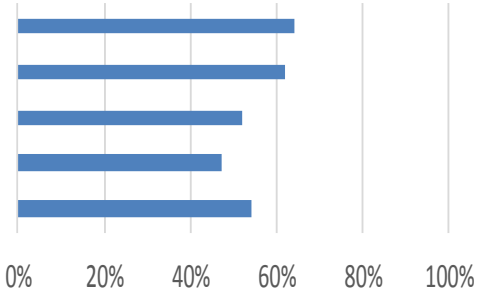
大学情報セキュリティベンチマークリストの評価結果

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	15
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	15
③ 中小規模大学　入学定員2,000人未満　複数学部有り	58
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	23
全回答大学	111

合計の平均点数	平均点	100点中の割合	前年増減
① 大規模大学	64	64%	2%
② 中規模大学	62	62%	5%
③ 中小規模大学	52	52%	2%
④ 単科大学・短期大学	47	47%	1%
全回答大学	54	54%	3%

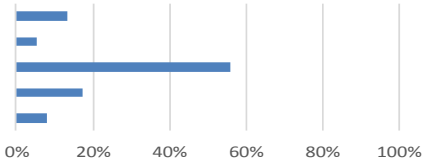


第1部　経営執行部の情報セキュリティに対する取組み

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	前年増減
①	15	14%	5%
②	6	5%	−4%
③	62	56%	−1%
④	19	17%	1%
⑤	9	8%	−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。

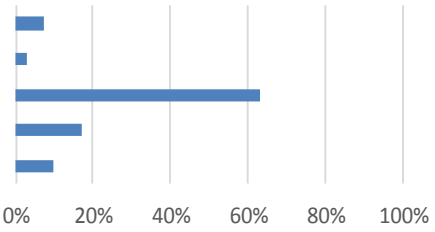
① 経営執行部の方針により、学内ルールの策定とその周知徹底を行っている。
② 経営執行部の方針により、学内ルールの策定を行っているが、周知徹底はできていない。
③ 経営執行部ではなく情報センター等部門により、学内ルールを策定し、その周知徹底を行っている。
④ 経営執行部ではなく情報センター等部門により、学内ルールを策定しているが、周知徹底はできていない。
⑤ 学内ルールの策定とその周知徹底を検討している。
⑥ 学内ルールの策定はしていない。

選択肢	選択数	割合	前年増減
①	36	32%	10%
②	17	15%	−5%
③	24	22%	0%
④	17	15%	−2%
⑤	16	14%	−2%
⑥	1	1%	−1%

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	前年増減
①	8	7%	2%
②	3	3%	−1%
③	70	63%	−5%
④	19	17%	5%
⑤	11	10%	−1%

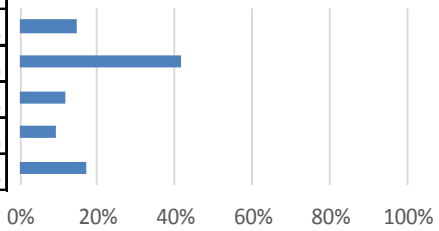


問4　今年度、貴大学のICT予算（物件費に限定）の中で、セキュリティ対策に充当している費用の割合。

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

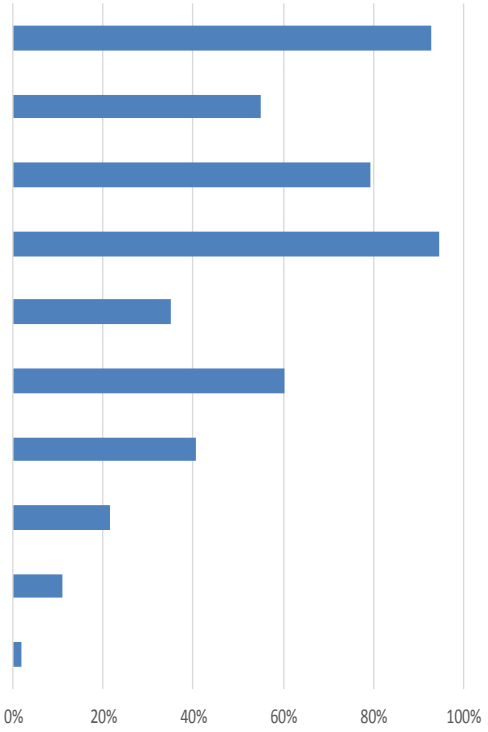
選択肢	選択数	割合	前年増減
①	16	14%	0%
②	46	41%	−2%
③	13	12%	0%
④	10	9%	−3%
⑤	19	17%	3%

（該当部分の算出不可等7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	前年増減
① ファイアウォール	103	93%	5%
② 侵入検知システム	61	55%	9%
③ VLANなどネットワーク関連	88	79%	3%
④ ウイルス対策ソフト・サービス	105	95%	0%
⑤ セキュリティ監視サービス	39	35%	−1%
⑥ フィルタリングソフト（Web、メール）	67	60%	−1%
⑦ 暗号化対策	45	41%	3%
⑧ USB、SDカード、DVDなどの書き込み制御ソフト	24	22%	2%
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	12	11%	3%
⑩ その他　（IPS,ネットワーク検疫など）	2	2%	−3%

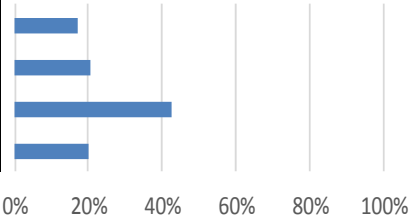


第2部　重要な情報資産の把握と管理対策について

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。

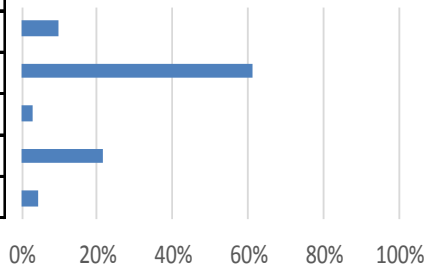
選択肢	選択数	割合	前年増減
①	19	17%	4%
②	23	21%	−3%
③	47	42%	5%
④	22	20%	−6%



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。

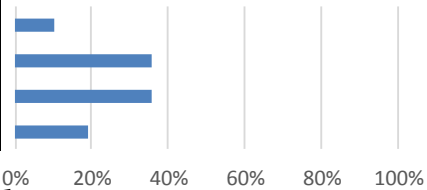
選択肢	選択数	割合	前年増減
①	11	10%	3%
②	68	61%	−1%
③	3	3%	1%
④	24	22%	2%
⑤	5	5%	−5%



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	前年増減
①	11	10%	0%
②	39	35%	−5%
③	39	35%	1%
④	21	19%	4%

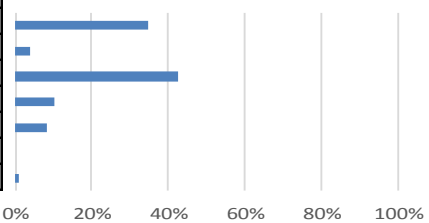


第3部　組織的・人的な対応について

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。

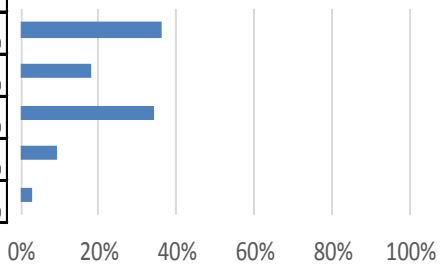
選択肢	選択数	割合	前年増減
①	38	35%	2%
②	4	4%	0%
③	47	43%	2%
④	11	10%	−2%
⑤	9	8%	0%
⑥	0	0%	−1%
⑦	1	1%	−1%



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	前年増減
①	40	36%	10%
②	20	18%	−4%
③	38	34%	−5%
④	10	9%	0%
⑤	3	3%	−1%

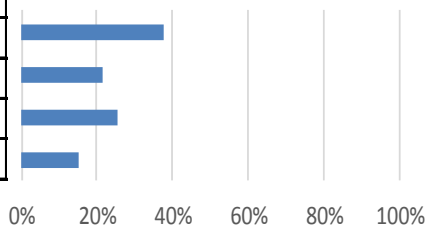


【⑤その他への回答内容】
・ 就業規則で守秘義務を明記しているが、契約書等では明記していない
・ 守秘義務に関して違反した場合に罰則を設定

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	前年増減
①	42	38%	10%
②	24	22%	−6%
③	28	25%	−1%
④	17	15%	−3%

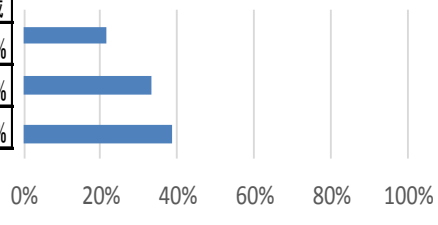


問4　情報セキュリティに関する業務委託を外部組織と契約する際に、情報漏洩や情報消失・破壊など障害対応について責任の所在を明確にし、外部組織による定期的な点検・大学による点検の監視など障害を予防するための取り決めをしていますか。

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	前年増減
①	24	22%	5%
②	37	33%	−1%
③	43	39%	−4%

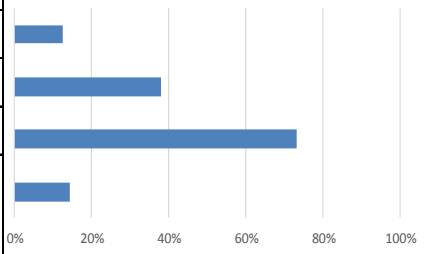
（該当契約なし等7校無回答）



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）

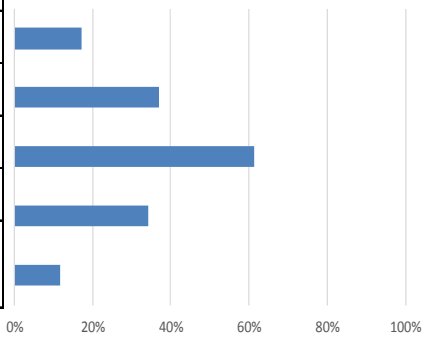
（1）危機意識の共有化

危機意識共有化の方法	選択数	割合	前年増減
① 学内外の情報セキュリティ研修会参加の義務化	14	13%	1%
② FD・SD,教授会,職員会議などでの定期的な情報提供	42	38%	2%
③ Webサイトや学内文書による定期的な情報提供	81	73%	-4%
④ その他(Webサイト・メール・学内文書で必要に応じて情報提供,eラーニング研修の義務化,情報セキュリティ研修会の実施、セキュリティハンドブックやクラウドサービス利用ガイドラインの配布,FD・SDにて不定期に情報提供,情報セキュリティ委員会の年1回実施,メール等で不定期な情報提供,脅威となる事象発生時に情報提供・周知・注意喚起など)	16	14%	-3%



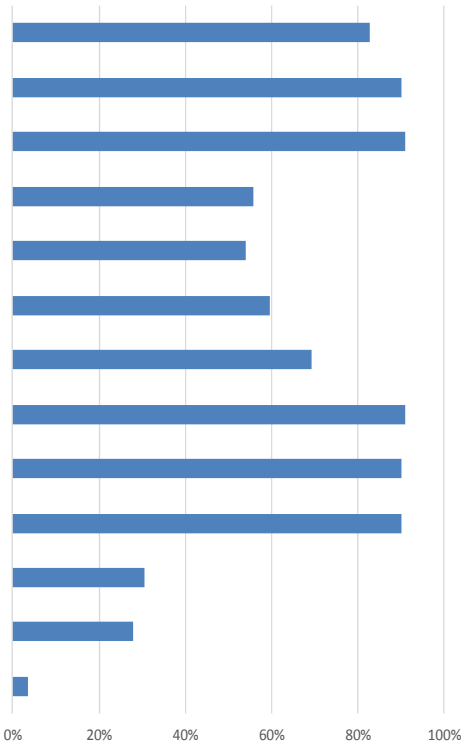
（2）学内ルールの周知徹底と遵守の確認

学内ルール周知徹底･遵守の方法	選択数	割合	前年増減
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	19	17%	-3%
② 教授会、職員会議などでのルールの周知と遵守の確認	41	37%	6%
③ Webサイトでのルールの紹介と遵守の呼びかけ	68	61%	-4%
④ 説明会でのルールの紹介と遵守の呼びかけ	38	34%	-3%
⑤ その他(メール・通達等で注意喚起,新任教職員・学生等にリーフレット配布,入職時に実施,脅威発生時の周知など)	13	12%	3%



（3）攻撃に対する防御対策

防御対策の内容	選択数	割合	前年増減
① 公的機関を装った偽装メールの注意喚起	92	83%	0%
② メール添付ファイル開封の注意喚起	100	90%	-1%
③ メールにリンクされたURL接続の注意喚起	101	91%	-2%
④ USBメモリなど外部持ち込みの注意喚起	62	56%	6%
⑤ 脅威となる事象の被害状況報告と対策説明	60	54%	4%
⑥ IDの管理やパスワードの定期的な見直し注意喚起	66	59%	0%
⑦ 不正アクセスの監視と異常事態の発見	77	69%	10%
⑧ ファイアウォールや迷惑メールの設定	101	91%	-2%
⑨ VLANなどネットワークのアクセス制限の設定	100	90%	2%
⑩ 無線LANの暗号化及び認証方式の導入	100	90%	3%
⑪ データ暗号化の導入	34	31%	-1%
⑫ クラウドに対する利活用の注意喚起	31	28%	6%
⑬ その他(SNS・スマホ・写真データ・機器メンテ・ネットトラブルに対する注意喚起,多要素認証,パスワードポリシー厳格化（10桁）,Web詐欺サイト注意喚起,SNSへパスワードアップロード禁止)	4	4%	0%

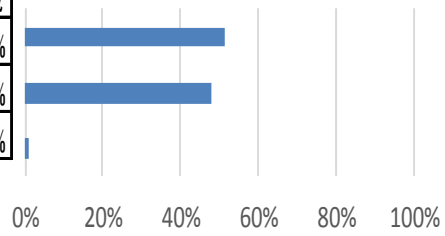


第4部　技術的・物理的対策について

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。

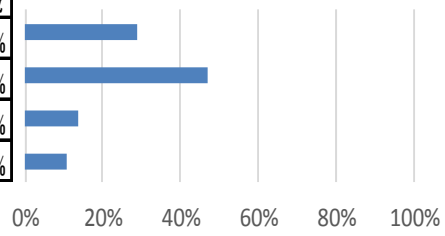
選択肢	選択数	割合	前年増減
①	57	51%	7%
②	53	48%	−7%
③	1	1%	0%



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。

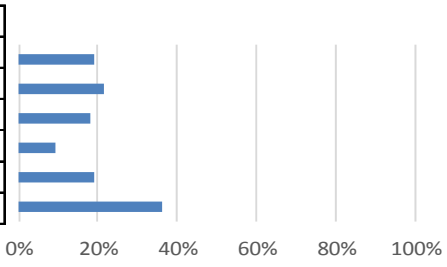
選択肢	選択数	割合	前年増減
①	32	29%	−3%
②	52	47%	11%
③	15	14%	0%
④	12	11%	−8%



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。

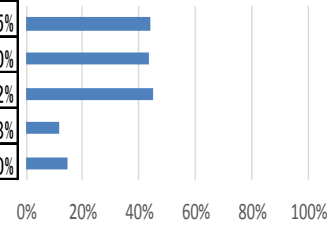
選択肢	選択数	割合	前年増減
①	21	19%	2%
②	24	22%	6%
③	20	18%	6%
④	10	9%	5%
⑤	21	19%	−7%
⑥	40	36%	−7%



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	前年増減
①	49	44%	5%
②	48	43%	0%
③	50	45%	2%
④	13	12%	8%
⑤	16	14%	0%

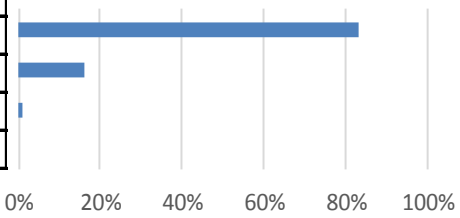


【⑤その他への回答内容】
- パスワード設定を利用マニュアルや授業等で注意喚起
- パスワードに有効期限を設定
- 2段階認証の義務化や推奨
- AD構築・運用
- 人事データに基づいたID管理
- 全ての利用者で識別と認証を実施

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。

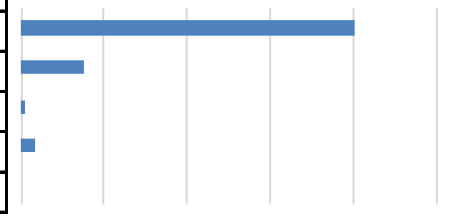
選択肢	選択数	割合	前年増減
①	92	83%	7%
②	18	16%	−6%
③	1	1%	0%
④	0	0%	−1%



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。

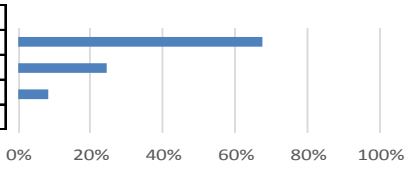
選択肢	選択数	割合	前年増減
①	89	80%	2%
②	17	15%	−5%
③	1	1%	0%
④	4	4%	3%
⑤	0	0%	0%



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。

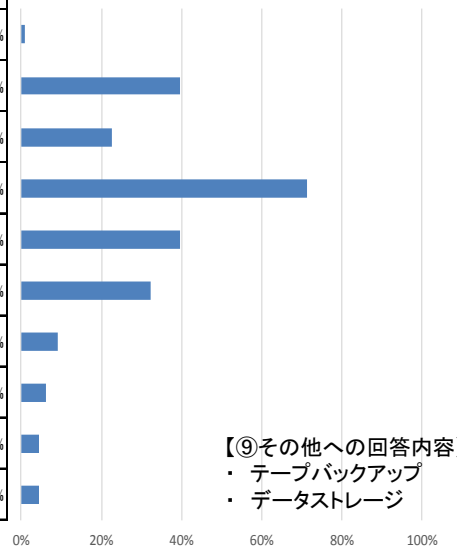
① ぜい弱性に対して最新の修正プログラムを用いて対応している。
② 最新の修正プログラムを適用するまでの間、当面の対応としてぜい弱性を狙った攻撃を回避するソフトウェアもしくはハードウェアを導入して対応している。
③ ぜい弱性対策を検討している。
④ ぜい弱性対策はしていない。

選択肢	選択数	割合	前年増減
①	75	68%	6%
②	27	24%	0%
③	9	8%	−3%
④	0	0%	−3%



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	前年増減
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。	1	1%	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。	44	40%	8%
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。	25	23%	1%
④ バックアップは毎日行っている。	79	71%	1%
⑤ バックアップは一定の期間で行っている。	44	40%	−6%
⑥ 学内でシステムの二重化を行っている。	36	32%	−7%
⑦ 部門単位でシステムの二重化を行っている。	10	9%	3%
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。	7	6%	−1%
⑨ その他のバックアップ方法	5	5%	1%
⑩ バックアップへの備えについて検討している。	5	5%	−1%

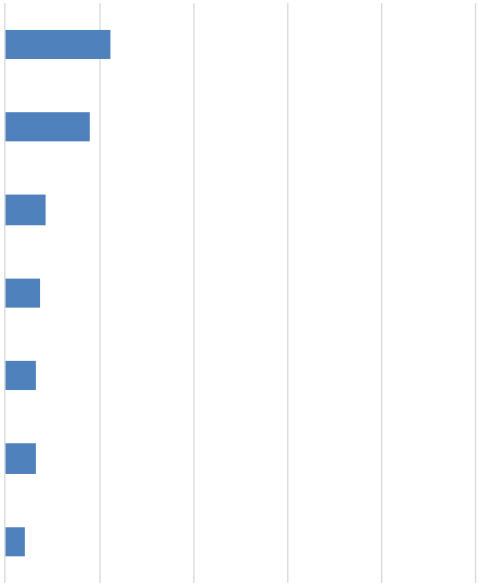


【⑨その他への回答内容】
- テープバックアップ
- データストレージ

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を記述してください。**

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	21	22%
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	17	18%
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	8	9%
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	7	7%
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	6	6%
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	6	6%
第4部　技術的・物理的対策について 問８　重要な情報資産をバックアップ。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	4	4%



※　項目を回答した目標設定校は94校、上記はその中での上位7項目

※　その他には、第1部の問3・4・5、第2部の問2・3、第4部の問1・2・3・4・6・7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額実績とその内容について**

  - 増額なし（回答記入64校中、47校・7割）
  - 削減傾向（1件）
  - 予算化されていない

  - 増加傾向
  - セキュリティ教育のためのeラーニング、標的型攻撃メール訓練費用で増額
  - セキュリティアセスメント等費用で増額
  - IT基盤全体を見直す大規模構内プロジェクトで増額
  - 500万円増額
  - ファアイアウォール更新に伴いIPSやログ保管等の対策強化で500万円増額
  - ファイアウォール導入とOffice365ATP等で700万円増額
  - セキュリティ監視外注費用で900万円増額
  - 次世代型エンドポイント導入、情報セキュリティアセスメント費用で350万円増額
  - ログ解析SOCサービス正式利用で500万円増額
  - 振る舞い型及びサンドボックス機能のメールサーバ導入で1,600万円増額
  - ネットワーク接続時のセキュリティチェック設備で600万円増額
  - メールセキュリティ強化で1,400万円増額
  - クラウドサービスへのデータベースバックアップ、セキュアなオンラインストレージサービス導入で3,000万円増額
  - セキュリティソリューション導入で4,000万円増額

回答大学の情報

４．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）人的な取り組み

- 標的型攻撃メール訓練実施（4件）
- 情報セキュリティ教育実施、CSIRT活動開始
- 専任教職員向け教育

- 教職員・学生に情報セキュリティ冊子を配布（2件）
- 教員へ情報セキュリティに関するWebアンケート実施、資産管理システムによる事務端末から外部記録媒体への書き込み制限、教員へのウィルス対策ソフト配布

- 情報セキュリティポリシーや関連ガイドラインの制定・施行（3件）
- ネットワークセキュリティ向上のためのワーキング設置
- 管理業者を変更予定で、この機会に各種体制、予算額、セキュリティの内容、各種ルールなどの刷新を行う方向で検討
- 情報システム係を設置し、専門知識を有する職員を配置

- 事務組織での情報資産棚卸調査

回答大学の情報

４．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（２）物理的な取り組み

- 多要素認証を導入
- 2段階認証利用の促進
- ワンタイムパスワード導入、IPS導入
- ネットワーク監視、IDS導入を検討
- セキュリティ監視サービス導入
- AI型アンチウィルスの導入
- 脅威情報提供サービスJLIST導入
- WAF導入
- Webサイト改ざん監視
- 標的型攻撃メール対策でSandBox導入
- サーバ室に入退室管理システムを導入
- G Suiteを活用しており2段階認証の学内推奨と上層部で評価中、2008Server更新
- バックアップや情報共有を安全に行うためクラウドサービスを利用
- インシデント発生の際の迅速な初動対応が可能となり、感染被害を最小限となるよう事務端末へのEDR機能のあるエンドポイントを導入
- 業務用事務PCの仮想端末化
- 大学公認クラウドストレージサービス導入、教育・研究・業務において他のクラウド利用及びUSBによるデータの受け渡しを禁止。また、メールへのファイル添付を原則禁止することの検討
- アカウントアダプター導入
- エンドポイント対策としてMS Defender ATPに段階的に切り替えを開始予定
- MACアドレスによる学内LAN接続監視
- 全学的にVLANなどでネットワーク分離を開始
- メール環境の移行、回線高速化に伴うセキュリティ強化、無線環境の充実と暗号化強化を予定
- 標的型攻撃メールや侵入検知などの対策だけでなく、外部へデータが不正に流出しない対策を検討
- 情報コンセントへの接続や持ち込みPCチェックを強化