佐賀大学 セキュリティーポリシーの制定

大谷 誠、只木 進一 (総合情報基盤センター)

1 始めに

近年の急速な高度情報社会の進展により、大学において情報の電子化やインターネットを介して電子化された情報をやり取りするといったことが日常的に行われるようになってきました。これに伴って、情報の漏洩や紛失、改ざんや不正アクセスといったセキュリティー上の脅威が高まっており、実際に事件も多く発生しています。また、個人情報の保護についても近年強く求められるようになっています。

このような背景から、情報に関する「セキュリティーポリシー」を制定する大学や企業が増えてきました。佐賀大学においても、セキュリティーポリシーを制定し、学内に公開しています。本稿では、平成9年度に改訂した佐賀大学におけるセキュリティーポリシーの内容について、我々が具体的にどのようなことに気を付けなければいけないのかについて簡単に説明します。

2 セキュリティーポリシーの位置付け

佐賀大学におけるセキュリティーポリシーは、佐賀大学の情報セキュリティーの水準を適切に維持していくための基本的水準を定めたものです。あくまで基本的水準を定めているものであり、各部局の必要性や特性に応じて、それぞれのセキュリティーポリシーやセキュリティー保護のための手順や規程を、別途整備する場合があります。

佐賀大学におけるセキュリティーポリシーでは、情報セキュリティーを維持していく上での「組織体制」や、対象者がやるべき「セキュリティー対策」を定めています。

このセキュリティーポリシーの対象者とは、本学教職員のうち情報及び情報システム(業務で利用するPCなども含む)を取り扱う人です。適応範囲は異なりますが、学生も該当します。よって、佐賀大学を構成する全ての人が該当することになります。

それでは、我々はセキュリティーに関して具体的にはどのようなことを把握し、情報や情報システムを扱っていく必要があるのでしょうか。

3 情報セキュリティー対策

セキュリティーポリシーでは、我々が情報や情報システムを扱う上で、主に以下のような事柄を把握・実行・検討する必要があると定めています。

- **情報セキュリティ管理体制**

  情報のセキュリティーを守るには、セキュリティーを管理する組織・体制が重要になってきます。佐賀大学に置ける情報セキュリティー管理体制(**図1**)は以下のようになっています。

  まず最高責任者として、「最高情報セキュリティ責任者(CISO)」を配置しています。このCISOは、佐賀大学における情報セキュリティー対策に関する事務を統括します。実際には、

この業務を情報統括責任者が行います。

CISO は、監査に関する事務を統括する「情報セキュリティ監査責任者」も配置します。その他に、必要に報じて情報セキュリティーに関する専門的な知識及び経験を有した専門家を「最高情報セキュリティアドバイザー」として配置します。

また CISO は、各部局単位に「情報セキュリティ責任者」を置き、そのうち、情報セキュリティ責任者を統括する者を「統括情報セキュリティ責任者」とします。佐賀大学では、報セキュリティ責任者は各部局長、統括情報セキュリティ責任者は情報統括室長となります。情報セキュリティ責任者は、各部局単位で情報セキュリティーに関する事務を統括します。

その他に、情報システムごとに「情報システムセキュリティ責任者」、管理単位ごとにセキュリティ対策を行う「情報システムセキュリティ管理者」が配置することがあります。

教職員は、このような情報セキュリティー管理体制の基に情報システムを利用することになります。システムに障害などが発生した場合には、管理体制に基づいた報告を行う必要があります。

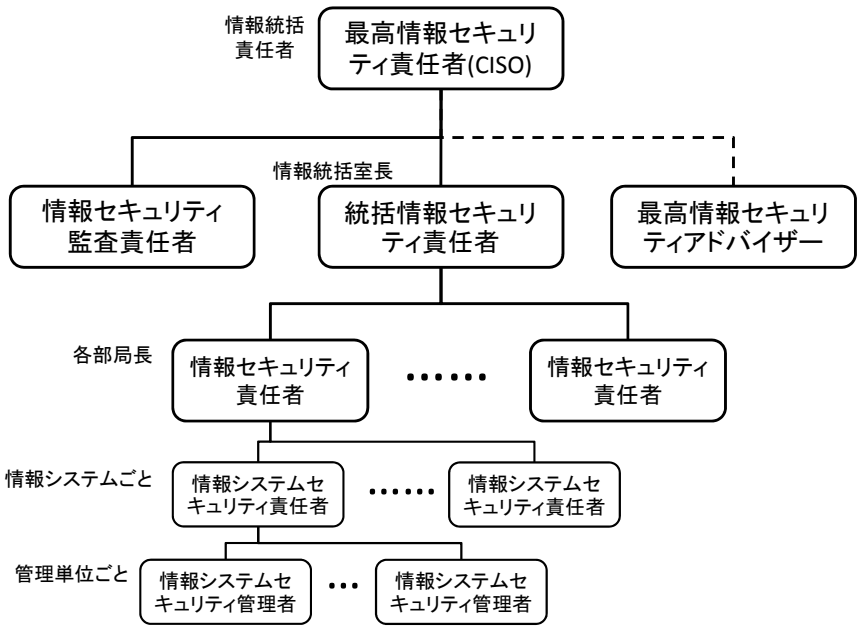

図 1 情報セキュリティー管理体制

- **情報セキュリティー教育**

  日頃から「情報」の扱いに関する十分な知識を習得しておくことが、情報セキュリティーを守る上で重要となります。佐賀大学においては、定期的に情報セキュリティー対策に関する教育活動が計画されます。この計画に従って、情報セキュリティー対策の教育を受けて下さい。

- **情報の取り扱い**

  情報のセキュリティーを守る上で、情報をどのように扱っていくかも重要となります。そこで、情報を取り扱う上で以下のようなことに気を付けなければいけません。

大学の業務遂行目的以外で、情報システムに係わる情報を作成したり、入手や利用したりしてはいけません。また、業務遂行目的で作成した情報は、その情報の性質に応じて、取扱制限(学外秘等)が必要かどうかの有無を検討し、取扱制限が必要な場合には明示するようにしないといけません。また、大学の業務遂行目的であっても、制限の掛かっている情報を許可なく学外に持ち出したりしてはいけません。

また、情報を保存している記憶媒体(CD-ROM,USB メモリ等)も適切に管理する必要があります。それらの情報を必要に応じて暗号化する等の対策をとる必要もあります。破棄についても適切に行う必要があり、記憶媒体を破棄する場合は、情報の復元を困難な状態にして破棄しなければいけません。コンピュータ上の情報も文書情報と同じように、重要性に応じた取扱が必要となります。

- **認証**

電子化された情報や情報システムにアクセスする際、必要に応じて「認証」を求められる(ユーザ ID やパスワードなど)ことがあります。この際は、以下のようなことに気を付けなければいけません。

自分に付与されたユーザ ID 以外を用いて情報システムを利用してはいけません。具体的には、他人の資格で情報システムを利用してはいけないということです。また、他人にユーザ ID を付与したり貸与したりしてもいけません。その他に、パスワードが他人に直ぐ分かるような状態にして放置したりしてはいけません。本人しか分からないパスワードである必要があります。

また、教職員が普段業務に使用する PC にも様々な重要文章が保存されていると思います。とって、業務に利用する PC も認証を行うようにし、権限のないものが重要情報にアクセスできないようにしなければいけません。

- **障害や違反発生時における報告**

情報システムに障害が発生した場合、迅速に対応することが、情報のセキュリティーを守る上で重要となります。そこで、情報システムの障害に気が付いた場合などは以下のような対応を行う必要があります。

情報システムの障害の発生や情報セキュリティー関係規程への重大な違反を知った場合には、それに関係する者に連絡するとともに、定められた報告手順によって情報セキュリティ責任者(各部局長)にその旨を報告する必要があります。情報セキュリティ責任者に報告された重大なセキュリティー案件は、統括セキュリティ責任者から CISO に報告され、その後に文部科学省や IPA(情報処理推進機構)といった各組織に報告されます。

また障害が発生した場合の対策手順の有無を確認して、その対策が実施できる場合にはその手順に従う必要もあります。もし手順が確認できない場合は、障害などによる被害の拡大防止に努めることも必要です。

- **情報システムや端末(PC 等)の利用**

  情報システムや業務に利用する PC がコンピュータウィルスに感染すると、そこから情報が流出してしまう可能性があります。そこで、情報システムや利用する PC などにおいて、アンチウイルスソフトウェア等による不正プログラム(ウィルスなど)の自動検査機能を有効にしておかなければいけません。また、アンチウイルスソフトウェア等にかかわるアプリケーション及び不正プログラム定義ファイル等について、これを常に最新の状態に維持しなければいけません。その他に、定期的に全ての電子ファイルに不正プログラムの有無を確認するようにしてください。佐賀大学で利用を禁止されたソフトウェアを利用してはいけません。

  モバイル PC(本学支給のもの)によって、機密情報を扱う必要がある場合は、盗難防止対策を行う必要があります。また学外に持ち出す必要がある場合には、必要に応じて情報を暗号化する必要もあります。

  本学支給のものでない PC 等を利用する場合には、原則として端末用ネットワーク(Opengate)へ接続し、認証を行ってから利用するようにしてください。

  また、端末(PC 等)の設置・利用に関しては、別途「キャンパス情報ネットワーク端末設置規程」といった規程も定められています。

以上が、我々が日常情報を扱う上で気を付けなければならない事柄を大まかにまとめたものです。これ以外にも状況に応じて気を付けなければならない事項もあります。詳しくは「佐賀大学 セキュリティポリシー*」の原文や、これに関連する規程類をご覧ください。

4　まとめ

急速な高度情報社会の進展によって、パソコンなどを用いて多くの情報を簡単に保存し、管理できるようになりました。このような情報の電子化は便利な反面、セキュリティー上のリスクも増大させてしまいます。このようなリスクは、情報システムのセキュリティー対策だけで防げるものではなく、個人個人のセキュリティーに対する意識を高め、慎重に情報を扱っていくことが重要となります。

この文章やセキュリティーポリシーを皆様に一度お読みいただき、佐賀大学の情報セキュリティー水準の維持にご協力ください。

5　今後の予定

今後、佐賀大学のセキュリティーポリシーに基づき、情報システムや Web サーバの構築に関する規程や、電子メール利用規程やモバイル PC 利用要項といった様々な規程等が定められる予定です。このような規程などもあわせてご覧ください。

---

* 国立大学法人佐賀大学セキュリティーポリシー第２版
  http://www.saga-u.ac.jp/gakunai/joho/secu.pdf