特集　情報セキュリティ

大学でのサイバーセキュリティ対応体制のステップアップに向けたヒント

一般社団法人JPCERT
コーディネーションセンター　洞田　慎一

1．はじめに

国立大学も私立大学も、大規模校も小規模校も、何らかのインシデントを経験しているでしょう。したがって、深刻な被害に至る前に何かしらのサイバーセキュリティ対策が求められているのではないでしょうか。セキュリティ対策の第一歩として、インシデント対応等において中核となるCSIRTを組織することの重要性は誰もが認めるところです（次ページ図）。

Computer Security Incident Response Center。コンピュータセキュリティに関するインシデントに対処するための組織。国内の他のCSIRTがどのような活動をしているかなど、CSIRT構築および運用における実態調査[13]も参考にしてください。

大学でのサイバーセキュリティ対策の現況調査[2]によると、情報セキュリティポリシーが未策定の大学は、公立大学で12.4％、私立大学で30.4％まで減ってきています。既に国立大学ではすべての大学にCSIRTが設置されるに至っています。大学のサイバーセキュリティ対策が表面的な部分では進展していると言えるでしょう。

CSIRTを中心にサイバーセキュリティ対策を着実に前進させている大学が存在する一方で、具体的に何をどのように進めたらよいかと悩んで躊躇したままの大学も少なくありません。「対策をするために必要な人や予算などのリソースが確保できていない」、「何から対策を始めてよいのかわからない」、「専門的知識や経験のある人がいない」、「採用や育成も課題である」、「対策や対応で学内からの理解や協力が得られない」といった現場の悩みを聞くことがあります。また、日本経済新聞社が国立大学に行ったアンケート調査に関する報道[3]でも類似した悩みがあげられていました。

（1）検討が求められているサイバーセキュリティ対策

多くの大学が情報セキュリティーポリシの策定を終え、これからインシデントへの対応など、具体論を進めていく段階にあると考えられます。その中で、発生するインシデントに対応できるようにしたいという問題意識は共通しているように思います。このことは、政府の「サイバーセキュリティ戦略」[4]においても垣間見ることができます。この文章では、大学のセキュリティ課題として、「事案に適切かつ迅速な対処をするための能力の向上に向けた取組」や「組織的かつ着実に実施するための体制」の検討があげられています。

インシデントに対して、どのように対処していけばよいだろうか、膠着状態に陥っているともいえる状況をブレークスルーして前進させるためには、様々なステークホルダーのセキュリティに対する意識の問題に立ち戻ることが重要です。すなわち、組織のすべての構成員が、それぞれの立場においてサイバーセキュリティ対策への意識をもち、それに裏打ちされた対策・対応の成熟度を一つ一つ高めていくことが不可欠でしょう。

（2）サイバーセキュリティ対策の目的

サイバーセキュリティ対策の目的は、大学という組織の社会的体裁を守ることだけではありません。大学が提供する基本的な価値である研究教育環境の品質と安定性を維持するために、セキュリティが不可欠になっているのです。例えば、教育・研究環境改革の一環として大学等の教育・研究環境のスマート化[5]が進み、学生らは当たり前のようにスマートフォンやネットワークを活用して大学の様々なシステムや教育コンテンツにアクセスしてサービスを受けています。しかし、手放し状態のまま進めればシステム的な脆弱性が増し、サイバー攻撃を受けてシステム全体が瓦解する可能性が考えられます。そのような事態になれば、単にシステムの問題として済ませられるレベルを超え、大学経営上の課題として考えねばならないでしょう。政府のサイバーセキュリティ戦略は、大学に「安全・安心な教育・研究環境の確保」をセキュリティ対策の目的として、経営上の問題と位置付けるよう求めています。

サイバーセキュリティ対策は、大学に限らず、社会的な要請でもあります。将来を担う学生への

経営リスクと情報セキュリティ　～ CSIRT：緊急対応体制が必要な理由 ～

概要

1．企業経営と危機管理

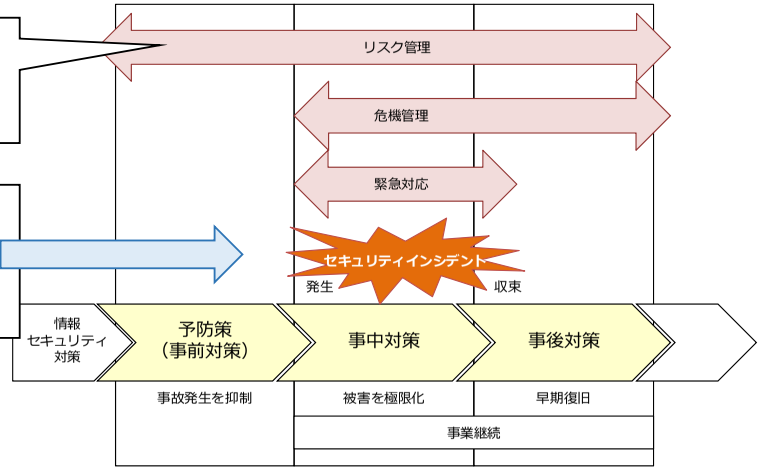
なぜ
やらなければ
ならないのか

企業を取り巻く環境変化

- 企業の
  モラルハザード
- 法令施行に伴う
  内部統制強化の動き
- 事業継続に対する
  関心の高まり
- APT

情報資産に係るリスク管理
- 情報資産の流出/喪失リスク
- 法令違反/モラル違反のリスク
- 事業中断のリスク

情報資産を巡るトラブル
- 重要情報の流出/滅失
- インサイダー取引
- 不正アクセス
- システム障害

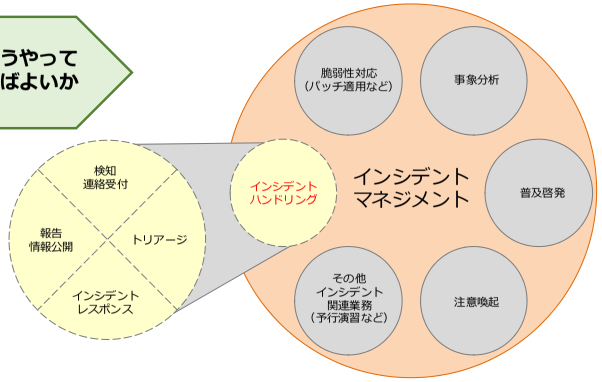


- 環境変化を背景に、企業のリスクは多様化・変質し、情報資産を巡るトラブルも頻発
- リスクに関する対応方針を示すことは経営層の法令遵守
- 企業は、費用対効果に配慮した予防策とともに、事故前提の考え方に基づく危機管理/緊急対応体制を確立すべき

2．危機管理/緊急対応体制の実現に向けて

- 緊急対応体制として、組織内CSIRT機能の整備が有効
- 国内外で組織内CSIRTの導入事例が増加
- 既存の体制との役割分担や整合が課題
  経営層が先導して社内横断的な調整・連携を実現すべき

何をどうやって
始めればよいか



CSIRT構築の狙い・期待効果

<関連情報の集約と効率的活用>
情報集約、効率化、ノウハウ蓄積
→　インシデントに強い組織へ

<組織のセキュリティレベルの向上>
再発防止策のフィードバック
によるセキュリティレベルの向上

<社内外に向けたメッセージ>
顧客、取引先、関係機関等に対する
「安全・安心」のメッセージ

<他組織との連携>
CSIRT間の連携から得た知見で
解決困難な問題の対処が可能に

<ビジネスへの展開>
CSIRTの機能や経験を活かした
サービスを自社ビジネスとして展開

3．危機管理/緊急対応体制の活用に向けて

- インシデント対応から得た再発防止策を組織にフィードバック
- 要員不足時にはアウトソーシングの活用も視野に入れて検討
- 要員の育成と従業員の育成・啓発が鍵
- 投入する資源のバランスに留意

どうやって
維持・向上
させるか

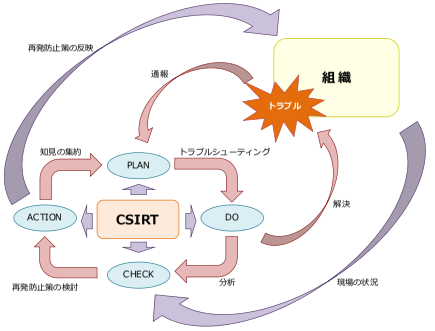


図　経営リスクと情報セキュリティ（JPCERT/CC CSIRTマテリアル[1]より抜粋）

教育の一環として、サイバーセキュリティの素養を醸成すること[6]は大学の使命の一つであると考えられます。学生らは、セキュリティ・リテラシー教育コースを通じてだけではなく、彼らが学ぶ教育・研究環境におけるサイバーセキュリティ対策の実態を通じても、セキュリティ文化を体得していくでしょう。教育・研究環境のサイバーセキュリティ対策がおざなりであれば、学生の目には教えられたサイバーセキュリティが絵に描いた餅のように映るのではないでしょうか。大学におけるサイバーセキュリティへの対策は、システム整備のおまけ程度でお茶を濁してよい問題ではないと考えます。

本稿では、大学の組織を念頭に、実効的なインシデント対応体制を構築し成熟させていくためのアプローチについて、いくつかのヒントを紹介したいと思います。

2．大学でのサイバーセキュリティ対策を進める上での課題

私立大学（本協会加盟校）では2017年度現在、約80％の組織で情報セキュリティに対応する組織が存在します[7]。しかしながら、インシデント対応手順の準備や、情報資産の目録整備といった、インシデント時に機敏に対処するための取り組みは進んでいるとは言えません。

機敏なインシデント対応を可能にするは、様々な事前準備や環境の整備が欠かせません。インシデント対応の手順やインシデント対応組織の構築に関する資料は複数あります。

インシデント対応や対応体制について触れたものとして、CSIRTマテリアル[1]があります。また、サイバー経営ガイドライン[14]での「付録C インシデント発生時に組織内で整理しておくべき事項」も、インシデント対応や調査において必要な情報をまとめていく際に、参考となるでしょう。

本協会でも大学情報セキュリティ研究講習会で対応フローの説明やそれを用いた演習カリキュラムの説明がなされており、そうした資料に既に触れている担当者も多いでしょう。しかしながら、現実のインシデントでは、対応がスムーズに行かないことの方が多いものです。例えば、対応に必要な情報が手元になく、それを集めようとしている間に時間ばかりが経過していってしまうことはしばしば経験されているのではないかと思います。

大学での実効性のあるCSIRTの構築に際して、陥りやすい関門として、（1）学内の理解に関する問題、（2）正確な技術情報の入手に関する問題、（3）セキュリティ対策の成熟度の向上へのロードマップに関する問題の３つをあげることができます。順に説明していきます。

（1）学内の理解に関する問題

インシデント対応を迅速かつ円滑に進めるために学内の理解が不可欠なことは、すぐに想像がつくでしょう。例えば、研究室や部局でインシデントが発生したとき、インシデント対応を進めるには、当該研究室等の協力が必須です。協力が得られなければ、結果としてうやむやのまま事案をクローズせざるを得ません。

研究室や部局の協力が得られない背景には、インシデント対応を行うCSIRTが情報系センターのスタッフで構成されていることに起因する、組織的な距離感も問題の一旦にあるでしょう。それをCSIRT側から力づくで突破しようとして事態が悪化するケースもあります。例えば、次に紹介する標的型メールへの耐性訓練の事例も、そうした失敗の一つではないでしょうか。

大学の教員に対して科研費や、学会や会議などの主題を囮に用いた標的型メール攻撃が確認されている中で、標的型メール攻撃訓練を実施する大学も増えているようです。標的型攻撃に似せて訓練用に作ったメールを利用者に送り付け、不用意にメールの添付文書を開いた利用者に警告を促すという訓練です。しかしながら、この種の訓練をCSIRTへの学内の理解がない環境下で強行すると、訓練用のメールを受け取った利用者、中でも引っかかって警告を見せられた利用者の中には「なぜ利用者を騙そうとするのか」などと反発を募らせる者が出てしまうことがあります。実際に、その種のトラブルがSNSなどに投稿されたり、訓練用と見られるメールが学外の専門機関に届けられたりすることさえあります。本当の攻撃メールを受け取った時に取るべき行動を、訓練を通じて学んで欲しいというCSIRTの側の考えや想いは、利用者に正しく伝わっていたのでしょうか。実際に標的型攻撃メールを受け取った時に、CSIRTと利用者の間ですれ違いがある中では、インシデントに気づく機会を逸してしまうでしょう。後になって外部の専門機関の観測をトリガーとしてようやく気がつき対応を開始することになります。時間が経過した後では、既に調査すべき証跡を失っているなど、報告にも対策にも行き詰ってしまう可能性もあります。

学内の理解に関する問題は、CSIRTと他の部門等との横方向だけではなく、サイバーセキュリティ対策を進めるラインの縦方向でも見られることがあります。CIO/CISOなどの経営陣に始まり、CIO/CISO補佐などのマネージメント層、CSIRTなどの現場に到る縦方向のラインが機能していないケースです。典型的な例が丸投げです。現場がサイバーセキュリティ対策を「やらされている」と感じている組織では対策を進めようとするモチベーションが湧かないでしょう。また、インシデント対応には、戦略と適切なリソース（人的、予

算等）の投入が不可欠ですが、それには経営陣の関与が欠かせません。実際に、上からのサポートもなく担当者が一人で問題を抱え込んで頓挫している組織が多く見られます。サイバーセキュリティ対策に一人で駆けずり回る、いわゆる「一人CSIRT、一人SOC」の状況は、担当者がモチベーションをもって活動できている間はよいですが、それが途切れたり異動したとたんに瓦解すると言う意味で、組織にとっての脆弱性であると言えます。こうした問題はセキュリティ関連ラインにおける業務の「丸投げ」の結果でもあるのです。

（2）正確な技術情報の取得や活用に関する問題

標的型攻撃も侵入の手口や、使用されるマルウエアなど、インシデント対応に必要な実務知識は刻々と変化しています。そうした技術情報を的確かつ迅速に入手せずして、効果的なインシデント対応は不可能です。例えば、広くばらまかれているマルウエア添付メールへの対応においては、類似したインシデントやマルウエアに関する公開情報から、対応に必要な情報を入手できる場合があります。また、無償で公開されているサービスやソフトウエア、あるいはOSの機能などを活用することで劇的に調査が進む場合もあります。

しかし、CSIRTの担当者が最新の情報を十分に得ていない場合、インシデントの深刻度を低く評価し過ぎてしまって、適切な対応を早期にとる機会を逃しかねません。例えば、標的型攻撃のようにネットワーク内に侵害が進んでいる場合に、判断を誤れば、被害範囲の拡大を許すのみならず、後からの調査に必要な攻撃の痕跡を消してしまい、攻撃の経緯の解明を遠ざけることさえあるのです。

（3）インシデント対応の成熟度の向上が意識できていない問題

セキュリティ対策は、一日にして成らずであって、リスクアセスメントに始まり、対策を立案し、実施して結果を評価するというループを反復するプロセスに本質があります。しかしながら、資料[7]によると、多くの大学でインシデントの対応手順が未整備のままであったり、情報資産に対するリスクアセスメントができていない状態の中で、アクセスコントロールの設定だけは進めている状況にあります。しかしながら、それはたまたま目についた問題に対してその場しのぎの対応に陥っている可能性はないでしょうか。

こうした、場当たり的な対応の背景には、セキュリティ対策の成熟度を高めていくロードマップを描けていないという状況があります。ロードマップ無しでは、いつまでたってもインシデントに的確に対応できない「名ばかりCSIRT」から脱出できないでしょう。

これら３つの問題に対する対策、言い換えれば、CSIRTなどインシデントへの対応体制を組織したものの、「一人CSIRT」や「名ばかりCSIRT」の状態からいかに脱するかの方策につながるヒントを次に考察します。

３．サイバーセキュリティ対策を進める上でのヒント

２章で、大学でインシデント対応を進める上で躓きやすい３つの問題をあげました。これらの問題は、大学の組織としてのサイバーセキュリティ対策への姿勢や成熟度の課題に帰着します。

大学でサイバーセキュリティ対策を進める上で、この成熟度を向上させる取り組みを一つでも進めていくことが望まれます。セキュリティ対策やCSIRTの役割への学内の理解向上に始まり、セキュリティ対策の成熟度を向上させる取り組みのロードマップを描き、それに基づいて進めていくことが肝要です。しかしながら現状では、サイバーセキュリティ対策に意識のある少数の人だけが頑張るだけの状態に至ってしまっているのではないでしょうか。

とはいえ、大学全体のガバナンスや文化の変化を待つのではなく、大学等の土壌に即した改善が望ましいのではないかと考えます。役所や企業のような、大学以外の組織での取り組みやガバナンスの成功事例を取り込もうとしても根付かないでしょう。各大学の組織文化に即した進め方を工夫する必要があります。CSIRT等サイバーセキュリティ対策に取り組む学内組織が学内からの信頼を得つつ活動し、インシデント対応の経験を積みつつ成熟していく理想的な状態に至るためのヒントを次に提案します。こうした状況が生み出されれば、日常的な好循環を通じて自然とサイバーセキュリティ対策が前進していくと考えられます。

（1）ヒント１：インシデント対応のあるべき姿を想像する

「ウチは狙われない」という考えは、昨今の事例を見れば、どのような組織においても幻想に過ぎません。「ウチが狙われている中での対策や体制はどうあるべきか」を思い描いてください。そうした施策なしに、「やれと言われてやっている」情報セキュリティーポリシーの策定や対応体制の整備、「サンプルとなる規程集を参考にするだけで手一杯」という状況になってはいないでしょうか。

例えば、高等教育機関の情報セキュリティ対策のためのサンプル規程集[8]があります。

本情報セキュリティ対策問題研究小委員会が2018年に公開した情報セキュリティポリシーの要素及び関連規程作成の解説[9]では、サンプルとなる規程集を写しただけで、対策が取れるという

ことではなく、大学にカスタマイズすることが重要であると解説されています。カスタマイズのためには、大学組織がどうあるべきかの考察が肝要です。

サイバーセキュリティ対策の中でも、特にインシデント対応についてのデザインは重要です。大学のCSIRTが、学内の利用者に向けて提供するサービスは、それを具現化したものとなります。学内の理解を得る方法や、成熟度の評価と向上施策も検討すべきです。こうしたデザインなしに漫然とインシデント対応やサイバーセキュリティ対策を進めても、場当たりな対応に陥ってしまう可能性があります。

デザインを実際に進める際には、サイバーセキュリティ対策の先進組織を参考にするとよいでしょう。特に、大学間でのCSIRTが情報交換を行う機会が最近は複数あり、情報を得やすくなっています。

（2）ヒント２：現在の成熟度を確認する

限られた時間の中で、手順書も無しに行われるインシデント対応は、一部の「スキルがある担当者」だけに頼って負荷が集中し、スキルや経験を組織として共有できない状況に陥ります。

これを回避するために、組織のセキュリティ対策の成熟度を評価することを提案します。「今、何ができていて、何ができていないのか」を理解し、成熟度として評価することが出発点です。

ここではインシデントへの対応に特化したものとして、日本セキュリティオペレーション事業者協議会(ISOG-J)「セキュリティ対応組織の教科書v2.1」[10]におけるチェックシート「セキュリティ対応組織成熟度セルフチェックシート」を紹介します。これを用いることで、セキュリティ対応組織運営、分析、インシデントへの対応などの項目について自己評価することができます。チェックシートは、レーダチャートなどで結果をみることができるため、現在の成熟度だけでなく、項目ごとの強みや弱みなどを俯瞰して分析できます。こうしたチェックシートは値を調べる以外にも効用があります。各項目を評価する際、周囲と議論して検討することになるでしょう。その議論は、「どうして、この段階にとどまっているのだろうか」など現状の認識を深めるとともに、「どうしたら、この段階を超えていけるだろう」など、向上施策のアイデアを得る絶好の機会となります。チェックリストは、自己点検だけで無く、そうした議論の呼び水にもなるのです。

また、事案に適切かつ迅速に対応していくために、資料を基にした検討だけでなく、演習や訓練を実施して経験として身につけることも重要です。日本ネットワークセキュリティ協会(JNSA)から公開されている「CISO ハンドブック」[11]にも、インシデントに迅速な対応ができるように、インシデントを模擬した机上演習を検討するよう書かれています。手を動かしてみることで、組織の弱点や長所に気がつけるだけでなく、対策手順を作る際の参考にもできるでしょう。

標的型メール攻撃訓練を例とすれば、不審なメールを受け取った利用者が手順にしたがって行動できるか、その際にCSIRTは期待通りに機能するかが検討できると考えられます。不審なメールを受け取った以後の行動や手順を利用者に示すためには、セキュリティポリシーの策定にとどまらず、具体的な行動を記した対策手順の整備が不可欠です。その整備を通じて、具体的な行動を検討することができるし、対応組織や対策のあるべき姿を検討することにも繋がります。

ただし、対策手順は文章化することが大切なのではありません。例えば、メモであっても意図が伝わりさえすれば十分な場合もあります。重要なことは、対策手順の妥当性を訓練や実践を通じて点検し、見直すべき点があれば改善を加えることを繰り返して、対策手順を成熟したものに磨き上げていくことです。

（3）ヒント３：組織連携にて組織外の情報を活用する

CSIRTの能力開発のための参考として、専門機関等の文書を読み解く以外に、他組織の取り組みから学ぶことも重要です。特に、類似した背景をもつ他の大学が行った取り組みや発信情報は、学ぶところが多く、経営陣をはじめとする学内の理解を求める際にも有効なツールとなり得ます。

組織外の情報活用が効果的なことは、大学組織に限ったことではありません。最近ではISACの設置や業界内での情報共有が増えつつあります。

Information Sharging and Analysis Center

ISACなどの同業他社の集まりは、必ずしも先進する組織が未成熟な他組織を助けるばかりではなく、業界内で共通する課題や脅威に対する対処能力の向上や、サプライヤチェーンを含めた業界全体としての対策の強化に資する側面も重要視されています。

セキュリティベンダ等の専門機関からの情報と比べて、同類の他組織から提供される情報の信頼性を低く見る声もあるでしょう。一方、日常生活を振り返ってみると、店を選んだり書籍を購入したりする際に友人の意見や評価を参考にする場面がしばしばあります。ISAC等の同業他社間の情報交換はこれに似ています。必ずしも全てを鵜呑みにする必要はありませんが、類似した視点からの意見や経験情報は他では得難い参考情報となるはずです。これは実生活でも当てはまりますが、専門機関からの情報にせよ、同業他社からの情報にせよ、他者からの情報を深く考えないまま鵜呑

みにするという姿勢は正しくありません。得た情報に対して自組織で評価し適用することが肝要です。自組織の現状に合わせて、情報を活用し、対策を向上させ、また情報を発信するという好循環を作ることを意識できるとよいでしょう。

また、学外の情報をうまく活用する上で、担当者が能動的に学外の会合に出かけられるような風土づくりも大切です。確かに、学内の業務で時間がとれない等の困難もあるでしょうが、学内の業務をより効果的に進める上でも外からの情報は欠かせないはずです。

4．まとめ～大学等でのサイバーセキュリティ対策に対する一考察～

本稿では、大学でのサイバーセキュリティ対策について課題点と対策のポイントを考察しました。

情報セキュリティポリシーの策定が一巡し、大学に求められているサイバーセキュリティ対策の中心が、現実に発生するインシデントに対応するための実効性の伴った組織の構築（マネージメント面、技術面）に移りつつあると考えられます。そうしたフェーズの課題に取り組んでいる読者に、本稿で提案したヒントが示唆を与えることが一つでも二つでもあると幸いです。

サイバーセキュリティ対策を計画するだけでなく実践的な対応ができるように進めていかねば、苛烈さを増しているサイバー攻撃の現実には対処できないことを最後に強調しておきたいと思います。

例えば、2018年２月に発生した国立研究開発法人産業技術総合研究所（産総研）のインシデントに関する報告書[12]を引用すると、「しかし、改めてその実態を振り返ると、CISOと２名のCISO補佐の下で統括情報セキュリティ責任者を担う情報基盤部長が中心となる体制を構築したものの、情報基盤部に研究部門を十分に支援するだけの要員が確保できていなかったこと、情報セキュリティの担当職員が情報化推進担当も兼務せざるを得ず情報セキュリティ対策に組織的に取り組めていなかったこと、研究部門自らが管理するネットワークや情報機器におけるリスクを十分に把握できなかったこと等により、事案の発生を防ぐことができなかった。（原文引用）」と書かれています。CISOなど体制が整えられていたにも関わらず、組織全体では対策やガバナンスが十分に機能していなかったことが読み取れます。この問題は産総研だけに限ったものではないでしょう。情報セキュリティポリシーを策定し、CIO/CISO、そしてCSIRTを構築した段階で止まっていないか、自らの組織に当てはめて考えてみてください。

単に机上での計画だけで終わってしまっていないか、実際に実効性を伴った動きができるのか、そのための課題が何であるかを検討することが極めて重要であり、様々なサイバー攻撃の脅威に晒される大学にとって喫緊の課題ではないかと考えます。机上で検討した計画が、それこそ机上の空論とならぬよう、実効性を伴った計画に練り上げる努力を重ねていくことが大学のセキュリティ対策にあたる関係者に望まれています。

参考文献および関連URL

[1] JPCERT/CC,「CISRTマテリアル」, https://www.jpcert.or.jp/csirt_material/ (2015年11月26日).

[2] 文部科学省,「平成29年度「学術情報基盤実態調査」の結果報告について－大学における大学図書館及びコンピュータ・ネットワーク環境の現状について－」, http://www.mext.go.jp/b_menu/houdou/30/03/1402588.htm (2018年３月23日).

[3] 日本経済新聞,「国立大、サイバー対策道半ば　予算・人不足が鮮明」, https://www.nikkei.com/article/DGXMZO35447354X10C18A9CR8000/ (2018年９月18日).

[4] 内閣サイバーセキュリティセンター,「サイバーセキュリティ戦略」, http://www.nisc.go.jp/active/kihon/pdf/cs-senryaku2018.pdf (2018年７月27日).

[5] 白井克彦,「これからの大学の情報化―情報化による教育改革―」, CAUA ViewPoint, Vol. 10 (2010).

[6] 岡村耕二,「リテラシー教育としてのサイバーセキュリティ」,CAUA View Point, Vol.17 (2017).

[7] 浜正樹,「情報セキュリティベンチマーク評価結果から見た課題」, JUCE Journal, No. 4 (2018).

[8] 国立情報学研究所,「高等教育機関における情報セキュリティポリシー策定について」, https://www.nii.ac.jp/service/sp/ (2017年10月18日)

[9] 私立大学情報教育協会, 情報セキュリティ関連の動画コンテンツ, http://www.juce.jp/sec2018/secpol.html (2018年).

[10] ISOG-J,「セキュリティ教科書 v2.1」, https://isog-j.org/output/2017/Textbook_soc-csirt_v2.html (2018年９月).

[11] JNSA,「CISOハンドブック」, https://www.jnsa.org/result/2018/act_ciso/ (2018年5月11日).

[12] 産総研,「産総研の情報システムに対する不正なアクセスに関する報告」, https://www.aist.go.jp/pdf/aist_j/topics/to2018/to20180720/20180720aist.pdf (2018年7月20日).

[13] JPCERT/CC,「CSIRT構築および運用における実態調査」, https://www.jpcert.or.jp/research/CSIRT-survey.html (2018年12月18日).

[14] 経済産業省,「サイバーセキュリティ経営ガイドライン」, http://www.meti.go.jp/policy/netsecurity/mng_gguid.html (2017年11月16日).