18. 情報セキュリティへの取組

[到達目標]

組織の社会的責任（Social Responsibility）への積極的姿勢を求める声が高まる中で、国内外を問わず近年の情報化推進は、各事業体の内部活動に留まらず社会のインフラの一部を担う者としての責務を果たすことを求めていること、また、人権保障の側面から発祥した個人情報保護法により個人情報に関する管理義務が定められたことなどから、**情報セキュリティへの取組は、組織の社会的責任の１つ**となっている。保有する情報の機密性・完全性・可用性を担保するため、情報の漏洩・改竄・破壊・システム停止などの**セキュリティリスクを適切に管理**していくことが、どの事業体においも喫緊の課題である。

青山学院は、**この課題への取組を学院全体の組織的活動として捉え、学院を構成する全員の理解と協力により、実効性と継続性のある仕組の導入を推進することを目標としている。**

１．現在の活動内容

(1) 活動開始までの経緯

青山学院は、多くの個人情報を預かる「学校」という事業を営んでいることを充分に認識し、「情報セキュリティ」を重要な施策として位置づけてきたが、大学相模原キャンパスの開学を機に、さらに充実したセキュリティ管理をめざし、コンピュータシステムの周辺に重点をおいた技術的対応を中心として再考し、セキュリティポリシーの整備を推進した。

しかしながら､その後数年の社会の流れの中で､情報セキュリティが対象とするものが変化し、前述に特化したものだけではなくなった。現在、その対象は、事業体を支える資源の１つである「情報資産」すべてをさし、情報セキュリティは、リスクマネジメントであると同時にそのリソースマネジメントの一環としても位置づけられ、技術的、人／組織的、物理的な対策（1-(2)-②に詳細を記述）を組み合わせた情報を安全に取扱う仕組（コントロール)、及びそれをPDCA（Plan→Do→Check→Action）サイクルで維持していく仕組（マネジメント）を柱として適切な資源管理をサポートする役割を担うようになった。

この流れを受け、青山学院では、**保有する「情報資産」すべてについて包括的な管理体制を整えることが重要であるという結論を導出し**、2005年１月に基本構想を策定、学院全体のセキュリティポリシーの構築、及びその具体的仕組の導入と維持管理をめざし､「情報セキュリティマネジメントへの取組」として新たな活動を開始した。

(2) 活動計画と体制

① 活動の基本姿勢

青山学院では、保有する多くの情報資産の中でも、学校という組織の特性として中心となる情報の主体が『個人』であるため、学生・生徒・児童・園児、また卒業生や、それに係わる保護者・保証人等における、センシティブ情報を含む個人情報が多くの割合を占めていることにとくに留意している。これらは、学院が健全な事業活動や学問の発展を続けていく上で必要とした“個人から預かった資産である”という認識に立った上で厳格に管理されなければならないものであり、**守るものは情報自体というよりも、実際には個人のプライバシーである**と考えている。個人情報の漏洩・流出等によりその持ち主である『人』に損害や危害が及ぶ可能性があることを忘れることなく、学院の教育方針に「すべての人と社会とに対する責任を進んで果

たす人間の形成を目的とする」とあるように、個人情報を含む情報の安全管理に対しても前向きに取組むことが学院の構成員１人１人の使命と考えるものである。

②　活動における重点項目

ⅰ　情報資産管理の最適化

情報セキュリティは、情報資産に着目し基礎となる情報資産管理を整備することが優先課題となる。学院は１つの法人として情報を共有・連携していることを考慮し、収集・蓄積・活用の方法について、さらに**管理責任・権限とともに組織横断的な仕組を整備**し、局所最適を積み重ねるのではなく、**情報資産管理の全体最適化を図る**必要がある。

ⅱ　技術的対策の有効性

業務において、その割合が増加し続けている電子情報を保護し、また、自らの電子情報保護に留まらず、外部との流通や連携が活発になるほど社会のインフラの一部を担う者としての責務を果たすことは不可欠となり、技術的対策は一層重要となる。日々更新される最新のセキュリティ関連情報を入手し、**適時適切な対策を積極的に講じていく**ことが求められる。

ⅲ　組織的対策の重要性

学校は、より良い教育をめざし、内部で多くの情報が共有・連携されるという特性を持っているため、一般の企業に比べて技術的対策のみで網羅することが困難な組織であるといえる。この組織の特性をカバーするためには、技術的対策に加えて、情報資産を保有する**現場組織の管理責任・権限の体制、業務手順の整備**など、組織的対策の導入に重点をおく必要がある。

ⅳ　人的対策における危険抑止への取組

情報資産にまつわる事故を起こすのは〝人〟であることを考慮し、悪意のないインシデントや、意図せず他者の情報資産を侵害し加害者になってしまうケースなどを防止する。**情報に触れるすべての組織・構成員の日常的な動作の中に正しい理解が浸透し、互いに連携することで、抑止効果をめざす**。また、危険有無の予測や発生の察知、及び発生してしまった場合の措置についても、適切かつ迅速な対応が取れることを目標とする。

ⅴ　日常の業務プロセスに浸透した実効性のある取組

環境に則した取組方針を設定し、**実際の場面において充分に機能することのできる実効性のある取組**でなくてはならない。日々の情報の取扱い自体に有効な仕組の構築が必要である。情報には、収集～利用～保管・保存～廃棄というライフサイクルがあり、ほかに輸送、委託、提供、返却、といった場面も存在する。**業務プロセスの中で、このサイクルがどのように展開されているのかを把握し、伝播・利用していく組織における取扱いを点検する**必要がある。

ⅵ　業務マニュアルへの展開による実効性のある取組

情報セキュリティに関する方針・規定・共通手順書などの策定を行うにしても、実際にはこれらだけで機能するわけではない。現場で有効なものにするためには、具体的な運用手順書の設置や、業務マニュアルを加筆・修正する必要がある。**策定した方針等を基礎として部署ごとの業務マニュアルなど細部へ展開**し、また、各種の関連規定についても不整合が生じないよう配慮する必要がある。

ⅶ　定期レビューによる継続性のある取組

情報セキュリティは方針や規定を策定することによって完結する一過性の取組ではない。セキュリティを業務の仕組と有機的に結合させ継続していく性質のものである。したがって、**定期的に自己点検や内部・外部監査などのレビューを実施することが不可欠**である。マネジ

メントサイクルの中で、規定に準拠していること、及び準拠できる規定になっていることの双方を確認し、業務手順との整合性を保つことが重要なポイントでもある。また、全体のコンプライアンス・プログラムや危機管理などの施策との調和を保ち、**一貫した内部統制の中に位置づけていく**必要がある。

viii　迅速かつ的確な事故対応への取組

リスクの低減を行うと同時に、残存リスクに対する対応を検討しておく必要がある。災害や事故が発生した場合に、迅速かつ的確な対応により被害を最小限に留め、できるだけ短時間に代替手段により再開することで主幹機能を継続していくこと、また、関係者への説明責任を果たすことは、事前策とならんで重要である。学院の危機管理の一環として、事前に計画・準備、メンテナンスしておく必要がある。

ix　物理的セキュリティ再検討の機会

キャンパスの再開発は、情報が保管されている情報機器そのものや文書などの媒体について、それらを保管するファイル、書棚、保管庫、部屋、施設、建物の施錠、配置、管理区域の確保、入退館（室）管理等の設置環境を再検討し、**防災・防犯のセキュリティをバランスよく高める好機**と考えられる。

x　公的認証制度の期待効果

公的認証機関に登録をすることで、適切な保護措置を講じる体制を整備している事業者であるということを示す客観的根拠となる。認証取得には、全員の理解と協力が不可欠であり、これを１つの目標として捉えることで、コンセンサスの形成に繋がることも期待できる。ただし、認定取得をめざす場合に、そのこと自体にだけ目標がおかれた結果、**形骸化した仕組のみが残されるような事態になることは避けなければならない**。その点に充分留意することを前提とした認証制度の利用を検討する。

xi　情報倫理に関する育成

情報社会は、学生・生徒も参画者の一員である。学生・生徒が学校生活を送る中で、インターネットなど外部との通信は、ネットワークを経由し一般社会に関わる状態にあり、社会生活のマナーや危険回避の常識が直接試される場となる。したがって、**学生・生徒を被害から守り、また加害者にしない、情報倫理教育への取組**が必要となる。

③　活動の具体的な推進計画と体制

i　推進計画

次の工程計画に沿って、資産分類×組織ブロックを組み合わせた対象ごとに進めていく。**最終的にはすべてを情報セキュリティポリシーとして取り纏めるとともに、それに基づいた実際の仕組を導入する。**

［工程計画］

Ⅰ　情報資産の把握
Ⅱ　情報リスクの把握と対策
Ⅲ　規定類の文書化
Ⅳ　トライアル運用と啓蒙
Ⅴ　運用への展開

［資産分類］

Ａ　紙及びそれに準ずる媒体
Ｂ　電子データ及びその格納・操作・伝播等の手段

C　情報資産となる用品
D　情報資産を管理する什器・機器類
E　情報資産を管理する設備・施設・建物及びサービス等の環境
［組織ブロック］
1　事務組織
2　教育組織
2-1　高等部・中等部・初等部・幼稚園
2-2　大学・女子短期大学
3　機能横断的組織

ⅱ　推進体制

体制は、維持体制への移行を考慮し整備する。学院構成員全員での取組として維持していくためには、意思や情報の伝達に透過性を持ち迅速かつ的確な報告及び対応が行われる、また、ナレッジを共有できる体制をめざしていく必要がある。この維持体制が確立されるまでの間、2005年３月に発足した法人所管のプロジェクトチームが中心となり、具体的な活動により計画を推進する。

(3) 現在までの活動の内容と成果

現在は、まずはじめのステップとして事務組織が所管する紙媒体の情報資産調査に着手している。おもな活動内容と成果は次のとおりである。

① 事務組織内で保有する「紙及びそれに準ずる媒体」の把握

まず学校の中でも多く情報を保有していると考えられる「事務組織」について、情報の流れが最も把握しづらい紙媒体及びそれに準ずる可搬性のある電子媒体を対象として調査し、**情報資産台帳の作成**を行った。本調査により対象となった**資産の現在の管理状況や課題を明確にすることができた**。また、**事務組織の全員が参画する活動となったことからその存在や意義が能動的に認識**され、セミナー等の受身の啓蒙よりも、「情報セキュリティマネジメント」導入の第一歩として有効な手段であった。

② クリアデスク（机・保管庫・倉庫等）による環境整備及び余分リスクの排除

①の資産台帳を作成するにあたり、まず情報資産を把握しやすい状態にすることを目的として、本来の「クリアデスク」の意味合いを発展させ、個人の机より発して保管庫・倉庫に至る資産の保管・保存場所の環境整備を行った。**情報資産が整理整頓され、最も余分なセキュリティリスクと考えられる不要文書類を廃棄処分に回す**ことができた。さらに２次的効果として、確保した空きスペースを有効に再利用することが可能になったこと、また、**情報量を必要最小限に留めたこと及び格納場所をすぐに特定できるようになったことは、業務の効率化にもつながった**。

③ 機密抹消処理スキームの確立・手順書作成、及び実行

①により排出された機密書類の廃棄処分について、選定した業者に機密抹消処理を業務委託し、セキュリティリスクの低減を実効することを前提とした**廃棄のスキームを確立**し、後述④の策定に先駆けて、**情報資産の廃棄に関する手順書（暫定版）を作成**、また、①②の終了後、**手順書にしたがって廃棄を実行**した。

④ セキュリティポリシーの最上階層となる「情報セキュリティ基本方針」の策定と周知

①～③の実行がほぼ安定してきたことを受けて、情報セキュリティへの取組姿勢である基本

方針を策定し学院全体に周知した。

⑤ 関連業務への展開

ⅰ 「青山学院個人情報に関する規則」等の施行

学院の所有する情報のうち多くを占める個人情報については、保護法の全面施行をうけ2005年７月に標記規則を設置し、法律が定めるところの個人情報に関するセキュリティについては、先行して指針を宣言し、注意喚起を行った。

ⅱ 文書保存年限の見直しと関連規定の整備

不要となった文書を廃棄するために、適切な保存年限が不可欠であるため、その見直しを行った。

ⅲ 情報セキュリティフォローアップ監査（内部監査）の導入

維持向上のための施策として、PDCAマネジメントサイクルのC（チェック）について、自己点検と並行して内部監査を導入することとした。

ⅳ 歴史資料保存関連規定の整備

保存すべき情報のうち、学院の歴史を示す情報についての一元管理を定義することとなった。

２．現在の活動内容と到達目標との比較

業務（活動）の性質上、個々の事象に対して充分な検討を積み重ね、具体的施策の実行を伴わせながら成長させていく取組であることから、進行はゆっくりであり完了に至った部分はまだ少ない。しかしながら、目標に向かって着実に進んでおり、現在、1-(3)に記述した活動が完了に近づいた時点で、**個々人や組織としての意識の向上といった側面で、学院全体へ取組が浸透し始めたと考えられ**、次に、推進過程の中程となる**展開期へ順調に移行することが可能な段階まで到達したといえる。**

３．現在抱えている問題点とその具体的改善方針・改善計画、今後の展望

(1) 現在特に留意すべき事項と改善計画

本計画の導入部分について、一応の完了を2008年３月と予定しており、情報セキュリティポリシーの策定や運用への移行までには時間がかかる。その間に早急に手当すべき事象が顕在化した場合には、その対応に特に留意する必要があると考える。

情報資産調査により発見された**情報セキュリティリスクについては、すべてのポリシーの確立を待たずに実効性を優先し、すぐに対策を講じて実施すべき**と考え、この部分については、前述の基本方針（暫定）に基づいた、「基準書」また「共通手順書」の一部として先行して整備していくよう、すでに活動を開始した。

(2) 今後の展望

① 短期的な展望（リスクマネジメントの側面）

２で述べたように、計画の展開期に到達した。今後は、これまでに蓄積したノウハウを活かして活動を広げていくことを考える。情報資産も**紙媒体以外の資産について、組織も教員組織について、対象とした活動を開始**するよう準備を進めている。また、3-(1)に記述した活動を行うとともに、研修会などによる**教育・啓蒙活動を開始**する。このようにさまざまな活動を並行して行い、さまざまな側面から働きかけることでさらに取組を強化し、**実効性・継続性のある取組が完了した時に、学院のリスクマネジメントの一環として位置づけられることになる。**そ

の目標に向かって推進する。

② 中長期的な展望（リソースマネジメントの側面）

情報セキュリティは「情報資産の管理」といった戦略的側面も持ち合わせている。近年、J-SOX法や新会社法でいわれる「内部統制」とも無関係ではなく、情報セキュリティを起点とした統制活動を行っている事業体も多く見受けられる。このような時流の中で、**業務改善や組織運営など学院を支えるインフラ活動の一部として整備を推進**したいと考える。