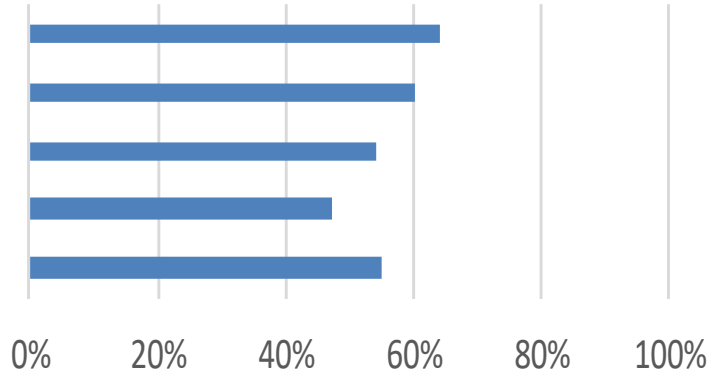
大学情報セキュリティベンチマークリストの評価結果

大学の規模	回答校
① 大規模大学　入学定員3,000人以上　複数学部有り	10
② 中規模大学　入学定員2,000人以上3,000人未満　複数学部有り	9
③ 中小規模大学　入学定員2,000人未満　複数学部有り	38
④ 単科大学(自然科学,社会科学,人文科学,医歯薬,その他)、短期大学	13
全回答大学	70

合計の平均点数	平均点	100点中の割合	前回増減
① 大規模大学	64	64%	0%
② 中規模大学	60	60%	-4%
③ 中小規模大学	54	54%	1%
④ 単科大学・短期大学	47	47%	-6%
全回答大学	55	55%	0%

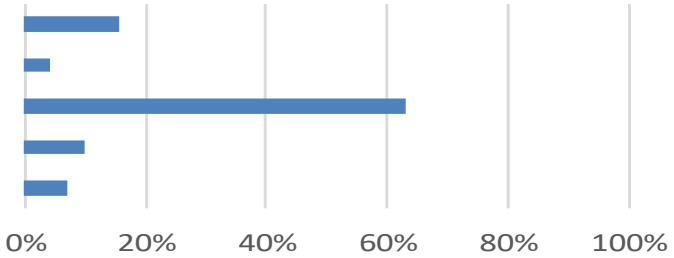


第1部　経営執行部の情報セキュリティに対する取組み

問1　サイバー攻撃による情報資産、金融資産の窃取・漏洩・破壊など情報管理やシステム運用に関する脅威となる事象について、担当役員もしくはそれに準ずる法人・大学執行部メンバーが統括責任者としてリーダーシップを発揮し、危機意識の共有化に努めていますか。

① 経営執行部が中心となり、全学組織を対象に危機意識の共有化に努めている。
② 経営執行部の方針により、学部単位など部門の管理責任者を通じて危機意識の共有化に努めている。
③ 経営執行部の方針により、情報センター等部門を通じて危機意識の共有化に努めている。
④ 経営執行部による危機意識の共有化はしていないが、現在、検討している。
⑤ 経営執行部による危機意識の共有化はしていない。

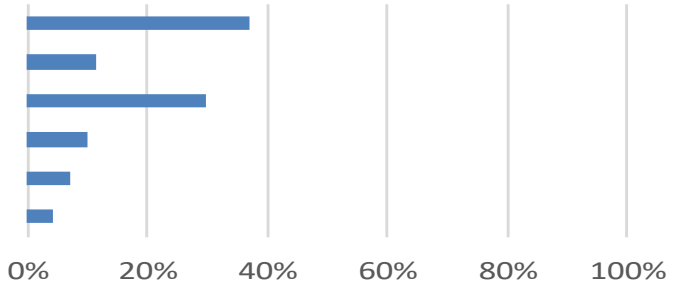
選択肢	選択数	割合	前回増減
①	11	16%	3%
②	3	4%	−5%
③	44	63%	3%
④	7	10%	−2%
⑤	5	7%	1%



問2　経営執行部の方針により、情報セキュリティポリシーや情報セキュリティ管理に関する規程など学内ルールを策定し、周知徹底に努めていますか。

① 経営執行部の方針により、学内ルールの策定とその周知徹底を行っている。
② 経営執行部の方針により、学内ルールの策定を行っているが、周知徹底はできていない。
③ 経営執行部ではなく情報センター等部門により、学内ルールを策定し、その周知徹底を行っている。
④ 経営執行部ではなく情報センター等部門により、学内ルールを策定しているが、周知徹底はできていない。
⑤ 学内ルールの策定とその周知徹底を検討している。
⑥ 学内ルールの策定はしていない。

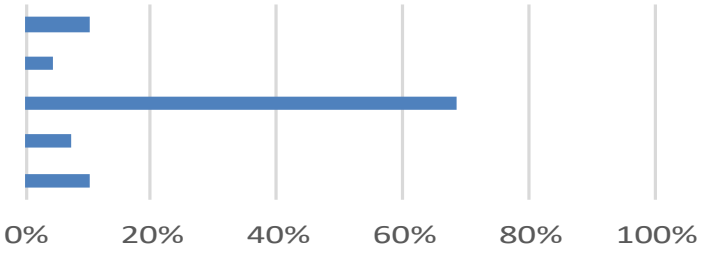
選択肢	選択数	割合	前回増減
①	26	37%	2%
②	8	11%	−8%
③	21	30%	8%
④	7	10%	0%
⑤	5	7%	−2%
⑥	3	4%	0%



問3　サイバー攻撃に対する防御体制について、経営執行部により何らかの対策を構築していますか。

① 経営執行部が中心となり、全学組織を対象に防御体制を構築している。
② 経営執行部の方針により、学部単位など部門の管理責任者を通じて防御体制を構築している。
③ 経営執行部の方針により、情報センター等部門を通じて防御体制を構築している。
④ 経営執行部として防御体制を構築していないが、現在、検討している。
⑤ 経営執行部として防御体制を構築していない。

選択肢	選択数	割合	前回増減
①	7	10%	2%
②	3	4%	−6%
③	48	69%	8%
④	5	7%	2%
⑤	7	10%	−6%

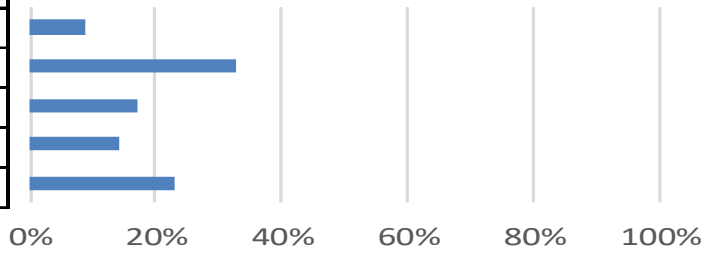


問4　今年度、貴大学のICT予算（物件費に限定）の中で、セキュリティ対策に充当している費用の割合。

① 予算化はしていない。
② 3%以下
③ 4%～6%
④ 7%～9%
⑤ 10%以上

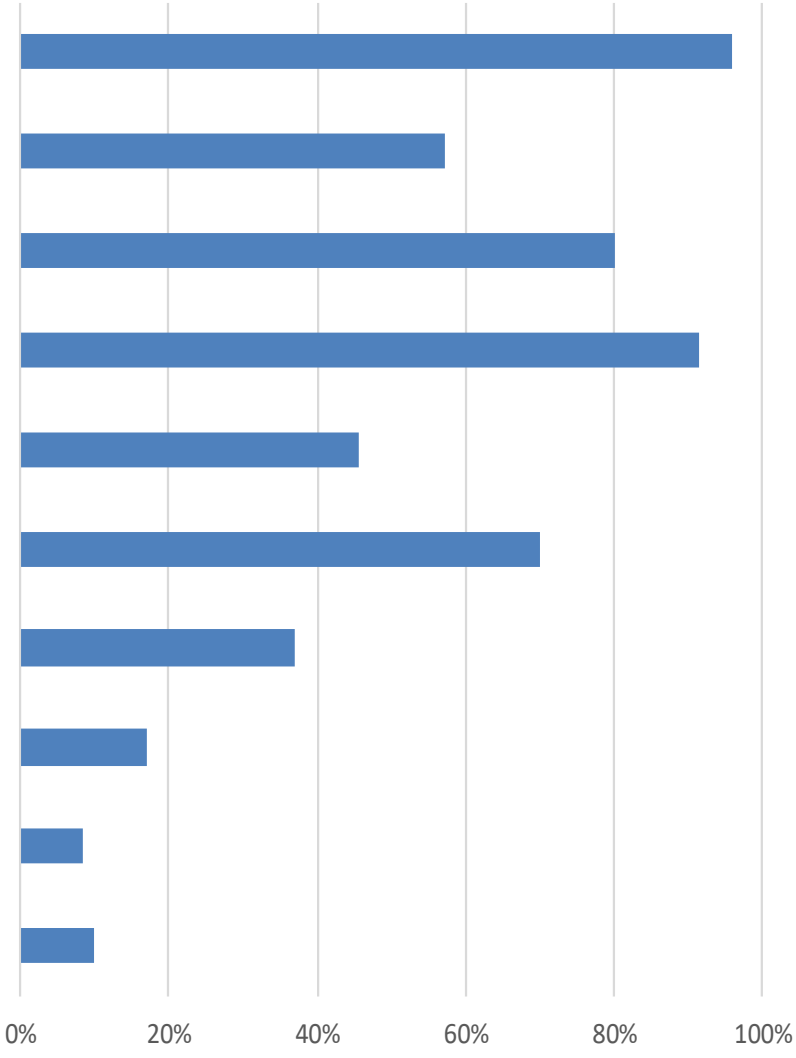
選択肢	選択数	割合	前回増減
①	6	9%	3%
②	23	33%	−3%
③	12	17%	−8%
④	10	14%	4%
⑤	16	23%	5%

（該当部分の算出不可等3校無回答）



問5　上記セキュリティ対策費の中で、費用をかけている内容。（複数回答）

セキュリティ対策費	選択数	割合	前回増減
① ファイアウォール	67	96%	2%
② 侵入検知システム	40	57%	-3%
③ VLANなどネットワーク関連	56	80%	-2%
④ ウイルス対策ソフト・サービス	64	91%	-3%
⑤ セキュリティ監視サービス	32	46%	11%
⑥ フィルタリングソフト（Web、メール）	49	70%	1%
⑦ 暗号化対策	26	37%	5%
⑧ USB、SDカード、DVDなどの書き込み制御ソフト	12	17%	1%
⑨ 不審なファイルを外部から保護された仮想環境で確認を行う攻撃対策ツール	6	9%	-9%
⑩ その他　（EDRソフトウェア、IPS、情報セキュリティポリシー策定支援、インシデント対策体制の構築、情報漏洩検知サービス、標的型攻撃メール訓練サービス、DNS型セキュリティ対策）	7	10%	1%

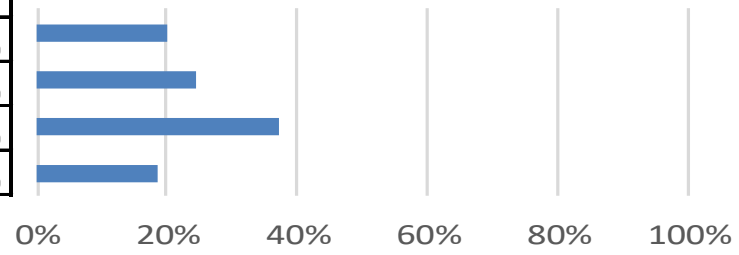


第2部　重要な情報資産の把握と管理対策について

問1　重要な情報資産（金融資産情報を含む）の目録作成を実施。

① 実施しており、毎年見直しを行っている。
② 実施しているが、定期的な見直しは行っていない。
③ 検討している。
④ 実施していない。

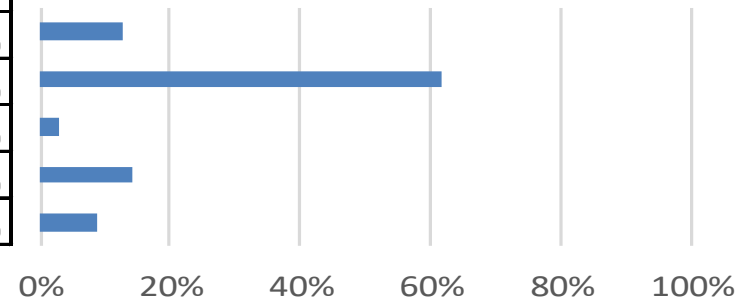
選択肢	選択数	割合	前回増減
①	14	20%	1%
②	17	24%	−3%
③	26	37%	−1%
④	13	19%	3%



問2　重要な情報資産に対するアクセス制御及びリスク評価を行っていますか。

① 重要な情報資産に対するアクセス制御及びリスク評価を行っている。
② 重要な情報資産に対するアクセス制御を行っている。
③ 重要な情報資産に対するリスク評価を行っている。
④ 検討している。
⑤ 実施していない。

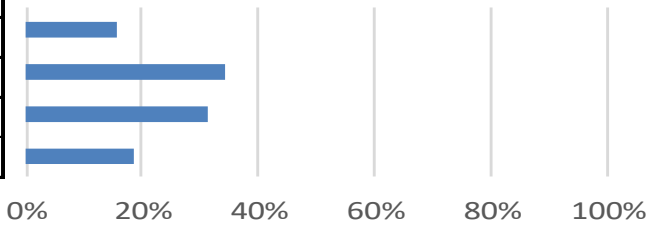
選択肢	選択数	割合	前回増減
①	9	13%	0%
②	43	61%	−4%
③	2	3%	−1%
④	10	14%	0%
⑤	6	9%	5%



問3　個人データや機密情報など重要な情報資産の管理について、入手から保管、消去・破棄に関わる責任者・扱者、取扱手順、処理の履歴・点検などが定められていますか。

① 責任者・取扱者、取扱手順、処理の履歴・点検を定め、定期的に確認をしている。
② 責任者・取扱者、取扱手順、処理の履歴・点検を定めているが、定期的な確認はしていない。
③ 検討している。
④ 定めていない。

選択肢	選択数	割合	前回増減
①	11	16%	−1%
②	24	34%	7%
③	22	31%	−5%
④	13	19%	0%

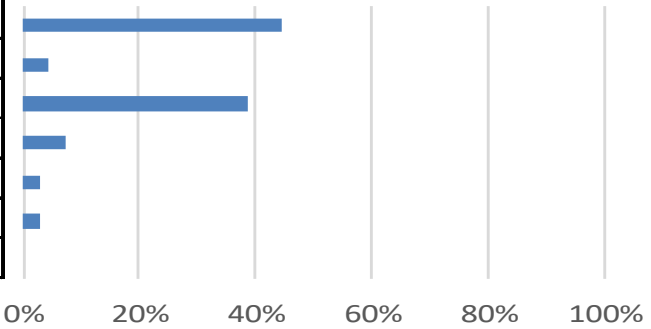


第3部　組織的・人的な対応について

問1　情報セキュリティに関する意思決定、脅威となる事象に対応する組織が設置されていますか。

① 経営執行部として統括責任者を置き、情報セキュリティに関する専門の検討組織を設置し、実施組織として情報センター等部門を設置している。
② 統括責任者は置いていないが、情報セキュリティに関する専門の検討組織を設置し、実施組織として情報センター等部門を設置している。
③ 情報センター等部門を中心に対応している。
④ 情報センター等部門ではなく、情報セキュリティなどの検討委員会で対応している。
⑤ 組織の設置を検討している。
⑥ 組織の設置はしていないが、外部業者に委託している。
⑦ 組織の設置は考えていない。

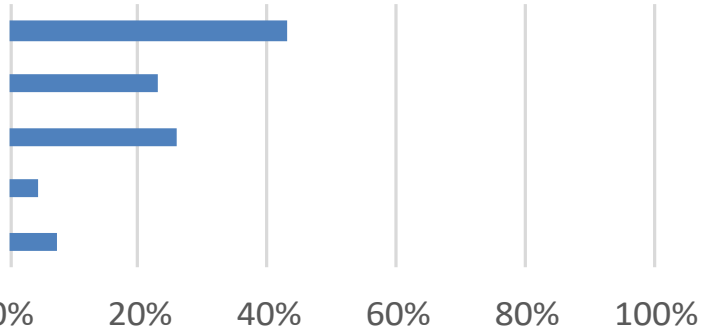
選択肢	選択数	割合	前回増減
①	31	44%	2%
②	3	4%	0%
③	27	39%	−3%
④	5	7%	1%
⑤	2	3%	−2%
⑥	2	3%	2%
⑦	0	0%	0%



問2　教職員（非常勤・派遣を含む）の採用・退職に際して、守秘義務を書面で明確にしていますか。また、情報セキュリティポリシーに違反した場合の罰則が規定されていますか。

① 守秘義務の内容を書面で明確にしている。また、違反した場合の罰則を規定している。
② 守秘義務の内容を書面で明確にしているが、罰則規定は設けていない。
③ 守秘義務を書面で明確にしていないが、就業中の罰則で規定している。
④ 書面での明確化と罰則規定のいずれも対応していない。
⑤ その他

選択肢	選択数	割合	前回増減
①	30	43%	8%
②	16	23%	4%
③	18	26%	−5%
④	3	4%	1%
⑤	5	7%	3%

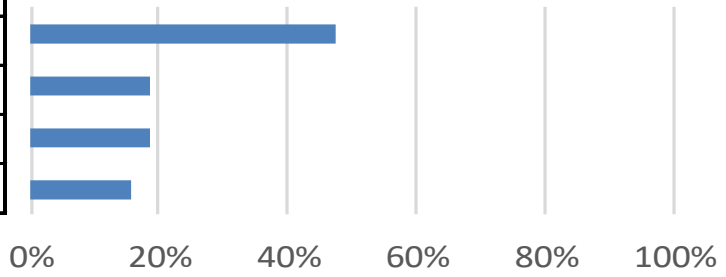


【⑤その他への回答内容】
- 入職時に学内諸規定を順守する書面にサインを求めており、就業規則に懲戒の規程がある
- 部門により異なる
- 守秘義務の内容を書面で明確にして罰則規定を設けおり情報セキュリティポリシーは検討中
- 規程集に守秘義務や罰則の記載あるが、職員の採用・退職時に明示なし

問3　脅威となる事象の学内連絡体制及び処理の責任体制は確立されていますか。また、対応手順は整備されていますか。

① 脅威となる事象の学内連絡体制及び処理の責任体制を確立し、対応手順も整備している。
② 学内の連絡体制と責任体制を確立しているが、対応手順は整備していない。
③ 学内の連絡体制を確立しているが、責任体制の確立と対応手順の整備はできていない。
④ 学内の連絡体制及び責任体制の確立と対応手順の整備はできていない。

選択肢	選択数	割合	前回増減
①	33	47%	5%
②	13	19%	−6%
③	13	19%	−2%
④	11	16%	3%

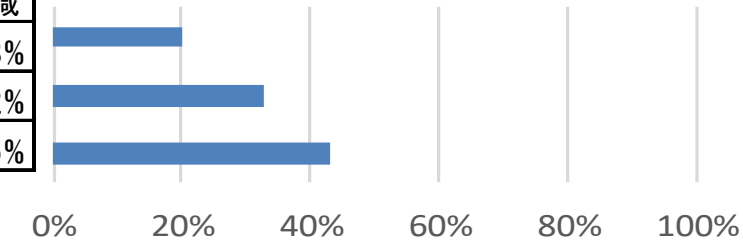


問4　情報セキュリティに関する業務委託を外部組織と契約する際に、情報漏洩や情報消失・破壊など障害対応について責任の所在を明確にし、外部組織による定期的な点検・大学による点検の監視など障害を予防するための取り決めをしていますか。

① 障害対応の取扱いについて契約書の中で、外部組織及び大学による定期的な点検・監視について取り決めをしている。
② 障害対応の取扱いについて契約書の中で、外部組織による定期的な点検に留めている。
③ 障害対応の取扱いについて契約書で取り決めていない。

選択肢	選択数	割合	前回増減
①	14	20%	3%
②	23	33%	2%
③	30	43%	−5%

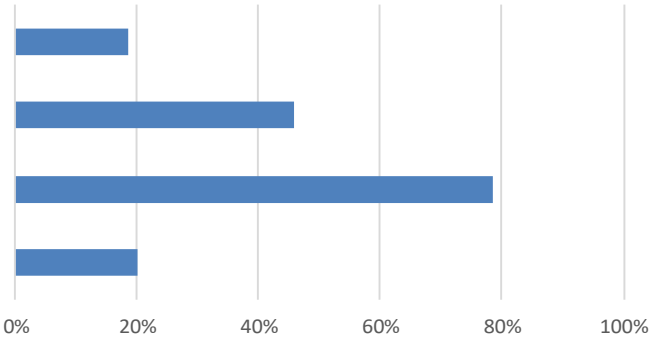
（該当契約なし等3校無回答）



問5　経営執行部または部門単位で実施している危機意識の共有化、学内ルールの周知徹底・遵守の確認、攻撃に対する防御対策の内容について選択してください。（複数回答可）

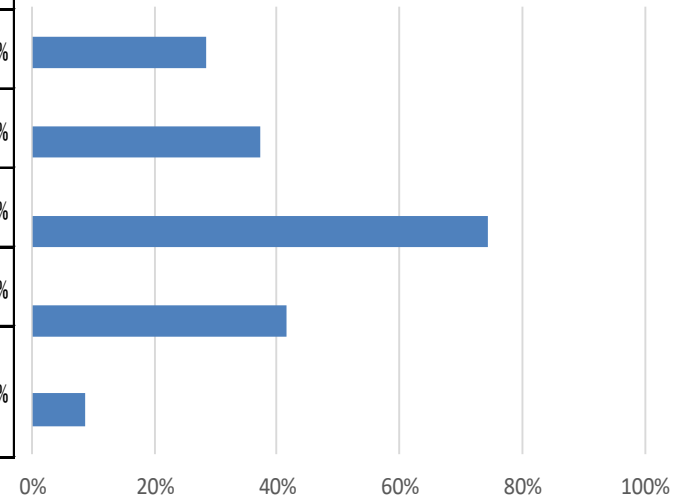
（１）危機意識の共有化

危機意識共有化の方法	選択数	割合	前回増減
① 学内外の情報セキュリティ研修会参加の義務化	13	19%	2%
② FD・SD,教授会,職員会議などでの定期的な情報提供	32	46%	6%
③ Webサイトや学内文書による定期的な情報提供	55	79%	5%
④ その他(教職員を対象とした標的型攻撃メール訓練の実施、脅威や重大な事象発生した際に周知、脅威となる事象の被害事例や対応方針を教職員にメールで情報提供、アクシデント発生時の情報共有、情報セキュリティハンドブック・クラウドサービス利用ガイドラインを発行して教職員へ配付、学内ルールは策定中、講習会・Webサイトでの情報提供を随時実施、メール配信・Teamsへの投稿、不定期にメールで注意喚起)	14	20%	1%



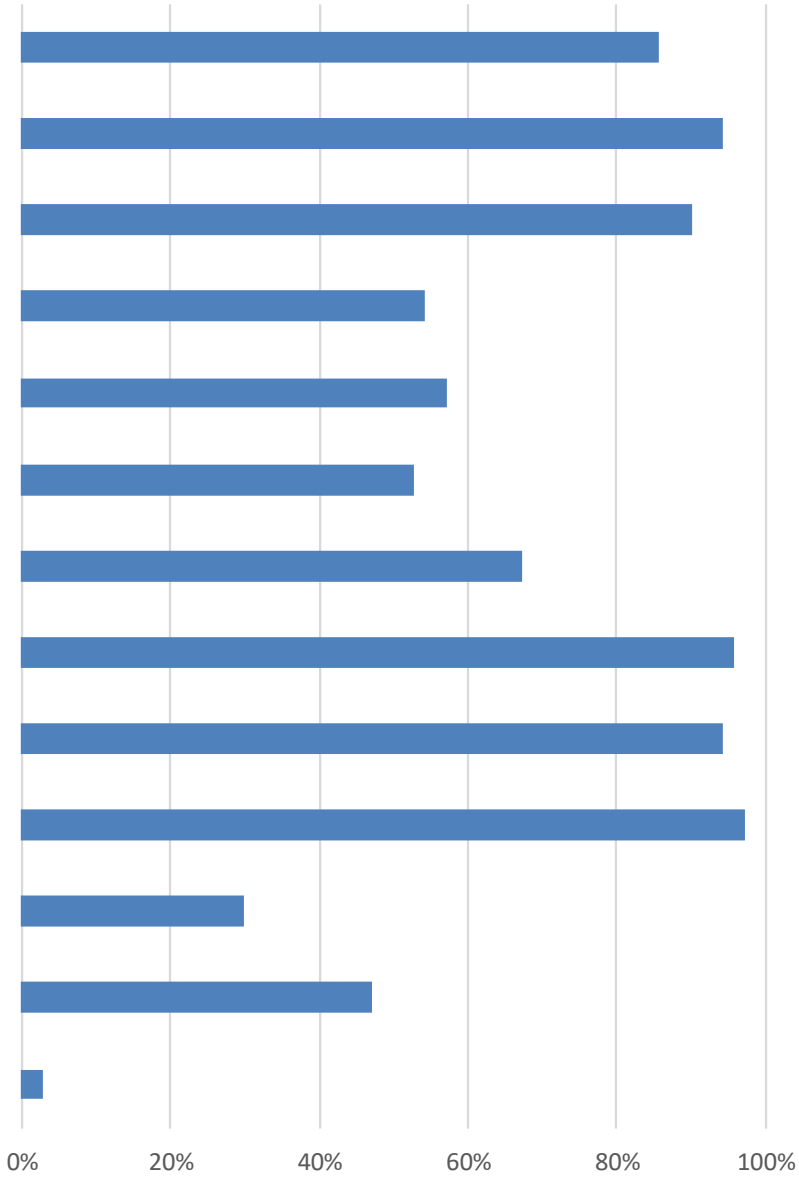
（２）学内ルールの周知徹底と遵守の確認

学内ルール周知徹底・遵守の方法	選択数	割合	前回増減
① 情報センター等部門によるルールの周知とアンケートでの点検・確認	20	29%	2%
② 教授会、職員会議などでのルールの周知と遵守の確認	26	37%	6%
③ Webサイトでのルールの紹介と遵守の呼びかけ	52	74%	8%
④ 説明会でのルールの紹介と遵守の呼びかけ	29	41%	16%
⑤ その他(学内発信文書、通達文による周知、規程集を常時閲覧可能な状態としている、メール・ポータルサイトでの通知、学内ルールは策定中)	6	9%	3%



（３）攻撃に対する防御対策

防御対策の内容	選択数	割合	前回増減
① 公的機関を装った偽装メールの注意喚起	60	86%	-4%
② メール添付ファイル開封の注意喚起	66	94%	3%
③ メールにリンクされたURL接続の注意喚起	63	90%	-1%
④ USBメモリなど外部持ち込みの注意喚起	38	54%	-6%
⑤ 脅威となる事象の被害状況報告と対策説明	40	57%	5%
⑥ IDの管理やパスワードの定期的な見直し注意喚起	37	53%	-2%
⑦ 不正アクセスの監視と異常事態の発見	47	67%	-1%
⑧ ファイアウォールや迷惑メールの設定	67	96%	0%
⑨ VLANなどネットワークのアクセス制限の設定	66	94%	-1%
⑩ 無線LANの暗号化及び認証方式の導入	68	97%	0%
⑪ データ暗号化の導入	21	30%	-2%
⑫ クラウドに対する利活用の注意喚起	33	47%	-4%
⑬ その他（EDRソフトウェア、DNSセキュリティ導入、学内ルールは策定中）	2	3%	3%

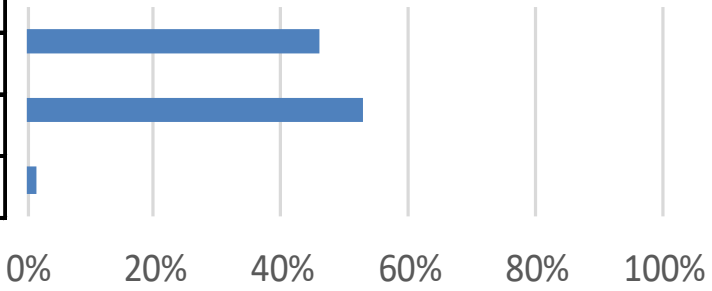


第4部　技術的・物理的対策について

問1　ファイアウォールを導入し、ポリシーに基づきログ管理や通信を定期的に点検していますか。

① システムログを取得・解析し、通信を定期的に点検している。
② システムログの取得のみで解析していない。
③ システムログの取得はしていない。

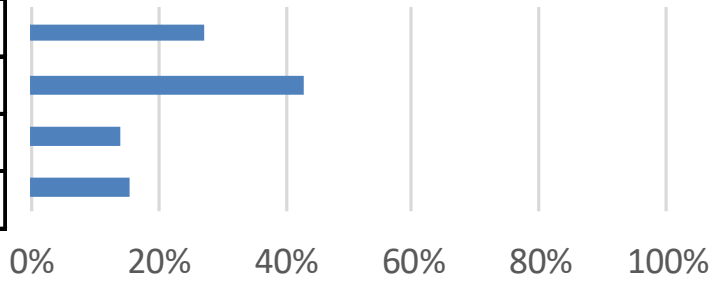
選択肢	選択数	割合	前回増減
①	32	46%	−1%
②	37	53%	0%
③	1	1%	1%



問2　侵入検知システムなどを導入し、不正通信や不正プログラムを監視する対策を行っていますか。

① 侵入検知システムなどを導入し、定期的に通信の監視を行っている。
② 侵入検知システムなどを導入し、通信の監視を行っている。
③ 侵入検知システムなどの導入を検討している。
④ 侵入検知システムなどは導入していない。

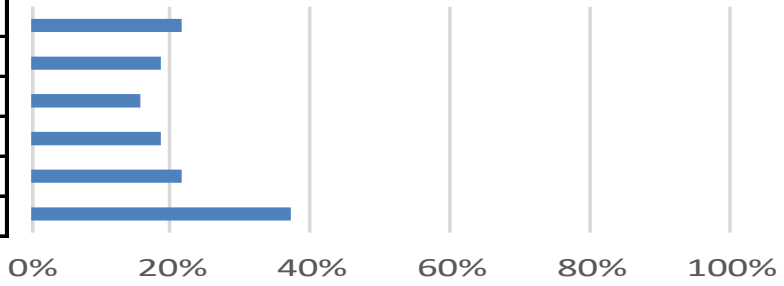
選択肢	選択数	割合	前回増減
①	19	27%	−4%
②	30	43%	−5%
③	10	14%	5%
④	11	16%	4%



問3　重要な情報資産についてUSBメモリ・ノートPCなどの持ち出し・持ち込みの禁止と制限。（複数回答）

① USBメモリの使用を禁止している。
② ノートPCの持ち出し・持ち込みを禁止している。
③ ノートPCの持ち出しは原則禁止しているが、暗号化で保護する場合のみ許可している。
④ 外部クラウドサービス利用の制限を行っている。
⑤ 持ち出し・持ち込みの制限を検討している。
⑥ 持ち出し・持ち込みの制限はしていない。

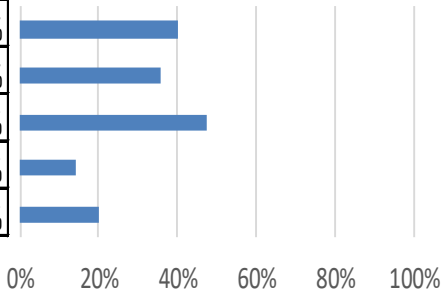
選択肢	選択数	割合	前回増減
①	15	21%	−1%
②	13	19%	−3%
③	11	16%	−1%
④	13	19%	1%
⑤	15	21%	2%
⑥	26	37%	−1%



問4　利用者IDの管理として、利用者の識別と認証を行っていますか。（複数回答）

① 共用IDの利用対象・範囲を定期的に見直している。
② パスワードの更新を定期的に呼びかけている。
③ 誕生日など推測しやすいパスワードを設定しないよう登録画面で注意喚起している。
④ ワンタイムパスワードの利用を呼びかけている。
⑤ その他

選択肢	選択数	割合	前回増減
①	28	40%	0%
②	25	36%	2%
③	33	47%	-5%
④	10	14%	-2%
⑤	14	20%	2%

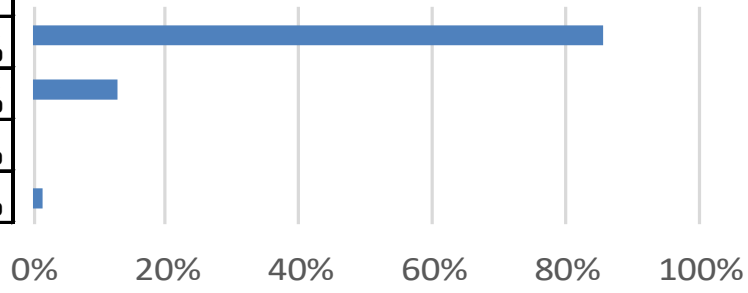


【⑤その他への回答内容】
- 多要素認証（7件）
- 学生にはアクセス制限を実施
- ADの構築・運営
- システム管理者IDと一般ユーザIDを明確に使い分けて利用
- 個人IDの共用とパスワード使い回し禁止の呼びかけ
- パスワード条件で文字数、英数大小文字、姓名不可など設定
- 個人IDを共用しないように呼び掛け
- 外部漏洩可能性のパスワードは利用しないように注意

問5　情報システムやコンテンツへのアクセス制限を行っていますか。

① 全学的にアクセス制限を行っている。
② 一部の部門（職員組織、学部、学科など）でアクセス制限を行っている。
③ アクセス制限を検討している。
④ アクセス制限は行っていない。

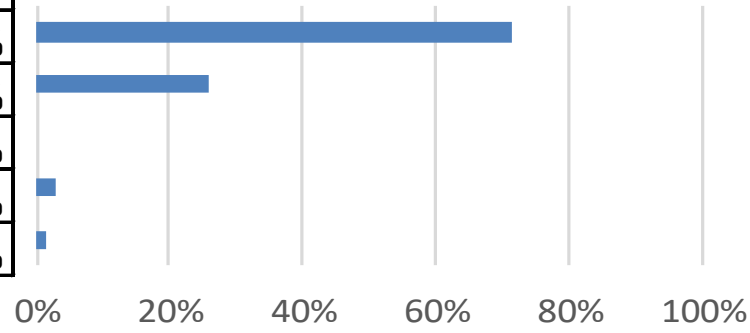
選択肢	選択数	割合	前回増減
①	60	86%	0%
②	9	13%	0%
③	0	0%	−1%
④	1	1%	1%



問6　リスクを軽減するため、ネットワークの分離を行っていますか。

① 全学的にVLAN（仮想的なネットワーク）などでネットワークを分離している。
② 事務部門など一部のネットワークをVLANなどで分離している。
③ VLANなどでネットワークの分離を検討している。
④ その他のネットワーク分離対策
⑤ ネットワークの分離はしていない。

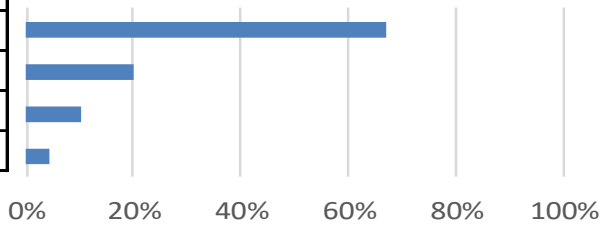
選択肢	選択数	割合	前回増減
①	50	71%	−6%
②	18	26%	4%
③	0	0%	0%
④	2	3%	3%
⑤	1	1%	0%



問7　外部に公開しているサーバのぜい弱性対策を行っていますか。

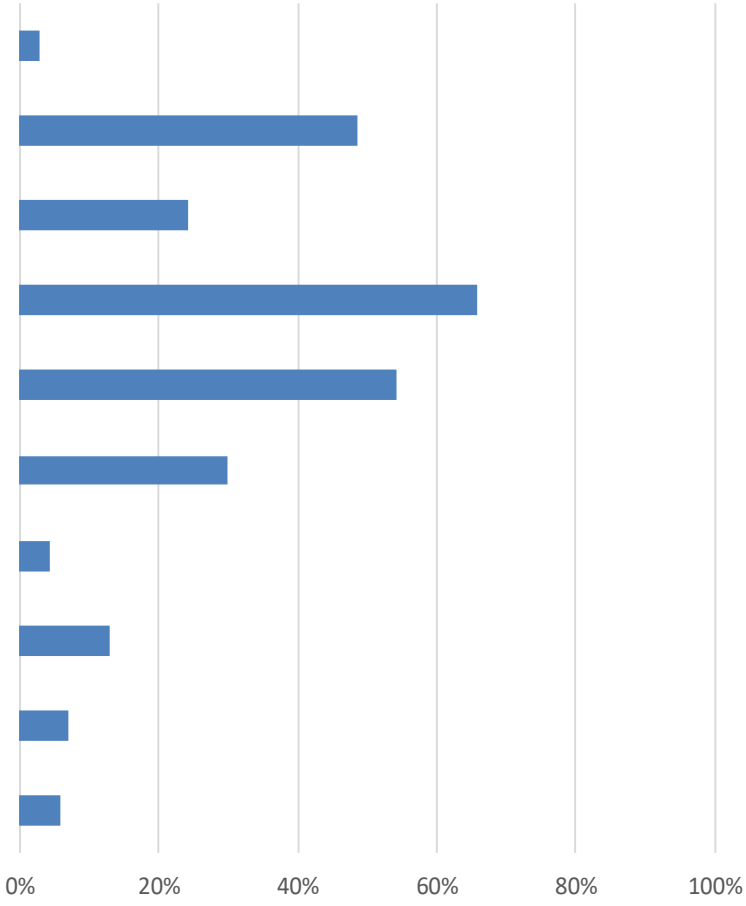
① ぜい弱性に対して最新の修正プログラムを用いて対応している。
② 最新の修正プログラムを適用するまでの間、当面の対応としてぜい弱性を狙った攻撃を回避するソフトウェアもしくはハードウェアを導入して対応している。
③ ぜい弱性対策を検討している。
④ ぜい弱性対策はしていない。

選択肢	選択数	割合	前回増減
①	47	67%	−2%
②	14	20%	2%
③	7	10%	0%
④	3	4%	1%



問8　重要な情報資産をバックアップしていますか。また、システム障害等を想定し、必要最低限の業務ができる備えをしていますか。（複数回答）

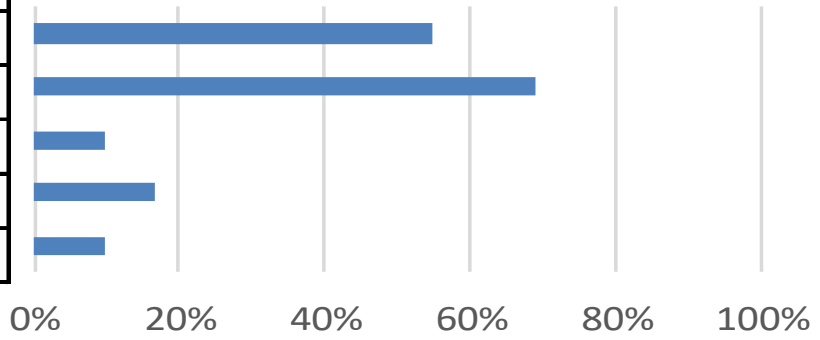
重要な情報資産のバックアップ方法	選択数	割合	前回増減
① 遠隔地域の大学と業務提携によりバックアップデータを保管している。	2	3%	0%
② 遠隔地のデータセンターなどにバックアップデータを保管している。	34	49%	5%
③ 他のキャンパスにバックアップデータを保管している。	17	24%	1%
④ バックアップは毎日行っている。	46	66%	−4%
⑤ バックアップは一定の期間で行っている。	38	54%	10%
⑥ 学内でシステムの二重化を行っている。	21	30%	−2%
⑦ 部門単位でシステムの二重化を行っている。	3	4%	−5%
⑧ バックアップの一つの方法として紙媒体で保管している。	9	13%	4%
⑨ その他のバックアップ方法（カートリッジテープ、クラウドストレージ）	5	7%	6%
⑩ バックアップへの備えについて検討している。	4	6%	1%



問9　コンピュータフォレンジックスに関係した対策が自組織で実行できますか。（複数回答）

①　ハードウェアの調査をすることが可能。
②　ソフトウェアの調査をすることが可能。
③　フォレンジックスを実施する組織がある。
④　フォレンジックスに関係した法的、制度的な仕組みを理解している組織がある。
⑤　リスクの評価を適切に定義し、適切なフォレンジックスを実行している。

選択肢	選択数	割合	前回増減
①	23	55%	20%
②	29	69%	30%
③	4	10%	6%
④	7	17%	9%
⑤	4	10%	9%

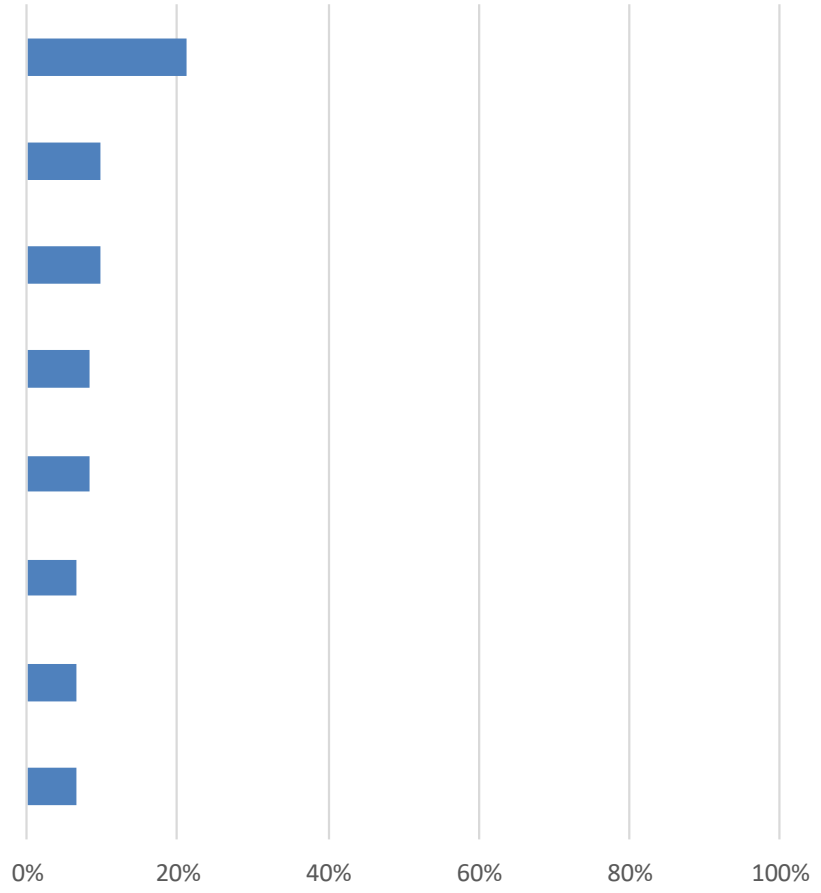


・　項目に回答したのは、42校（60％：前年5%増）で、上記はその中での割合を提示。

回答大学の情報

• ベンチマークリストの中で、今年度に評価を向上させたいと考えている項目

評価を向上させたい項目	選択数	割合
第3部　組織的・人的な対応について 問５　経営執行部または部門単位で危機意識の共有化、学内ルールの周知徹底・遵守の確認、攻撃に対する防御対策	13	21%
第1部　経営執行部の情報セキュリティに対する取組み 問２　経営執行部の方針により、情報セキュリティポリシーや規程など学内ルールを策定し、周知徹底に努める	6	10%
第3部　組織的・人的な対応について 問１　情報セキュリティに関する意思決定、脅威となる事象に対応する組織の設置	6	10%
第1部　経営執行部の情報セキュリティに対する取組み 問１　担当役員、法人・大学執行部メンバーが統括責任者としてリーダーシップを発揮し、危機意識の共有化に努める	5	8%
第4部　技術的・物理的対策について 問４　利用者IDの管理として、利用者の識別と認証を行う	5	8%
第2部　重要な情報資産の把握と管理対策について 問１　重要な情報資産の目録作成を実施	4	7%
第3部　組織的・人的な対応について 問３　脅威となる事象の学内連絡体制及び処理の責任体制確立や対応手順の整備	4	7%
第4部　技術的・物理的対策について 問１　ファイアウォールを導入し、ポリシーに基づきログ管理や通信を定期的に点検	4	7%



※　項目を回答した目標設定校は61校、上記はその中での上位8項目

※　その他には、第1部の問5、第2部の問3、第3部の問4、第4部の問2・3・7・8・9が目標項目として選択された

回答大学の情報

・ セキュリティ対策予算の増減と増額の内容について

・　増額なし（回答記入48校中、36校・75％）

・　多要素認証必須化の予算
・　セキュリティ機能追加で約30万円、UTMの保守費増加で約10万円程度の増加
・　ワンタイムパスワードシステム追加で保守費約40万円増加
・　セキュリティポリシー策定支援費、悪意のあるサイトへアクセス制限システム費などで約3百万円増額
・　CSIRT構築費用で約5百万円
・　セキュリティポリシー策定支援とアンチウィルスソフト導入等で約8百万円
・　標的型攻撃対応システム等の導入で約14百万円
・　メール用セキュリティ対策とEDRの導入で15百万円増額
・　FWログ分析サービス、Active Directoryサーバ監視サービス、IT資源管理ツールの検証導入等で約2千万円、
・　CSIRT発足を目標に掲げ、セキュリティ対策（CSIRT、サイバー保険、ネットワーク出入口施策）の目的で約2千万円
・　UTM導入検討約2億円
・　増額で約8億円

回答大学の情報

人的（組織・教育）、物理的（ハード・ソフト）セキュリティ対策の新たな取り組みについて

（１）人的な取組み
- 標的型攻撃メール対策訓練（2件）
- 情報資産データの電子帳簿管理
- 情報セキュリティ監査実施に向け、情報資産の洗い出し、関連規程の整備
- セキュリティ対策基準の見直し
- CSIRTの設置
- 4月1日にCSIRTを設置し、サイバーセキュリティ対策を行った。また、SD研修を企画・実施し、教職員に対して、高等教育機関等において要求される情報セキュリティ基準を解説し、遵守すべき本学セキュリティ規程を確認した
- 教職員全員を対象にしたeラーニング研修
- FDの取組みとして、教育用ネットワークにおける教員向けモラル研修を実施
- 定期的な情報セキュリティ教育及び注意喚起、情報セキュリティポリシーの等の定期的な見直し
- e-Learningによるセキュリティ教育を毎年実施しており、外国人教員対応として今年度から英語版を準備
- 情報システム部門1名増員

（２）物理的な取組み
- 多要素認証の導入（3件）
- 事務系ネットワークに不正アクセスが出来ないように既存システムから新たな機器へ入替
- SSL-VPN環境の整備
- Firewall（LITM)を更新して監視機能の強化予定
- 2022年から4年間をサイバーセキュリティ対策等基本計画として、今年度は、FWログ分析サービス、ActiveDirectoryサーバ監視サービスの導入、インシデント対策の実績をもとに事故対応マニュアルの見直しを行っている
- 各種ネットワークサービス運用サーバの仮想化、大容量ストレージ導入でプライベートクラウド構築
- 効果的なセキュリティ対策について情報収集中