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

文京学院大学教授
本協会大学情報セキュリティ研究講習会運営委員長　浜　　正樹

1．はじめに

本協会では、2016年度より「情報セキュリティベンチマーク」として、加盟校の情報セキュリティ対策状況を調査しています。回答校数は、2018年度は対前年比15％増加（119校→138校）です。特に、中小規模校が増加しています。情報セキュリティ問題意識が高まり、実際の施策の検討へ進んでいると期待されます。全回答大学の平均点は51点です。規模別の平均点は、大規模大学62点、中規模大学57点、中小規模大学50点、単科大学46点となっています。本稿では、このベンチマーク結果から抜粋して課題を説明します。なお、下記に報告する各設問の回答校数は特記しない限り138校です。

2．経営執行部の情報セキュリティに対する取り組み

第一部「経営執行部の情報セキュリティに対する取り組み」の問１では、危機意識の共有化を行っている部門について聞いています。図１がその結果です。

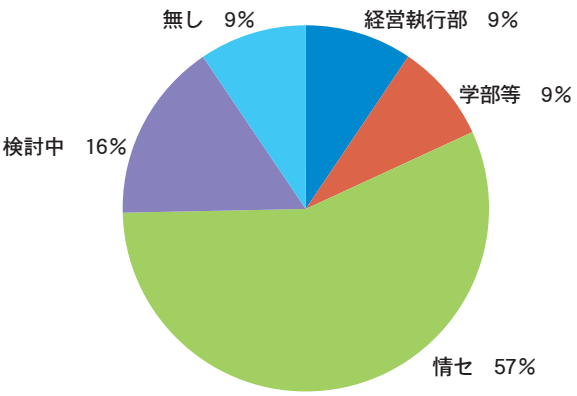

図１　危機意識の共有化部門

60％近くが情報センター中心です。後程触れますが、経営執行部への危機意識の訴求が優先課題です。

問２では、経営執行部が情報セキュリティポリシーや規程の策定と周知徹底を行っているか聞いています。この設問では、2017年度と同様に大規模校の方が対応が進んでいます。同ベンチマークで聞いた改善課題の優先度では、この項目が１位で26％の回答校が選択しています。実際、情報センターとして策定した内規はあるものの、なかなか学内で周知して規程にできないといった声がよく挙がります。成功例としては、文書規程等の他の規程策定に上手く含めていったケースが報告されています。

問４では、ICT予算の中でのセキュリティ対策費用の割合を聞いています。45％以上の回答校で、予算の３％以下であると回答がありました。私情協では、10％を目指すよう薦めています。予算用途としては、ウイルス対策ソフト・サービス、ファイアウォール、VLAN機器が上位を占めていますが、侵入検知システム、暗号化対策、セキュリティ監視サービスが次に検討されるべき項目です。

3．組織的・人的な対応について

第三部「組織的・人的な対応について」の問１では、セキュリティ対策組織の有無について聞いています。次ページ図２にその結果を示します。

統括責任者・検討組織・情報センターが揃っているか、もしくは情報センターが中心か、という大きく２つに分かれている傾向が見て取れます。理想的に３つが揃っている回答校の規模別比率では、大規模・中規模校で45％、中小規模校で

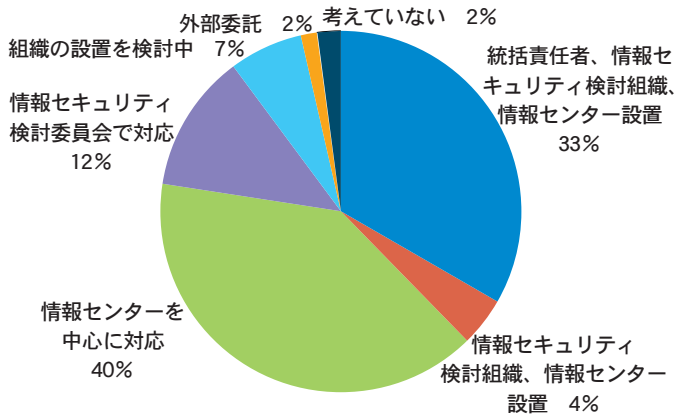

図２　セキュリティ対応組織

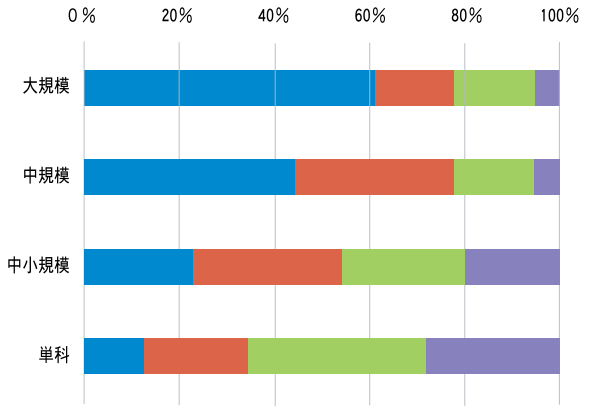

図４　脅威事象への学内連絡・処理・対応（大学規模別）

37%、小規模校で22%です。問２では、教職員の守秘義務の明確化と情報セキュリティポリシー違反の罰則規定について聞いています。実現が難しい要件と思われます。実際に、情報セキュリティという観点での罰則規定まで設けている大学は回答校の25%に過ぎません。実現方法としては、セキュリティポリシー内で「学則や職務規定に則り処罰する」と記載している大学の事例が参考になります。問３では、脅威事象の学内連絡体制及び処理の責任体制の確立と対応手順の整備について聞いています。回答の集計結果は図３の通りです。

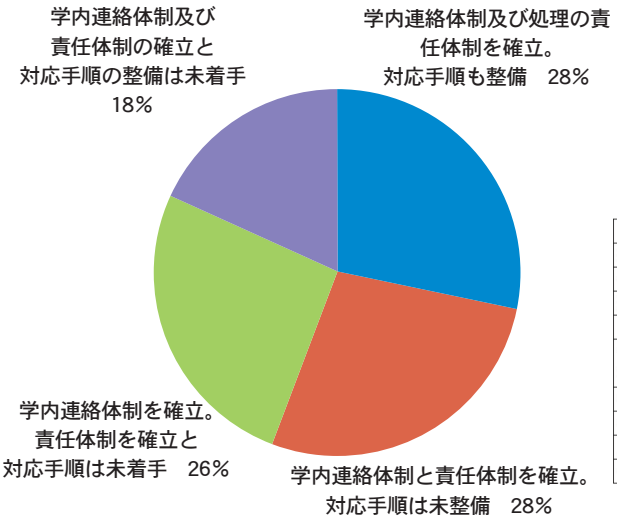

図３　脅威事象への学内連絡・処理・対応

上記の設問の回答を大学の規模別集計を下記の図４に示します。

大規模校の方が責任体制は確立しています。一方で、対応手順については、全般的に未着手であることが分かります。このベンチマークでも優先したい改善項目として対応手順の策定が３位（９%）です。

USBメディアによるデータ流出や不正アクセスといったインシデントごとに、毎年少しずつ対応手順を策定することが現実的と思われます。

４．情報セキュリティを守る現場が考える次の施策

本協会では、大学情報セキュリティ研究講習会を開催しています。今年度は、本ベンチマークの結果も踏まえて、大学の情報セキュリティ課題についてディスカッションしました。その成果物として、アクションプランを立てて貰いました。回答の一部のみですが、下の表１のような順位になっています。

表１　施策項目の選択数

施策項目	数
組織構築（情報セキュリティ担当委員会、CISO、CISRT設置含む）	15
情報セキュリティポリシー・規程の策定・見直し	14
経営陣へのサイバーセキュリティリスク説明	11
サイバーセキュリティリスクの教育・啓発	11
情報セキュリティ事故対応手順の確立（連絡網の整備、他部署との担当把握含む）	9
情報資産台帳の作成・整備	6
情報セキュリティ予算申請	4
監視システムの整備状況確認	4
情報セキュリティ事故対応訓練（標的型攻撃メール訓練含む）	3

対応手順策定に進みたいが、学内の啓発が優先という状況が見て取れます。

しかし、実は、重要な作業が下位に挙がっています。第二部の問１で設定した重要な情報資産の目録作成です。回答の集計結果は、次ページ図５

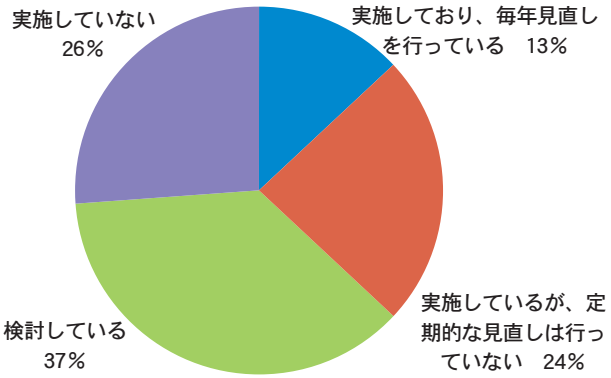

図５　重要情報資産の目録作成状況

の通りです。

「検討している」と「実施していない」を合わせると60％以上となります。2017年度から改善が見られていない点が懸念されます。ただし、目録作成にも注意点があります。実際に、毎月１回の頻度で目録の棚卸をされている大学の事例もありますが、大きな労力がかかってしまっているとのことでした。未着手の場合は、情報資産の種類や漏洩事故発生時の対応（どこに届けるか？誰の名前で公表するか？など）について決めておくだけでも違います。

５．情報セキュリティ責任者（CISO）の果たす役割

さて、ここまでベンチマーク結果を踏まえて、私立大学のセキュリティに対する状況や現場で考える次に対応すべき施策などについても紹介してきました。

しかし、これらを実行に移していくには、やはり年次計画やロードマップを作成していかなければ、経営執行部を説得できないものです。

そのためには、セキュリティ関係の仕事の全体像を捉えていかなければなりません。大学のCISOは、体系的にその業務が整理されているわけではありません。一方で、一般企業ではCISOの役割が明確になっています。そこで、１つの例ですが、経済産業省とIPAが作成したCISOが指示するべき項目を大学に読み替えた例が下記の表２です。

表２　大学のCISOが果たすべき役割

No.	指示項目	施策対象
1	セキュリティリスクの認識、組織全体での対応方針の策定	セキュリティポリシー、コンプライアンス
2	セキュリティリスク管理体制の構築	CISO、情報セキュリティ委員会
3	セキュリティ対策のための資源（予算、人材等）確保	セキュリティ予算、研修
4	セキュリティリスクの把握とリスク対応に関する計画の策定	情報資産台帳
5	セキュリティリスクに対応するための仕組みの構築	多層防御、検知システム
6	セキュリティ対策におけるPDCAサイクルの実施	定時報告、外部監査
7	インシデント発生時の緊急対応体制の整備	CSIRT、初動マニュアル
8	インシデントによる被害に備えた復旧体制の整備	復旧計画
9	同一法人内の学校や業務委託先等を含めた全体の対策及び状況把握	契約書
10	情報共有活動への参加を通じた攻撃情報の入手とその有効活用及び提供	JPCERT/CC CISTA参加

４．であげた次の施策の位置付けを確認するために該当項目に色をつけると下記の表３になります。

こういった表を参考に、何年目に、どの施策を実施していくかという考え方で進めれば、分かりやすい説明が可能になっていくと思われますので、活用をご活用下さい。

表３　大学のCISOが果たすべき役割

No.	指示項目	施策対象
1	セキュリティリスクの認識、組織全体での対応方針の策定	セキュリティポリシー、コンプライアンス
2	セキュリティリスク管理体制の構築	CISO、情報セキュリティ委員会
3	セキュリティ対策のための資源（予算、人材等）確保	セキュリティ予算、研修
4	セキュリティリスクの把握とリスク対応に関する計画の策定	情報資産台帳
5	セキュリティリスクに対応するための仕組みの構築	多層防御、検知システム
6	セキュリティ対策におけるPDCAサイクルの実施	定時報告、外部監査
7	インシデント発生時の緊急対応体制の整備	CSIRT、初動マニュアル
8	インシデントによる被害に備えた復旧体制の整備	復旧計画
9	同一法人内の学校や業務委託先等を含めた全体の対策及び状況把握	契約書
10	情報共有活動への参加を通じた攻撃情報の入手とその有効活用及び提供	JPCERT/CC CISTA参加