

# 情報セキュリティの取り組み

情報基盤デザイン部門

上繁義史

## 1. はじめに

ICT の世界が日進月歩であるといわれていますが、それと同様、情報セキュリティ上の脅威も日に日に増えています。一度その脅威が現実のインシデントに発展すると、その被害が個々人の範囲にとどまらず、組織全体や世界に及ぶことが考えられます。そこで、長崎大学では第 2 期中期目標及び中期計画(平成 22 年度～平成 27 年度)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 2 期中期目標

「情報マネジメント体制を整備し、情報セキュリティを向上させる。」

### 第 2 期中期計画

「情報資産の安全管理を高めるための体制を整備するとともに、高度情報セキュリティに対応した人材を育成する。」

この考えは第 3 期中期目標及び中期計画(平成 28 年度～平成 33 年度)にも取り入れられています。

### 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、平成 26 年度～平成 28 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. 推進体制～情報セキュリティプロジェクト

平成 26 年度より、情報メディア基盤センターが ICT 基盤センターに改組され、情報セキュリティに関する活動は本センターの他の活動と同様、最高情報責任者(CIO)が統括するプロジェクトの一つとなりました。メンバーは部局横断的に構成され、大学全体の情報セキュリティの維持にあたります。平成 26 年度のプロジェクトのメンバーは以下の通りです。

リーダー:金丸 邦康(工学研究科教授、最高情報セキュリティ責任者(CISO)補佐)

メンバー:上繁 義史(ICT 基盤センター准教授)

土田 徹 (学術情報部情報企画課主査)

長崎 隆志(学術情報部情報企画課主任)

岩崎 蓉子(学術情報部情報企画課班員)

平成 27 年度、平成 28 年度において、上野 恒信 学術情報部長(平成 27 年度より最高情報セキュリティ責任者補佐)をグループリーダーとし、下記の体制で活動に取り組みました。

リーダー:上野 恒信(学術情報部長、最高情報セキュリティ責任者(CISO)補佐)

メンバー:上繁 義史(ICT 基盤センター准教授)

清川 聖一(学術情報部情報企画課長)

土田 徹 (学術情報部情報企画課主査)

長崎 隆志(学術情報部情報企画課主任)  
神田 洋平(学術情報部情報企画課班員)  
岩崎 蓉子(学術情報部情報企画課班員)  
佐藤 慶一(学術情報部情報企画課班員)

### 3. 長崎大学情報セキュリティポリシーの改訂

平成 21 年度に長崎大学セキュリティポリシーが第 3 版に改訂されてから 5 年が経過し、大学での教育と研究における ICT 利活用が大幅に進みました。それと同時に、世界的に情報セキュリティ上の脅威が拡大するようになりました。また、これに伴い、不正アクセスを前提として、インシデント対応や、情報の管理運用体制の強化が、今まで以上に要求されるようになってきました。そこで、平成 26 年度に第 3 版の主要な政策を踏襲しつつ、最新の情報セキュリティ対策を盛り込んで、強化をはかることになりました。

改訂にあたり、「政府機関の情報セキュリティ対策のための統一基準群(平成 26 年度版)」「情報セキュリティ政策会議作成」などを参考に、情報セキュリティプロジェクトで素案を作成し、情報セキュリティ委員会(平成 26 年 4 月 1 日設置)などの審議を経て、平成 26 年 11 月 14 日に第 4 版が施行されました。その概要は Web 上で公開しており、長崎大学公式 Web から「長崎大学について」、「情報セキュリティポリシー」の順にリンクをたどるか、下記 URL を直接入力することによりご覧いただけます。

<http://www.nagasaki-u.ac.jp/ja/about/guidance/security/index.html>

次節で改訂のポイントを紹介します。

#### 3.1 組織体制の見直し

長崎大学における情報セキュリティ体制組織図を下図に示します。図の網掛けの箇所が今回の改訂で大きく変化した箇所です。

「長崎大学情報化統括責任者等の設置に関する規則」(平成 26 年 3 月 28 日制定)において、最高情報セキュリティ責任者(CISO)、最高情報セキュリティ責任者補佐(CISO 補佐)、情報セキュリティ監査責任者が規定化されたことによる見直しが行われました。併せて CISO を委員長とする情報セキュリティ委員会が新設となりました。

情報セキュリティインシデント(事故)に対応するための、情報セキュリティ対策チーム(CSIRT)を新設することとなりました。CSIRT については、学内規則(要項)にて設置規則が制定される予定です。

第 3 版以前で定義されていた情報システムセキュリティ管理者を情報システムセキュリティ管理責任者に変更し、より強力なセキュリティ対策をお願いすることになりました。

#### 3.2 最新のセキュリティインシデントに対応した対策基準を追加

大きく以下の 6 つのポイントについて、新たな基準が追加されました。

1. 長崎大学ドメイン名の使用
2. 複合機、特定用途機器(ネットワークに接続される測定機器など)、DNS の設置・運用開始・運用終了時の対策
3. ソーシャルメディアサービスによる情報発信時の対策
4. USB メモリ等の外部電磁的記録媒体取り扱いと対策
5. 約款による外部サービス(クラウドサービス等)の利用に関する対策
6. 標的型攻撃への対策

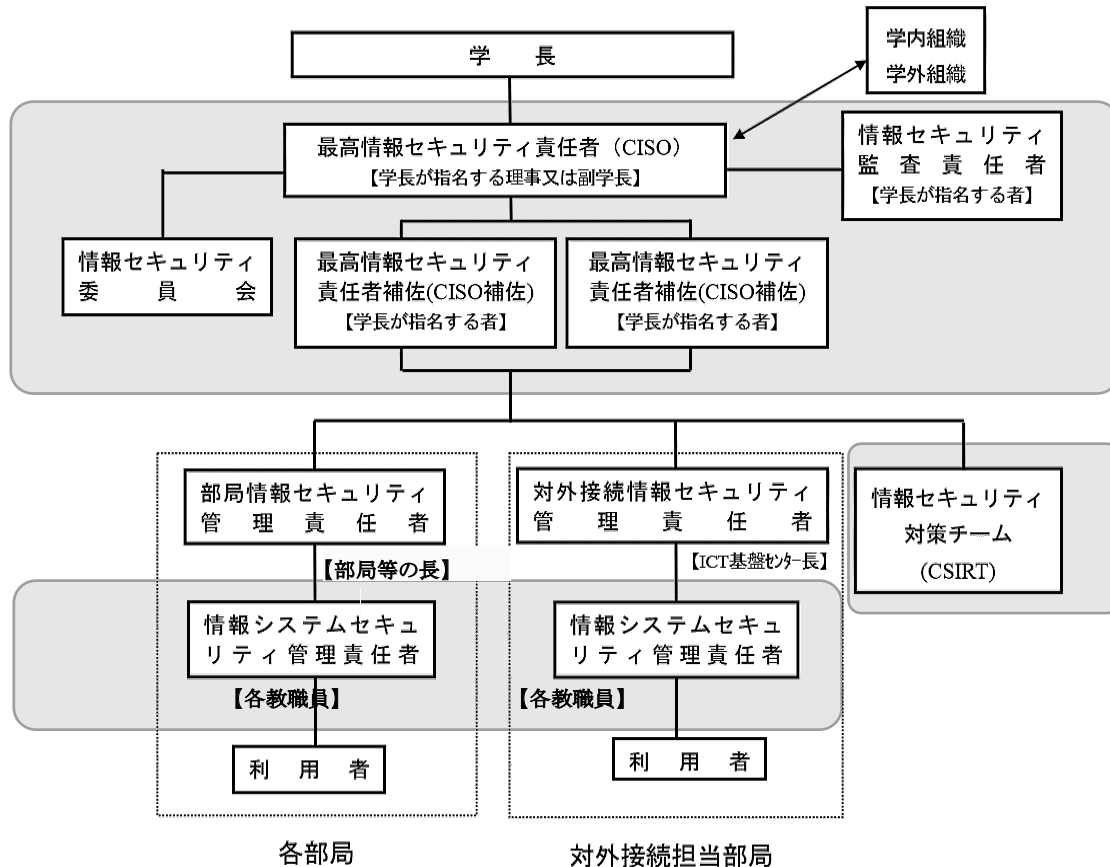


図1 長崎大学における情報セキュリティ体制図

## 4. 情報セキュリティに関する啓発活動

### 4.1 情報セキュリティ説明会

教職員が係わる個人情報の漏洩事故が複数年にわたって発生したことから、「国立大学法人評価委員会の評価結果(平成25年度に係る業務の実績に関する評価結果)」において、個人情報の適切な管理に「課題」があるという厳しい評価がなされました。そのことを踏まえ、ID・パスワードの管理及び職務上利用するUSBメモリ等の取り扱いについて教職員の皆さんに説明し、協力をお願いするため、各部署等を訪問し説明会を行いました。日程及び参加者数は以下の通りです。

表1 情報セキュリティ説明会の開催状況

No	部局名	開催日	開催場所	参加者
1	産学官連携戦略本部	3/12(木) 15:00～15:30	産学官連携戦略本部 2F 研修室	15
2	多文化社会学部	2/19(木) 14:30～15:00	事務局第1会議室	31
3	教育学部	3/4(水) 14:00～14:30	SCS 教室	42
4	経済学部	2/12(木) 15:00～15:30	大会議室	47
5	医学部医学科・原研	3/25(水) 15:30～16:00	医学部ポンペ会館 2F 第二会議室	28
6	医学部保健学科	3/19(木) 15:40～16:10	保健学科大学院生室 2	33
7	歯学部	3/4(水) 16:30～17:00	歯学部教授会室(C棟 8 階)	23

8	薬学部	2/18(水) 15:00～15:30	柏葉会館 2 階会議室	33
9	工学研究科	1/21(水) 14:30～15:00	工学部 1 号館 2 階大会議室	47
10	水産・環境科学総合研究科	2/18(水) 14:30～15:00	環境科学部 1 階大会議室	59
11	熱帯医学研究所	2/25(水) 11:00～11:30	グローバルヘルス総合研究棟 1F セミナー室	70
12	病院	3/11(水) 14:30～15:00	医学部ポンペ会館 2F 第二会議室	25
13	病院	3/31(火) 17:30～18:00	病院 第三講義室	256
14	保健・医療推進センター	2/17(火) 11:30～12:00	セミナー室又は打ち合わせ室	12
15	大学教育イノベーションセンター	1/23(金) 9:30～10:00	第 5 会議室(教育学部 2 階)	14
16	言語教育研究センター	3/17(火) 16:45～17:15	第 5 会議室(教育学部 2 階)	5
合計				740

## 4.2 情報セキュリティ講習会

学生及び教職員を対象として、年 1 回の講習会を企画し実施してきました。各年度の概要を説明します。

### 4.2.1 平成 26 年度

平成 26 年度は、講師として(一社)JPCERT/CC の村上 晃氏をお招きし、インターネットを取り巻く環境の変化の中で、Web サイト改ざん、フィッシングサイトの乱立、金融系マルウェアなど新たな脅威の動向や事例をご紹介いただくとともに、個人レベルでも被害に合わないためのポイントや注意点を分かり易く解説いただきました。

日時	平成 26 年 9 月 19 日(金) 15:30～17:00
演題	被害にあわないためのポイント
講師	村上晃氏((一社)JPCERT/CC 経営企画室 兼 エンタープライズサポートグループ 部門長 兼 早期警戒グループ 担当部門長 兼 マネージャー
会場	C45 教室(文教キャンパス)
参加者数	60 名

### 4.2.2 平成 27 年度

平成 27 年度は、講師として(独)情報処理推進機構(IPA)から平原 隆氏をお迎えして、下記要領で講演していただきました。日本年金機構の情報漏えい事故で話題となった標的型攻撃やスマートフォンからの情報漏えいなど、様々なセキュリティ上の脅威とその対策について、IPA 制作の動画も交えながら、分かりやすく解説していただきました。

なお、平原氏には平成 28 年 1 月に長崎大学情報セキュリティ監査責任者(情報セキュリティポリシー参照)に就任していただき、本学の情報セキュリティ政策について助言をいただいています。

日時	平成 27 年 11 月 26 日(木) 15:00～16:30
演題	情報漏えい対策とスマートフォンのセキュリティ ～昨今の脅威と対策について～
講師	平原 隆 氏 (独)情報処理推進機構(IPA)専門委員、NPO 法人「サイバーネットワーク研究センター」副理事長、(株)シーアイエー代表取締役社長
会場	グローバル教育・学生支援棟 3 階 G-38 教室(文教キャンパス)(文教キャンパス)
参加者数	51 名

#### 4.2.3 平成 28 年度

平成 28 年度も平原 隆氏に講師としてご登壇いただき、下記要領で実施しました。標的型攻撃を中心とした攻撃とその対策、インシデント発生時の対応などについて、具体的な事例を織り交ぜながら講演いただきました。

日時	平成 28 年 12 月 14 日(水) 14:30～16:00
演題	標的型攻撃など最新セキュリティ事情～あなたのパソコンはこうやって乗っ取られる～
講師	平原 隆 氏 (株)シーアイエー代表取締役社長、(独)情報処理推進機構(IPA)専門委員、NPO 法人「サイバーネットワーク研究センター」副理事長、長崎大学情報セキュリティ監査責任者
会場	グローバル教育・学生支援棟 3 階 G-38 教室(文教キャンパス)(文教キャンパス)
参加者数	88 名

#### 4.3 情報セキュリティ基礎講習会

上記の情報セキュリティ講習会において、時間の都合がつかなかったり、キャンパスの移動が大変だったり、「参加したいが困難」という方や「最初の(最低限の)対策を知りたい」という方に向けて、下記の要領で情報セキュリティ基礎講習会を開催しました。この講習会は 2 月下旬～3 月上旬の 3 週間にわたって、文教、片淵、坂本の各キャンパスにて開催しました。

日時	平成 29 年 2 月 14 日(火)～3 月 2 日(木) 16:00～17:00
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 准教授)
会場	附属図書館 中央館 地下多目的ルーム(火曜日 2 月 14 日・21 日・28 日) 附属図書館 経済学部分館 グループ学習室(水曜日 2 月 15 日・22 日・3 月 1 日) 附属図書館 医学分館 セミナー室(木曜日 2 月 16 日・23 日・3 月 2 日)
参加者数	合計 49 名

#### 4.4 情報セキュリティパンフレット作成・配布

##### 4.4.1 学生向け情報セキュリティパンフレット

昨今、スマートフォンの利用が一般的となったことや、必携パソコンの制度の開始(平成 26 年度入学生より)に伴い、学生への情報セキュリティの啓発を強化するため、下記 7 項目の基本的対策を説明した、全 8 ページのパンフレットを作成しました。これを 10,000 部印刷し、各学部・研究科を通じて学生に配付しました。また、平成 27 年度以降、新入生には、情報基礎特別授業の際に配布するようにしています。

1. セキュリティホールをふさごう
2. セキュリティ対策ソフトは最新に
3. フィッシング詐欺への対策
4. ワンクリック詐欺への対策
5. 生活上の盲点に気をつけよう
6. 無線 LAN、正しく設定しよう
7. SNS、気をつけて使おう

#### 4.4.2 教職員向け情報セキュリティパンフレット作成

私たちの業務全般が ICT に大きく依存する中で、私たち一人一人が着実に基本的な情報セキュリティ対策を行う必要があることから、下記の内容からなる、教職員向けパンフレット(全 16 ページ)を作成しました。同パンフレットを 5,000 部印刷し、平成 28 年 3 月に教職員の皆様に配付しました。

1. はじめに
2. セキュリティ対策を日常生活から考える
3. 脅威！リスクは知らない間に忍び寄る
4. どこでも使える 8 つの基本的対策
  - ① OS やアプリを最新の状態にしましょう
  - ② セキュリティ対策ソフトを確実に使いましょう
  - ③ パスワードを適切に管理しましょう
  - ④ 情報の持ち運びに気をつけましょう
  - ⑤ メールリンクや添付ファイルに気をつけましょう
  - ⑥ クラウドのストレージサービス利用には気をつけましょう
  - ⑦ SNS は気をつけて使いましょう
  - ⑧ 情報を捨てるときには一工夫しましょう
5. 簡単！セキュリティのセルフチェック
6. 長崎大学情報セキュリティポリシーによって目指すもの
7. 長崎大学の ICT 環境、詳しくは Web で！
8. 問合せ・連絡先

### 5. 情報セキュリティマネジメントシステム(ISMS)の取り組み

平成 25 年度に当センター(当時は情報メディア基盤センター)及び情報企画課が情報セキュリティマネジメントシステム(ISMS)について、国際標準規格 ISO/IEC 27001 に基づく第三者機関からの認証を取得しました。以下では、それ以降の主な取り組みをご報告いたします。

#### 5.1 ISMS 新規格移行に伴うサーベイランス審査及び移行審査(平成 26 年度)

国際標準規格 ISO/IEC27001 が平成 25 年 10 月に改訂されたことに伴い、認証を継続する場合には、平成 27 年 9 月までに新規格(ISO/IEC27001:2013)に移行して第三者機関による審査に合格する必要性が生じました(平成 25 年度の取得においては、旧規格(平成 17 年に標準化)で受審したため)。

ISMS の新規格は、情報セキュリティ以外のマネジメントシステム関連の規格(ISO 9001 や ISO14001 など)との共通部分(PDCA サイクルなど)の整合性を取りながら、現状に即した内容に改めるものとなっています。新規格の文書構成を図 2 に示します(旧規格の構成については、「センターレポート 2013」を参照)。

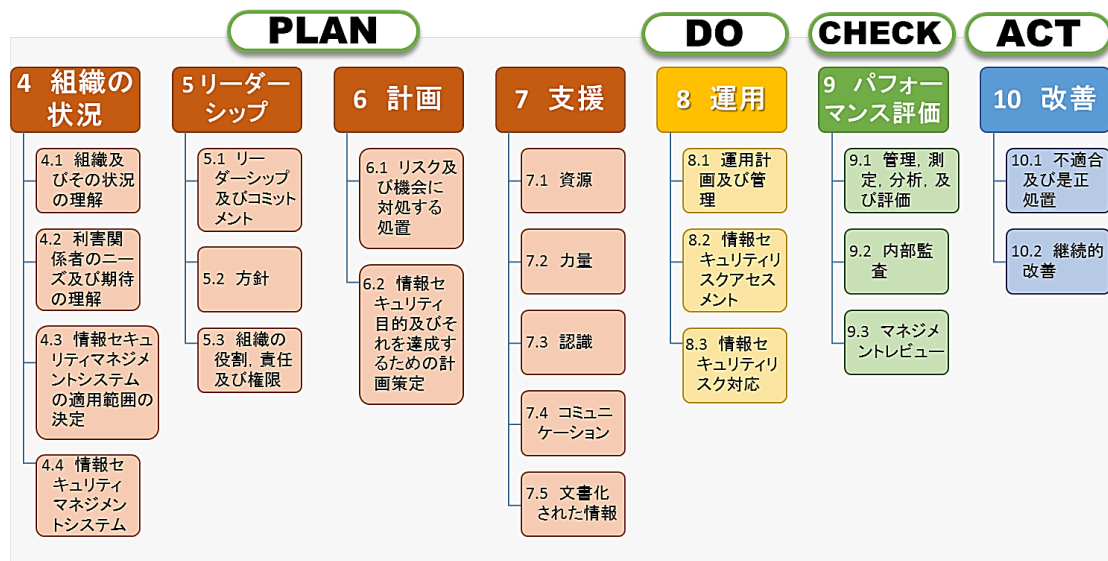


図 2 ISO/IEC27001:2013 (JIS Q 27001:2014) の文書構成

平成 26 年度は、新規格の改訂内容の詳細について分析しました。新規格で新たに対応が必要な項目がある一方、旧規格と同様のものも多くみられたことから、ISMS のマニュアル群の変更を最小限にとどめて、PDCA サイクル全体について見直しを行いました。平成 27 年 2 月 20 日にサーベイランス審査(認証期間中の継続審査、審査は BSI グループジャパン社が担当)を受審し、新規格への適合性についても合格いたしました。平成 27 年 3 月 10 日に認証書(図 3 参照)が発行されました。



図 3 ISMS 認証書(平成 27 年 3 月 10 日発行分)

## 5.2 ISMS 更新審査及び拡大審査受審(平成 27 年度)

平成27年度、私たちのISMSの活動に新たにIR室が加わることになりました。そのため、改めてPDCA

サイクルの見直しを行い、それらをISMSのマニュアル群に反映させ、IR室の情報資産の確認やリスクアセスメントの追加を行いました。

これらのISMSの活動について、平成28年1月20日(水)～1月22日(金)に再認証審査が行われました。今回はIR室へのISMSの認証範囲拡大のために、拡大審査も併せて実施されました。審査の結果、再認証審査及び拡大審査に合格し、平成28年3月4日に審査機関より認証書(図4参照)が交付されました。数点の観察事項(改善することが望ましい事案)が、ISMS担当者の力量の測り方や内部監査に関して数件見られたので、その後に改善策を検討し、マニュアルなどを更新しました。

**bsi.**  
Certificate of Registration

情報セキュリティマネジメントシステム - ISO/IEC 27001:2013 / JIS Q 27001:2014

This is to certify that: 国立大学法人長崎大学 NAGASAKI UNIVERSITY  
〒852-8581 1-14 Bunkyo-machi,  
長崎県 Nagasaki-shi,  
長崎市 Nagasaki  
文政町1-14 852-8521  
Japan

認証登録番号: JS 590859

所在地 認証登録範囲  
国立大学法人長崎大学 情報企画課、ICT基盤センター及びIR室が提供する大学総合  
〒852-8581 情報サービス  
2014年1月1日付付与認証登録番号 第448号  
The general information service provided for Nagasaki  
University by the following departments:  
- Information Planning Division  
- Center for Information and Communication Technology  
- Institutional Research Office  
Statement of Applicability, Issue on 27/May/2015, Version 4

情報企画課、ICT基盤センター及びIR室が提供する大学総合サービス  
2014年1月1日付付与認証登録番号 第448号  
The general information service provided for Nagasaki University by the following  
departments:  
- Information Planning Division  
- Center for Information and Communication Technology  
- Institutional Research Office  
Statement of Applicability, Issue on 27/May/2015, Version 4

For and on behalf of BSI: 代表取締役社長 竹尾 直幸

初版認証登録日: 2013/03/04 有効期限: 2016/03/04  
最新更新日: 2016/02/11 有効期限: 2019/03/03

Page: 1 of 2

...making excellence a habit.

Page: 2 of 2

図4 ISMS 認証書(平成28年3月4日発行分)

### 5.3 サーベイランス審査(平成28年度)

平成28年度は前年の更新審査及び拡大審査で指摘された観察事項について、上記の改善策を具体的かつ適切に実践しました。その結果、平成29年2月20日に受審したサーベイランス審査にも無事合格しました。

ISMSの活動も4年にわたって推進してきましたが、今後のCSIRTの設置などとも関連して、そのノウハウはICT基盤センター、情報企画課、IR室の範囲にとどまらず、大学全体に還元しうものになってきました。平成29年度以降、大学への還元を推進したいと考えています。

## 6. 情報セキュリティ自己点検システム構築

教職員の情報セキュリティ対策の状況について各自で棚卸しして、情報セキュリティに関する意識を高めることにより、本学の情報セキュリティの更に強化することを目的として、情報セキュリティ自己点検システムを構築しました。本システムはWebブラウザからアクセスして、「必須の点検項目」及び下記5分野の「任意の点検項目」について、自身のセキュリティの対応状況に照らして回答するものです。設問数は各10問となっております。



1. ID とパスワードの管理
2. 情報の取り扱い
3. パソコン等の機器の管理
4. 基本的なセキュリティ対策
5. その他一般

本システムにて回答すると、自分の対応状況がどの程度望ましいかをパーセントで表示するとともに、必要に応じて改善のためのヒントが表示されるようになっています。これによって、適切な対策が取られていたことが確認できたり、取り組みが不十分な事柄について改善に向けたヒントを得たりすることができま

す。

平成 28 年 1 月 6 日より運用を開始し、平成 28 年 3 月までに 2,109 人の方々に回答いただきました。自己点検の結果の分布を集計したところ、図 5 のようになりました。大学全体のセキュリティレベル向上のため、更なる啓発に努めたいと思います。

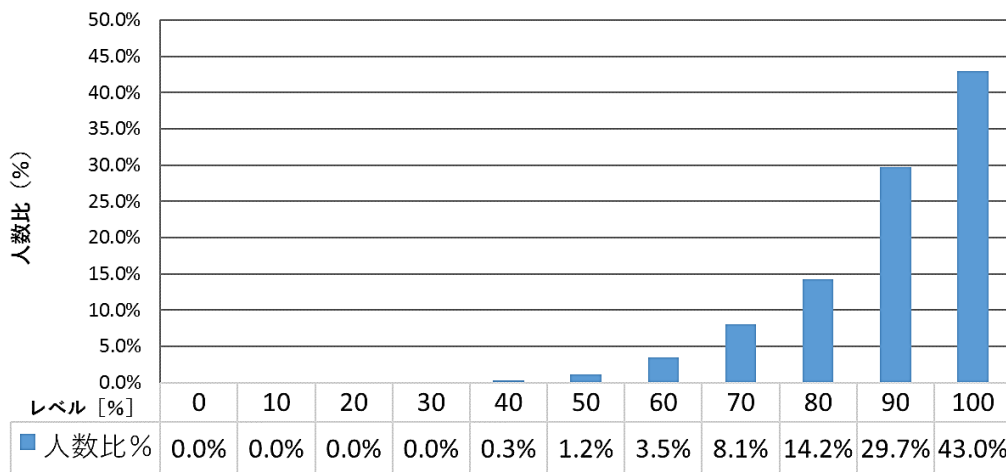


図 5 情報セキュリティ自己点検結果(平成 28 年 1 月～3 月実施分)

自由記述にて回答内容においては、以下のような傾向が見られました。

- ・ 情報セキュリティの維持や情報管理の重要性を再認識したというコメントが見られました。
- ・ セキュリティ対策ソフトの定義ファイル更新を意識していなかったとのコメントが見られました。
- ・ パスワードの使い回しへの対策が難しいとのコメントがありましたが、管理対象のパスワードが多いためと考えられます。
- ・ 学会から USB メモリを持参するよう要求されるなど、USB メモリの取り扱いで苦心しているとのコメントが見られました。

本システムには、教職員ポータルに掲載されたリンクをたどるか、下記 URL を直接入力いただくことによりアクセスできます。平成 28 年度以降も継続して実施していますので、教職員の皆様の積極的なご利用をお願いいたします。

<https://scheck.nagasaki-u.ac.jp/>

## 7. 長崎県サイバーセキュリティに関する相互協力協定

様々なサイバー攻撃が、大学だけでなく社会全体で取り組むべき問題として認識されるようになりました。その中で、セキュリティに関する情報をいかに収集・共有し、より効果的なセキュリティ対策を講じてい

くかが社会の課題となってきました。国ではサイバーセキュリティ基本法が平成 28 年 11 月に制定され、国や地方自治体、大学等の役割などが規定されました。平成 32 年の東京オリンピックに向けて、サイバーセキュリティ人材が約 20 万人不足するとの試算もあり、サイバーセキュリティ人材の確保が様々な業界において喫緊の課題と言えるようになりました。(独)情報処理推進機構において「情報処理安全確保支援士」(通称、登録セキスペ)の資格が設けられ、サイバーセキュリティ人材の国家資格を付与するようになりました。産業界で「産業横断人材定義リファレンス(機能と業務にも届くセキュリティ人材定義)」(産業横断サイバーセキュリティ人材育成検討会、平成 28 年 9 月 14 日公開)が策定されるなど、必要とされる人材像を明確化する動きもあります。

これに呼応した動きとして、地域でのサイバーセキュリティ確保のため、産学官が協業するための協定を締結するケースが出てきました。長崎県において、平成 29 年 1 月 24 日に産学官 14 機関が調印して「長崎県サイバーセキュリティに関する相互協力協定」が締結されました。産学官の協定としては全国で 4 例目であり、協定の参加機関数としては最大規模です。この協定は、協定機関の相互理解による高い信頼と協力関係に基づき、安全安心なサイバー空間の実現を目指すことを目的としています。参加機関は長崎県、長崎県警、長崎県商工会議所連合会、長崎県商工会連合会、長崎県中小企業団体中央会、(公財)長崎県産業振興財団、(一社)長崎県情報産業協会、西日本電話(株)長崎支店、(株)ラック、トレンドマイクロ(株)、長崎大学、長崎県立大学、長崎総合科学大学、佐世保工業高等専門学校です。協力内容としては、以下の 5 項目が取り決められています。

- (1) サイバー空間に脅威に関する情報の共有
- (2) サーバー空間の脅威への対処に係る技術的支援
- (3) サイバー空間の脅威に対処できる人材の育成
- (4) サイバー空間の脅威に立ち向かう社会全体の意識の向上
- (5) その他協定機関が必要と認めるサイバーセキュリティに関する事項

今後、ICT 基盤センターでもこの協定に貢献すべく、活動を展開する予定です。

## 8. まとめ

本稿では、平成 26 年度～平成 28 年度の情報セキュリティに関する活動を振り返りました。情報セキュリティポリシーの改訂、啓発活動(情報セキュリティ説明会、情報セキュリティ講習会、情報セキュリティ基礎講習会、学生向け・教職員向け情報セキュリティパンフレット作成)、情報セキュリティマネジメントシステム(ISMS)に関する取り組み実施状況(各年度での第三者機関の審査を中心に)、情報セキュリティ自己点検に関するシステム構築・実施状況、長崎県サイバーセキュリティに関する相互協力協定をご紹介します。

情報セキュリティの活動は一過性ではなく、継続していくことが大変重要です。特にバイオ・セーフティ・レベル 4(BSL-4)施設の稼働に向けた取り組みが国の支援の下で進められていることもあり、長崎大学においても今まで以上のセキュリティレベルが要求されるようになるものと思われます。その中で、学生や教職員の皆様のお力が必要不可欠です。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。