情報セキュリティに関する取り組みについて

上繁義史（ICT 基盤センター 情報基盤デザイン部門長）

1. はじめに

AI や IoT など，情報技術に関する新たなトレンドが生まれる一方で，これらの最新技術を悪用して，情報セキュリティ上の脅威は増大する一方です。また，外部からの攻撃だけでなく，利用上の問題（例えば公開範囲の設定ミス）によって意図せずに外部から（本来機密とすべき）情報が閲覧可能になるといった，日常業務から生じる内部の脅威もあります。

上述の脅威が現実の情報セキュリティインシデント（事故）に発展すると，その影響が広範に及ぶことが想像されます。そこで，長崎大学では情報セキュリティポリシーの中で目指すべき事柄として以下の項目を挙げています。

「

① 本学の情報セキュリティに対する侵害を阻止。
② 学内外の情報セキュリティを損ねる加害行為を抑止。
③ 情報資産に関して，重要度による分類とそれに見合った管理。
④ 情報セキュリティに関する情報の取得を支援。
⑤ 本学の構成員等による学内外への情報セキュリティの侵害を防止し，構成員等に対する教育を実施すること。
⑥ 本学のセキュリティレベルの達成度について，セキュリティ監査を実施し随時見直しを行うこと。

」

また，第 2 期（平成 22 年度～平成 27 年度）及び第 3 期（平成 28 年度～平成 33 年度）の中期目標及び中期計画の中で，情報セキュリティに関して以下の内容を掲げ，大学全体の情報セキュリティの維持，向上に努める姿勢を明確にしました。

第 3 期中期目標
「法令遵守の徹底及び管理・監査体制の強化を図る。」
第 3 期中期計画
「情報セキュリティ対策の徹底と個人情報を含む情報資産の安全管理の強化を図るため，最高情報セキュリティ責任者（CISO）を中心に情報セキュリティ自己点検制度の導入など強化対策を実施する。」

本稿では，2017 年度（平成 29 年度）～2018 年度（平成 30 年度）の情報セキュリティに関する諸活動について報告いたします。

2. CSIRT 発足とその活動

2.1. 「情報セキュリティ対策の実施に関する要項」制定

2017 年 3 月 27 日に「情報セキュリティ対策の実施に関する要項」が制定されました。この要綱の第 1 条を以下に引用します。この条文に述べられている「情報セキュリティインシデントに対応するための体制」が情報セキュリティ対策チーム（CSIRT）です。

「(目的)

第 1 条　この要項は，長崎大学(以下「本学」という。)における情報セキュリティ対策の強化及び情報セキュリティインシデントに対応するための体制について必要な事項を定め，もって情報セキュリティ対策の徹底と個人情報を含む情報資産の安全な管理に資することを目的とする。」

従前より長崎大学においては ICT 基盤センターと学術情報部情報企画課が中心となって，様々な情報セキュリティ対策を講じてきましたが，文部科学省より，各大学に対して，2016 年度（平成 28 年度）～2018 年度（平成 30 年度）の「情報セキュリティ対策基本計画」策定の指示があり，その中に緊急のセキュリティに関する事象（インシデントなど）に対処できる体制の明確化が含まれていました。CSIRT はそのような背景から誕生しました。

2.2. CSIRT の活動状況

CSIRT の業務範囲は主に外部からの攻撃等による情報セキュリティインシデントへの対応とその予防のための支援です。「情報セキュリティ対策の実施に関する要項」の対応する条文を引用すると，以下のようになります。

「(情報セキュリティ対策チーム)

第 3 条　本学に，情報セキュリティインシデントに対応するため，情報セキュリティ対策チーム(以下「CSIRT」という。)を置く。

(中略)

3　CSIRT は，次に掲げる業務を行う。

(1)　情報セキュリティインシデントの正確な把握に関すること。

(2)　情報セキュリティインシデントの被害の拡大防止を図るための応急措置に関すること。

(3)　情報セキュリティインシデント発生の原因特定及び復旧に関すること。

(4)　情報セキュリティインシデントに係る関係機関への連絡調整に関すること。

(5)　情報セキュリティインシデントの再発防止のための技術的な支援等に関すること。」

これまでの CSIRT としての活動としては，学内でのウイルス感染に関する調査活動や情報流出につながる事象に関する応急措置，原因特定，事後対応などが挙げられます。対応の件数としては，表 1 のとおりです。

表 1　CSIRT による情報セキュリティインシデントへの対応件数

年度	件数
2017 年度（平成 29 年度）	19 件
2018 年度（平成 30 年度）	11 件

2.3. CSIRT への連絡窓口

大学では，2017 年（平成 29 年）4 月に CSIRT への連絡窓口を開設しましたので，情報セキュリティインシデントに気づいた場合には，以下の連絡窓口に連絡をお願いします。

連絡いただく際には，下記の内容をお知らせください。

- 事案発生日時
- 事案発生場所
- インシデント内容，被害状況
- 通報者の氏名・連絡先

【CSIRT 連絡窓口】

平日：095-819-2022（学術情報部情報企画課内）

E-mail：ｃｓｉｒｔ（アットマーク）ｍｌ．ｎａｇａｓａｋｉ－ｕ．ａｃ．ｊｐ

3. 三大学間情報セキュリティ相互監査の取り組み

3.1. 取組の経緯と準備

この取り組みは佐賀大学，九州工業大学，長崎大学の 3 大学において，情報系センター及び担当部局を対象として，情報セキュリティ対策の現状と課題を把握するために実施されるものです。佐賀大学から本取り組み参加への呼びかけがあり，九州工業大学及び本学が同意したにより，2017 年度に実施のための準備が進められることになりました。

相互監査においては，それぞれの大学における機密性の高い情報セキュリティの話題を取り扱うため，まず 2017 年 7 月に大学間で秘密保持に関する覚書を取り交わしました。

実施に先だって，テレビ会議により 3 大学を接続して打ち合わせを数回行いました。その主な議題は

1. 相互監査のスキーム
2. 開催の日程
3. 相互監査の項目
4. 相互監査実施報告の様式

です。2 については，国立高専機構が作成した情報セキュリティ監査のチェックリストを参考に佐賀大学にて原案が作成され，3 大学の打ち合わせを通じて完成させました。相互監査チェックリストの詳細は，上述の秘密保持に関連するため，本項ではその概要について表に示すにとどめます。

表 2　相互監査チェックリストの概要

番号	大項目	小項目数
1	情報セキュリティの基本方針	2
2	組織，危機管理，自己点検及び見直し(情報セキュリティのための組織)	5
3	情報システムの利用に関すること（規程等）	12
4	利用者 ID 及びパスワードの運用管理	6
5	情報システムの運用管理(セキュリティを保つべき領域を含む)	5
6	情報システムの調達及び外部委託	4
7	ネットワーク管理及び IP アドレス管理	3
	計	37

3.2. 第 1 回相互監査

第 1 回相互監査は 2018 年 2 月～3 月に実施されました。監査の日程は表 3 に示す通りです。被監査校に監査校担当者が訪問し，ヒアリングや現地視察を通じて，監査を行います。第 1 回は初めての相互監査であることから，相互監査チェックリストに含まれる全 37 項目について監査が行われました。本学からは ICT 基盤センター，学術情報部情報企画課の 3 名で対応しました。

監査の実施後に，相互監査実施報告書を作成し，被監査校に送付しました。本学も同報告書を受領しました。報告書には有用な指摘が含まれており，その後の情報セキュリティ対策に活かされています。

表 3　2017 年度相互監査の日程

日時	被監査校	監査校
2018 年 2 月 6 日（火）13:30-17:00	長崎大学	佐賀大学，九州工業大学
2018 年 2 月 19 日（月）13:30-17:00	佐賀大学	九州工業大学，長崎大学
2018 年 3 月 16 日（金）13:30-17:00	九州工業大学	長崎大学，佐賀大学

3.3. 第 2 回相互監査

第 2 回相互監査は 2018 年 9 月に実施されました。日程は表 4 に示す通りです。第 2 回以降は相互監査チェックリストのうち，重点項目を定めて監査を行うことが申し合わされました。第 2

回相互監査においては，大項目「3.　情報システムの利用に関すること（規程等）」の 12 項目を重点項目としました。

今回の監査では，第 1 回に比べて時間的余裕があったことから，ヒアリングに加えて，被監査校の情報系センターの施設見学（現地監査）を行いました。

表 4　2018 年度相互監査の日程

日時	被監査校	監査校
2018 年 9 月 3 日（月）13:30-17:00	佐賀大学	九州工業大学，長崎大学
2018 年 9 月 6 日（木）13:30-17:00	九州工業大学	長崎大学，佐賀大学
2018 年 9 月 10 日（金）13:30-17:00	長崎大学	佐賀大学，九州工業大学

4. 情報セキュリティに関する啓発活動

4.1. 情報セキュリティ講習会の開催

例年，年 1 回外部講師による情報セキュリティ講習会を開催しています。外部講師には，情報セキュリティの第一線で活躍されている方に依頼しており，情報セキュリティの最新事情や実践すべき対策について解説いただいています。これにより，一人でも多くの構成員に情報セキュリティの取り組みへの協力をいただき，大学全体のセキュリティレベルの向上に貢献することを目的としています。

両年度の開催について，概要を表 5 にまとめます。

表 5　情報セキュリティ講習会の概要

2017 年度（平成 29 年度）	
開催日	2017 年 12 月 1 日（金）14：30-16：00
演題	最近のサイバー攻撃手法とその未然防止及び発生時の適切な対応について
講師	平原隆氏（長崎大学情報セキュリティ監査責任者，株式会社シーアイエー代表取締役社長）
講演概要	近年，情報セキュリティ対策はビジネス上の必須事項と言え，経営者の認識が第一歩である。最近の攻撃の手法として，標的型攻撃とランサムウェアが紹介され，その基本的な対策は，前者については，全てのソフトを最新に保ちつつ，メール本文も確認すること，後者については，適切にバックアップを取ることを上げていた。 今後大学において求められるセキュリティの対象として，メール（特に海外出張時），IoT 機器，SNS について解説がなされ，併せて基本的な対策の考え方が紹介された。
会場	グローバル教育・学生支援棟 3 階 G3A 教室（文教キャンパス）

	参加者数	80 人（学生，教職員）
2018 年度（平成 30 年度）		
	開催日	2018 年 11 月 7 日（水）14：30-16：00
	演題	サイバーセキュリティ最前線 〜ネットにつながる全てが狙われる〜
	講師	浦田孝広氏（長崎県警察本部 警務部警務課 サイバーセキュリティ戦略室 係長）
	講演概要	近年，デジタル機器の多くがインターネットに接続されるようになり，それに伴い，インターネットを利用した犯罪への不安が高まっている。 標的型攻撃が知られているが，その認知件数は増加傾向にあることが紹介された。また，サイト閲覧やメッセージアプリを利用したウイルス感染などの脅威も紹介された。一般に知られるレベルの基本的な情報セキュリティ対策を確実にとっていくことが必要であることが説明された。 講演ののち，標的型メールの本文中のリンクを用いたウイルス感染のデモが行われ，容易に乗っ取ることが可能であることが紹介された。
	会場	グローバル教育・学生支援棟 3 階 G3A 教室（文教キャンパス）
	参加者数	79 人（学生，教職員，学外者一般）

4.2. 情報セキュリティ基礎講習会の 3 キャンパス開催

2016 年（平成 28 年）3 月以降，教職員向けにパンフレット「『安全』を引き寄せる 8 つの情報セキュリティ対策」が配布されています。これは ICT 基盤センターが原案を作成し，情報セキュリティ委員会から発行されたものです。

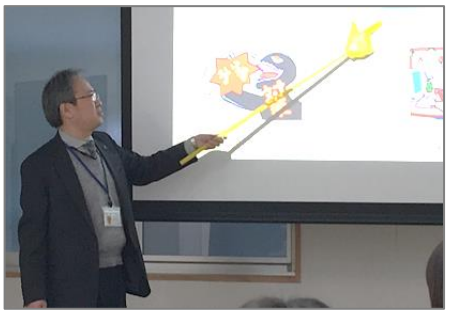
情報セキュリティ基礎講習会では，その内容について事例を交えながら解説しています。併せて情報セキュリティ対策が必要な理由や組織における情報セキュリティの在り方などの話題を提供して，大学全体のセキュリティレベル向上を目指しています。開催時期は概ね 9 月と 2-3 月です。本講習会を文教，坂本，片淵の 3 キャンパスにて，同一内容で数多く開催することで，教職員の業務の都合に合わせて参加できるように配慮しています。開催通知を教職員ポータルに投稿して参加者を募るだけでなく，講習会会場での直接参加も受け付けて，一人でも多く参加いただけるようにしました。

本講習会は今後も実施していく予定ですので，本学に着任後間もない方には強く受講をお勧めします。知識のリフレッシュにも役立ちますので，最近講習会に参加されていない方やリピーターの方も是非ご参加ください。

本講習会の開催概要を表 6 に示します。

表 6　情報セキュリティ基礎講習会の概要

演題	『安全』を引き寄せる 8 つの情報セキュリティ対策
講師	上繁義史（ICT 基盤センター 情報基盤デザイン部門長）

<table>
<tr><td>開催日</td><td colspan="2">2017 年 9 月 12 日（火），9 月 13 日（水），9 月 14 日（木），
9 月 19 日（火），9 月 20 日（水），9 月 21 日（木），
9 月 27 日（水），9 月 28 日（木），9 月 29 日（金）
2018 年 2 月 20 日（火），2 月 21 日（水），2 月 22 日（木），
2 月 27 日（火），2 月 28 日（水），3 月 1 日（木），
3 月 6 日（火），3 月 7 日（水），3 月 8 日（木）
2018 年 9 月 4 日（火），9 月 5 日（水），9 月 6 日（木），
9 月 11 日（火），9 月 12 日（水），9 月 13 日（木），
9 月 25 日（火），9 月 26 日（水），9 月 27 日（木）</td></tr>
<tr><td>講演概要</td><td colspan="2">最初になぜ情報セキュリティ対策が必要なのか，社会的背景について説明し，情報セキュリティ，セキュリティリスクの考え方を紹介した。
つづいて，個人と対比させつつ，企業団体等で組織的にセキュリティ対策に取り組む必要性を説明し，情報セキュリティポリシーの概要を紹介した。
パンフレット「『安全』を引き寄せる 8 つの情報セキュリティ対策」の各項目を解説しつつ，標的型攻撃対策としてのメールの気を付け方やパスワードの対策などについて詳細に解説した。
  </td></tr>
<tr><td>会場</td><td colspan="2">文教キャンパス：附属図書館 中央館　地下多目的ルーム
坂本キャンパス：附属図書館 医学分館　セミナー室
片淵キャンパス：附属図書館 経済学部分館　経済学部分館</td></tr>
<tr><td rowspan="3">参加者数</td><td>2017 年 9 月開催分</td><td>17 人</td></tr>
<tr><td>2018 年 2-3 月開催分</td><td>26 人</td></tr>
<tr><td>2018 年 9 月開催分</td><td>8 人</td></tr>
</table>

4.3. 学生向け情報セキュリティ自己点検の試行

2015 年度（平成 27 年度）より教職員向けの情報セキュリティ自己点検を実施しています。これは，教職員一人一人が自分のセキュリティ対策の現状について振り返るとともに，必要に応じて新たな対策を講じる契機とすることで，情報セキュリティ対策を確実に実施していくことを目的としています。

学生については，学部 1 年次の教養教育科目「情報基礎」（全学部 1 年前期，必修，2 単位）の中で特別授業などを通じて情報セキュリティについて学ぶ機会があるものの，それ以降については（全学モジュールなど一部の授業を除けば），学習機会は皆無に等しいのが実情です。学生の PC 必携化が進む中で，そのセキュリティレベルを確保，向上させるために，教職員同様に学生も自身のセキュリティ対策の現状について把握する必要があります。そこで，学生向け情報セキュリティ自己点検を行うこととし，2018 年（平成 30 年）10 月から試行として学内に開示しました。設問は日本語と英語で表示され，留学生にも配慮しています。ランダムに選ば

れた 10 問の設問に回答することにより，自身のセキュリティ対策の状況や今後とるべき対策についての解説が表示される仕組みとなっています。先生方には，授業などで是非実施するように勧めていただければ幸いです。

下図に情報セキュリティ自己点検システムのログイン画面及びメニュー画面を示します。

図 1　学生向け 情報セキュリティ自己点検システムの画面例

5. まとめ

本項では，2017 年度（平成 29 年度）～2018 年度（平成 30 年度）における情報セキュリティ対策に関する話題として，CSIRT の活動，三大学間情報セキュリティ相互監査の取り組み，情報セキュリティの啓発活動について紹介しました。本項では取り上げませんでしたが，不正通信検知のための監視，情報セキュリティマネジメントシステム（ISMS）に関連する活動も継続的に実施しています。

情報セキュリティの維持は，ICT 基盤センターと学術情報部情報企画課の活動だけでなく，学生，教職員の皆様の支援が欠かせません。今後とも是非ご理解，ご協力くださいますようお願いいたします。