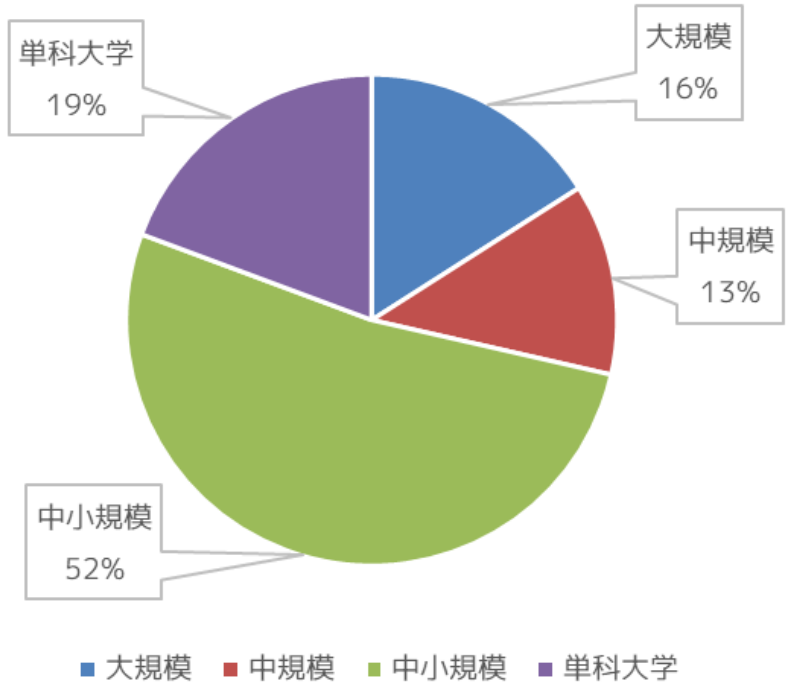
大学情報セキュリティベンチマークテスト結果
2017

私立大学情報教育協会

回答校の規模

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	19
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	62
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
⑤　全回答大学	119



回答校の平均点

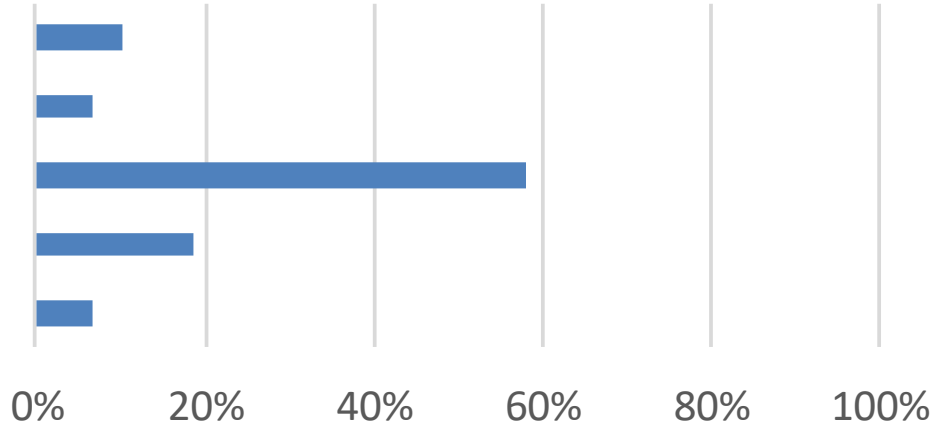
合計の平均点数	平均点	100点中の割合	前年増減
①　大規模大学	61	61%	−2%
②　中規模大学	55	55%	0%
③　中小規模大学	49	49%	−1%
④　単科大学・短期大学	49	49%	2%
⑤　全回答大学	52	52%	0%

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。

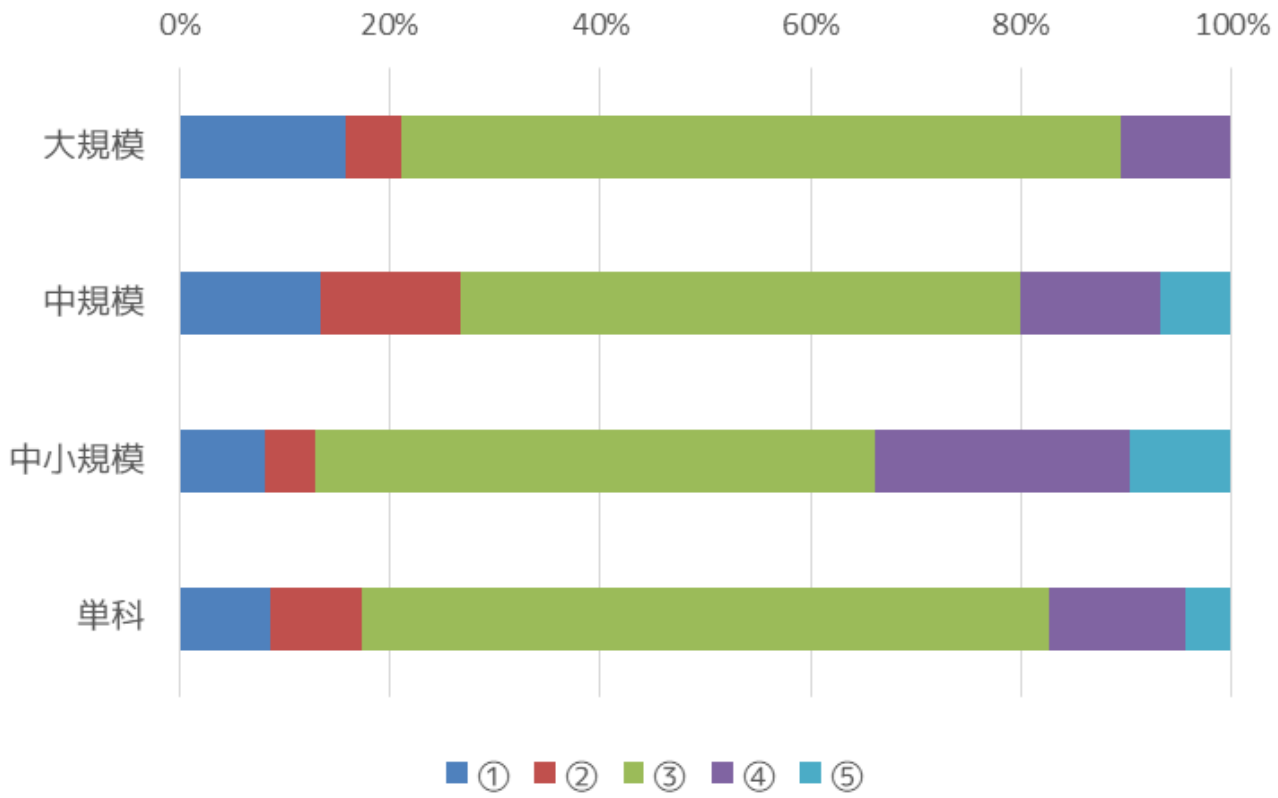
① 経営執行部が中心となり、全学組織を対象に危機意識の共有化に努めている。
② 経営執行部の方針により、学部単位など部門の管理責任者を通じて危機意識の共有化に努めている。
③ 経営執行部の方針により、情報センター等部門を通じて危機意識の共有化に努めている。
④ 経営執行部による危機意識の共有化はしていないが、現在、検討している。
⑤ 経営執行部による危機意識の共有化はしていない。

選択肢	選択数	割合	前年増減
①	12	10%	0%
②	8	7%	4%
③	69	58%	0%
④	22	18%	0%
⑤	8	7%	−4%



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。

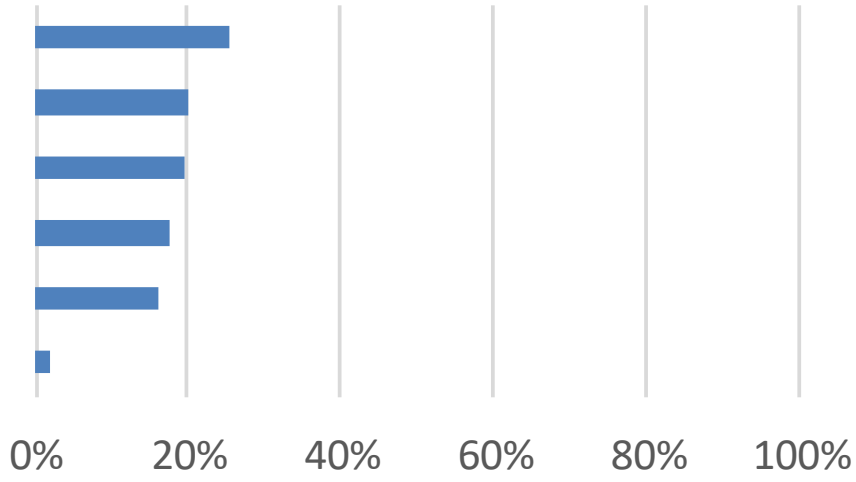
① 経営執行部が中心となり、全学組織を対象に危機意識の共有化に努めている。
② 経営執行部の方針により、学部単位など部門の管理責任者を通じて危機意識の共有化に努めている。
③ 経営執行部の方針により、情報センター等部門を通じて危機意識の共有化に努めている。
④ 経営執行部による危機意識の共有化はしていないが、現在、検討している。
⑤ 経営執行部による危機意識の共有化はしていない。



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。

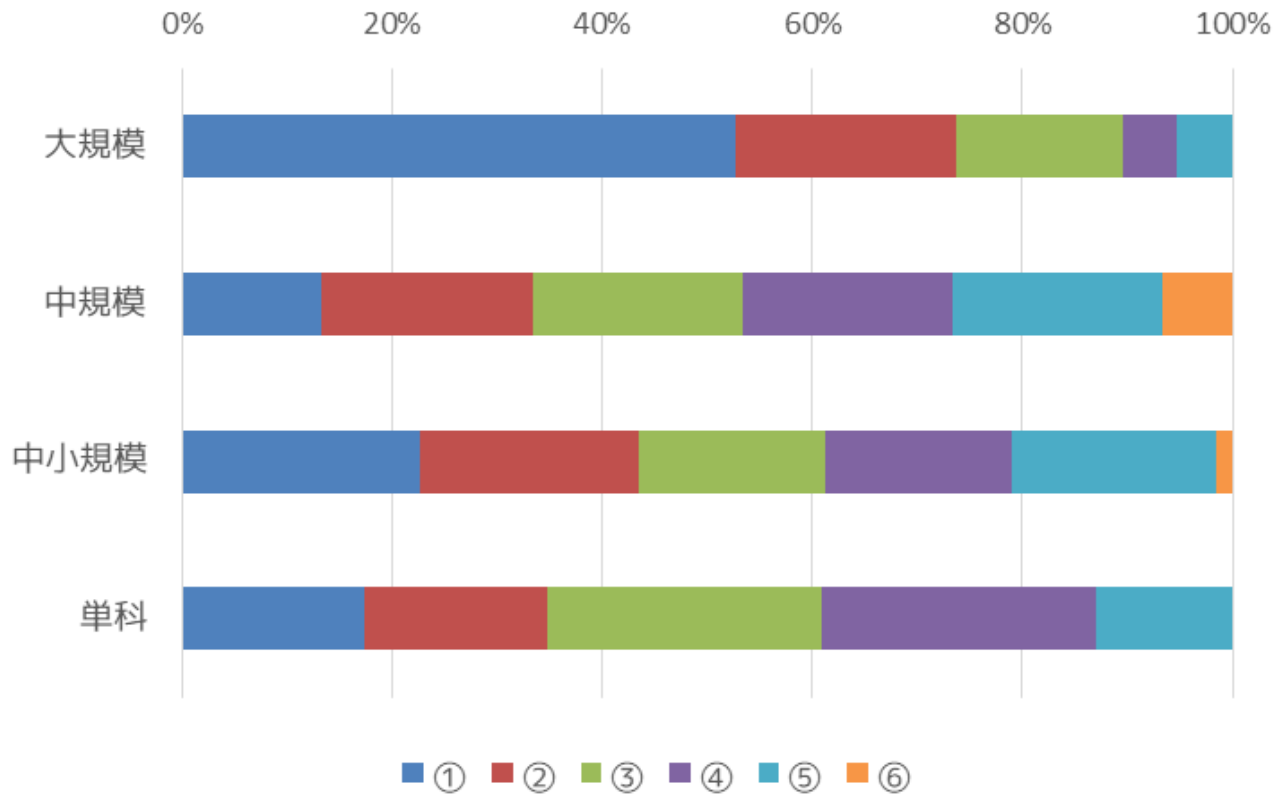
① 経営執行部の方針により、学内ルールの策定とその周知徹底を行っている。
② 経営執行部の方針により、学内ルールの策定を行っているが、周知徹底はできていない。
③ 経営執行部ではなく情報センター等部門により、学内ルールを策定し、その周知徹底を行っている。
④ 経営執行部ではなく情報センター等部門により、学内ルールを策定しているが、周知徹底はできていない。
⑤ 学内ルールの策定とその周知徹底を検討している。
⑥ 学内ルールの策定はしていない。

選択肢	選択数	割合	前年増減
①	30	25%	4%
②	24	20%	2%
③	23	19%	−6%
④	21	18%	2%
⑤	19	16%	−2%
⑥	2	2%	−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。

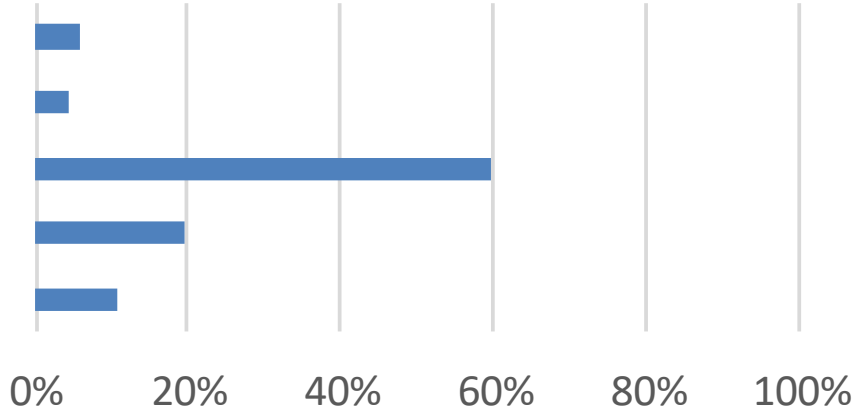
① 経営執行部の方針により、学内ルールの策定とその周知徹底を行っている。
② 経営執行部の方針により、学内ルールの策定を行っているが、周知徹底はできていない。
③ 経営執行部ではなく情報センター等部門により、学内ルールを策定し、その周知徹底を行っている。
④ 経営執行部ではなく情報センター等部門により、学内ルールを策定しているが、周知徹底はできていない。
⑤ 学内ルールの策定とその周知徹底を検討している。
⑥ 学内ルールの策定はしていない。



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。

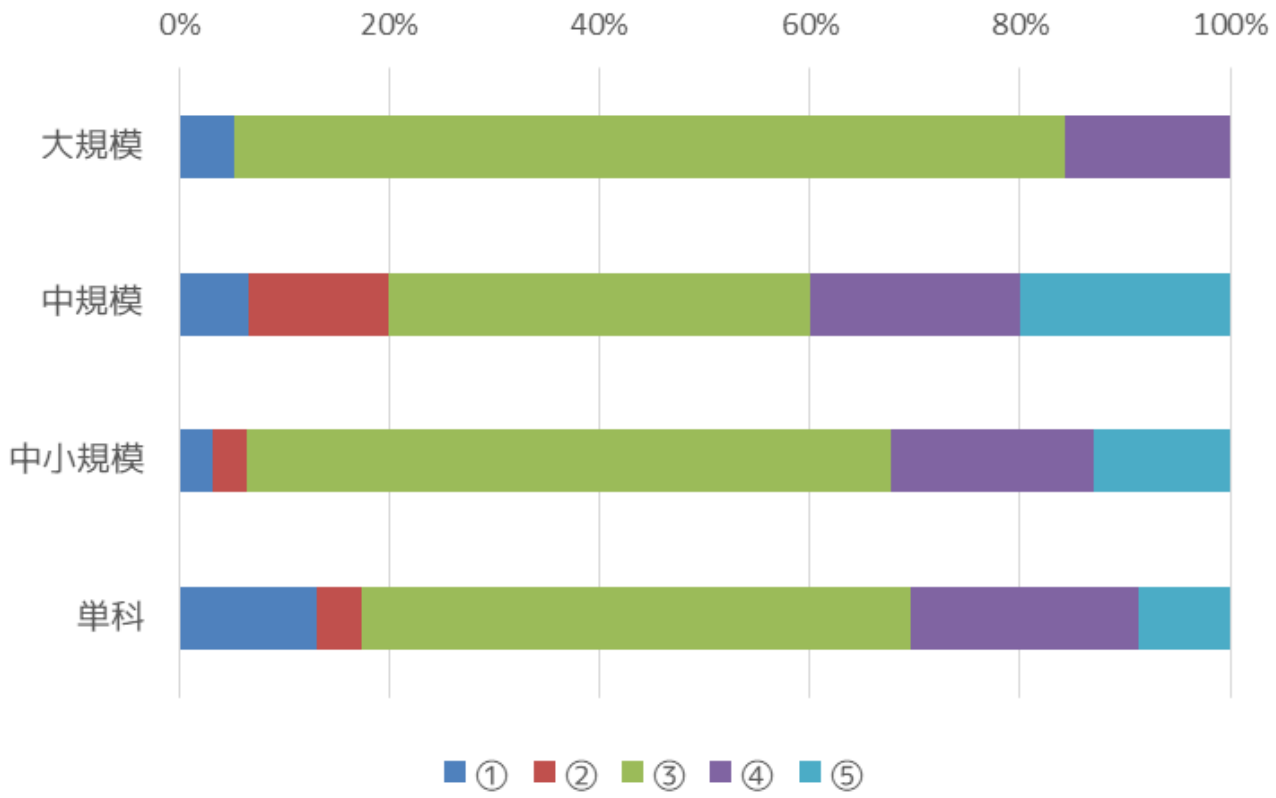
① 経営執行部が中心となり、全学組織を対象に防御体制を構築している。
② 経営執行部の方針により、学部単位など部門の管理責任者を通じて防御体制を構築している。
③ 経営執行部の方針により、情報センター等部門を通じて防御体制を構築している。
④ 経営執行部として防御体制を構築していないが、現在、検討している。
⑤ 経営執行部として防御体制を構築していない。

選択肢	選択数	割合	前年増減
①	7	6%	1%
②	5	4%	2%
③	71	60%	−3%
④	23	19%	1%
⑤	13	11%	−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。

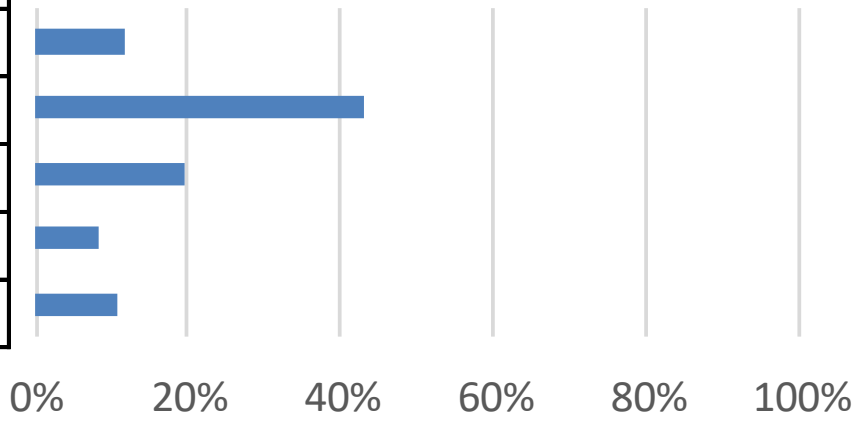
① 経営執行部が中心となり、全学組織を対象に防御体制を構築している。
② 経営執行部の方針により、学部単位など部門の管理責任者を通じて防御体制を構築している。
③ 経営執行部の方針により、情報センター等部門を通じて防御体制を構築している。
④ 経営執行部として防御体制を構築していないが、現在、検討している。
⑤ 経営執行部として防御体制を構築していない。



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。

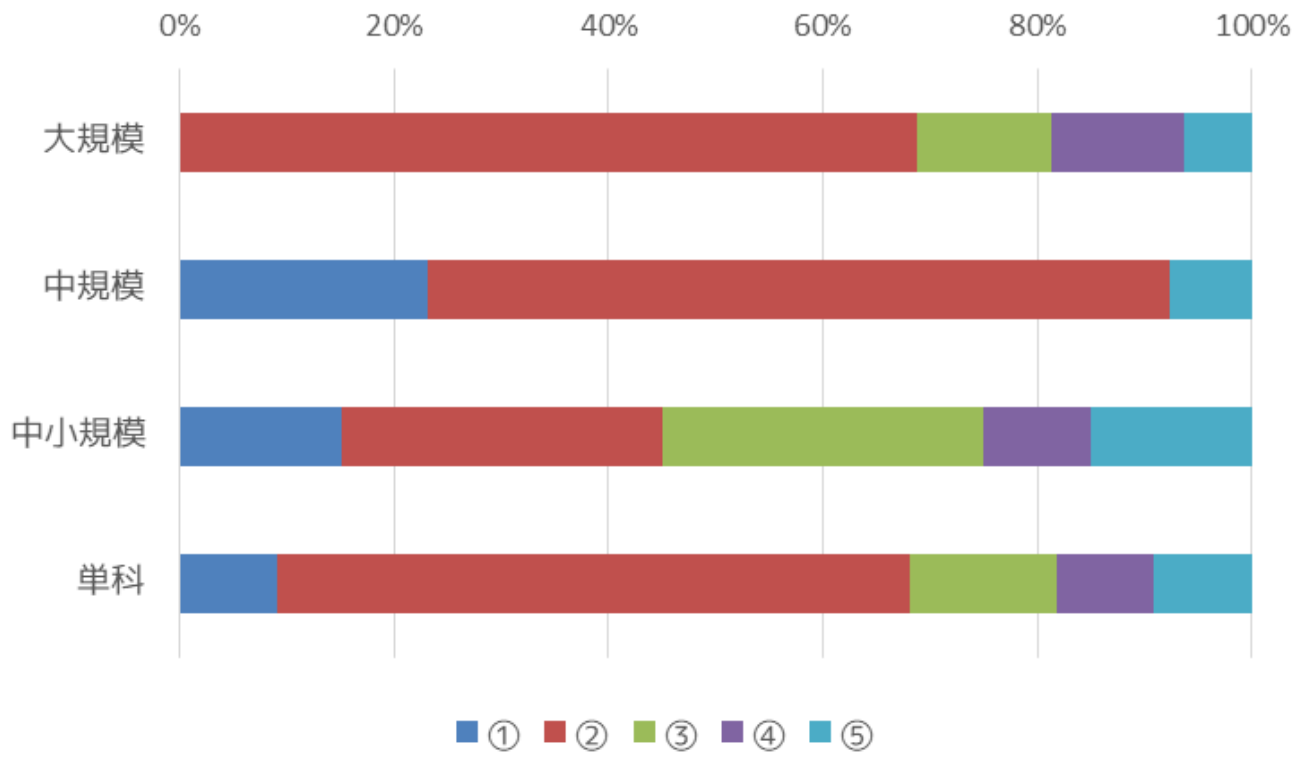
① 予算化はしていない。
② ３％以下
③ ４％～６％
④ ７％～９％
⑤ １０％以上

選択肢	選択数	割合	前年増減
①	14	12%	1%
②	51	43%	6%
③	23	19%	−7%
④	10	8%	−2%
⑤	13	11%	2%



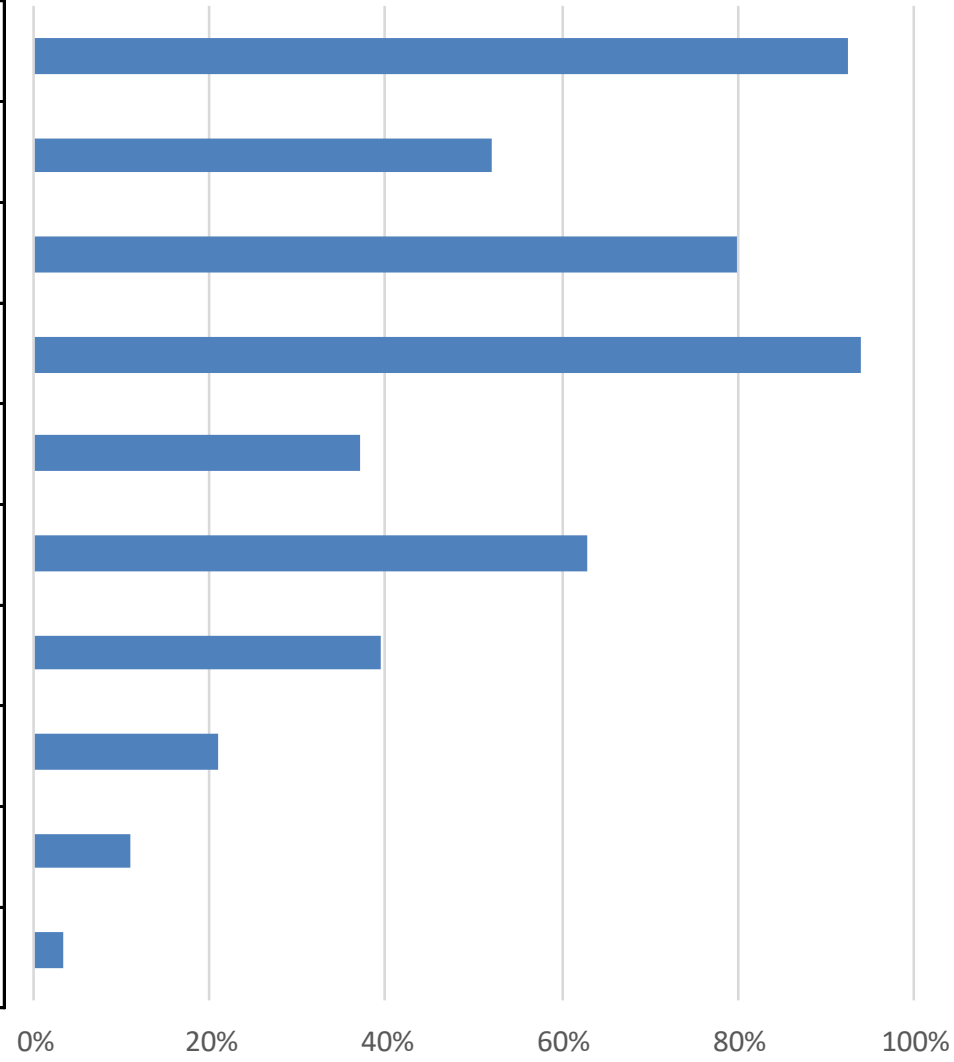
問４　今年度、貴大学のICT予算（物件費に限定）の中で、セキュリティ対策に充当している費用の割合。

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



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	110	92%	3%
② 侵入検知システム	62	52%	0%
③ VLANなどネットワーク関連	95	80%	10%
④ ウイルス対策ソフト・サービス	112	94%	2%
⑤ セキュリティ監視サービス	44	37%	-2%
⑥ フィルタリングソフト（Web、メール）	75	63%	2%
⑦ 暗号化対策	47	39%	9%
⑧ USB、SDカード、DVDなどの書き込み制御ソフト	25	21%	4%
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	13	11%	7%
⑩ その他　（講習・研修会等への参加, ログ収集ソフト, IPS, クライアント資源管理）	4	3%	0%

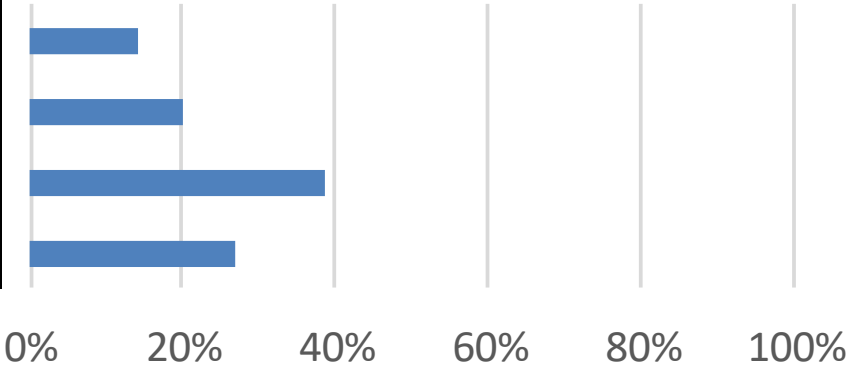


第2部
重要な情報資産の把握と管理対策について

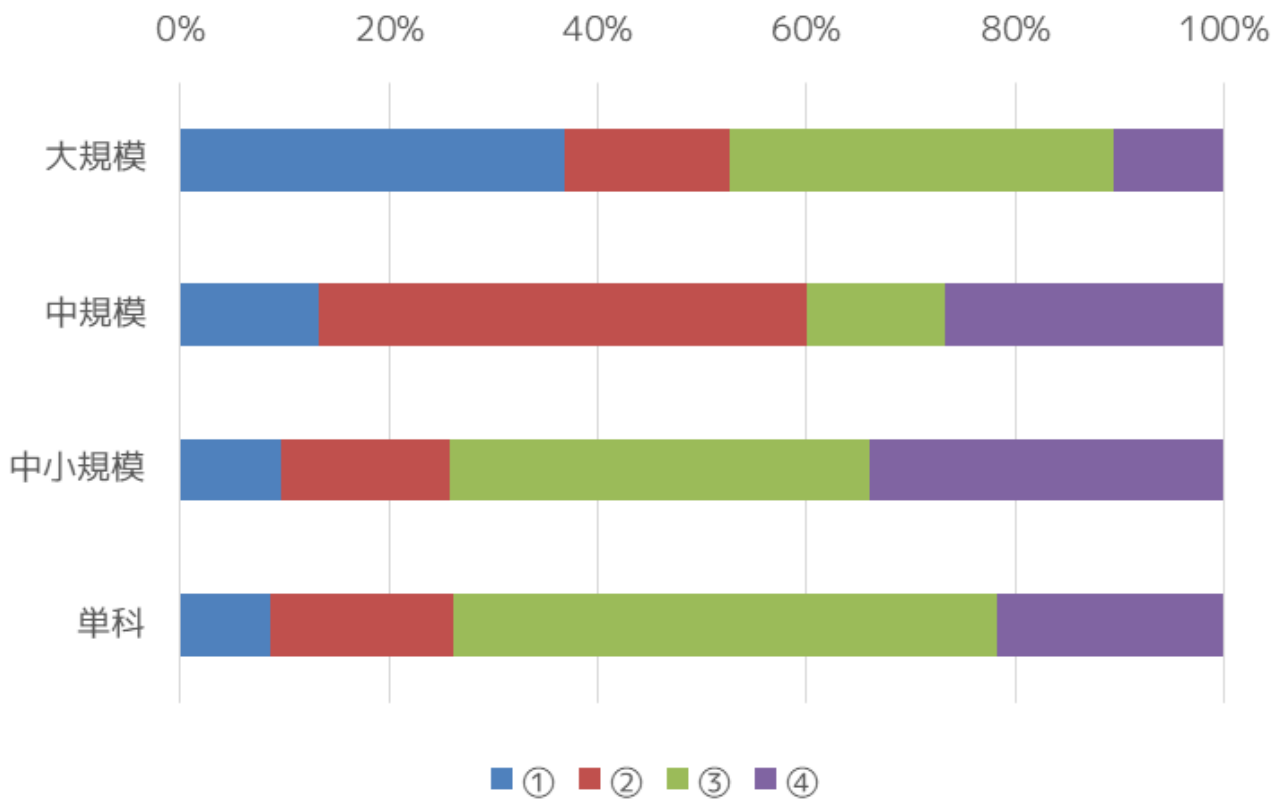
問１　重要な情報資産（金融資産情報を含む）の目録作成を実施。

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	17	14%	−7%
②	24	20%	−2%
③	46	39%	9%
④	32	27%	0%



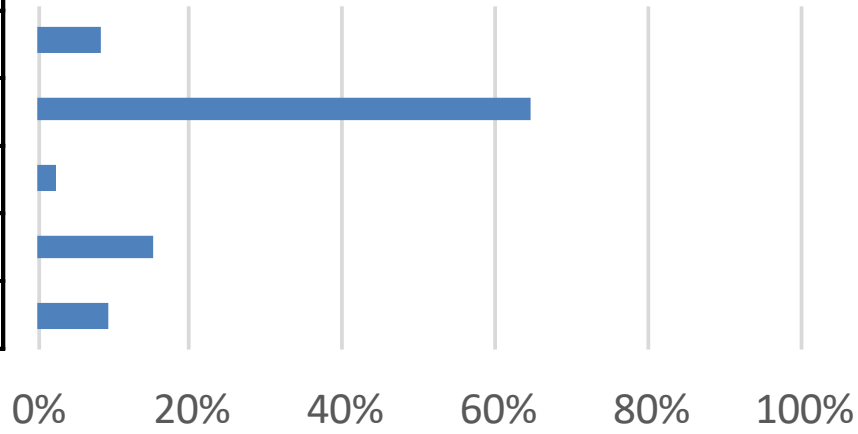
問１　重要な情報資産（金融資産情報を含む）の目録作成を実施。
① 実施しており、毎年見直しを行っている。
② 実施しているが、定期的な見直しは行っていない。
③ 検討している。
④ 実施していない。



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。

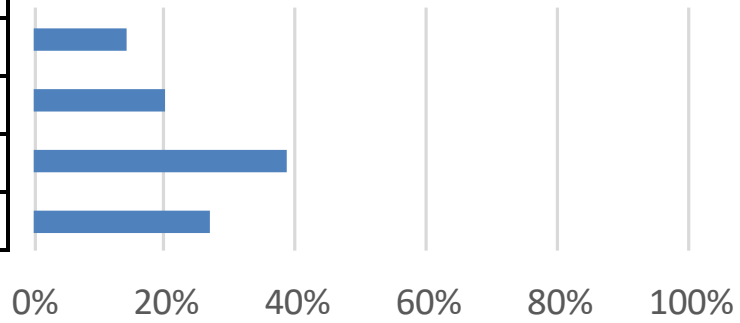
① 重要な情報資産に対するアクセス制御及びリスク評価を行っている。
② 重要な情報資産に対するアクセス制御を行っている。
③ 重要な情報資産に対するリスク評価を行っている。
④ 検討している。
⑤ 実施していない。

選択肢	選択数	割合	前年増減
①	10	8%	−5%
②	77	65%	5%
③	3	3%	1%
④	18	15%	0%
⑤	11	9%	−1%



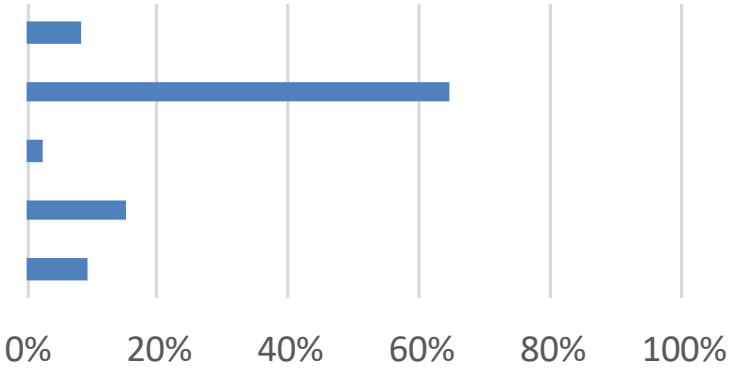
問１　重要な情報資産（金融資産情報を含む）の目録作成を実施。
① 実施しており、毎年見直しを行っている。
② 実施しているが、定期的な見直しは行っていない。
③ 検討している。
④ 実施していない。

選択肢	選択数	割合	前年増減
①	17	14%	−7%
②	24	20%	−2%
③	46	39%	9%
④	32	27%	0%



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。

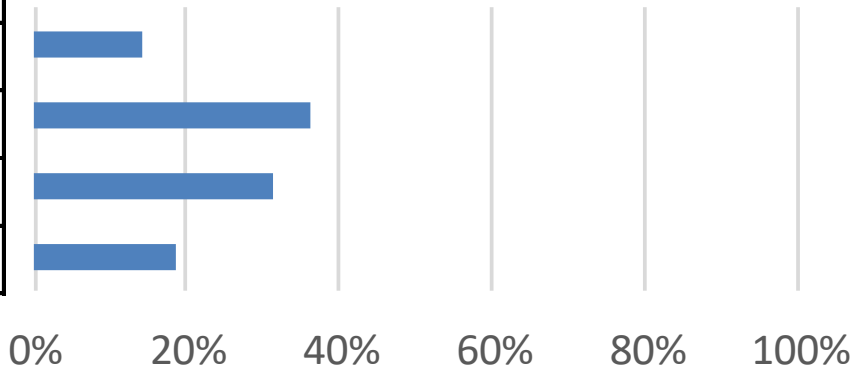
選択肢	選択数	割合	前年増減
①	10	8%	−5%
②	77	65%	5%
③	3	3%	1%
④	18	15%	0%
⑤	11	9%	−1%



重要資産の目録が無いのに、アクセス制御？

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	17	14%	0%
②	43	36%	−4%
③	37	31%	2%
④	22	18%	2%



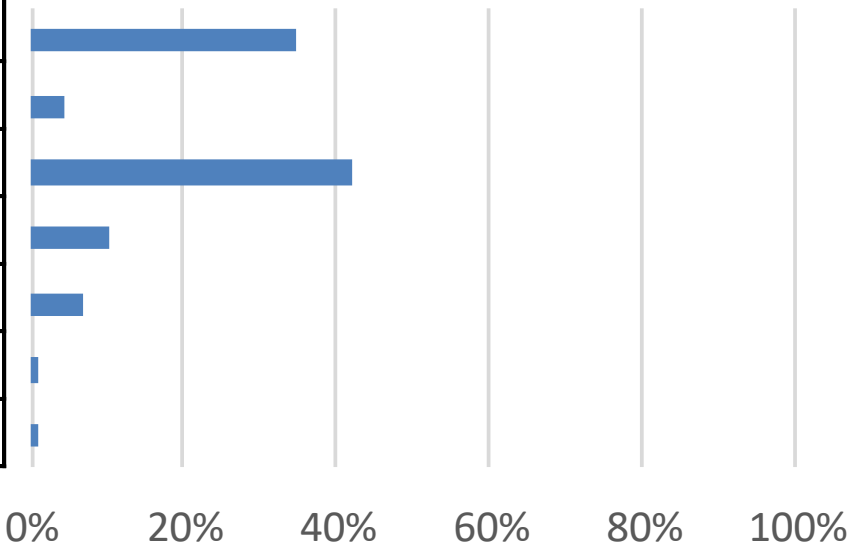
重要資産の目録作成を優先しましょう

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。

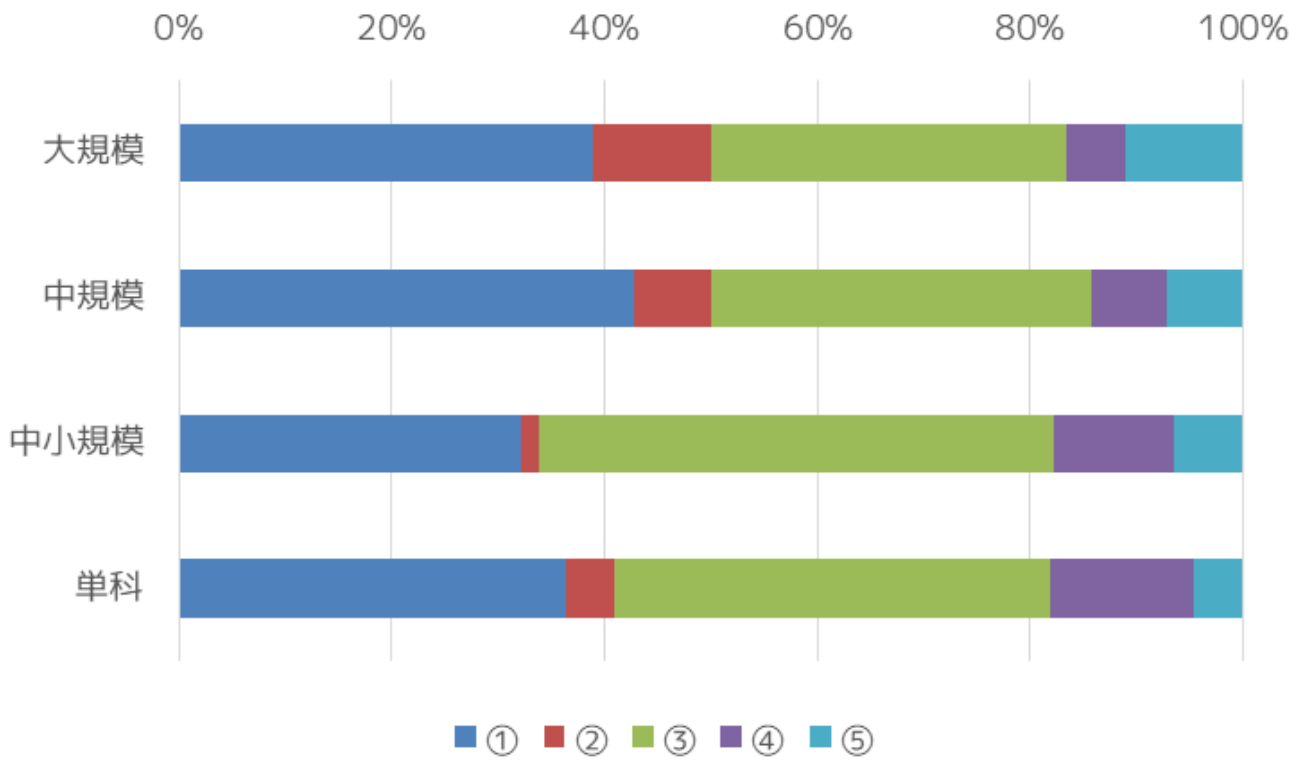
① 経営執行部として統括責任者を置き、情報セキュリティに関する専門の検討組織を設置し、実施組織として情報センター等部門を設置している。
② 統括責任者は置いていないが、情報セキュリティに関する専門の検討組織を設置し、実施組織として情報センター等部門を設置している。
③ 情報センター等部門を中心に対応している。
④ 情報センター等部門ではなく、情報セキュリティなどの検討委員会で対応している。
⑤ 組織の設置を検討している。
⑥ 組織の設置はしていないが、外部業者に委託している。
⑦ 組織の設置は考えていない。

選択肢	選択数	割合	前年増減
①	41	34%	5%
②	5	4%	−2%
③	50	42%	−4%
④	12	10%	0%
⑤	8	7%	1%
⑥	1	1%	−1%
⑦	1	1%	−1%



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。

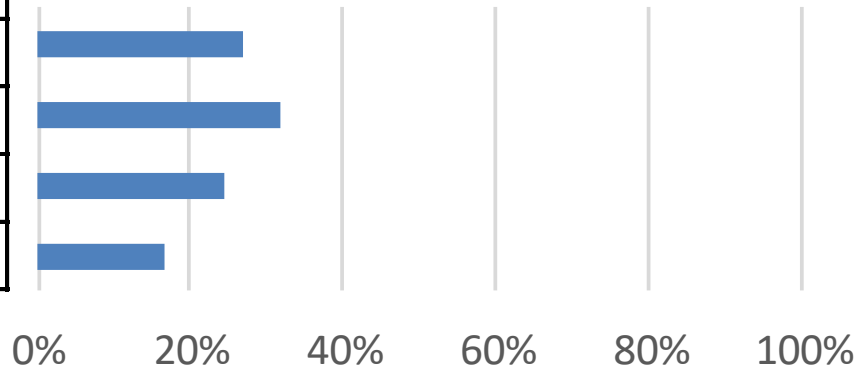
① 経営執行部として統括責任者を置き、情報セキュリティに関する専門の検討組織を設置し、実施組織として情報センター等部門を設置している。
② 統括責任者は置いていないが、情報セキュリティに関する専門の検討組織を設置し、実施組織として情報センター等部門を設置している。
③ 情報センター等部門を中心に対応している。
④ 情報センター等部門ではなく、情報セキュリティなどの検討委員会で対応している。
⑤ 組織の設置を検討している。
⑥ 組織の設置はしていないが、外部業者に委託している。
⑦ 組織の設置は考えていない。



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。

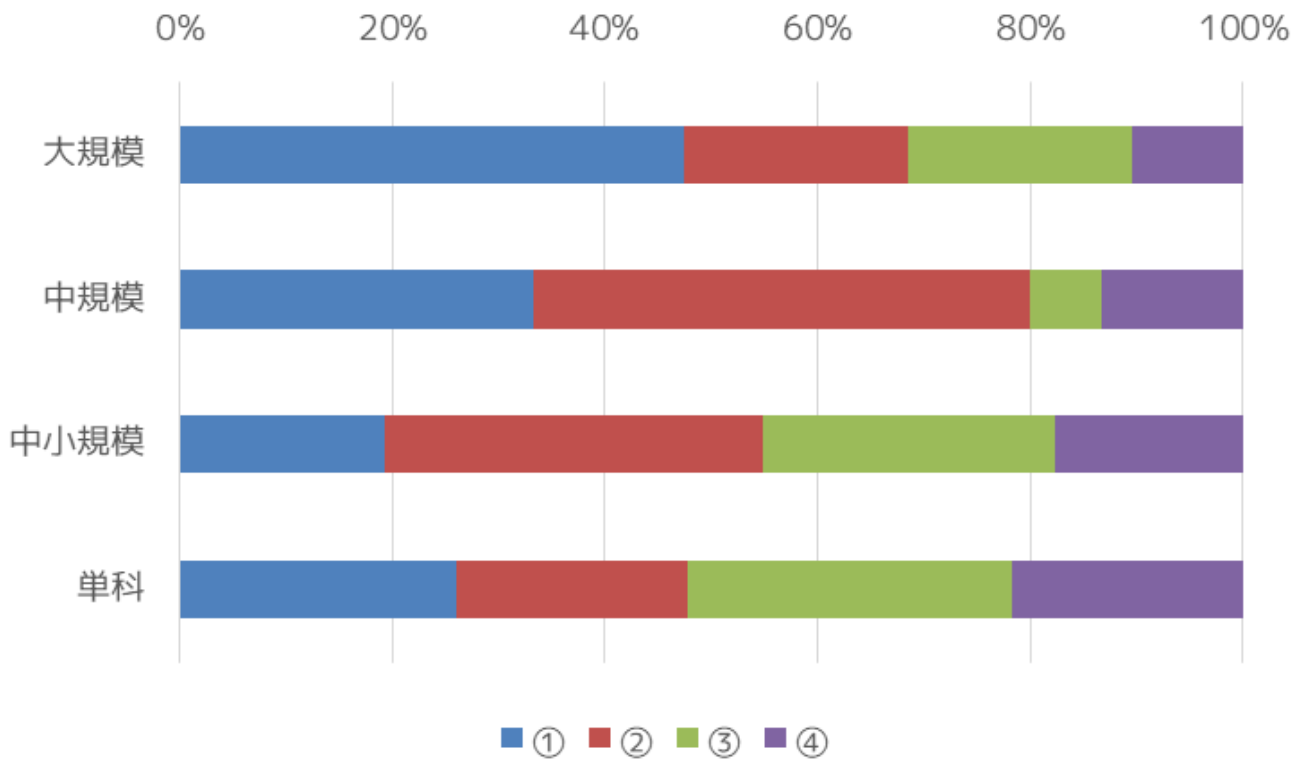
① 脅威となる事象の学内連絡体制及び処理の責任体制を確立し、対応手順も整備している。
② 学内の連絡体制と責任体制を確立しているが、対応手順は整備していない。
③ 学内の連絡体制を確立しているが、責任体制の確立と対応手順の整備はできていない。
④ 学内の連絡体制及び責任体制の確立と対応手順の整備はできていない。

選択肢	選択数	割合	前年増減
①	32	27%	2%
②	38	32%	1%
③	29	24%	−5%
④	20	17%	2%



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。

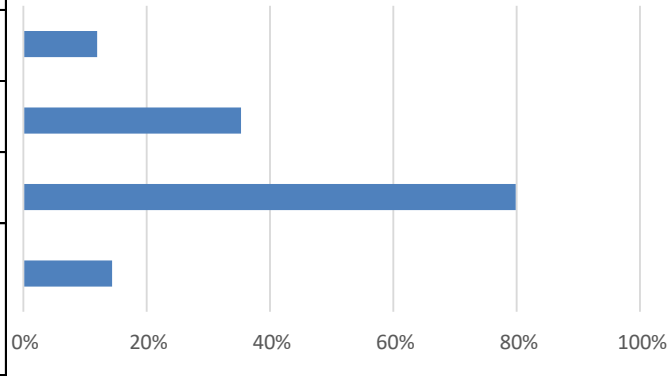
① 脅威となる事象の学内連絡体制及び処理の責任体制を確立し、対応手順も整備している。
② 学内の連絡体制と責任体制を確立しているが、対応手順は整備していない。
③ 学内の連絡体制を確立しているが、責任体制の確立と対応手順の整備はできていない。
④ 学内の連絡体制及び責任体制の確立と対応手順の整備はできていない。



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）

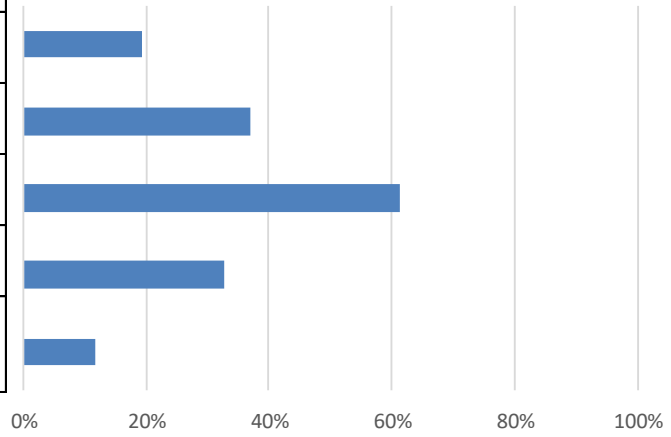
（１）危機意識の共有化

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	12%	−6%
② FD・SD,教授会,職員会議などでの定期的な情報提供	42	35%	1%
③ Webサイトや学内文書による定期的な情報提供	95	80%	8%
④ その他(不定期な情報提供,重大事象発生時に実施,外部講師を招いた講習会開催,情報セキュリティ委員会から各学部・各部署へ周知,職員は入局時に実施し教員は実施していない,教育計画中など)	17	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	23	19%	−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	44	37%	−1%
③ Webサイトでのルールの紹介と遵守の呼びかけ	73	61%	3%
④ 説明会でのルールの紹介と遵守の呼びかけ	39	33%	−1%
⑤ その他(メール,通達,利用案内,新入職員研修で周知,教育計画中など)	14	12%	−3%

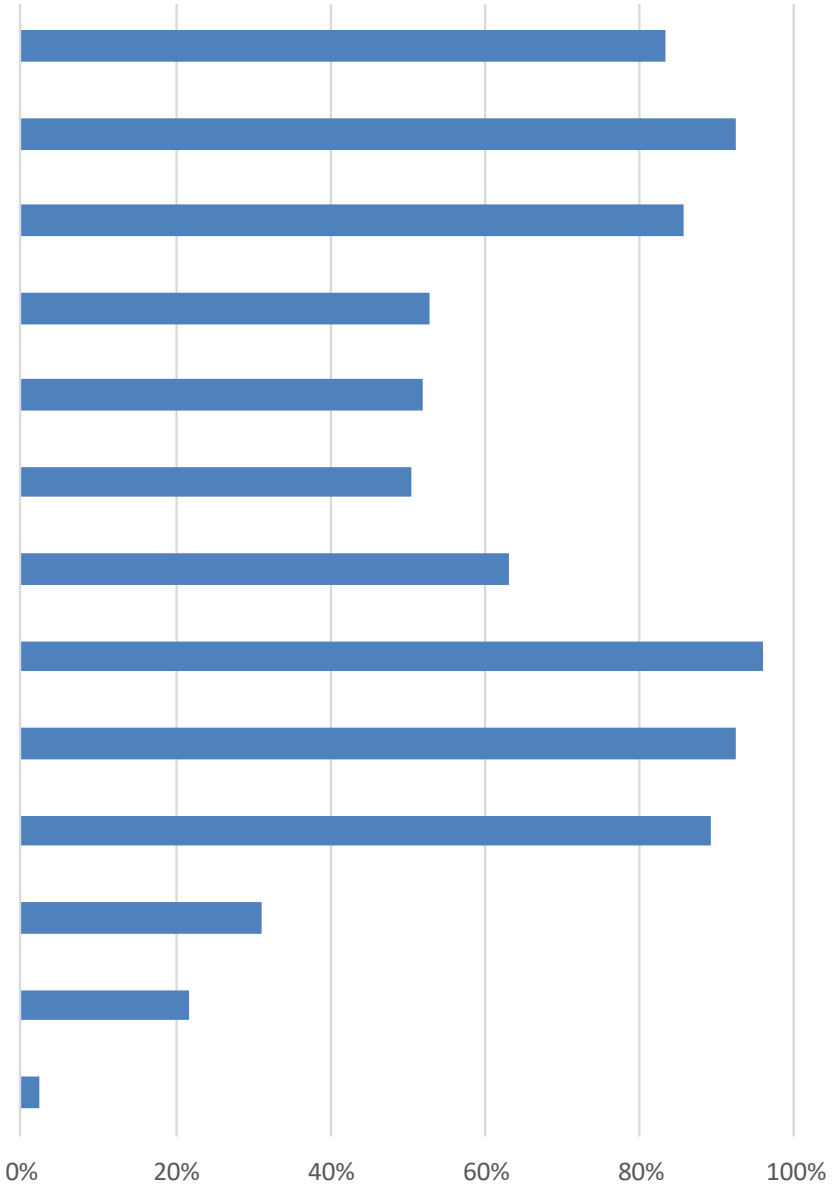


Webの告知だけで安心してはいけません！

教授会での告知は、議事録が残るので、インシデントが発生した場合の事後対応の際に有効

（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	99	83%	3%
② メール添付ファイル開封の注意喚起	110	92%	2%
③ メールにリンクされたURL接続の注意喚起	102	86%	4%
④ USBメモリなど外部持ち込みの注意喚起	63	53%	-8%
⑤ 脅威となる事象の被害状況報告と対策説明	62	52%	9%
⑥ IDの管理やパスワードの定期的な見直し注意喚起	60	50%	7%
⑦ 不正アクセスの監視と異常事態の発見	75	63%	1%
⑧ ファイアウォールや迷惑メールの設定	114	96%	2%
⑨ VLANなどネットワークのアクセス制限の設定	110	92%	6%
⑩ 無線LANの暗号化及び認証方式の導入	106	89%	-2%
⑪ データ暗号化の導入	37	31%	5%
⑫ クラウドに対する利活用の注意喚起	26	22%	-3%
⑬ その他(SNS,スマホに対する注意喚起,標的型攻撃メール訓練)	3	3%	1%

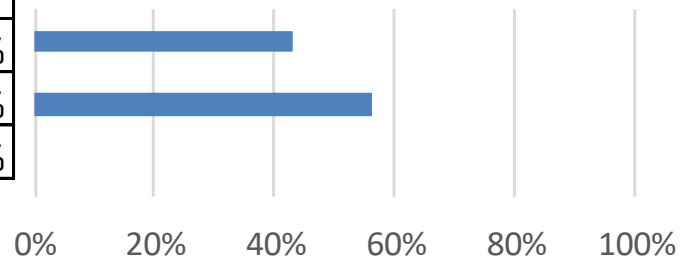


第4部
技術的・物理的対策について

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。

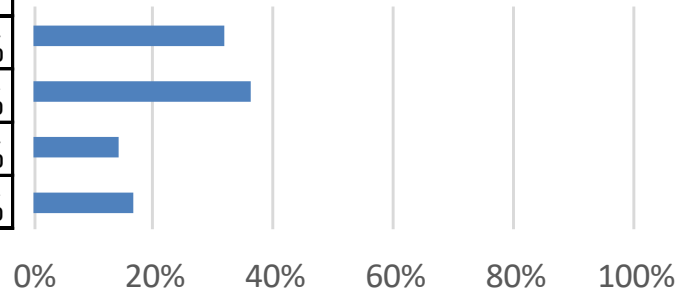
選択肢	選択数	割合	前年増減
①	51	43%	−1%
②	67	56%	2%
③	0	0%	−2%



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	38	32%	2%
②	43	36%	−5%
③	17	14%	3%
④	20	17%	−2%

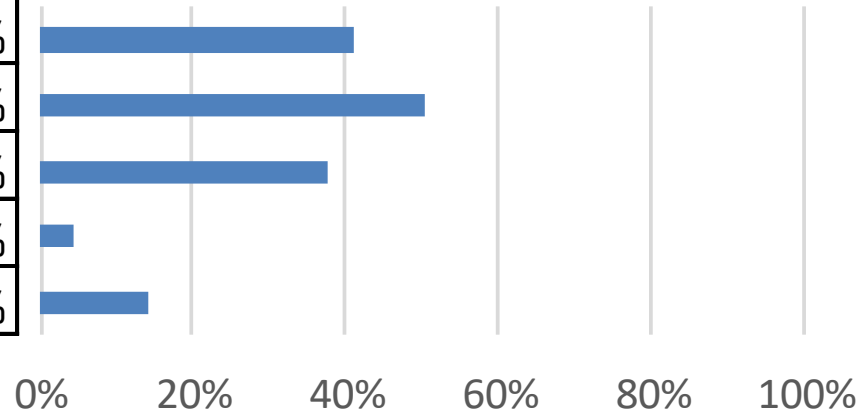


②は、危ないです！

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	41%	3%
②	60	50%	3%
③	45	38%	−4%
④	5	4%	−1%
⑤	17	14%	−4%



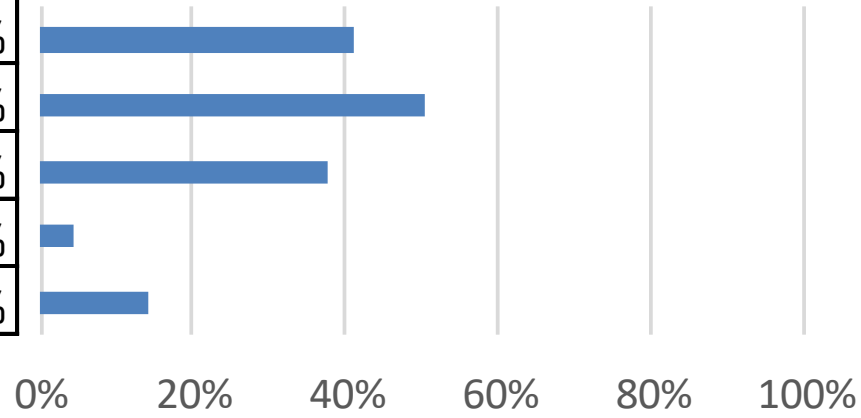
【⑤その他への回答内容】

・　統合認証
・　不審なアクセス・認証の監視
・　教職員証による認証
・　人事データに基づいて利用者IDを管理
・　初期パスワードに有効期限
・　強制的に推測できないメールPWを配布
・　推測しやすいパスワードを設定しないよう説明

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	41%	3%
②	60	50%	3%
③	45	38%	−4%
④	5	4%	−1%
⑤	17	14%	−4%



【⑤その他への回答内容】

・　統合認証
・　不審なアクセス・認証の監視
・　教職員証による認証
・　人事データに基づいて利用者IDを管理
・　初期パスワードに有効期限
・　強制的に推測できないメールPWを配布
・　推測しやすいパスワードを設定しないよう説明

共用アカウントは使ってはいけません

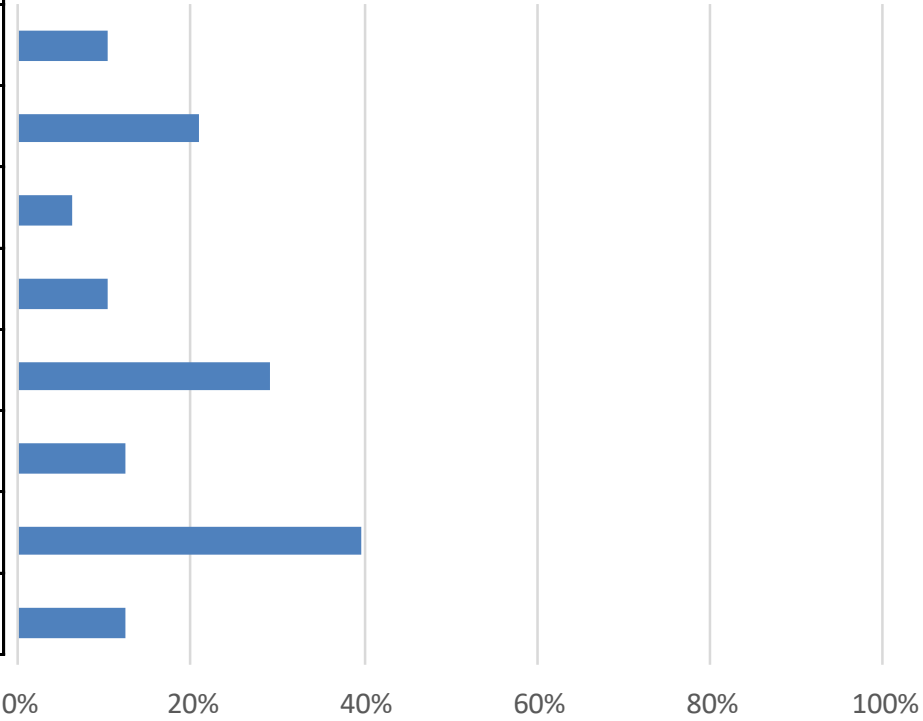
定期的に見直していてはいけません！

パスワード文字列の複雑さは、システム側で
チェック・強制しましょう！

回答大学の情報

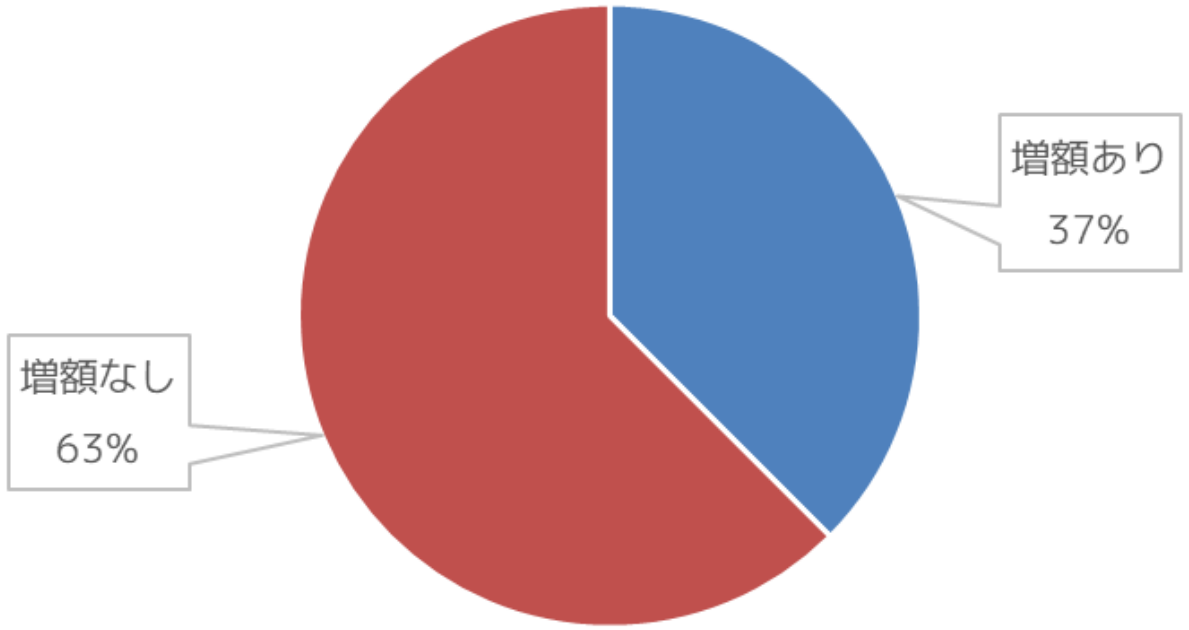
過去に教育・研究・経営活動に直接影響を与えるような脅威となる事象の有無を選択してください。

脅威となる事象の内容	選択数	割合	前年増減
① 添付メールによる個人情報の学外漏洩	5	10%	−1%
② 添付メールによる端末の破壊	10	21%	0%
③ システムへの不正侵入による個人情報の学外漏洩	3	6%	2%
④ システムへの不正侵入によるシステムの破壊	5	10%	6%
⑤ 大量のデータ送信によるサービス停止	14	29%	−11%
⑥ ホームページの改ざん	6	13%	10%
⑦ 端末使用を不能にして身代金を要求する攻撃	19	40%	14%
⑧ その他	6	13%	−17%



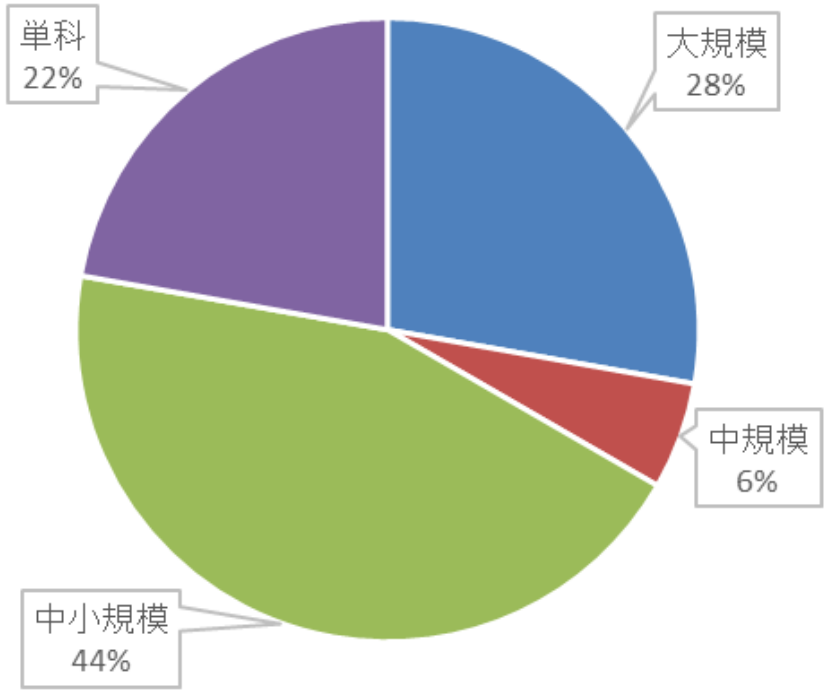
【⑧その他への回答内容】
・PC盗難、学内情報USB紛失
・プロキシサーバの不正利用
・ファイル共有ソフトでの情報漏えい
・ 不正侵入の踏み台
・ アカウント情報の不正取得
・ SPAMメールの大量送信によるメール受信拒否

セキュリティ対策予算の増額実績とその内容



N=48

セキュリティ対策予算の増額実績とその内容



N=18

セキュリティ対策予算の増額実績とその内容

1. 事務局ファイアウォール更新：　700万円（中規模）
2. 内部不正通信検知システム：　3600万円（中小規模）
3. Webサーバ脆弱性対策：　270万円（中小規模）
4. IPS、IT資産管理ツール：　150万円（中小規模）
5. ネットワーク監視機器購入：　500万円（単科）
6. システムのセキュリティ監査：　500万円（単科）
7. 講習会：　100万円（単科）

人的なセキュリティ対策の新たな取り組み

1. CSIRT設置（3件）
2. CISOとセキュリティ委員会設置（2件）
3. 情報セキュリティ事故発生時の対応体制を構築（2件）
4. 情報セキュリティに関する外部監査実施
5. 標的型攻撃メール対応訓練の実施
6. アンケート・自己点検
   ① 全教職員にチェックシートによる自己点検を実施し、結果を教授会や教職員Webで公表
   ② 事務職員にアンケート実施
   ③ 教員に個人PCのウィルス対策についてアンケート調査と指導

物理的なセキュリティ対策の新たな取り組み

1. 標的型攻撃対策機器の導入（3件）
2. IPS導入（4件）
3. メールシステムのセキュリティオプション（4件）
4. WAF導入（1件）
5. 事務システムファイルサーバの暗号化（１件）
6. 研究室等の外部公開用サーバ全てに脆弱性診断と対応支援を定期的に実施

ご協力頂いた方々

満永拓邦氏（東京大学情報学環）

松田亘氏（東京大学情報学環）

藤本万里子氏（東京大学情報学環）

ご清聴有難うございました。