令和6年度
情報セキュリティ意識調査
集計結果

2025年3月31日
長岡技術科学大学情報セキュリティ専門部会
機密性2A（学内限定）

2024情報セキュリティ意識調査_集計

設問番号	質問	選択肢	対象者数	回答	回答率
1	所属を選択してください。	1.機械系	37	27	73.0%
		2.電気電子情報系	39	37	94.9%
		3.情報・経営システム系	23	19	82.6%
		4.物質生物系	45	39	86.7%
		5.環境社会基盤系	27	26	96.3%
		6.量子原子力系	19	15	78.9%
		7.システム安全系	23	19	82.6%
		8.技術科学イノベーション系	35	28	80.0%
		9.基盤共通教育系	17	13	76.5%
		合計	265	223	84.2%
		10.技術支援センター	25	23	92.0%
		合計	25	23	92.0%
		11.大学戦略課　企画広報室	7	7	100.0%
		12.大学戦略課　国際・高専連携戦略室	18	17	94.4%
		13.総合情報課	16	14	87.5%
		14.総合情報課　基金・卒業生室	2	2	100.0%
		15.産学連携・研究推進課	25	22	88.0%
		16.産学連携・研究推進課　地域共創室	12	11	91.7%
		17.総務課	20	18	90.0%
		18.総務課　人事労務室	21	17	81.0%
		19.財務課	29	24	82.8%
		20.施設課	10	10	100.0%
		21.学務課	27	24	88.9%
		22.学生支援課	26	25	96.2%
		23.入試課	8	7	87.5%
		24.監査室	3	3	100.0%
		合計	224	201	89.7%
		25.その他	34	27	79.4%
		合計	34	27	79.4%
		累計	1062	921	86.7%
2	役職を選択してください。	1.役員	6	2	33.3%
		2.教員（常勤・非常勤を含む）	213	176	82.6%
		3.技術職員（常勤・再雇用を含む）	25	23	92.0%
		4.事務職員（常勤・再雇用を含む）	131	120	91.6%
		5.URA・UEA	10	10	100.0%
		6.非常勤職員（事務補佐員・技術補佐員・研究支援者・秘書等）	144	126	87.5%
		7.派遣職員	17	15	88.2%
		8.その他	2	2	100.0%
		累計	548	474	86.5%

2024情報セキュリティ意識調査_集計

大区分	中区分	設問番号	質問	選択肢	対象者数	回答	回答率
情報セキュリティの意識に関する設問		4	本学の情報システムを利用した情報発信は、学内にとどまらず、社会へ広く伝達される可能性があり、法令遵守など責任を持った行動をとられなければならないことを認識していますか？	はい	474	473	99.8%
				いいえ	474	1	0.2%
		5	法令遵守にあたっては、本学情報セキュリティポリシー※1や関連法令※2があることを認識し、内容を理解※3しようと心がけていますか？	はい	474	472	99.6%
				いいえ	474	2	0.4%
		6	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？	はい	474	404	85.2%
				いいえ	474	70	14.8%
		7	パスワードは十分な長さと複雑さ※を設定していますか？（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	474	450	94.9%
				いいえ	474	24	5.1%
		8	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？	はい	474	474	100.0%
				いいえ	474	0	0.0%
		9	二段階認証やワンタイムパスワード等のアカウント認証の強化策が提供されている場合は、可能な限り利用していますか。	はい	474	469	98.9%
				いいえ	474	5	1.1%
		10	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？（複数選択可）	大学が定期的に実施する不用物品等廃棄において廃棄している	474	252	53.2%
				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	474	39	8.2%
				専門業者に依頼し、データを消去している	474	7	1.5%
				データ消去用の専用ツールを使用して消去している	474	31	6.5%
				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	474	43	9.1%
				物理的・磁気的に破壊している	474	96	20.3%
				特に何もしていない	474	4	0.8%
				廃棄したことがない	474	184	38.8%
		11	情報セキュリティインシデントのリスクが高いと考える事例を選択してください。（複数選択可）	誤送信や誤共有による情報漏えい	474	457	96.4%
				マルウェア感染	474	360	75.9%
				悪意ある第三者による不正アクセスや不正使用	474	350	73.8%
				システムやネットワークの踏み台としての悪用	474	239	50.4%
				なりすまし（フィッシングやアカウント乗っ取りなど）	474	324	68.4%
				データの改ざん（不正な変更によるリスク）	474	235	49.6%
				データの破壊（意図的な破損や消去）	474	195	41.1%
				データの喪失（アクセス不能、バックアップ不足、操作ミスによる消失など）	474	268	56.5%
				内部者による不正行為（情報の持ち出し、意図的な漏えいなど）	474	292	61.6%
				無線LANやVPNの不適切な使用	474	278	58.6%
				ソフトウェアやシステムの脆弱性の悪用	474	280	59.1%
		12	そのほか、情報セキュリティインシデントのリスクが高いと考える事例があれば記載してください。		474		0.0%
		13	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が記載されている緊急対応図があることを知っていますか？	知っている	474	391	82.5%
				知らない	474	83	17.5%

2024情報セキュリティ意識調査_集計

大区分	中区分	設問番号	質問	選択肢	対象者数	回答	回答率
近年の学内におけるセキュリティ脅威や取組に関する設問	《障害に伴うデータ喪失の質問》	14	PC等のデバイスに保存した重要なデータを喪失したことはありますか？	はい	474	39	8.2%
				いいえ	474	435	91.8%
		15	データを喪失する原因として最もリスクが高いと考えるものは何だと思いますが？	人為的ミスによる誤削除・上書きなど	474	176	37.1%
				ハードウェアの故障	474	59	12.4%
				デバイスの紛失・盗難	474	214	45.1%
				ランサムウェア	474	24	5.1%
				上記以外	474	1	0.2%
		16	上記以外を選択した方は、データを喪失する原因として最もリスクが高いものを記載してください。		474		0.0%
		17	業務で利用するデータについてバックアップを行っていますか。	実施している（クラウド）	474	157	33.1%
				実施している（HDD・SSD）	474	144	30.4%
				実施している（ネットワークHDD（NASなど））	474	41	8.6%
				実施していないが検討している	474	28	5.9%
				実施していない	474	48	10.1%
				分からない	474	56	11.8%
	《偽セキュリティ警告（サポート詐欺）に関する質問》	18	18.上記のような警告画面が表示された場合、詐欺かもしれないと考えますか？	詐欺だと考える	474	322	67.9%
				状況によっては詐欺と考えてしまう	474	137	28.9%
				詐欺とは考えない	474	5	1.1%
				わからない	474	10	2.1%
		19	19.悪意のあるWebサイトを訪問した利用者に偽の警告画面を表示し、画面上に表示しているなりすましサポートセンターに電話をさせて金銭をだまし取る偽警告（サポート詐欺）を知っていますか。	内容を知っている	474	326	68.8%
				名前を聞いたことがある	474	126	26.6%
				内容も名前も知らない	474	22	4.6%
		20	偽警告（サポート詐欺）に遭遇したことはありますか？	はい（何度もある）	474	36	7.6%
				はい（1～2回ある）	474	125	26.4%
				わからない	474	11	2.3%
				いいえ	474	302	63.7%
	《セキュリティ啓発ポスターの関連質問》	21	身近なセキュリティ対策として取り組んでいるものを選んでください。（複数選択可）	不審なメールやサイトには注意する	474	464	97.9%
				部屋・机・ロッカーは施錠する	474	261	55.1%
				机の上はきれいにする	474	216	45.6%
				離籍の際はモニターロック（windowsの場合は［Windowsキー］＋［Lキー］）する	474	185	39.0%
				不要となった重要書類はシュレッダーする	474	368	77.6%
				ウィルス対策ソフトを利用する	474	301	63.5%
				ソフトウェアは常に最新の状態を保つ。	474	301	63.5%
				二段階認証・多要素認証を利用する	474	337	71.1%
		22	そのほか、身近なセキュリティ対策として取り組んでいることがあれば記載してください。		474		0.0%
		23	PC等のデバイスの盗難対策について取り組んでいるものを選んでください。（複数選択可）	部屋を不在にする場合は施錠する	474	381	80.4%
				暗号化されたUSBを利用する	474	71	15.0%
				重要な紙媒体は、施錠できる引き出しやキャビネットなどに保管する	474	257	54.2%
				デバイス本体に保存するデータは最小限としクラウドストレージを利用する	474	178	37.6%
				パソコンをワイヤーロックで固定する	474	53	11.2%
				定期的なバックアップを取得する	474	206	43.5%
		24	そのほか、PC等のデバイスの盗難対策について取り組んでいるものを選んでください。（複数選択可）		474		0.0%
	関心の高いセキュリティ脅威について確認	25	次のうち関心の高い情報セキュリティ脅威があれば選択してください。	ランサムウェアによる被害	474	261	55.1%
				サプライチェーンの弱点を悪用した攻撃	474	74	15.6%
				内部不正による情報漏えい等の被害	474	106	22.4%
				標的型攻撃による機密情報の窃取	474	183	38.6%
				不注意による情報漏えい等の被害	474	279	58.9%
				脆弱性対策情報の公開に伴う悪用増加	474	87	18.4%
				ビジネスメール詐欺による金銭被害	474	122	25.7%
				テレワーク等のニューノーマルな働き方を狙った攻撃	474	111	23.4%
				犯罪のビジネス化（アンダーグラウンドサービス）	474	95	20.0%
				上記以外	474	5	1.1%
		26	そのほか、関心の高い情報セキュリティ脅威があれば記載してください。		474		0.0%
足 補		27	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。		474		0.0%

令和6年度情報セキュリティ意識調査　集計結果　概要

・PC、記録デバイス等の廃棄には、**「大学が定期的に実施する不 用物品等廃棄」(53.2%)** が最も利用されている。

・インシデントリスクが高いと考えられている事案は、**「誤送信や誤共有による情報漏えい」(96.4%)** で、次点が**「マルウェア感染」(75.9%)**

・データ喪失の要因として最もリスクが高いと考えられているのは **「デバイスの紛失・盗難」(45.1%)** で、次点が**「人為的ミスによる誤削除・上書き」(37.1%)**

・**72.1%の人が業務で利用するデータのバックアップを取っており** 、最も利用されているのは**「クラウド」(33.1%)** で、次点が**「HDD・SSD」(30.4%)**

・サポート詐欺について**「内容を知っている」**と回答した人は**68.8%**であり、**「遭遇したことがある」**と回答した人は全体の**34%**となった。

・PC等のデバイスの盗難対策について最も取り組まれていることは、**「部屋を不在にする場合は施錠する」(80.4%)** 、次点で**「重要な紙媒体は施錠できる引き出しやキャビネットなどに保管する」(54.2%)** となった。

・最も関心の高い情報セキュリティ脅威は、**「不注意による情報漏えい等の被害」(58.9%)** で、次点で**「ランサムウェアによる被害」(55.1%)** であった。

調査内容

目的	本学が所有する情報資産の取扱方法や情報セキュリティに対する心構えについて、不適切な行為を未然に防ぎ、情報セキュリティ意識の更なる向上を目指す
対象	本学の全教職員（派遣職員等を含む）
変遷	平成25年度（2013年度）から毎年実施
実施期間	2025年2月3日（月）～2月28日（金）
実施方法	Googleフォーム
実施者	情報セキュリティ専門部会

回答状況（設問1～3） 所属別

所属	対象者	回答	回答率
系	265	223	84.2%
事務局	224	201	89.7%
技術支援センター	25	23	92.0%
その他	34	27	79.4%
合計	**548**	**472**	**86.1%**

回答状況（設問1～3） 所属別（教員）

選択肢	対象者数	回答	回答率
1.機械系	37	27	73.0%
2.電気電子情報系	39	37	94.9%
3.情報・経営システム系	23	19	82.6%
4.物質生物系	45	39	86.7%
5.環境社会基盤系	27	26	96.3%
6.量子原子力系	19	15	78.9%
7.システム安全系	23	19	82.6%
8.技術科学イノベーション系	35	28	80.0%
9.基盤共通教育系	17	13	76.5%
合計	265	223	84.2%

回答状況（設問1～3） 所属別（技術支援センター）

選択肢	対象者数	回答	回答率
10.技術支援センター	25	23	92.0%
合計	25	23	92.0%

回答状況（設問1～3） 所属別（事務局）

選択肢	対象者数	回答	回答率
11.大学戦略課　企画広報室	7	7	100.0%
12.大学戦略課　国際・高専連携戦略室	18	17	94.4%
13.総合情報課	16	14	87.5%
14.総合情報課　基金・卒業生室	2	2	100.0%
15.産学連携・研究推進課	25	22	88.0%
16.産学連携・研究推進課　地域共創室	12	11	91.7%
17.総務課	20	18	90.0%
18.総務課　人事労務室	21	17	81.0%
19.財務課	29	24	82.8%
20.施設課	10	10	100.0%
21.学務課	27	24	88.9%
22.学生支援課	26	25	96.2%
23.入試課	8	7	87.5%
24.監査室	3	3	100.0%
合計	224	201	89.7%

回答状況（設問1～3） 所属別（その他）

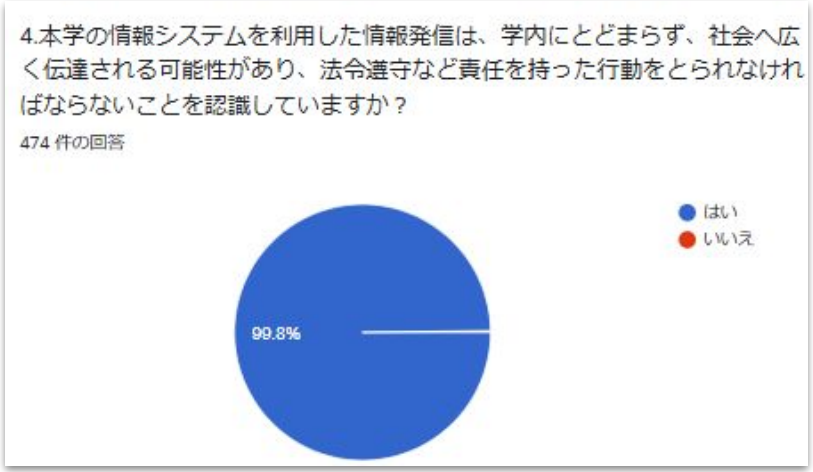
選択肢	対象者数	回答	回答率
25.その他	34	27	79.4%
合計	34	27	79.4%

回答状況（設問1～3） 役職別

選択肢	対象者数	回答	回答率
1.役員	6	2	33.3%
2.教員（常勤・非常勤を含む）	213	176	82.6%
3.技術職員（常勤・再雇用を含む）	25	23	92.0%
4.事務職員（常勤・再雇用を含む）	131	120	91.6%
5.URA・UEA	10	10	100.0%
6.非常勤職員（事務補佐員・技術補佐員・研究支援者・秘書等）	144	126	87.5%
7.派遣職員	17	15	88.2%
8.その他	2	2	100.0%
累計	548	474	86.5%

設問4

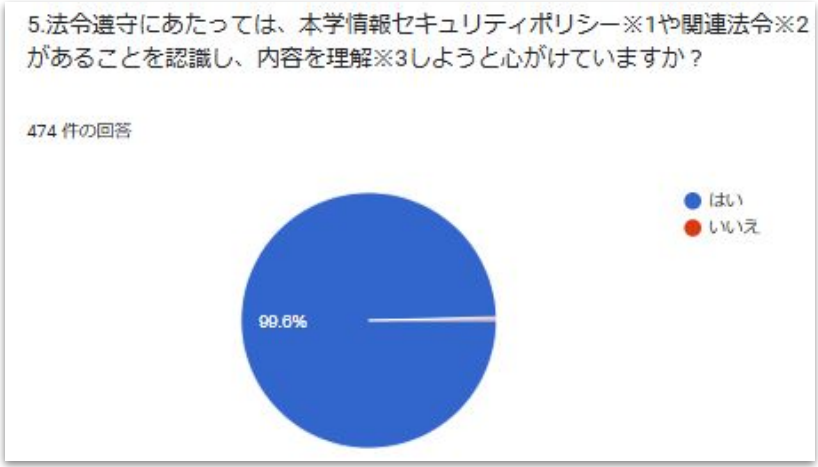
4.本学の情報システムを利用した情報発信は、学内にとどまらず、社会へ広く伝達される可能性があり、法令遵守など責任を持った行動をとられなければならないことを認識していますか？



99.8%の人が認識している と回答した。

設問5

5.法令遵守にあたっては、本学情報セキュリティポリシー※1や関連法令※2があることを認識し、内容を理解※3しようと心がけていますか？

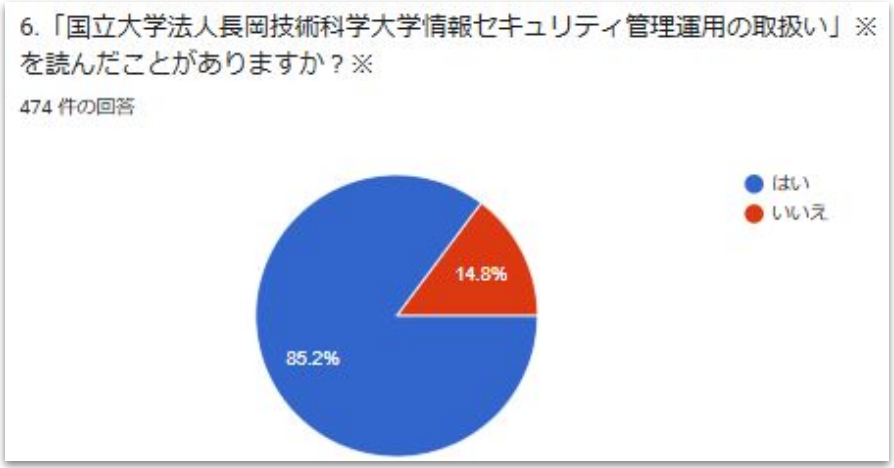


99.6%の人が内容を理解しようと心がけている　と回答した。

管理基本方針・管理基本規程・管理運用の取扱い

設問6

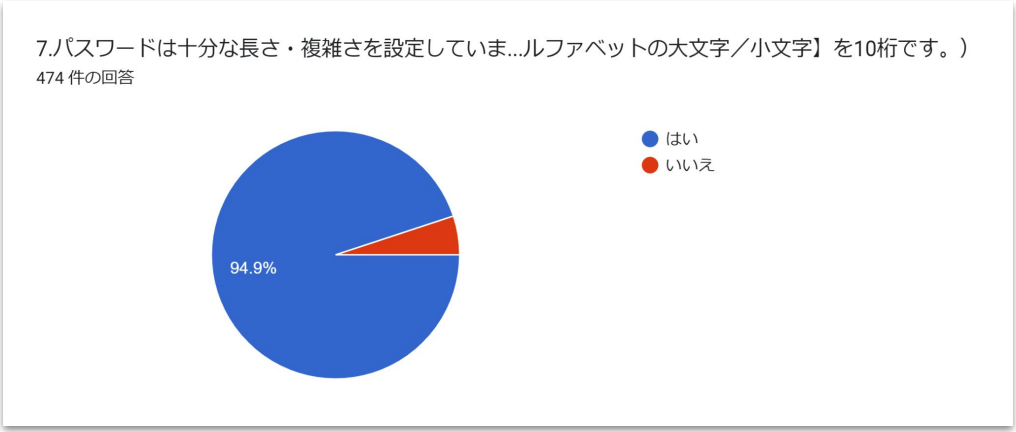
6.「国立大学法人長岡技術科学大学情報セキュリティ管理運用の取扱い」※を読んだことがありますか？※



セキュリティ管理運用の取扱いを読んだことがある人は**85.2%**となった。

設問7

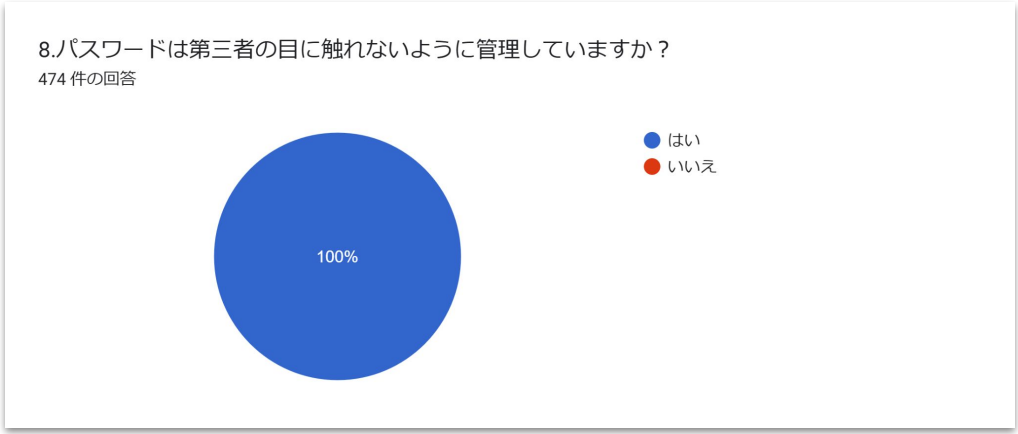
7.パスワードは十分な長さ・複雑さを設定していますか（目安は、【数字+アルファベットの大文字／小文字】を10桁です。）



94.9%の人がパスワードについて十分な長さ、複雑さを設定し　ていると回答した。

設問8

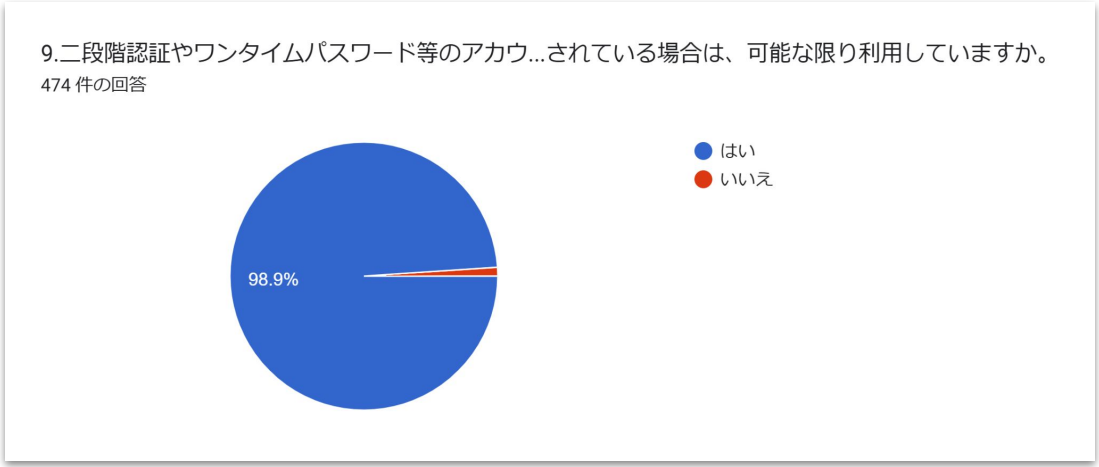
8.パスワードは第三者の目に触れないように管理していますか ？



パスワードは第三者の目に触れないように管理していると回答した人は100%　であった。

設問9

9.二段階認証やワンタイムパスワード等のアカウント認証の強化策が提供されている場合は、可能な限り利用していますか。



98.9%の方が二段階認証やワンタイムパスワード等のアカウント認証の強化策　を可能な限り利用していると回答した。

設問10

10. 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（複数選択可）

選択肢	回答	回答率
大学が定期的に実施する不用物品等廃棄において廃棄している	252	53.2%
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	39	8.2%
専門業者に依頼し、データを消去している	7	1.5%
データ消去用の専用ツールを使用して消去している	31	6.5%
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	43	9.1%
物理的・磁気的に破壊している	96	20.3%
特に何もしていない	4	0.8%
廃棄したことがない	184	38.8%

最も多い回答は**「大学が定期的に実施する不 用物品等廃棄において廃棄している」**であり、**53.2%** の人が回答した。

設問11

11.情報セキュリティインシデントのリスクが高いと考える事例を選択してください。（複数選択可）

選択肢	回答	回答率
誤送信や誤共有による情報漏えい	457	96.4%
マルウェア感染	360	75.9%
悪意ある第三者による不正アクセスや不正使用	350	73.8%
システムやネットワークの踏み台としての悪用	239	50.4%
なりすまし（フィッシングやアカウント乗っ取りなど）	324	68.4%
データの改ざん（不正な変更によるリスク）	235	49.6%
データの破壊（意図的な破損や消去）	195	41.1%
データの喪失（アクセス不能、バックアップ不足、操作ミスによる消失など）	268	56.5%
内部者による不正行為（情報の持ち出し、意図的な漏えいなど）	292	61.6%
無線LANやVPNの不適切な使用	278	58.6%
ソフトウェアやシステムの脆弱性の悪用	280	59.1%

最もリスクが高いと考えられているのは**「誤送信や誤共有による情報漏えい」**で**96.4%**の人が回答した。次点が**「マルウェア感染」**で**75.9%**の人が回答した。

設問12

12.そのほか、情報セキュリティインシデントのリスクが高いと考える事例があれば記載してください。

以下のような回答がありました。

📌 物理的リスク

- 盗難・紛失（PC、USBメモリ、スマホ）
- 施設の物理的セキュリティ不足
- 背後からの覗き見、公の場での機密会話

👥 人的リスク

- ITリテラシー・セキュリティ意識の低さ
- コンプライアンス意識不足
- ソーシャルエンジニアリングのリスク

💻 デバイス・メディア管理

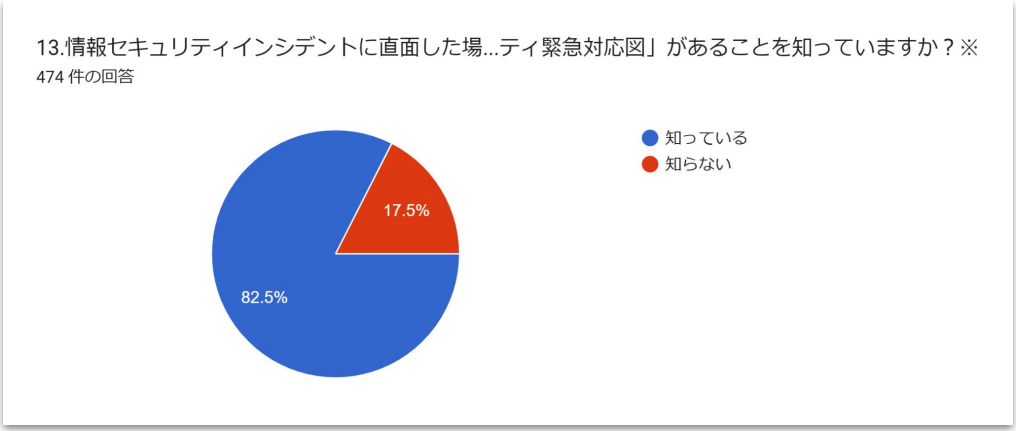
- PC・USBメモリの外部持ち出しリスク
- 情報を保存した媒体や書類の紛失
- USBメモリの管理不足

⚙️ システム・設定ミス

- クラウドの外部共有設定ミス
- パスワードの使い回し・漏洩
- OSの更新未実施、不用意なURLクリック

設問13

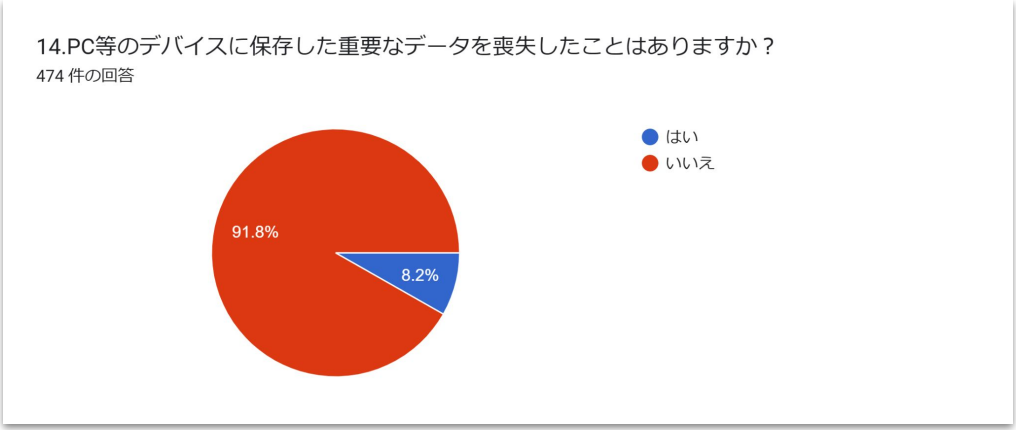
13.情報セキュリティインシデントに直面した場合の連絡先が記載されている「情報セキュリティ緊急対応図」があることを知っていますか？※



82.5%の人 が<u>セキュリティ緊急対応図</u>があることを知っていると回答した。

設問14

14.PC等のデバイスに保存した重要なデータを喪失したことはありますか？



8.2%の方が重要なデータの喪失したことがある　と回答した。

設問15

15.データを喪失する原因として最もリスクが高いと考えるものを選択してください。

選択肢	回答	回答率
人為的ミスによる誤削除・上書きなど	176	37.1%
ハードウェアの故障	59	12.4%
デバイスの紛失・盗難	214	45.1%
ランサムウェア	24	5.1%
上記以外	1	0.2%

その他のリスク

管理すべきデータが多くなり、手が回らなくなること。・誤操作・確認ミス・情報漏洩・ヒューマンエラー・デバイスの持ち出しと置き忘れデバイス（記録媒体）の紛失・ハードウェアの故障紛失盗難人為的ミス

最もリスクが高いと考えられているのは**「デバイスの紛失・盗難」（45.1%）** で、次点が**「人為的ミスによる誤削除・上書き」（37.1%）** であった。

設問16

16.上記以外を選択した方は、データを喪失する原因として最もリスクが高いものを記載してください。

以下のような回答がありました。

- 管理すべきデータが多くなり、手が回らなくなること。
- 誤操作
- 確認ミス
- 情報漏洩
- ヒューマンエラー
- デバイスの持ち出しと置き忘れデバイス（記録媒体）の紛失
- ハードウェアの故障紛失盗難人為的ミス

設問17

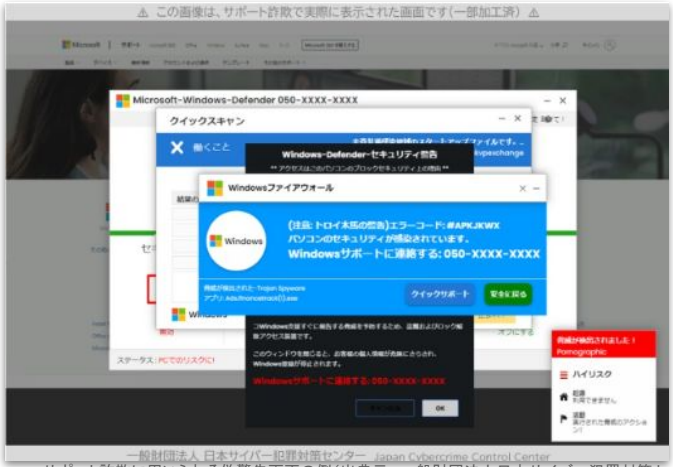
17.業務で利用するデータについてバックアップを行っていますか。

選択肢	回答	回答率
実施している（クラウド）	157	33.1%
実施している（HDD・SSD）	144	30.4%
実施している（ネットワークHDD（NASなど））	41	8.6%
実施していないが検討している	28	5.9%
実施していない	48	10.1%
分からない	56	11.8%

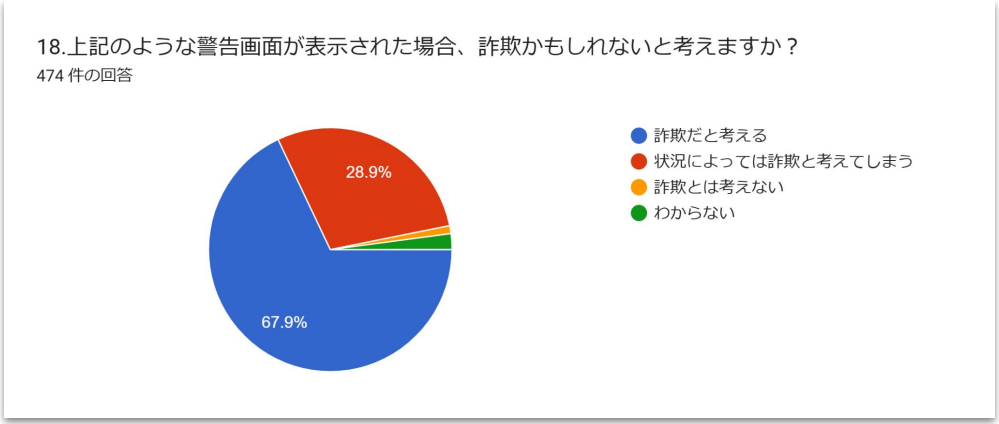
72.1%の人が業務で利用するデータのバックアップを取っている　と回答し、そのうち**「クラウド」を利用している人が33.1%**　で最も多く、次点で**「HDD・SSD」を利用している人が30.4%**となった。

設問18

18.上記のような警告画面が表示された場合、詐欺かもしれないと考えますか？



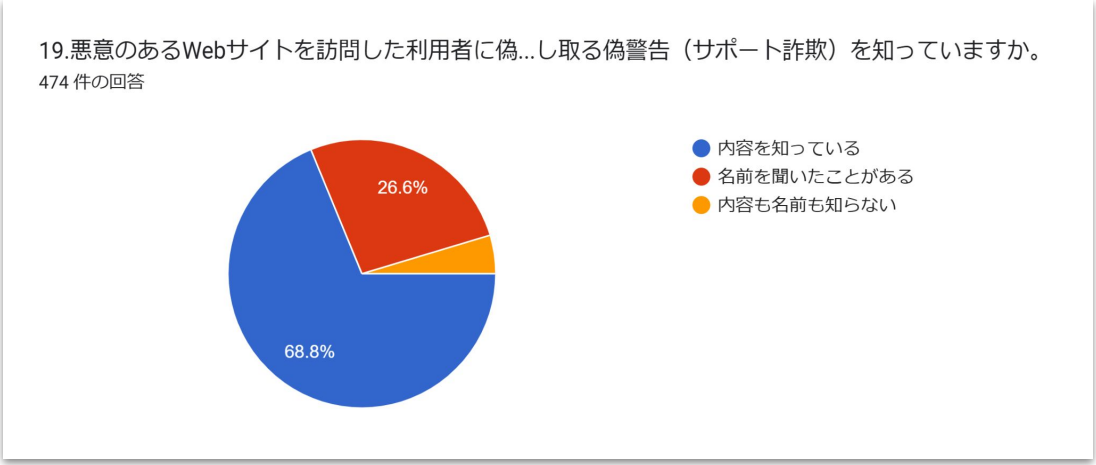
サポート詐欺に用いられる偽警告画面の例（出典元：一般財団法人日本サイバー犯罪対策センター（JC3）https://www.jc3.or.jp/threats/topics/article-396.html(学外サイト)）



サポート詐欺の警告画面について、**「詐欺だと考える」、「状況によっては詐欺と考える」人の割合は96.8%** となった。

設問19

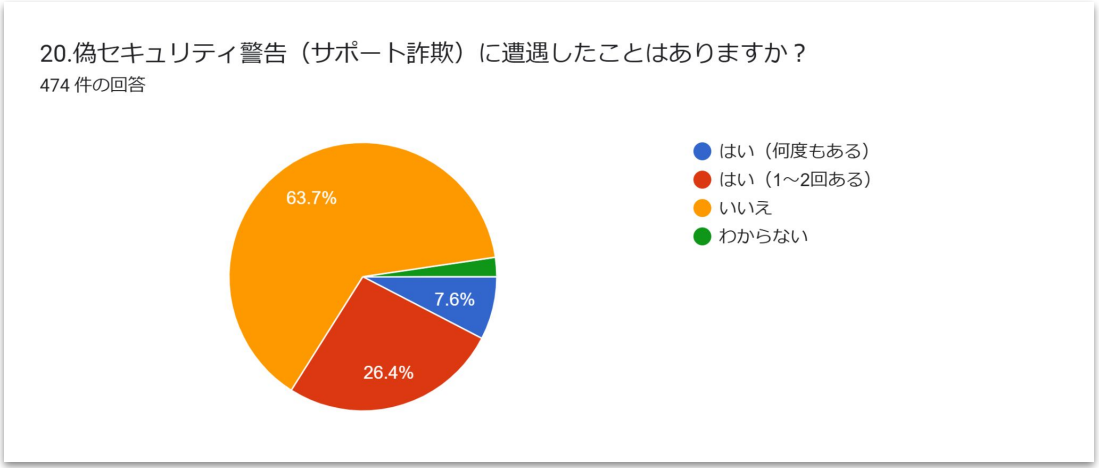
19.悪意のあるWebサイトを訪問した利用者に偽の警告画面を表示し、画面上に表示しているなりすましサポートセンターに電話をさせて金銭をだまし取る偽警告（サポート詐欺）を知っていますか。



サポート詐欺について**68.8%の人が「内容を知っている」**、**26.6%の人が「名前を聞いたことがある」**と回答した。

設問20

20.偽セキュリティ警告（サポート詐欺）に遭遇したことはありますか？



サポート詐欺に遭遇したことがある人は、全体の34%となった。

設問21

21.身近なセキュリティ対策として取り組んでいるものを選んでください。（複数選択可）

選択肢	回答	回答率
不審なメールやサイトには注意する	464	97.9%
部屋・机・ロッカーは施錠する	261	55.1%
机の上はきれいにする	216	45.6%
離籍の際はモニターロック（windowsの場合は［Windowsキー］＋［Lキー］）する	185	39.0%
不要となった重要書類はシュレッダーする	368	77.6%
ウィルス対策ソフトを利用する	301	63.5%
ソフトウェアは常に最新の状態を保つ。	301	63.5%
二段階認証・多要素認証を利用する	337	71.1%

身近なセキュリティ対策として最も取り組まれているのは、「不審なメールやサイトは注意する」で、次点で「不要となった重要書類はシュレッダーする」であった。

設問22

22.そのほか、身近なセキュリティ対策として取り組んでいることがあれば記載してください。

以下のような回答がありました。

データ管理・保護

- クラウドバックアップ（End-to-End暗号化）を活用
- USBメモリ・外付けHDDを極力持ち出さない
- ノートPCにはデータを保存せず、持ち出しを制限
- USBにもロックを設定

ネットワーク・システム対策

- 公共のフリーWiFiを使用しない
- 問題のあるサイト調査時は専用端末＆プライベートモード利用
- ウイルス対策ソフトを定期チェック
- ブラウザ拡張機能（NoScript等）を活用
- 不審な電話やSNSメッセージに注意し、個人情報を提供しない

物理的セキュリティ

- 物理的なセキュリティワイヤーを使用
- 業務終了後、PCを引き出しに収納＆施錠
- 重要書類は施錠可能な引き出しに保管
- デバイスをなるべく持ち歩かない

意識・リテラシー向上

- セキュリティ関連の情報を定期的に収集（雑誌・Webサイト）
- 状況判断を冷静に行い、不明点は相談
- 複数人でのチェックを実施

設問23

23.PC等のデバイスの盗難対策について取り組んでいるものを選んでください。（複数選択可）

選択肢	回答	回答率
部屋を不在にする場合は施錠する	381	80.4%
暗号化されたUSBを利用する	71	15.0%
重要な紙媒体は、施錠できる引き出しやキャビネットなどに保管する	257	54.2%
デバイス本体に保存するデータは最小限としクラウドストレージを利用する	178	37.6%
パソコンをワイヤーロックで固定する	53	11.2%
定期的なバックアップを取得する	206	43.5%

PC等のデバイスの盗難対策について最も取り組まれていることは、**「部屋を不在にする場合は施錠する」（80.4%）**、次点で**「重要な紙媒体は施錠できる引き出しやキャビネットなどに保管する」（54.2%）**となった。

設問24

24.そのほか、PC等のデバイスの盗難対策について取り組んでいることがあれば記載してください。

以下のような回答がありました。

デバイスの管理・持ち出し制限

- 不要な時は持ち出さない・持ち歩かない
- PCやUSBメモリーは学外に持ち出さない
- 公共の場ではデバイスから目を離さない

物理的・アクセス制限

- 生体認証・PINコード設定で不正ログインを防止
- USB挿込口にストッパーを入れ、無断使用を防ぐ
- 事務室への不審者の入室を防ぐ

データの保護・暗号化

- BitLocker設定でSSDの抜き取り対策
- PC記憶媒体を暗号化し、リモート初期化可能に設定
- DropboxやIMAPメールを活用し、ローカルにデータを保存しない

追跡・復旧対策

- ノートPCの位置情報追跡機能を有効化
- トラッキングシステムを導入
- 予備のPCを用意して対処可能な体制を整える

設問25

25.次のうち関心の高い情報セキュリティ脅威があれば選択してください。

選択肢	回答	回答率
ランサムウェアによる被害	261	55.1%
サプライチェーンの弱点を悪用した攻撃	74	15.6%
内部不正による情報漏えい等の被害	106	22.4%
標的型攻撃による機密情報の窃取	183	38.6%
不注意による情報漏えい等の被害	279	58.9%
脆弱性対策情報の公開に伴う悪用増加	87	18.4%
ビジネスメール詐欺による金銭被害	122	25.7%
テレワーク等のニューノーマルな働き方を狙った攻撃	111	23.4%
犯罪のビジネス化（アンダーグラウンドサービス）	95	20.0%
上記以外	5	1.1%

最も関心の高い情報セキュリティ脅威は、**「不注意による情報漏えい等の被害」（58.9%）**で、**次点で「ランサムウェアによる被害」（55.1%）**であった。

設問26

26. そのほか、関心の高い情報セキュリティ脅威があれば記載してください。

以下のような回答がありました。

- サイバー攻撃・不正アクセス
  - サーバへの悪意ある攻撃
  - なりすまし（見極めが難しい）
  - P2P利用によるマルウェア感染
- フィッシング・詐欺
  - スマホへの不審なメールやLINEメッセージの増加
  - 誤操作による意図しないアクセスや情報漏洩
- データ漏洩リスク
  - 海外からの学生・研究者によるデータ漏洩
  - AI生成ツールを介した情報漏洩
  - 外国産デバイスやアプリによる不正なデータ収集
- 物理的セキュリティの脆弱性
  - 建物のセキュリティ不足による不審者の侵入
- ウイルス対策・意識向上
  - 個人PCでのデータ管理とウイルス対策ソフトの対応状況への関心

設問27

27. 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。

以下のような回答がありました。

- セキュリティ対策の強化要望
  - 内部不正対策の強化（ダウンロード・送信の制限など）
  - 大学の物理的セキュリティ向上（建物の入り口に自動ロック導入など）
  - 定期的な情報セキュリティの注意喚起を継続してほしい

- 意識向上の重要性
  - 情報セキュリティ意識を全員で一斉に高めることが重要
  - 日本国籍以外の方のセキュリティ意識の低さが課題と感じる
  - セキュリティ事故のニュースを聞くと危機感を持つ

- 運用・管理の課題
  - セキュリティ更新作業の効率化（自動更新の導入など）
  - セキュリティ対策により届かないメールがある
  - 学内マニュアルへのアクセス制限により、一部の職員が情報を得にくい

- 個人の対策
  - 多忙時や疲れているときは操作を控え、慎重に対応
  - 不明点は相談しながら対応するよう心掛けている