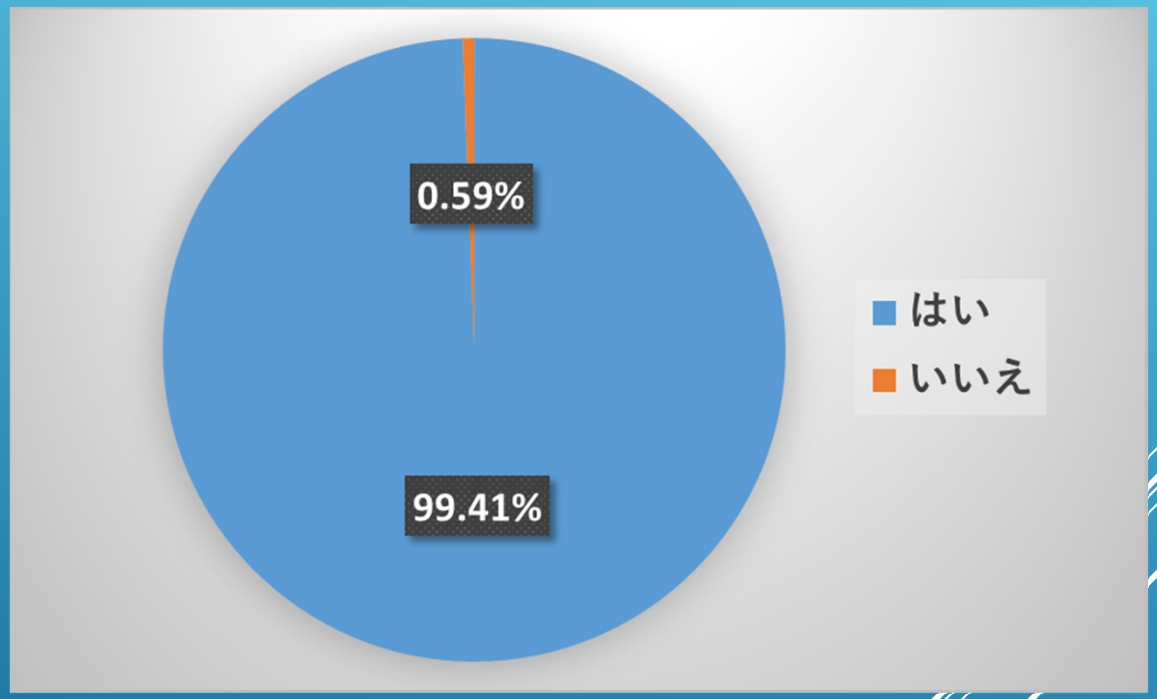
回答	回答率	回答数
はい	**85.80%**	**145**
いいえ	**14.20%**	**24**
合計	100.00%	169



※同じパスワードを使い回していると、もし漏えいしてしまった場合に同じパスワードを利用している全てのサイトを悪用される恐れがありますので、可能な限り使い分けるようにしましょう。

■ 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？

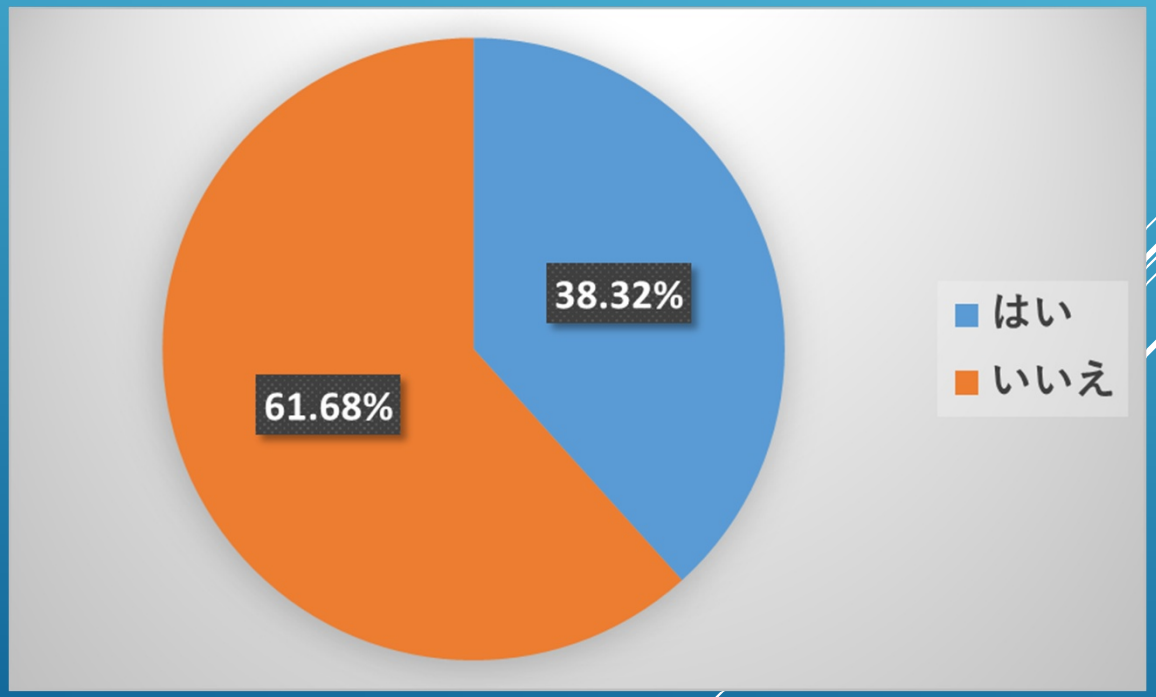
回答	回答率	回答数
はい	**99.41%**	**168**
いいえ	**0.59%**	**1**
合計	100.00%	169



※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。

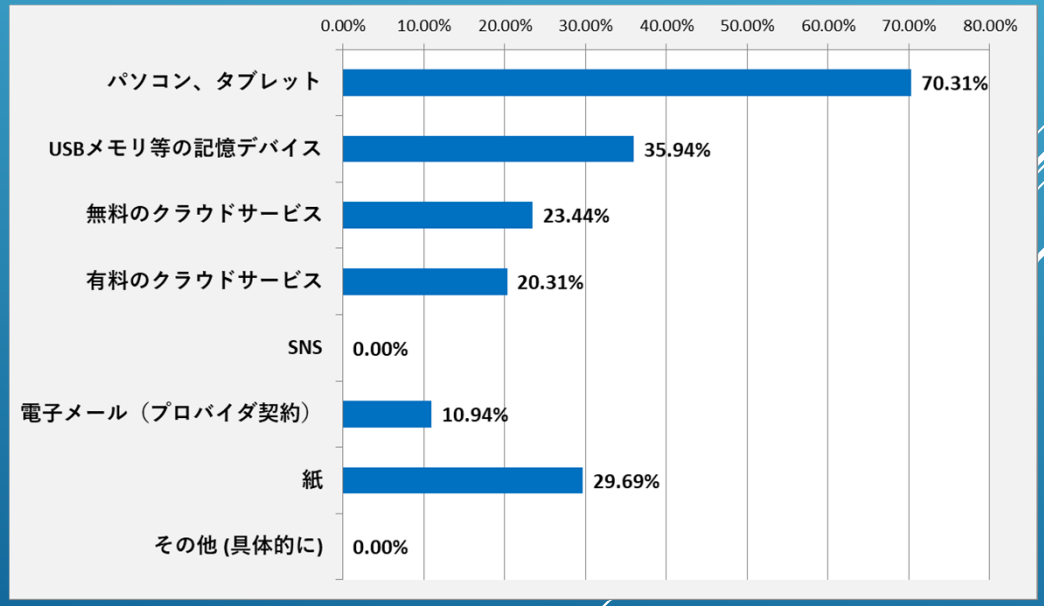
■ 今年度本調査時点において、業務の必要上、業務に関係する情報（非電子化情報も含む）を学外へ持ち出したことがありますか？

回答	回答率	回答数
はい	**38.32%**	**64**
いいえ	**61.68%**	**103**
合計	100.00%	167
未回答		2



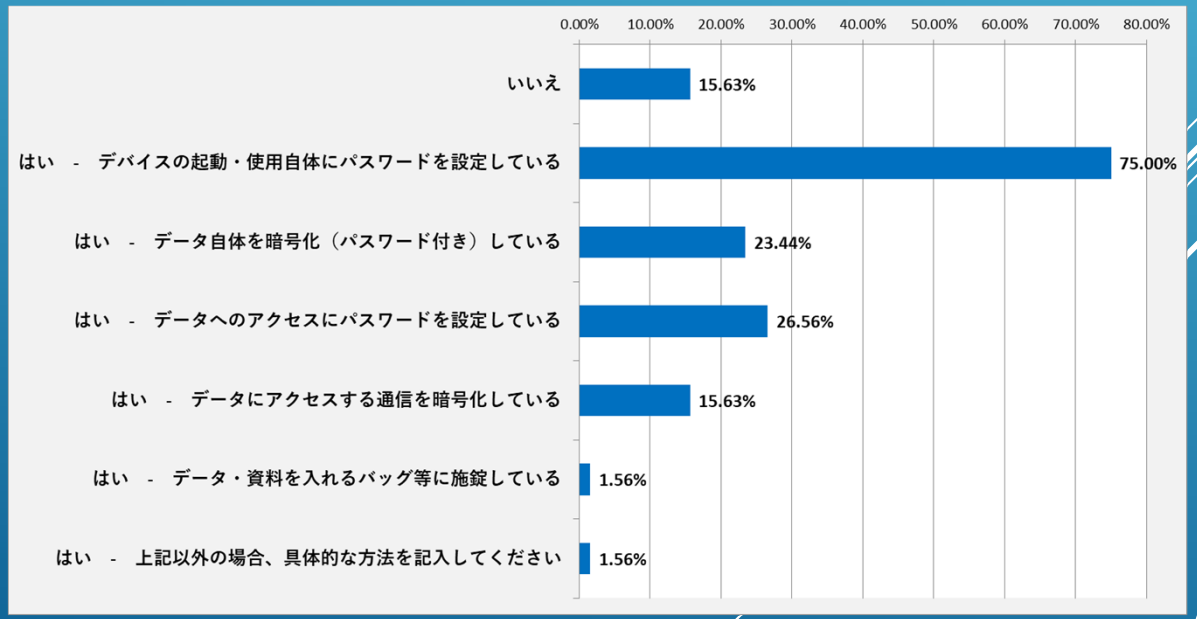
■ ※Q.8で「はい（持ち出したことがある）」と答えた人のみ回答してください（複数回答可）。持ち出した情報の媒体・方法は何ですか？

回答	延べ回答率	延べ回答数
パソコン、タブレット	70.31%	45
USBメモリ等の記憶デバイス	35.94%	23
無料のクラウドサービス	23.44%	15
有料のクラウドサービス	20.31%	13
SNS	0.00%	0
電子メール（プロバイダ契約）	10.94%	7
紙	29.69%	19
その他 (具体的に)	0.00%	0
合計（延べ）	37.87%	64
未回答		105



■ ※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？（複数回答可）

回答	延べ回答率	延べ回答数
いいえ	15.63%	10
はい　-　デバイスの起動・使用自体にパスワードを設定している	75.00%	48
はい　-　データ自体を暗号化（パスワード付き）している	23.44%	15
はい　-　データへのアクセスにパスワードを設定している	26.56%	17
はい　-　データにアクセスする通信を暗号化している	15.63%	10
はい　-　データ・資料を入れるバッグ等に施錠している	1.56%	1
はい　-　上記以外の場合、具体的な方法を記入してください	1.56%	1
合計（延べ）	37.28%	63
未回答		106

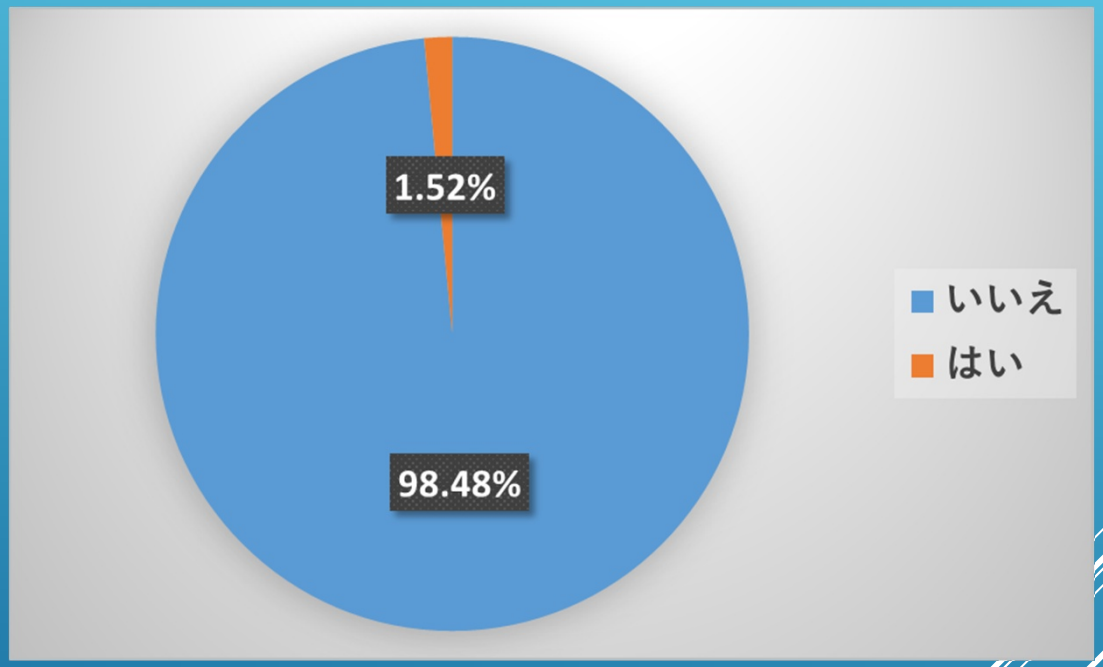


その他（具体的な方法）

- ハードディスクドライブの暗号化

■ ※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？

回答	回答率	回答数
いいえ	**98.48%**	**65**
はい	**1.52%**	**1**
合計	100.00%	66
未回答		103



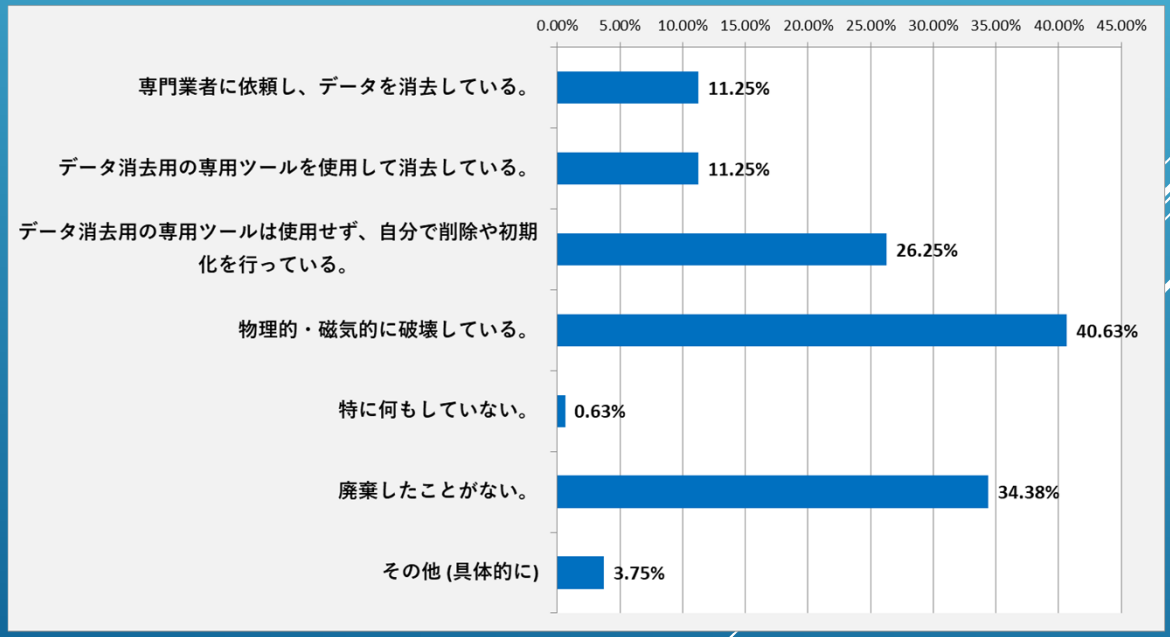
※外部に情報を持ち出す場合は、パスワード設定、暗号化、施錠、PC等にできるだけ情報を保存しないようにする（クラウドストレージの活用）等、セキュリティ対策を適切に行い、万が一情報を紛失しても被害を最小限に抑えることができるようにしましょう。

■ 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）？

回答	延べ回答率	延べ回答数
専門業者に依頼し、データを消去している。	**11.25%**	**18**
データ消去用の専用ツールを使用して消去している。	**11.25%**	**18**
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。	**26.25%**	**42**
物理的・磁気的に破壊している。	**40.63%**	**65**
特に何もしていない。	**0.63%**	**1**
廃棄したことがない。	**34.38%**	**55**
その他 (具体的に)	**3.75%**	**6**
合計（延べ）	94.67%	160
未回答		9

その他（具体的な方法）

- FD,CD,DVDに保存したデータは学内のシュレッダーで物理的に破壊し、HDD等は学内の機密情報廃棄の時に出している
- 機密保持契約を交わした回収業者により回収物品は直ちに物理的に破壊される
- 大学所定の廃棄日に所定の方法で廃棄している
- 大学が契約している業者に引き渡す
- 完全消去に不安があるため、詳しい人（教員）に消去を依頼している
- 上記範疇を越えていないが、PC廃棄の場合、HDDを取り出した上で別々に廃棄している

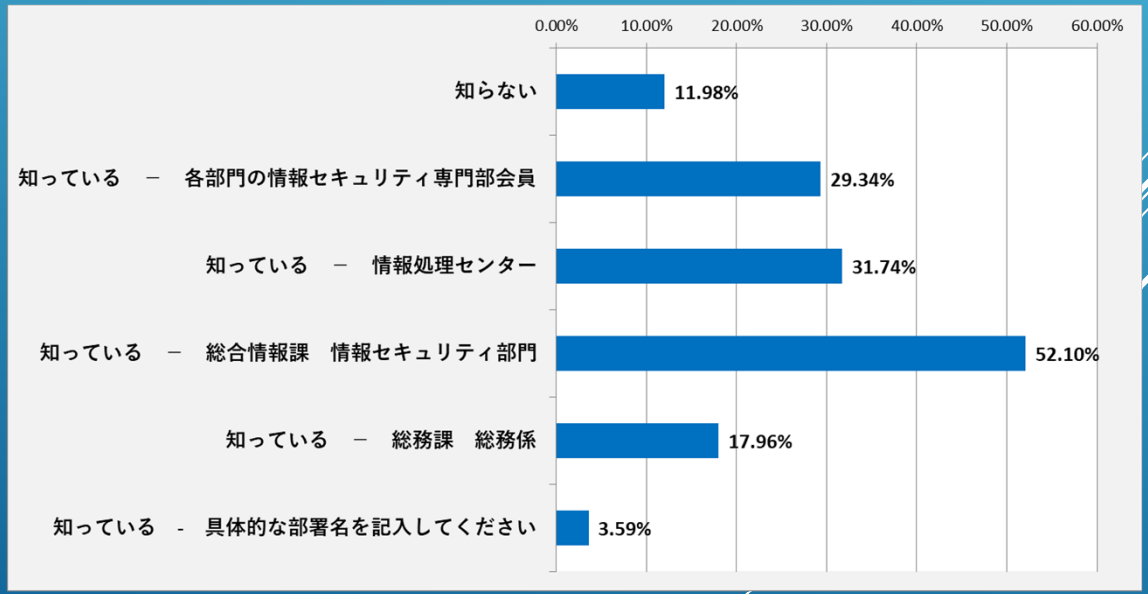


■ 情報セキュリティインシデントに直面した場合の連絡先を知っていますか？（複数回答可）

回答	延べ回答率	延べ回答数
知らない	11.98%	20
知っている　－　各部門の情報セキュリティ専門部会員	29.34%	49
知っている　－　情報処理センター	31.74%	53
知っている　－　総合情報課　情報セキュリティ部門	52.10%	87
知っている　－　総務課　総務係	17.96%	30
知っている　-　具体的な部署名を記入してください	3.59%	6
合計（延べ）	98.22%	166
未回答		3

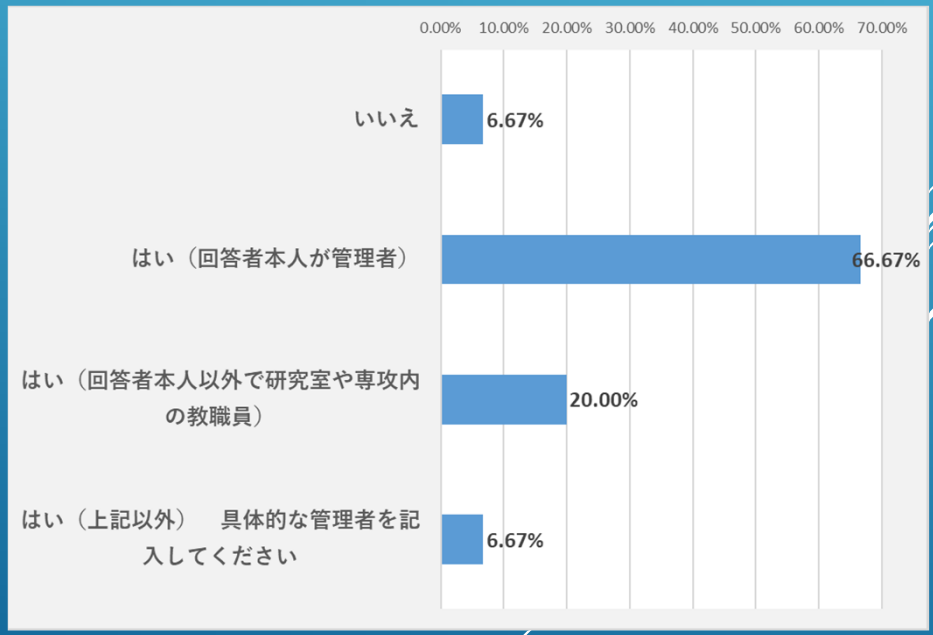
具体的な部署名等

- 所属専攻の技術職員
- 直属の上司、他社の担当業務で直面した場合は当該他者。想定経路によって連絡先が異なるのでは。
- 最高情報セキュリティ責任者
- 上長（雇用者）
- 下記に従う（http://www.nagaokaut.ac.jp/j/gakunai/security/security_taiou.pdf）
- 情報処理センター長および総合情報課



■ ※該当する教員の方は回答してください。研究室等に設置してあるPCや無線LANルータの管理者を設定していますか？

回答	回答率	回答数
いいえ	6.67%	5
はい（回答者本人が管理者）	66.67%	50
はい（回答者本人以外で研究室や専攻内の教職員）	20.00%	15
はい（上記以外）　具体的な管理者を記入してください	6.67%	5
合計	100.00%	75
未回答		94

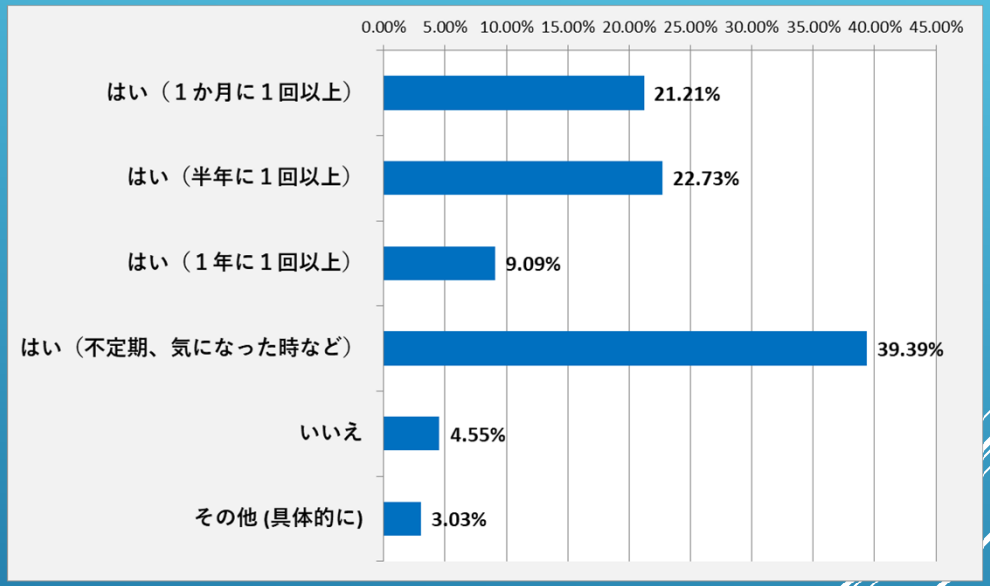


具体的な部署名等

- 所属課長
- 研究室の情報担当の学生
- 研究室の教員
- 所属学生の中の１名
- 秘書

■ ※該当する教員の方は回答してください。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に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？）

回答	回答率	回答数
はい（１か月に１回以上）	21.21%	14
はい（半年に１回以上）	22.73%	15
はい（１年に１回以上）	9.09%	6
はい（不定期、気になった時など）	39.39%	26
いいえ	4.55%	3
その他 (具体的に)	3.03%	2
合計	100.00%	66
未回答		104

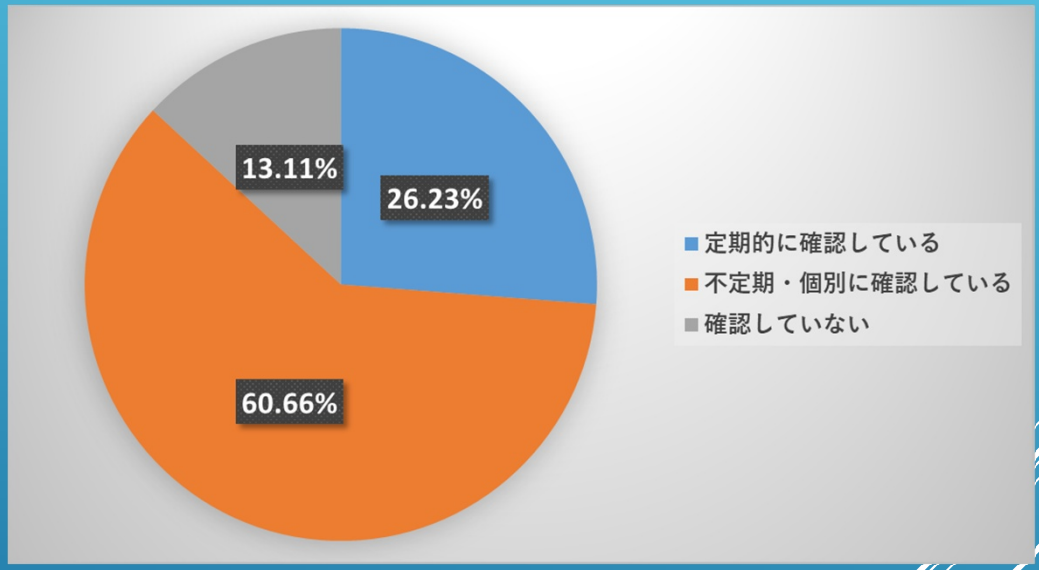


具体的な部署名等

- 学内無線LANシステムについては毎日利用者情報の集計を行っているが、個別のアクセスポイントについては、利用者が限定される状況であり、定期的な確認は行っていない
- わからない

■ ※該当する教員の方は回答してください。研究室等において、学生が学内LANに接続して使用するPCについて、セキュリティ対策ソフトが設定されていることを確認していますか？

回答	回答率	回答数
定期的に確認している	26.23%	16
不定期・個別に確認している	60.66%	37
確認していない	13.11%	8
合計	100.00%	61
未回答		109

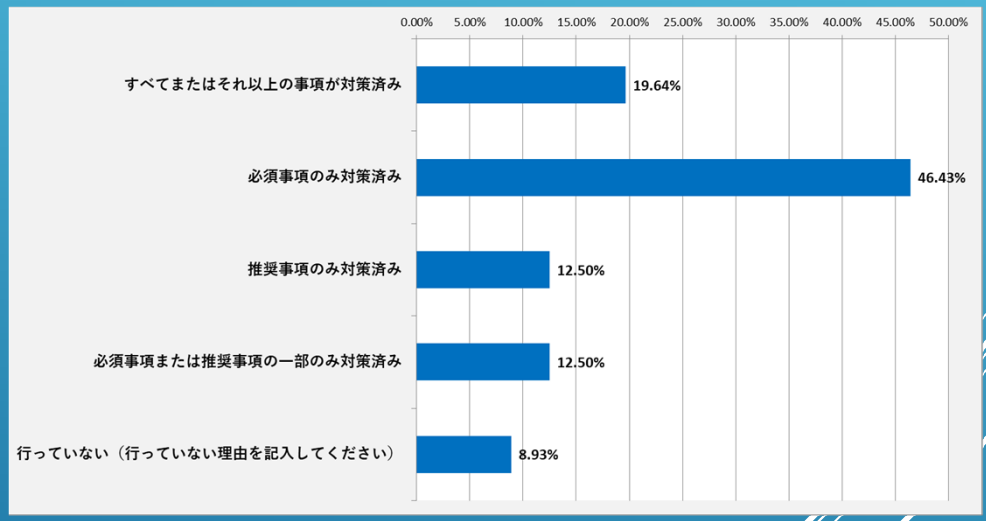


※セキュリティ対策ソフトが設定されていないPCを学生が使用している例が見受けられます。
PCの購入状況に従って、以下のとおり対策ソフトの設定をお願いいたします。
・公費で購入したPC：情報処理センターで管理しているセキュリティ対策ソフトの運用
・個人で購入したPC：個人で購入したソフトやフリーソフト等の運用または併用

■ ※該当する教員の方は回答してください。自身の居室や研究室に無線LANルータを設置している場合、情報セキュリティ強化のため「無線LANルータの取扱い」に規定している対策を行っていますか？

回答	回答率	回答数
すべてまたはそれ以上の事項が対策済み	19.64%	11
必須事項のみ対策済み	46.43%	26
推奨事項のみ対策済み	12.50%	7
必須事項または推奨事項の一部のみ対策済み	12.50%	7
行っていない（行っていない理由を記入してください）	8.93%	5
合計	100.00%	56
未回答		114

※行っていない理由は全て、無線LAN不設置または不使用



※2017年12月に「学内LANで使用する無線LANルータの取扱いについて（CISO決裁）」が教職員に対して注意喚起されています。「無線LANルータの取扱い」については学内専用ページ「情報ネットワーク・情報セキュリティの取扱い」を参照してください。

■ 今年度調査に関するまとめ

昨年度に引き続き、今年度も学外公開を行っているセキュアードサーバの一部に対して、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古いOSやミドルウェア等の使用、SSLの脆弱な暗号化方式の使用といった脆弱性が検出されました。来年度以降も引き続き計画的にセキュリティ監査を行っていきます。

今年度の調査で目立った点としては、「デバイスの起動・使用自体にパスワードを設定している」という回答が前年度比約15ptの上昇となっています。パスワードに関するセキュリティ対策の実施度が上がっていることは良いことです。

次に、持ち出した情報の媒体・方法について、「有料のクラウドサービスの使用」の回答が前年度比約12ptの上昇となっています。昨年末に、本学では外部に持ち出した情報の紛失が発生しました。本件を受けて、同様の案件に対するセキュリティ対策のひとつとして、本調査終了後に、主に教員を対象とするDropbox Businessの運用を開始しましたが、今後は、万が一の紛失に備え、同サービスが活用されることを期待しております。

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：
https://www.nagaokaut.ac.jp/gakunai/designated/security-top/security-top.html