特集　情報セキュリティ

情報セキュリティベンチマーク評価結果から見た課題

本協会セキュリティ研究講習会運営委員長
浜　正樹　（文京学院大学・教授）

1．はじめに

本協会では、加盟校に情報セキュリティベンチマーク評価をお願いしています。本稿では、2017年度の結果から課題を示します。この評価では、回答校を大規模大学（定員3,000人以上）、中規模大学（定員2,000人～3,000人）、中小規模大学（定員200人未満）、単科大学と分けて集計しています。今年度は52％の回答校が中小規模大学です。

2．経営執行部の情報セキュリティに対する取り組み

法人・大学の執行部が率先して危機意識の共有化を推進しているか調べると、図１の通り大学の規模に拠らず50～60％が情報センター部門中心で推進されていることが分かります。

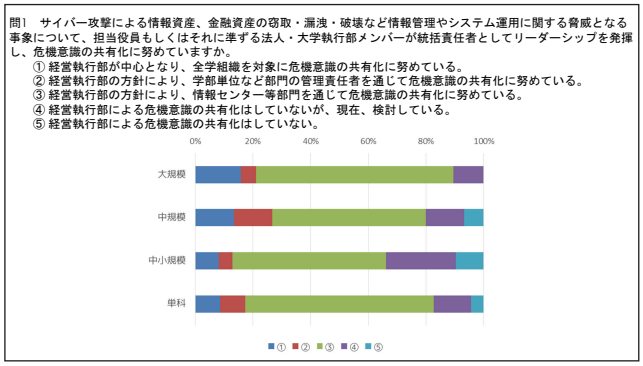


図１　経営執行部による危機意識共有

一方、図２の通りセキュリティポリシー等の策定・周知についての経営執行部の積極的関与は、大規模大学でその比率が高くなっています。

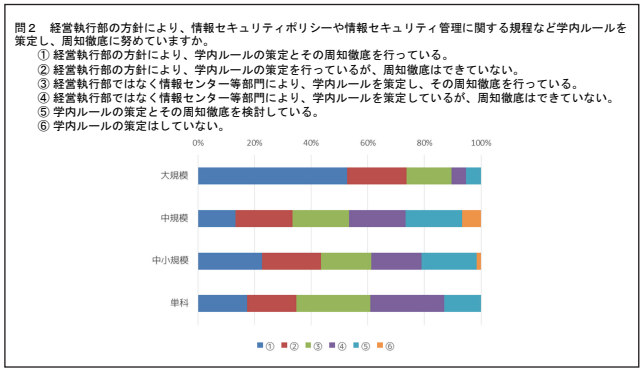


図２　経営執行部による学内ルール周知

また、ICT予算に対するセキュリティ予算の比率については、半数以上（55％）の大学が３％以下しか配分していません。10％以上の予算配分と回答した大学は全体の10％に過ぎませんでした。一般企業ではセキュリティ予算配分比率が10～12％と言われていますので、大学でも伸びを期待したいところです。回答校のセキュリティ予算の具体的内容は、事務局ファイアウォール、ネットワーク監視装置、システムセキュリティ監査などで、500～700万円の実績です。セキュリティ予算の対前年度増減について回答頂いた48校のうち63％が「増額なし」でしたが、これらの他校事例は予算要求の際に参考にできるでしょう。

3．重要な情報資産の把握と管理対策について

セキュリティ対策は、何を守るか明確にすることがスタート地点です。

図３によると、約70％の大学が情報資産目録作成を未実施ですが、アクセス制御を行っていると回答している大学も70％を越えています。回答校の状況を調査したところ、守るべき情報資産が不明確でもアクセス制御していると主張する大学が40％も存在していることが判明しました。これでは対策自体が無意味です。情報資産目録の作成を最優先課題にすべきです。重要度を２～３段階に抑えて選別しても充分です。

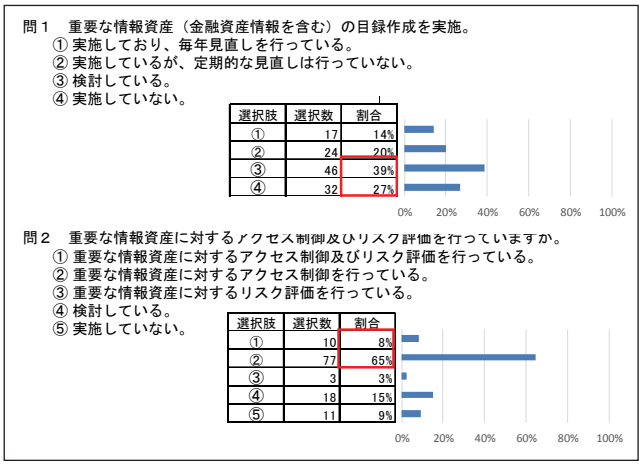


図３　重要情報資産の把握とアクセス制御

4．組織的・人的な対応について

本協会でもセキュリティの組織的対応を訴えていますが、図４によると、セキュリティへの対応組織は約80％の大学が有し、その位置づけは大学規模に依存しない状況が伺えます。位置づけとしては、情報センター部門中心ではなく、横断的な組織体制が望ましいところです。

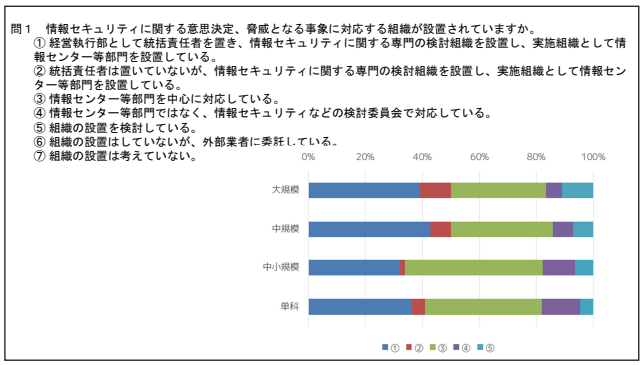


図４　情報セキュリティ組織の有無と位置づけ

一方、実際のインシデントへの対応手順の整備状況ですが、図５によると、規模によらずほぼ半分以上の大学で遅れが認められます。

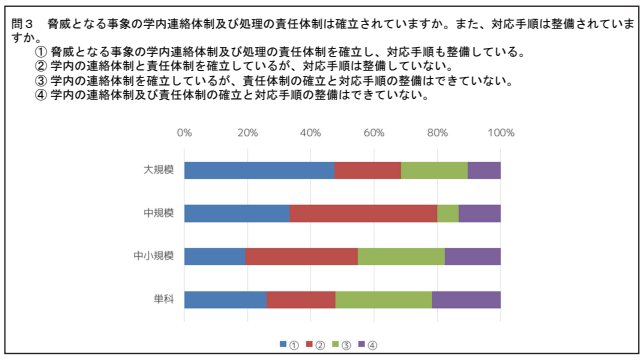
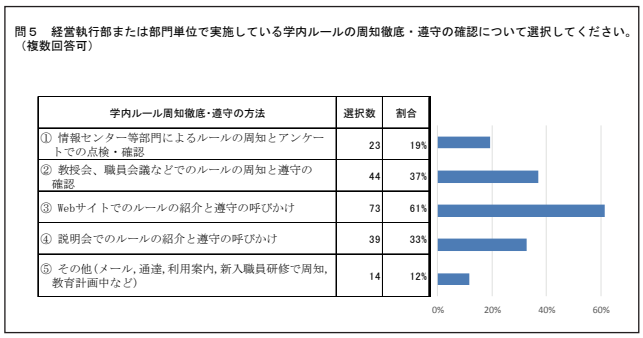


図５　インシデント連絡体制、対応手順の整備

まずできる範囲の手順作成を目標設定し、少しずつでも進めることが大事です。

次に、図６で、学内ルールの周知徹底・遵守の確認の方法の調査結果を示します。



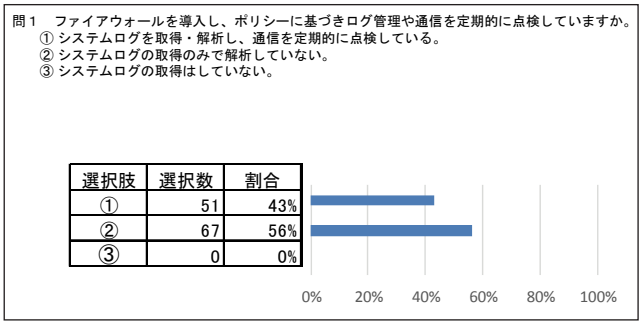
学内ルール周知徹底・遵守の方法	選択数	割合
① 情報センター等部門によるルールの周知とアンケートでの点検・確認	23	19%
② 教授会、職員会議などでのルールの周知と遵守の確認	44	37%
③ Webサイトでのルールの紹介と遵守の呼びかけ	73	61%
④ 説明会でのルールの紹介と遵守の呼びかけ	39	33%
⑤ その他（メール，通達，利用案内，新入職員研修で周知，教育計画中など）	14	12%

図６　学内ルールの周知徹底・遵守の確認の方法

図のようにWeb告知が主になっています。学内の危機意識の共有化についても同様の結果でした。しかし、Web告知だけで安心してはいけません。e-Learningで「動画＋ルール」の方が訴求できます。また、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大変有効です。

5．技術的・物理的対策について

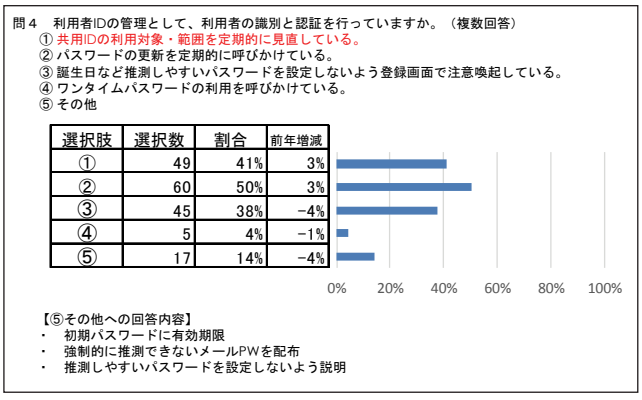
セキュリティ対策は、機器の設置だけでは完全ではありません。図７によると、ファイアウォールを設置しているものの、そのログ解析を行っていない大学が56％にも上ります。監視に携わる人的コストの確保も含め早急な対応が必須です。



選択肢	選択数	割合
①	51	43%
②	67	56%
③	0	0%

図７　ファイアウォールの設置と運用

さて、セキュリティ対策の最も基本的な位置づけである利用者IDの管理について図８を見てみましょう。ここで、問題視されるのは共有IDの利用を認めている大学が多いことです。外部からの侵入の際、非常に高い頻度で共有IDが狙われます。個人IDのみとする運用が望ましいでしょう。



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%

図８　利用者IDの管理

以上、ベンチマーク評価から問題点を指摘したきましたが、今後急がれる対策をあげれば、技術的には重要データの暗号化、人的には事故対応体制・手順の整備などということになると思われます。本稿がその根拠となることを祈っております。

なお、本稿を記すにあたり、東京大学情報学環の満永拓邦氏、松田亘氏、藤本万里子氏にご協力いただきました。