事業活動報告 NO. 3

サイバー攻撃等の対応状況の調査結果について

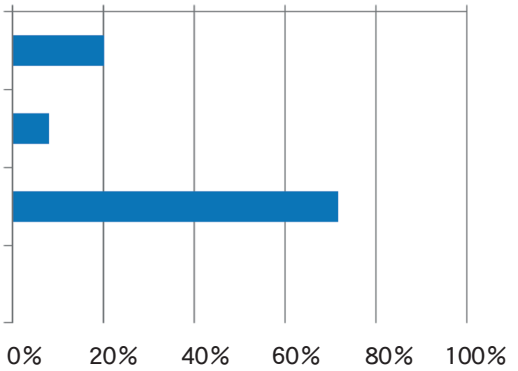
公益社団法人私立大学情報教育協会
大学情報セキュリティ研究講習会

サイバー攻撃は日を増して激化してきており政府機関や企業はもとより大学においても重要な情報が窃取される事態が発生しています。知を集積・創造する教育・研究活動を通じて社会の発展を支えていくために、組織として「情報資産を守る」という社会的に重要な責務を大学は担っております。しかしながら、本協会の平成24年度の「情報セキュリティ対策の自己点検・評価」によれば、大学として組織単位で情報セキュリティを点検・評価・改善しているところが極めて少なく、多くの大学が計画段階に留まっていることが伺えます。

そこで、教職員一人ひとりが情報資産を防御する意識を共有するための対策や情報セキュリティの強化に向けた課題、大学間でのサイバー攻撃に関する情報共有の在り方などの研究を行うため、加盟大学・短期大学261校に「サイバー攻撃へ危機意識を持つような取り組みの有無」、「情報を大学間で共有して一元化する仕組みの必要性」、「災害を想定した業務継続のため、大学間での相互補完・連携協定などの必要性」について調査を行い、160校から回答があった。以下に回答結果を紹介します。

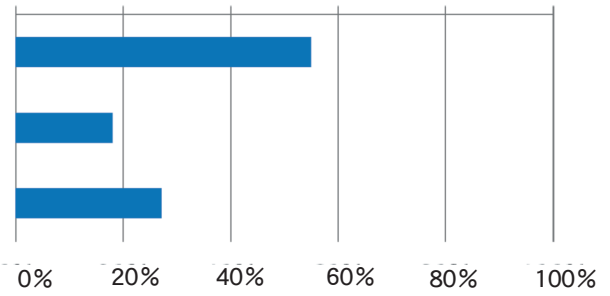
1．サイバー攻撃について勉強会などを通じて危機意識を持つような取り組みの有無

①取り組みを行っている	32校	20%
②取り組みの検討を始めている	13校	8%
③取り組みの必要性を感じている	115校	72%
④全く必要性を感じていない	0 校	0%



上記１の「①取り組みを行っている」内容についての主な意見（複数回答で合計49件）

情報収集・情報提供の実施	55%
打合せ会の実施と具体的な取り組み	18%
講習会の実施	27%



【情報収集・情報提供の実施】

- Webやセミナーで情報収集している（11件）
- 情報セキュリティ・インシデント等の情報収集を行っている（1件）

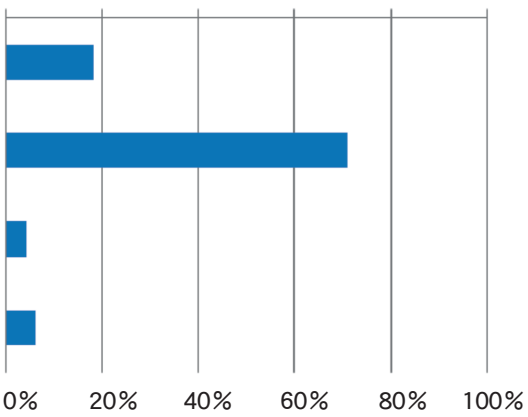
・　担当部門職員が学外機関の講習会に参加している（2件）
・　学外機関の会議に関係教職員を派遣している（1件）
・　IT関連企業より設備強化のための情報収集を行っている（1件）
・　学内に広報活動のためのニュースを月１回発行している（1件）
・　サイバー攻撃の危機意識を高めるため学内メール・Ｗｅｂで情報提供をしている（8件）
・　Webでセキュリティに関する啓発や危機感を持つよう定期的な告知を行っている（2件）

【打合せ会の実施と具体的な取り組み】
・　サイバー攻撃の対策に関する担当部門での打合せを行っている（3件）
・　情報センター関連部門会議にて発生事例の報告及び情報共有を行っている（2件）
・　学内サーバに対するセキュリティチェック結果を通知し、対処・改善させている（2件）
・　サイバー攻撃防御サービスの導入と攻撃状況のモニタリングを開始した（1件）
・　標的型攻撃を意図したプロファイルを持つ電子メールのフィルタリング、フィルタリングの通過が発覚した際の受信者への注意喚起を行っている。電子メール記載URLクリックによるアクセス誘導の遮断・抑制を図り、不審アクセス元の記録・解析からフィルタリングに反映している（1件）

【講習会の実施】
・　全教職員にセキュリティ講習会を実施している（5件）
・　学生教育や職員研修の中でサイバー攻撃を取り上げて周知している（3件）
・　教職員に情報資産の自己管理についての講習を実施している（1件）
・　所属長を対象に警察署からサイバーテロに関する学内講演会を実施した（1件）
・　研究室のネットワーク管理者に対する定期的な講習を実施している（1件）
・　専任教職員向けに年に一回eラーニングで情報セキュリティ研修を実施している（1件）
・　グローバルIPアドレスを貸与している利用者に毎年セキュリティセミナー受講を義務付けている（1件）

２．サイバー攻撃への防御対策の一環で、情報を大学間で共有して他大学または他機関におけるインシデント事例と対処方法について情報を一元化する仕組みの必要性

①仕組みは必要	29校	18%
②仕組みは必要だが、仕組みの内容をどのように構築するかが明確でないと回答できない	114校	71%
③仕組みの必要性を感じない	7校	4%
④その他	10校	6%

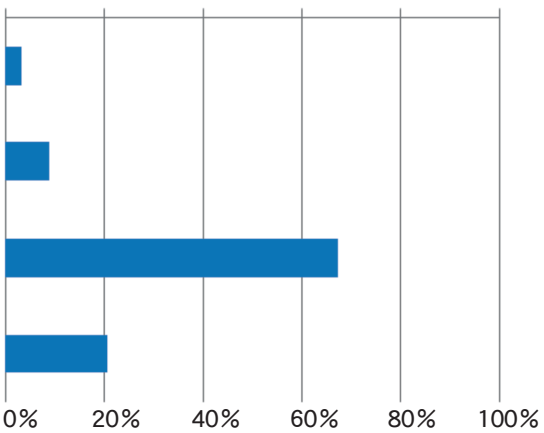


上記２「④その他」の主な意見（合計11件）
・　仕組みが必要という流れになるのは必至だが、一元化の前に各大学の実情に応じた対応があるのではないかと考える（1件）
・　IPA（情報処理推進機構）のWebがあるため、情報の一元化の必要性はあまり感じない。公表されている情報の有効活用が望ましい（2件）
・　既にIPAという組織がある中で、大学版を作ることは非効率と考える。ただし、大学とIPA間にお

ける双方向の情報共有を中心に、関係性を整理し協力関係を築く方が良い（1件）
- 新たに大学固有の仕組みを作る必要性が不明で、IPAなど既存の組織で良い（1件）
- IPA との情報連携が図れる講習会などを希望する（1件）
- 各大学の事例をどこまで公開し、その情報が有用なものか判断が難しい（1件）
- 大学間だけではなく、広域で情報を共有する仕組みが必要（2件）
- 具体的な対策（最新ファイアウォールへの入れ替えや、都度のセキュリティパッチ適用）の負荷が高いため、例えば、SINETに接続していれば、SINET側でネットワークレベルで監視及び対策を施すような仕組みがあれば良い（1件）
- インシデント事例公開により内部情報等の保全がされるか懸念がある（1件）

3．災害を想定した業務継続の対策として、教育・研究活動の成果としての情報資産の確保など、遠隔地の大学との情報資産の相互補完や大学間での連携協定の必要性

①遠隔地の大学と業務継続性・情報資産の相互補完について連携協定を構築したい	5校	3%
②連携協定までは考えないが、遠隔地の大学と重要情報資産に限定して相互補完の仕組みを作りたい	14校	9%
③外部のデータセンターを利用して情報資産の二重化を図りたい	108校	68%
④その他	33校	21%



上記３「④その他」の主な意見（合計26件）
- 大学間での連携協定は構築してはいないが、重要な情報資産は遠隔地でのバックアップを考えている（1件）
- 大学間では費用や設備、機密保持契約など協定を結ぶには障壁が高く業務継続対策は全体としては進まないと予想される。国立情報学研究所や私情協など中立機関での有償サービス提供を希望する（1件）
- 相互補完は双方が情報資産の保管を「請け負う」ことになり、責任や負担が大きいため、外部のデータセンターを共同で借りる等の方策がよいと考える（1件）
- 大学キャンパス間での情報資産の二重化を実施している（1件）
- 外部データセンタでの二重化を実施している（2件）
- サーバ室建物と新しい強固な建物の２棟にてバックアップ体制を構築している（1件）
- 同一法人や別キャンパスで相互に遠隔での情報資産の相互補完を検討している（8件）
- 別媒体へのバックアップのみの対策を行っている（1件）
- 業務継続性、情報資産の確保の必要性を認識しているが、具体的な施策を検討するまでには至っていない（5件）
- 未検討（5件）