ベンチマークリスト結果に見る
私立大学のセキュリティ課題

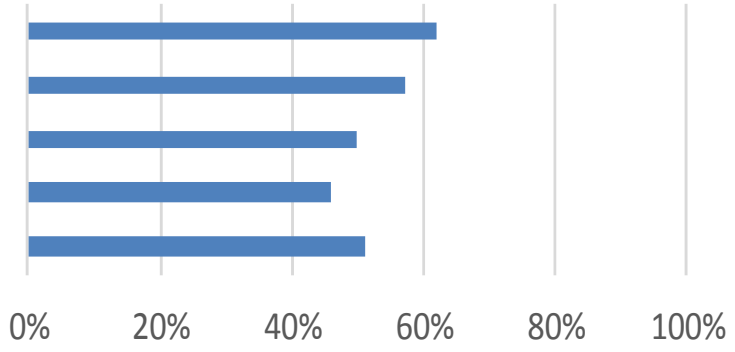
宮川　裕之

青山学院大学社会情報学部教授
情報セキュリティ研究講習会 前担当理事

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	18
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	18
③ 中小規模大学　入学定員2,000人未満　複数学部有り	70
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	32
全回答大学	138

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	62	62%	1%
② 中規模大学	57	57%	2%
③ 中小規模大学	50	50%	1%
④ 単科大学・短期大学	46	46%	−3%
全回答大学	51	51%	−1%

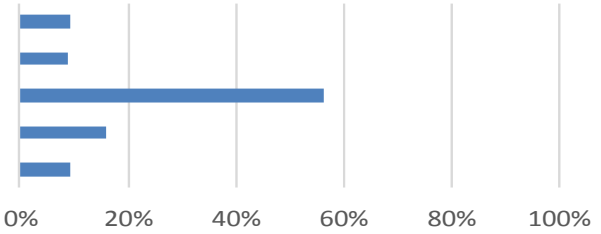


第1部　経営執行部の情報セキュリティに対する取組み

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。

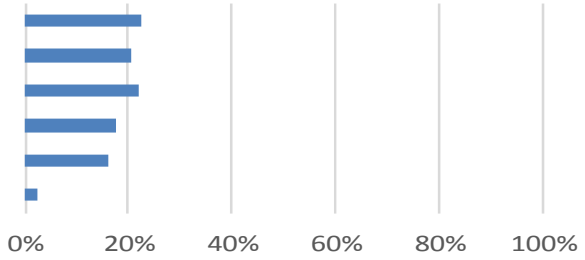
選択肢	選択数	割合	前年増減
①	13	9%	−1%
②	12	9%	2%
③	78	57%	−1%
④	22	16%	−2%
⑤	13	9%	2%



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。

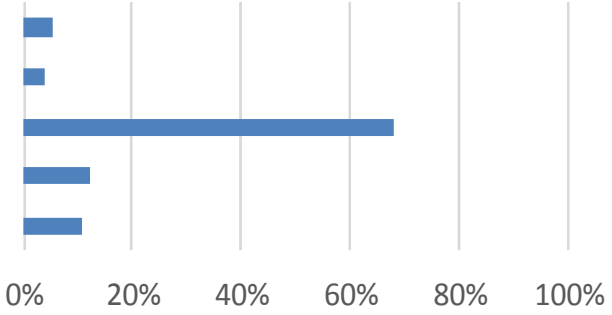
選択肢	選択数	割合	前年増減
①	31	22%	−3%
②	28	20%	0%
③	30	22%	3%
④	24	17%	−1%
⑤	22	16%	0%
⑥	3	2%	0%



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	前年増減
①	7	5%	−1%
②	5	4%	0%
③	93	68%	8%
④	17	12%	−7%
⑤	15	11%	0%

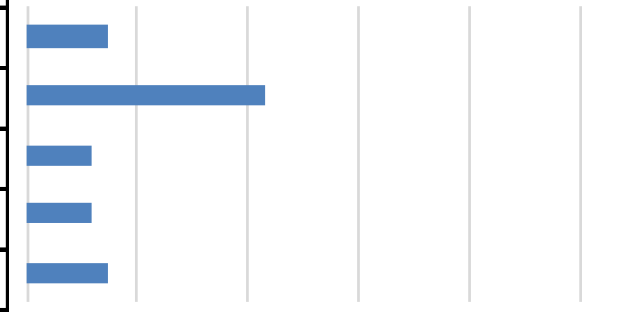


問4　今年度、貴大学のICT予算（物件費に限定）の中で、セキュリティ対策に充当している費用の割合。

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

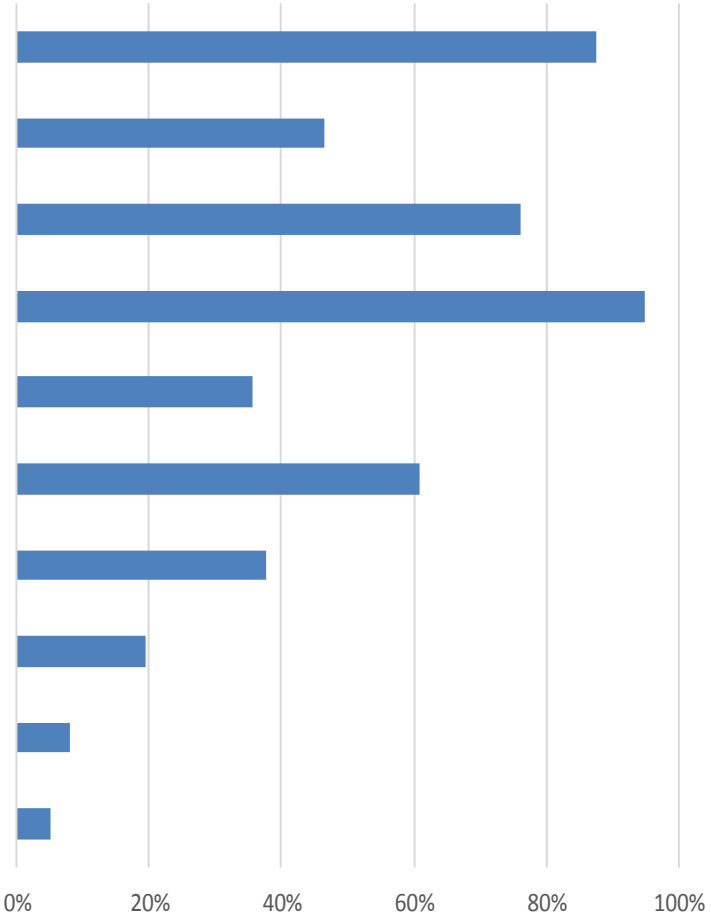
選択肢	選択数	割合	前年増減
①	20	14%	2%
②	59	43%	0%
③	16	12%	−7%
④	16	12%	3%
⑤	20	14%	3%

（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	121	88%	-4%
② 侵入検知システム	64	46%	-6%
③ VLANなどネットワーク関連	105	76%	-4%
④ ウイルス対策ソフト・サービス	131	95%	1%
⑤ セキュリティ監視サービス	49	36%	-1%
⑥ フィルタリングソフト（Web、メール）	84	61%	-2%
⑦ 暗号化対策	52	38%	-1%
⑧ USB、SDカード、DVDなどの書き込み制御ソフト	27	20%	-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	11	8%	-3%
⑩ その他　（ネットワーク強化,IPS,ログ収集ソフト,セキュリティレポート,研修会への参加など）	7	5%	2%

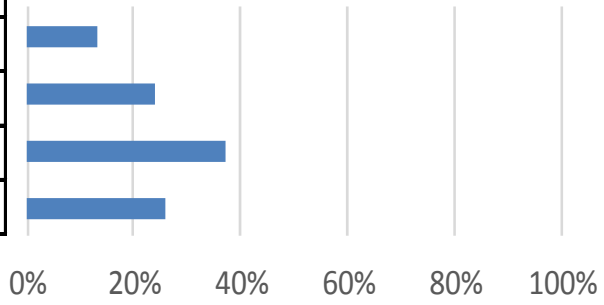


第2部　重要な情報資産の把握と管理対策について

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。

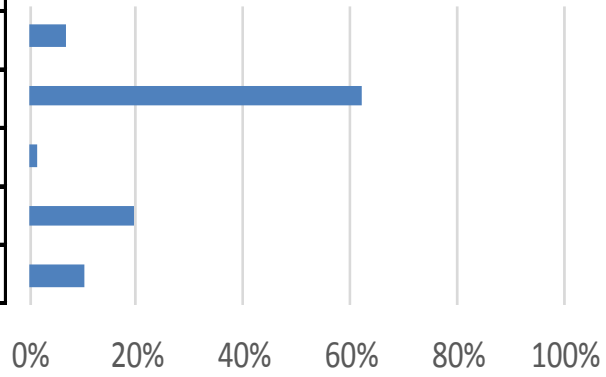
選択肢	選択数	割合	前年増減
①	18	13%	−1%
②	33	24%	4%
③	51	37%	−2%
④	36	26%	−1%



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。

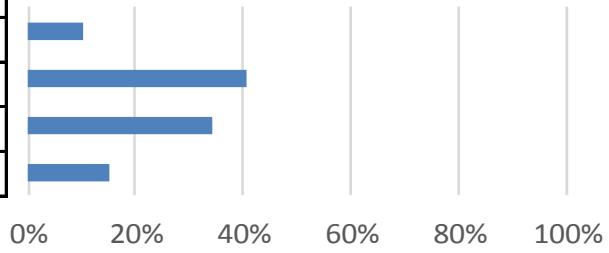
選択肢	選択数	割合	前年増減
①	9	7%	−1%
②	85	62%	−3%
③	2	1%	−2%
④	27	20%	5%
⑤	14	10%	1%



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	14	10%	−4%
②	56	41%	5%
③	47	34%	3%
④	21	15%	−3%

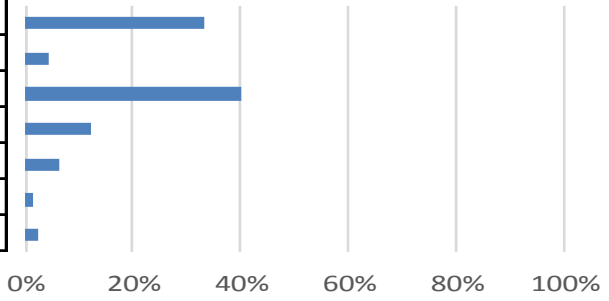


第3部　組織的・人的な対応について

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。

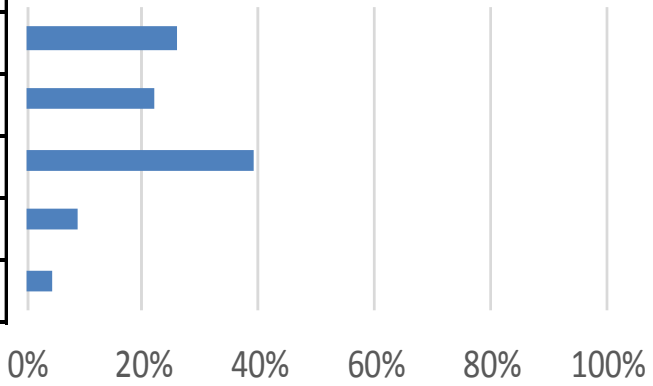
選択肢	選択数	割合	前年増減
①	46	33%	−1%
②	6	4%	0%
③	55	40%	−2%
④	17	12%	2%
⑤	9	7%	0%
⑥	2	1%	0%
⑦	3	2%	1%



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	36	26%	−8%
②	30	22%	2%
③	54	39%	4%
④	12	9%	6%
⑤	6	4%	−3%

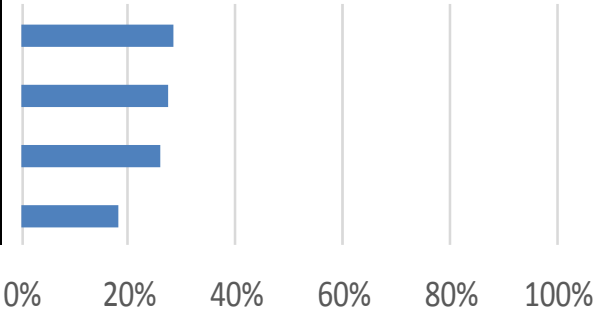


【⑤その他への回答内容】
- 契約書等で明記していない
- 罰則は規定していない
- 学則や職務規定に則り処罰するとセキュリティーポリシーで定めている
- 専任教職員のみ対応

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	39	28%	1%
②	38	28%	−4%
③	36	26%	2%
④	25	18%	1%

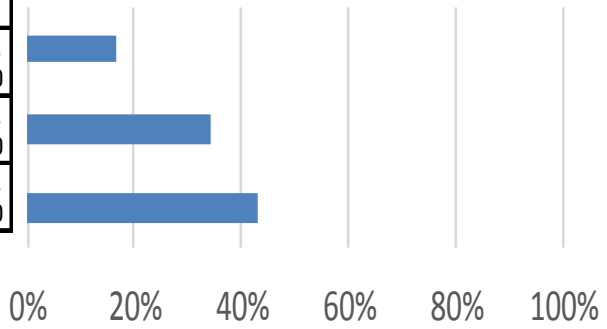


問4　情報セキュリティに関する業務委託を外部組織と契約する際に、情報漏洩や情報消失・破壊など障害対応について責任の所在を明確にし、外部組織による定期的な点検・大学による点検の監視など障害を予防するための取り決めをしていますか。

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	23	17%	−2%
②	47	34%	4%
③	59	43%	−1%

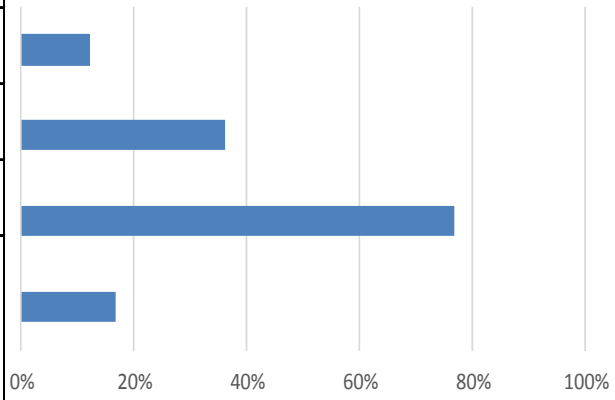
（該当契約なし等9校無回答）



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）

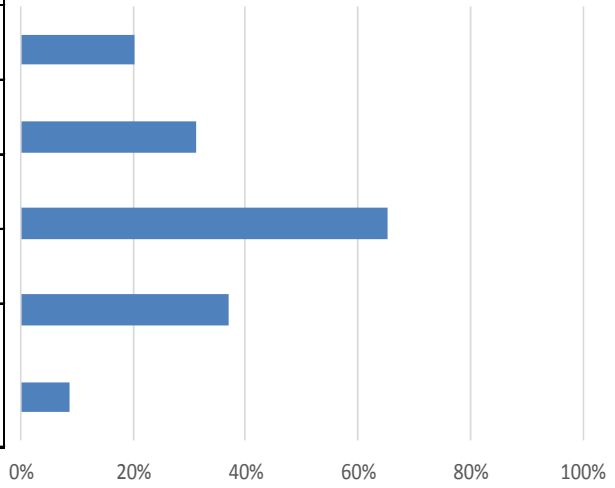
（１）危機意識の共有化

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	17	12%	0%
② FD・SD,教授会,職員会議などでの定期的な情報提供	50	36%	1%
③ Webサイトや学内文書による定期的な情報提供	106	77%	-3%
④ その他(eラーニング研修受講の義務化,セキュリティ講習会の不定期開催,Webサイト・学内文書や教授会などで不定期な情報提供,事象発生時に情報提供,教職員・学生便覧に記載し配布,入職時に研修を受講など)	23	17%	3%



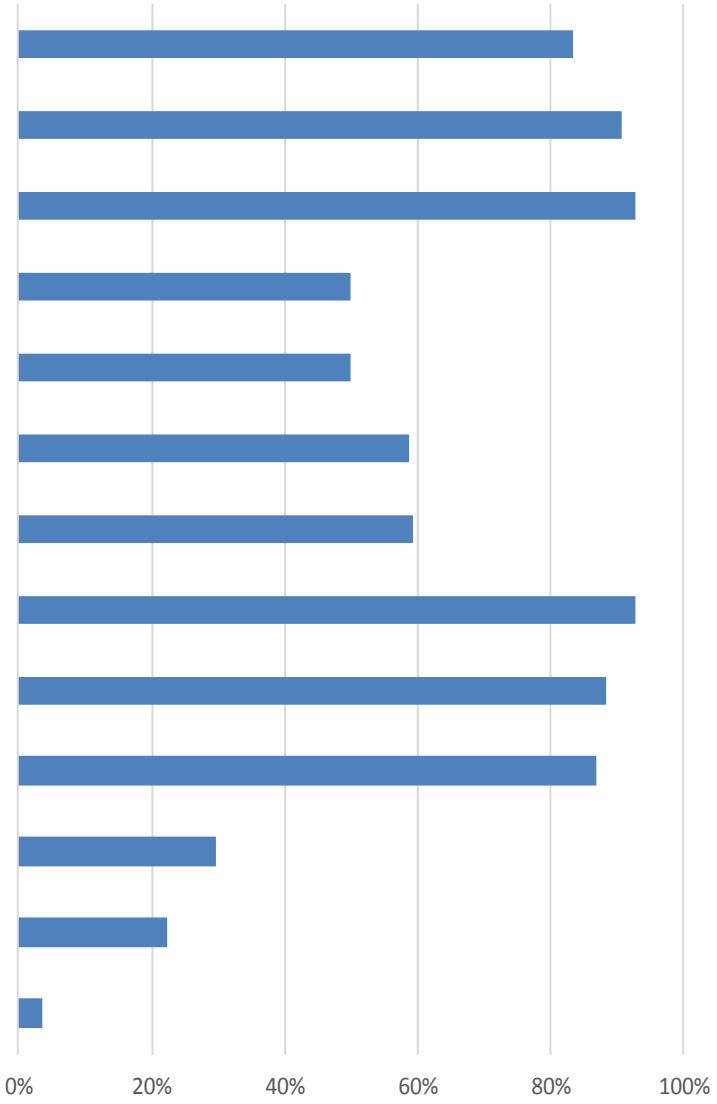
（２）学内ルールの周知徹底と遵守の確認

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	28	20%	1%
② 教授会、職員会議などでのルールの周知と遵守の確認	43	31%	-6%
③ Webサイトでのルールの紹介と遵守の呼びかけ	90	65%	4%
④ 説明会でのルールの紹介と遵守の呼びかけ	51	37%	4%
⑤ その他(冊子体マニュアルや本部・部内発信文書で周知,アカウント発行時の契約書に記載,IPAなどの情報をもとにメールで紹介,入職時やID付与時に周知,教育検討中など)	12	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	前年増減
① 公的機関を装った偽装メールの注意喚起	115	83%	0%
② メール添付ファイル開封の注意喚起	125	91%	-1%
③ メールにリンクされたURL接続の注意喚起	128	93%	7%
④ USBメモリなど外部持ち込みの注意喚起	69	50%	-3%
⑤ 脅威となる事象の被害状況報告と対策説明	69	50%	-2%
⑥ IDの管理やパスワードの定期的な見直し注意喚起	81	59%	9%
⑦ 不正アクセスの監視と異常事態の発見	82	59%	-4%
⑧ ファイアウォールや迷惑メールの設定	128	93%	-3%
⑨ VLANなどネットワークのアクセス制限の設定	122	88%	-4%
⑩ 無線LANの暗号化及び認証方式の導入	120	87%	-2%
⑪ データ暗号化の導入	41	30%	-1%
⑫ クラウドに対する利活用の注意喚起	31	22%	0%
⑬ その他(SNS、スマホ、写真データ、詐欺サイト等の注意喚起,仮想デスクトップの導入)	5	4%	1%

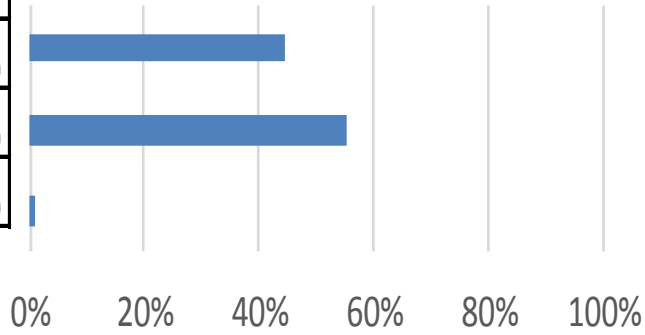


第4部　技術的・物理的対策について

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。

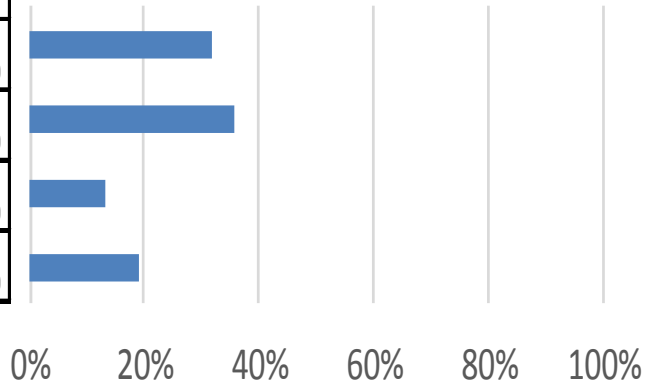
選択肢	選択数	割合	前年増減
①	61	44%	1%
②	76	55%	−1%
③	1	1%	1%



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。

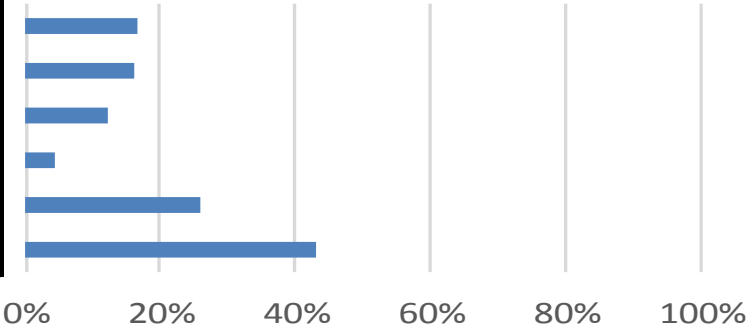
選択肢	選択数	割合	前年増減
①	44	32%	0%
②	49	36%	0%
③	18	13%	−1%
④	26	19%	2%



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。

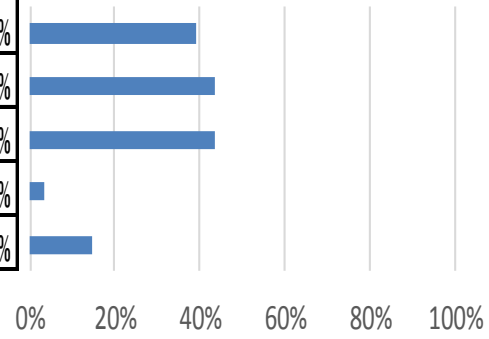
選択肢	選択数	割合	前年増減
①	23	17%	−1%
②	22	16%	2%
③	17	12%	−1%
④	6	4%	1%
⑤	36	26%	9%
⑥	59	43%	−3%



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	54	39%	-2%
②	60	43%	-7%
③	60	43%	5%
④	5	4%	0%
⑤	20	14%	0%

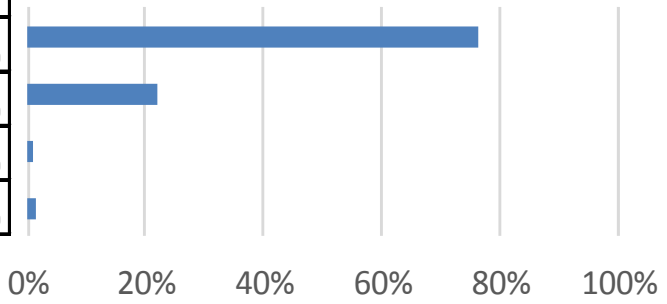


【⑤その他への回答内容】
- パスワードに有効期間を設定
- 推測されやすいパスワードを設定しないよう注意喚起
- ランダムに生成した10桁の複雑なパスワードを配布
- 外部にもれた可能性のあるパスワードは使わない
- 人事データに基づいたID管理
- 二段階認証の義務化
- 教職員証のICチップでの認証
- クライアント証明書の利用

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。

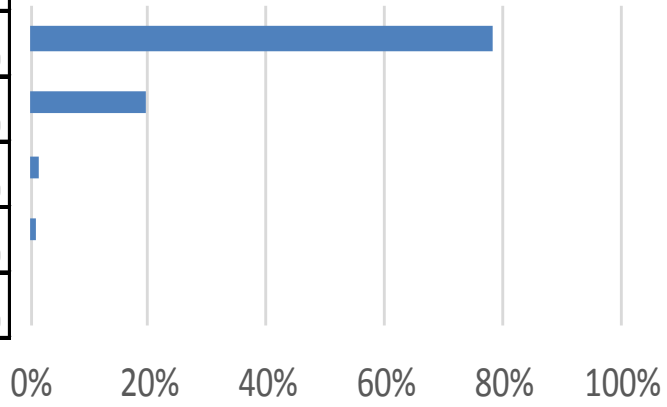
選択肢	選択数	割合	前年増減
①	105	76%	−2%
②	30	22%	2%
③	1	1%	0%
④	2	1%	0%



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。

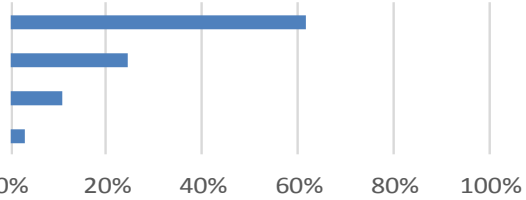
選択肢	選択数	割合	前年増減
①	108	78%	2%
②	27	20%	−4%
③	2	1%	1%
④	1	1%	0%
⑤	0	0%	0%



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。

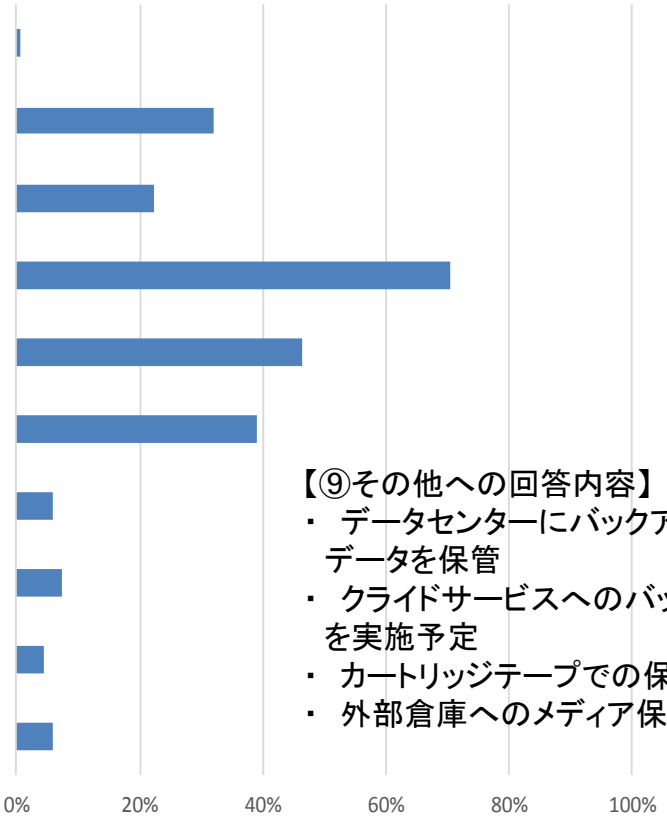
① ぜい弱性に対して最新の修正プログラムを用いて対応している。
② 最新の修正プログラムを適用するまでの間、当面の対応としてぜい弱性を狙った攻撃を回避するソフトウェアもしくはハードウェアを導入して対応している。
③ ぜい弱性対策を検討している。
④ ぜい弱性対策はしていない。

選択肢	選択数	割合	前年増減
①	85	62%	−9%
②	34	25%	5%
③	15	11%	5%
④	4	3%	0%



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%	−1%
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	32%	1%
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。	31	22%	−2%
④ バックアップは毎日行っている。	97	70%	−9%
⑤ バックアップは一定の期間で行っている。	64	46%	4%
⑥ 学内でシステムの二重化を行っている。	54	39%	1%
⑦ 部門単位でシステムの二重化を行っている。	8	6%	0%
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。	10	7%	1%
⑨ その他のバックアップ方法	6	4%	−4%
⑩ バックアップへの備えについて検討している。	8	6%	2%

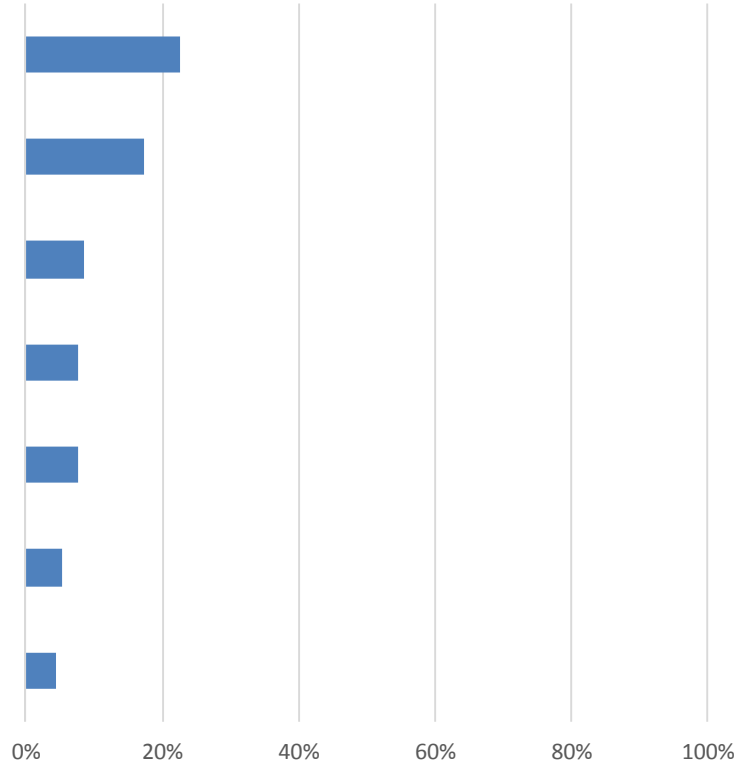


【⑨その他への回答内容】
- データセンターにバックアップデータを保管
- クライドサービスへのバックアップを実施予定
- カートリッジテープでの保管
- 外部倉庫へのメディア保管

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	26	23%
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	20	17%
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	10	9%
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	9	8%
第4部　技術的・物理的対策について 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	9	8%
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	5%
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	5	4%



※　項目を回答した目標設定校は115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・4・6・7・8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91校中68校で7割）
- 削減傾向（2件）
- 前年度にシステム入替のため今年度減額（2件）
- システム単位でのセキュリティ対策のため金額把握が困難
- 予算化されていない

- IPS（不正侵入防止システム）導入580万、職員向けiPadセキュリティ対策770万
- 対策に必要な情報取得の認証機器200万円、ログの蓄積・管理サーバ導入700万円
- 年々増加、昨年はWAF導入で500万円
- L7ファイアフォール増設100万円
- 職員端末用エンドポイントセキュリティ製品の導入700万円
- セキュリティポリシー策定支援250万円、WAF（Webアプリケーションファイアウォール）180万円
- システム入替、数百万増額
- セキュリティ診断100万円増額
- 価格改定のため100万円増額
- ウィルス対策ソフトウェア費用300万増額
- ウィルス対策ソフトの機能アップ20万円増額
- Office365利用のライセンス契約投資200～300万円増額
- セキュリティ対策予算2,000万円
- 情報セキュリティ対策事業費230万円増額

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

- 情報セキュリティポリシーを策定（3件）、改訂の検討中（1件）
- ドメイン管理規定、Webサーバ管理ガイドライン、インシデント対応手順のガイドラインを作成
- 特定重要データの管理に関するガイドラインの制定
- 情報セキュリティ対策委員会、小委員会を開催して、組織的な取り組みの実施
- 情報資産の把握、リスク評価、管理者・取り扱いの点検、セキュリティインシデント対応管理体制の構築と対応マニュアルを作成中

- 標的型攻撃メール訓練（3件）
- インシデント対応手順の策定・電子メール添付ファイル暗号化により情報漏洩対策（テスト実施）
- セキュリティ講習会の実施（5件：専任教職員対象、教員対象職員対象、学生対象）
- 教職員向け情報セキュリティ講習会をeラーニングに移行し、受講とテストを必須とし、情報セキュリティ教育の実施・徹底
- 外部のセキュリティ専門業者による内部監査及びセキュリティ講演会の実施
- セキュリティ意識の強化のため外部講師による講演会を実施

- ISMS（情報セキュリティマネジメントシステム）等を継続実施
- 産学連携によるサイバーセキュリティ関連実証実験への協力
- 各キャンパスに配置したICT支援員を通じて情報セキュリティの案内を実施
- ユーザ向けの情報セキュリティ啓蒙活動
- セキュリティに関する注意喚起のポスター掲示
- 情報セキュリティに関するガイドブックを学生、教職員に配付し、情報リテラシーの向上やセキュリティポリシーの定着
- ワンタイムパスワードの導入

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

- IPS（不正侵入防御システム）導入（2件）
- 資産管理システム運用開始、マルウェア検知システムとファイアウォール連携サービスの導入
- ファイアウォールのリプレイスによる安全性の向上、注意喚起の頻度を向上
- ファイアウォールログ監視サービスを開始
- アカウントアダプター（認証・アカウント管理など）の導入
- 事務PCにEDR（エンドポイント対策）製品を導入、MSSサービス（セキュリティ監視等）を契約、多要素認証の導入を検討中
- 情報漏洩・災害発生時などのリスク防止に仮想デスクトップ導入を検討、大学公認クラウドストレージサービスの導入でUSBなどの紛失による情報漏洩のリスクを低減

- データセンターを構築し、重要な情報資産システムのデータを保全・運用管理
- ネットワーク増強に供ない、セキュリティ対策の充実を計画
- リスク軽減のためのネットワーク分離の取り組みを推進
- VLANの見直しを予定
- 無線LANの認証をPSK方式からIEEE 802.1Xへ変更
- 分散しているサーバを集約し、セキュリティを向上

- メールシステムの2段階認証の義務化
- メールセキュリティ対策としてクラウドシステムに変更
- メールサーバの迷惑メール対策設定とウイルス対策ソフト設定を厳格化、ネットワーク監視機器の導入
- 有償のセキュリティ対策ソフトに入れ替え、UTM対応機器（統合脅威管理）の端末動作検証及び設定変更を実施
- Webサーバを外部委託し、バージョンを統一、全ページSSL化の実施