

令和3年度情報セキュリティ意識調査 所属別・役職別回答率

長岡技術科学大学総合情報課 2022/3/17

所属別回答率

所属	回答者数	対象者数	対象者回答率
事務局	180	199	90.5%
大学戦略課	18	18	100.0%
総合情報課	13	14	92.9%
研究・地域連携課	21	22	95.5%
総務課	36	41	87.8%
財務課	25	27	92.6%
施設課	7	8	87.5%
学務課	20	23	87.0%
学生支援課	19	23	82.6%
入試課	8	8	100.0%
国際課	11	13	84.6%
監査室	2	2	100.0%
専攻等	216	255	84.7%
機械創造工学専攻	25	32	78.1%
電気電子情報工学専攻	32	34	94.1%
物質材料工学専攻	27	32	84.4%
環境社会基盤工学専攻	26	30	86.7%
生物機能工学専攻	18	21	85.7%
情報・経営システム工学専攻	22	27	81.5%
原子力システム安全工学専攻	15	16	93.8%
技術科学イノベーション専攻	24	31	77.4%
システム安全工学専攻	14	17	82.4%
基盤共通教育部	13	15	86.7%
技術支援センター	30	31	96.8%
その他	32	36	88.9%
合計	458	521	87.9%

役職別回答率

役職	回答者数	対象者数	対象者回答率
事務職員（常勤）	108	114	94.7%
教員（常勤・非常勤含む）	176	213	82.6%
技術職員	28	29	96.6%
非常勤職員	119	134	88.8%
派遣職員	10	11	90.9%
その他	17	20	85.0%
合計	458	521	87.9%

※Q1～3は所属・役職・氏名の設問のため割愛

Q4. 本調査以前に、「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？（必須回答） ※情報ネットワーク・情報セキュリティの取扱いのページ（本学公式ホームページ内 学内アクセス限定） https://www.nagaokaut.ac.jp/gakunai/designated/security-top/security-top.html 情報セキュリティ規則関係 → 国立大学法人長岡技術科学大学 情報セキュリティ管理運用の取扱い		はい		いいえ						合計		
回答数		371		87						458		
回答率		81.0%		19.0%						100.0%		
Q5. パスワードは十分な複雑さ（長さ・文字の種類）※を設定していますか？（必須回答） ※目安は、【数字+アルファベットの大文字／小文字】を10桁です。		はい		いいえ						合計		
回答数		422		36						458		
回答率		92.1%		7.9%						100.0%		
Q6. 業務上利用しているシステム、サイト、端末毎にパスワードを使い分けていますか？（必須回答）		はい		いいえ						合計		
回答数		387		71						458		
回答率		84.5%		15.5%						100.0%		
Q7. パスワードは第三者の目に触れないように管理していますか？（必須回答）		はい		いいえ						合計		
回答数		457		1						458		
回答率		99.8%		0.2%						100.0%		
Q8. PC、記録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？（必須回答・複数選択可）		大学が定期的 に実施する 不用品等 廃棄にお いて廃棄 している	情報システム棟（旧情報 処理センター建物）の ハードディスククラッ シャー(HDD消去装置） 等を使用して消去してい る	専門業者に依頼し、デー タを消去している	データ消去用の専用ツール を使用して消去してい る	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	物理的・磁氣的に破壊し ている	特に何もしていない	廃棄したことがない	その他	延数合計	
延べ回答数		213	10	2	12	17	28	10	165	5	458	
延べ回答率		46.5%	2.2%	0.4%	2.6%	3.7%	6.1%	2.2%	36.0%	1.1%	100.0%	
その他（具体的回答）		先生にご相談したのち対応いたします										
		いまのところ機会がないです。										
		事務局1号棟印刷室のシュレッダーを切り替えて利用している										
		保存している										
		大切なデータは扱っていないPCのみを廃棄										
Q9. 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（内線番号やEメールアドレス）を知っていますか？（必須回答・複数選択可）		知らない	各専攻等の情報セキュリ ティ専門部会員	総合情報センターネット ワークインフラ部門（旧 情報処理センター）	総合情報課 情報セキュ リティ担当	総務課 総務係	その他					延数合計
延べ回答数		72	161	62	147	12	6					458
延べ回答率		15.7%	35.2%	13.5%	32.1%	2.6%	1.3%					100.0%
その他（具体的回答）		課のパソコンリーダーに相談										
		学生支援課										
		監査室に相談										
		所属研究室教員										
		上司										
		先生に相談したのち対応いたします										
Q10. 2021年4月1日以降に、在宅勤務を実施しましたか？（必須回答）		はい			いいえ						合計	
回答数		223			235						458	
回答率		48.7%			51.3%						100.0%	

【Q10. で「はい」と回答した場合】 Q11. 在宅勤務用端末に対して他人から画面が覗き見られないように対応※していますか？（必須回答） ※覗き見防止フィルタの貼付、離席時のスクリーンロック等。	はい	いいえ		合計
回答数	200	23		223
回答率	89.7%	10.3%		100.0%
【Q10. で「はい」と回答した場合】 Q12. 在宅勤務用端末は、他人と共有して使わないようにしていますか？（必須回答）	はい	いいえ		合計
回答数	215	8		223
回答率	96.4%	3.6%		100.0%
【Q10. で「はい」と回答した場合】かつ【Q12. で「いいえ」と回答した場合】 Q13. 在宅勤務用端末を他人と共有して使わざるを得ない場合は、業務用のユーザやアカウントを別途作成していますか？（必須回答）	はい	いいえ		合計
回答数	8	0		8
回答率	100.0%	0.0%		100.0%
【Q10. で「はい」と回答した場合】 Q14. 在宅勤務で利用する自宅のルータやモバイルWiFi等は、WiFiのセキュリティ方式として「WPA2」またはこれよりも新しい規格※を利用していますか？（必須回答・単一選択） ※最近「WPA2」より後に策定されたものとして、「WPA3」も登場しています。	はい	いいえ	わからない	合計
回答数	170	2	51	223
回答率	76.2%	0.9%	22.9%	100.0%
【Q10. で「はい」と回答した場合】 Q15. 在宅勤務用端末に機密情報を保管しなければならない場合※には、ファイル暗号化（パスワード設定等）を実施していますか？（必須回答・単一選択）※在宅勤務用端末のローカル（内蔵HDD等）に直接ファイルを保存する場合であり、クラウドストレージや学内で業務上利用しているファイルサーバ等に保存する場合は対象外です。	はい	いいえ	在宅勤務用端末には機密情報を保管していない	合計
回答数	68	11	144	223
回答率	30.5%	4.9%	64.6%	100.0%
Q16. Web会議を主催※したことがありますか？（必須回答） ※Zoom、Google Meet、Microsoft Teams等のWeb会議システムを利用した会議の予約、参加者への会議情報の通知等。	はい	いいえ		合計
回答数	268	190		458
回答率	58.5%	41.5%		100.0%
【Q16. で「はい」と回答した場合】 Q17. Web会議の開始時および途中参加者が出た際に、参加者の本人確認を実施していますか？（必須回答）	はい	いいえ		合計
回答数	188	80		268
回答率	70.1%	29.9%		100.0%
【Q16. で「はい」と回答した場合】 Q18. Web会議にアクセスするためのURLや会議参加のパスワードを不要なメンバーに伝えないようにしていますか？（必須回答）	はい	いいえ		合計
回答数	266	2		268
回答率	99.3%	0.7%		100.0%

【Q16. で「はい」と回答した場合】 Q19. Web会議の開催中に、必要に応じて不適切な参加者を退出させるなどし、会議を適切に進行していますか？（必須回答）	はい		いいえ	不適切な参加者に出会ったことがない	合計
回答数	67		1	200	268
回答率	25.0%		0.4%	74.6%	100.0%
Q20. 本調査や学内の情報セキュリティについて、御意見やコメント等がありましたら、お答えください。（任意回答）	具体的回答				合計
回答数	13				13
回答率	100.0%				100.0%
その他（具体的回答）	eduromeやSolitonといったネットワーク利用システムのアカウント情報を知っていることから、容易に外部から学内システムにアクセスする方法を知っている。そのため、自身のPCやスマートフォン等機器からアクセスをしないよう、セキュリティマインドを意識し続けていく所存である。				
	いつもご指導いただき、有り難うございます。助かっています。今後とも、どうぞ、宜しくお願い申し上げます。				
	クラウドストレージとしてはdropboxの方が、googleドライブより使い易いと感じる（公開期限の設定等、アクセス権限を細かく設定出来るため、またthunderbirdの自動リンクのアドオンがgoogleドライブはないため）、メール添付のが、全構成員がアクセス出来るのはgoogleドライブなので、例えば、授業の打ち合わせでも、技術職員の方が関わる学生実験等では、googleドライブを使わざるを得ないといった問題がある。学生は別として、全職員がdropboxを使える様にした方がよいのではと思う。				
	こうしたアンケートは、回答者に面倒ではありますが、意識を高めることにもつながるので、必要だと思います。ありがとうございます。 アンケートの項目は、送信者のメールアドレスを確認しているかや、なにかあったときの連絡先を検索などせずにすぐに連絡を取れるようにしているか（番号をPCの前に貼っている等々）、より具体的なことを確認してもよいかなと思います。 また実際にあった事例などの紹介も兼ねたアンケート項目にしてもいいかなあと。				
	例： 〇〇大学では、△△といったメールが届き・・・といったことがありましたが、これについて知っていますか？またこの事例を聞いて、なにか対応を取られましたか？				
	みたいな質問ということです。				
	なにか問題が起こった時に、どこに連絡すればよいのか、わかりやすいリンクを貼ったページがあるとうれしいです。				
	パスワードの管理に苦慮しています。業務用と個人用を分けていますが、数がどんどん多くなってきて、忘れないように、混同しないようにするのがたいへんです。どのように管理するのが、適切でしょうか。				
	プロキシがなくなって使いやすくなったとのことで、良かったです。				
	わからないことがあったときは教えてください。よろしく願いいたします。				
	情報元を一元化し、大学ホームページトップからアクセスできるようにしてほしい。				
	色々と難しく全部をフォローしきれないというのが本音です。				
	適切な管理であると思われる。				
	必要十分な処置をお願いします。				
	便利になった反面、大きな危険性をかかえてしまったことは、あまり知られてない（自分とは無関係と感じる）と思います。情報セキュリティに対するリスクマネジメント等は物凄く重要であり、担当者は時間を取られますし、高度な知識やスキルが必要だと思いますし、大変ですね...				