原著論文

学術情報処理研究 No.21
2017年9月

全学構成員向け情報セキュリティ・コンプライアンス教育コンテンツの再開発

Redevelopment of Contents in Information Security & Compliance Education for Hiroshima University Members

渡邉英伸†，岩沢和男†，西村浩二†
Hidenobu Watanabe†, Kazuo Iwasawa†, Kouji Nishimura†

h-watanabe@hiroshima-u.ac.jp, iwasawa@hiroshima-u.ac.jp, kouji@hiroshima-u.ac.jp

†広島大学情報メディア教育研究センター

† Information Media Center, Hiroshima University

概要

広島大学では，アカウント利用・更新制度と連携することで全学構成員が情報セキュリティ・コンプライアンス教育の受講を必須とする環境を構築し運用してきた．一方で，いろいろと混乱が生じ，2017 年度の実施に向けて教育コンテンツの再整理ならびに再開発が求められた．本論文では，再整理に至った課題と原因を紹介するとともに再開発した教育コンテンツの内容について報告する．

キーワード

教育，情報セキュリティ，コンプライアンス

1. はじめに

近年，情報セキュリティ教育を取り巻く環境は，目まぐるしく変化している．2014 年には，サイバーセキュリティ基本法が設立され，教育研究機関は，国や民間企業と連携協力を図りながら,「広くサイバーセキュリティに関する関心と理解を深めるためのサイバーセキュリティに関する教育及び学習の振興，啓発及び知識の普及その他の必要な施策を講ずること（第二十二条）」が求められるまでに至っている．

広島大学では，サイバーセキュリティ基本法が設立される前から情報セキュリティおよびコンプライアンスに関する教育を実施している．開始当初は在籍二年以上の学生および教職員を対象に実施し，その後 2008 年度に導入したアカウント年度更新制度[1]に対して情報セキュリティ・コンプライアンス教育の受講を義務化することで，受講率の向上に努めてきた．新入生に対しては，2011 年度から情報セキュリティ・コンプライアンス教育を開始し，2012 年度には対象を新採用教職員まで拡大した[2]．さらに，在籍一年目の構成員を対象としたアカウント利用確認制度を 2016 年度に新設し，情報セキュリティ・コンプライアンス教育の受講をアカウント利用の前提条件とする環境を構築した．そして，昨年度アカウント利用・更新制度と連携した情報セキュリティ・コンプライアンス教育を一年間運用し，90%以上の受講率を達成した．

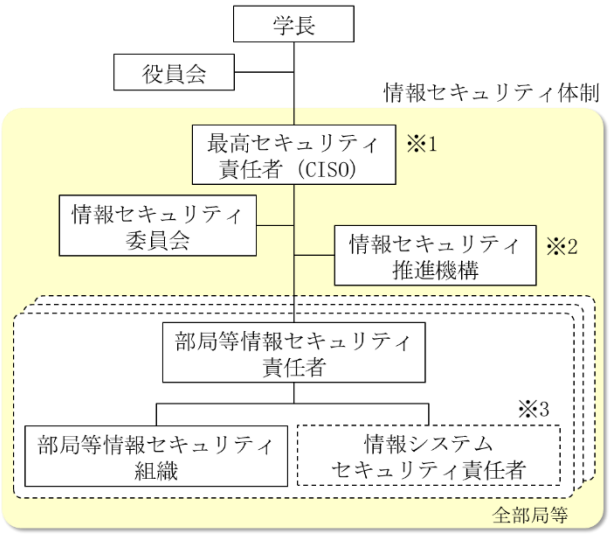
このように，広島大学ではアカウント利用・更新制度と連携した情報セキュリティ・コンプライアンス教育により，全構成員が年に一回は必ず情報セキュリティおよびコンプライアンスについて学習できる環境となっている．一方で，情報セキュリティ・コンプライアンス教育の内容について，「難しい」や「意味が分からない」などの意見は少なくない．2016 年度では利用確認に関する意見やコメントが多く寄せられた．また，留学生や高齢者の構成員が直接情報メディアセンターに助けを求めるケースもあり，2017 年度の実施に向けて教育コンテンツの再整理が求められた．

本論文では，2016 年度の教育コンテンツの内容を統合的な視点で見直し・改善を行った点について報告する．

以下，論文構成について述べる．2 章では，2016 年度の情報セキュリティ・コンプライアンス教育の教育コンテンツとその課題および原因について述べる．3 章では 2017 年度の教育コンテンツの設計内容を説明し，4 章で再開発した 2017 年度の教育コンテンツを紹介する．5 章で考察に触れ，最後に，6 章で本稿のまとめを述べる．

2. 2016 年度情報セキュリティ・コンプライアンス教育

広島大学では，情報セキュリティに関連する組織として最高セキュリティ責任者（CISO）の下で統括された情報セキュリティ委員会と情報セキュリティ推進機構が設置されている．情報セキュリティ委員会は大学の基本的な情報セキュリティポリシーの策定及び情報セキュリティに関する重要事項を検討する組織である．情報セキュリティ推進機構は企画立案，啓発や教育などの業務を遂行する組織である．情報メディア教育研究センターは，情報セキュリティ推進機構の一組織としても活動しており，全学の取り組みである情報セキュリティ・コンプライアンス教育の業務を委託されている．そして，教育コンテンツの方針策定，設計，作成，見直し，改善ならびに講習の実施等を遂行している．加えて，年 3 回開催される情報セキュリティ委員会において，実施計画，教材内容，受講状況の報告を行っている．図 1 に広島大学情報セキュリティ体制を示す．



※1　理事・副学長（社会産学連携担当）
※2　副理事（情報担当），情報メディア教育研究センター及び情報化推進グループで組織
※3　情報システムに対し，必要に応じて設置可能

図 1　広島大学情報セキュリティ体制

2.1. 教育コンテンツ

情報セキュリティ・コンプライアンス教育は，一年目の構成員が対象となる講習と二年目以降の構成員が対象となる講習から構成される．図 2 に情報セキュリティ・コンプライアンス教育コンテンツの構造を示す．なお，2016 年度の情報セキュリティ・コンプライアンス教育コンテンツの構造は図 2 の左図である．

2.1.1. 一年目の構成員が対象となる講習

一年目の構成員向けの教育コンテンツは，フレッシュマン講習，情報セキュリティ講座，修了試験から構成される．2011 年度から実施しているフレッシュマン講習は 60 分の座学形式の講習である．広島大学で実際に起こった事例などを通じて国の法令や大学の規則など個人が守らなければならないことを学び，実際の学生生活の中でその知識を活用できることを目的としている[3][4]．図 3 に 2016 年度フレッシュマン講習教材の目次を示す．フレッシュマン講習の教材は日本語，英語，中国語が用意され，紙媒体とデジタルデータが提供されている．2016 年度では，3 名の教員が担当し，講習会 31 回（東広島 20 回（うち英語 3 回，中国語 2 回），霞地区 6 回（うち英語 1 回（東広島からテレビ会議中継）），東千田地区 5 回）を実施した．なお，フレッシュマン講習の教育コンテンツ方針策定，設計，作成，見直し，改善ならびに講習の実施等の業務は，情報メディア教育研究センター内の我々が所属する情報セキュリティ研究部門が担当である．

情報セキュリティ講座は，オンライン学習支援システム Bb9 上で開講されている一年目の構成員向けのオンライン講習である．図 4 にオンライン情報セキュリティ講座の目次を示す．オンライン情報セキュリティ講座は，情報メディア教育研究センターの情報教育研究部門が担当する情報科目（情報活用基礎）で使用されているオンライン教材から，本教育に関連する部分を抽出したもの（ダイジェスト版）で 8 章 32 節のテーマから成る．ストーリー形式の解説付きで，各節ごとに確認テスト（三～六者択一問題が 3 問程度）が備わっている．また，修了

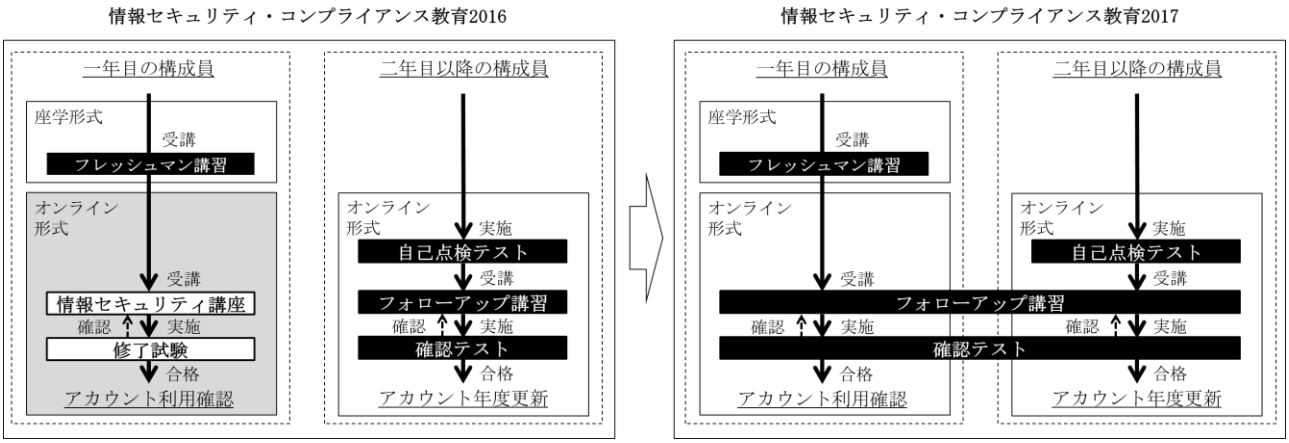


図 2　情報セキュリティ・コンプライアンス教育コンテンツの構造

試験は，オンライン情報セキュリティ講座の理解を確認するためのオンラインテストである．三・四者択一/多肢選択/記入問題が 22 問あり，110 満点中 90 点以上で合格となる．修了試験は合格するまで何回でも受験可能である．情報セキュリティ講座および修了試験は日本語・英語が用意されている．なお，情報セキュリティ講座は，2016 年度に在籍一年目の構成員を対象としたアカウント利用確認制度の新設にあわせて開設した講座であり，教育コンテンツ作成や見直し・改善については，そのまま情報教育研究部門が実施している．

2016 年度では，5,582 名が講習の対象であり，受講率は，92.9%であった（2017 年 3 月時点の集計）．このように，一年目の構成員は，座学形式のフレッシュマン講習とオンライン形式の情報セキュリティ講座を受講した後，入学日・着任日から 90 日以内に修了試験に合格することでアカウントの利用（アカウント利用確認ボタンの押下）が可能となる．

2.1.2. 二年目以降の構成員が対象となる講習

二年目以降の構成員向けの教育コンテンツは，すべてオンライン形式であり，自己点検テスト，フォローアップ講習, 確認テストから構成される. 自己点検テストは，二年目以降の構成員に対して広大の情報セキュリティポリシーに沿った対策・行動の実施状況を把握する目的で実施するものである．自己点検テストは，18 問のテストとしているが，問題の内容は年間を通じて広大の情報セキュリティポリシー実施手順に基づく対策・行動の状況を確認するものしかなく，解答の選択肢は，「はい」,「どちらかと言えば　はい」,「どちらかと言えば　いいえ」,「いいえ」である．このように，自己点検テストは自己の情報セキュリティ対策・行動の実態を報告するものであり，今回は，再整理すべき教育コンテンツの対象から外すこととしている．

情報セキュリティ・コンプライアンス教育の開始当初から実施しているフォローアップ講習は情報セキュリティに関する知識の再確認と最新の情報セキュリティに関する知識の補充を目的としたオンライン講習である．内容は，日常的にたいせつなこと，最近の情報セキュリティの脅威の 2 章構成になっている．フォローアップ講習では日本語・英語が用意されている．図 5 に 2016 年度の

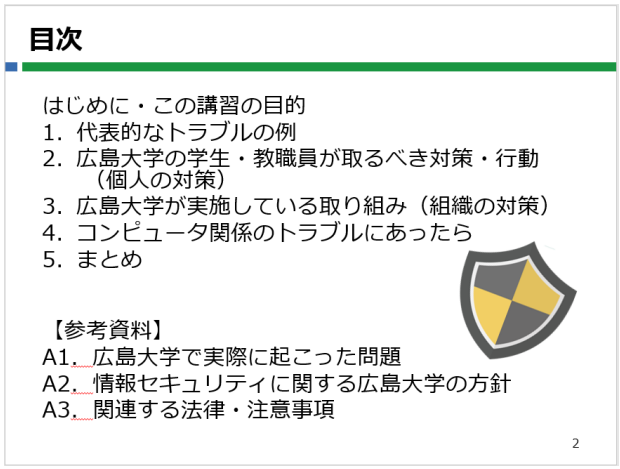


図 3　2016 年度フレッシュマン講習教材の目次

図 4　オンライン情報セキュリティ講座の目次

フォローアップ講習教材の目次を示す．また，確認テストは，フォローアップ講習の理解を確認するためのオンラインテストである．二者択一問題が 30 問あり，30 満点中 27 点以上で合格となる．確認テストも合格するまで何回でも受験可能である．2016 年度では，16,829 名が講習の対象であり，受講率は，93.9%であった（2017 年 3 月時点の集計）．

このように，二年目以降の構成員は，年度更新期間（2017 年度の場合は，4/2～4/30）及び年度更新猶予期間（5/1～6/30）内に自己点検テストの結果を提出し，フォローアップ講習を受講した後，確認テストに合格することでアカウントの利用更新（アカウント年度更新ボタンの押下）が可能となる．なお，フォローアップ講習の業務の遂行は，情報セキュリティ研究部門が担当である．

2.2. 課題と原因

2016 年 4 月 1 日～7 月 15 日に情報メディア教育研究センターが対応した情報セキュリティ・コンプライアンス教育に関する意見は前年よりも増えて 100 件近くの件数に上がった．その意見の多くが，「情報セキュリティ講座・修了試験の内容が難しい」，「修了試験の問題数が多い」，「留学生にとってテストに合格することが難しい」「言葉の意味が分からない」，「確認テストの問題数が多い」であった．そこで，教育コンテンツを再整理した結果，以下の原因が顕在化した．

- 一年目の構成員と二年目以降の構成員が学ぶべき内容や実施時期が異なることから，二つの講習が独立していたこと．
- 歴史的背景からフォローアップ講習・確認テスト，フレッシュマン講習，情報セキュリティ講座・修了試験という順に教育コンテンツが独立に作成されていたこと．
- 効率的な観点だけで数ヶ月かけて学習する情報科目のオンライン教材を情報セキュリティ講座・修了試験に流用したこと．
- 教材や問題の作成・更新に関する共通の方針を定めなかったこと．
- 教材・問題の見直しにおいても，担当部門に任せっきりにしてしまい，統合的かつ十分な見直しが無く，適切なフィードバックができていなかったこと．
- 日本人と留学生では前提知識が異なることが想定されておらず，留学生等に対して未知の問題となっていたこと．

これらの原因によって，フレッシュマン講習，情報セキュリティ講座・修了試験，フォローアップ講習・確認テストの 3 つの教育コンテンツが分断された状態となり，内容・レベル・問題数・解答形式等がバラバラになったと考えられる．そこで，2017 年度の情報セキュリティ・コンプライアンス教育コンテンツの再開発に向けては，情報セキュリティ研究部門が教育コンテンツ方針策定，設計，作成，見直し，改善ならびに講習の実施のすべてを担当するものとし，1）教育コンテンツの統合化，2）教育コンテンツ作成基本方針の明確化の 2 つの要件が重要と考えた．

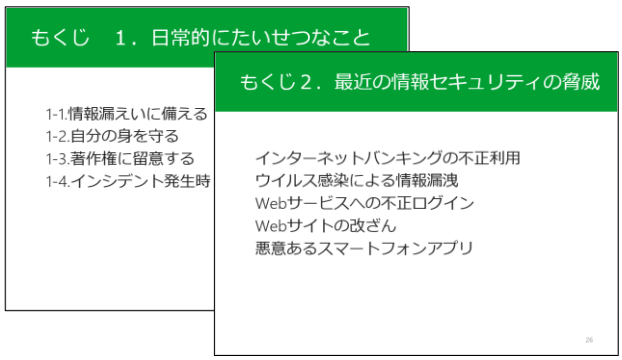


図 5　2016 年度フォローアップ講習教材の目次

3. 2017 年度情報セキュリティ・コンプライアンス教育コンテンツの設計

3.1. 教育コンテンツの統合化

2017 年度の情報セキュリティ・コンプライアンス教育コンテンツの構造を図 2 の右図に示す．2017 年度の実施に向けて，まず情報セキュリティ講座・修了試験を廃止する．そして，フレッシュマン講習の後にフォローアップ講習・確認テストを受講する構造とする．これにより，一年目の構成員は，座学形式のフレッシュマン講習で学んだことをフォローアップ講習で復習し，確認テストを実施するというプロセスを踏むことになる．つまり，フォローアップ講習の内容をフレッシュマン講習で手厚く教育する構造となるため，二年目以降の構成員との知識量の差を埋めることが可能になる．二年目以降の構成員に対しては，従来通りフォローアップ講習と確認テストのみとすることで，最近の脅威と最低限知っておくべき情報を重点的に復習できることになる．このように教育コンテンツの統合化により，段階的な学習体系の構造を確立する．

3.2. 教育コンテンツ作成基本方針の明確化

教育コンテンツの統合化にともない，フレッシュマン講習とフォローアップ講習の教材を整理した．そして，2017 年度の情報セキュリティ・コンプライアンス教育の教材は，3 つの大項目と 7 つの小項目に分類することと

表 1　2017 年度情報セキュリティ・コンプライアンス教育の対応関係

種類	対象	主な内容
フレッシュマン講習	一年目構成員	脅威事例（最近・学内）＋共通一般内容＋固有内容
フォローアップ講習	全構成員	脅威事例（最近）＋共通一般内容

した．これは，フレッシュマン講習の教材に対する意見が少ないことを考慮し，その教材の構造をベースとしたものである．大項目は，情報セキュリティにおける①脅威の事例，②共通一般内容，③学内固有内容となる．脅威の事例は，社会で起こっている脅威と学内で起こった脅威の 2 種類とする．共通一般内容は，個人が実施すべき対策と行動に関する内容とし，学内固有内容は，大学が実施している取組，インシデント時の対処，法律・注意事項などの補足情報とする．

次に，教材作成において 3 つの基本方針を定めた．一つ目は，実際に起きた脅威の事例を用いることである．特に，社会で起こっている脅威は，年々多種多様になっていることから，事例は最新かつ信頼性のある情報であることが求められる. 今回, 我々は毎年度公開される IPA の「情報セキュリティ 10 大脅威」を参考にするものとした. なお, 参考とする情報セキュリティ 10 大脅威は教材作成時期（年始頃）の時点の最新版とする．二つ目は，共通一般内容として，対策と行動を各 5 つとすることである．脅威が多種多様になれば当然対策・行動も多種多様になるが, それを IT 専門家ではない構成員に短時間ですべて理解させることは非現実的であり，情報セキュリティ・コンプライアンス教育の趣旨とも異なる. そこで, 共通一般内容については，最新かつ信頼性のある情報源から厳選し定義することが求められる．今回は情報セキュリティ 10 大脅威で示されている「情報セキュリティ対策の基本」と付録の「情報セキュリティ船中八策」を参考に, 5 つの対策と 5 つの行動を定義することにした. 三つ目は，学内固有内容として，フレッシュマン講習内容を踏襲することである．これは，過去に用いたフレッシュマン講習の教材内容と大きく乖離することを避けるためである．これらを整理すると，以下のようになる．

【大項目 1】: 情報セキュリティ脅威の事例
　小項目 1 : 社会で起こっている脅威
　　方針 1 :「情報セキュリティ 10 大脅威」を参考
　小項目 2 : 学内で起こった脅威
　　方針 3 : フレッシュマン講習内容を踏襲
【大項目 2】: 情報セキュリティにおける共通一般内容
　小項目 3 : 5 つの対策
　小項目 4 : 5 つの行動
　　方針 2 :「情報セキュリティ対策の基本」と「情報セキュリティ船中八策」を参考
【大項目 3】: 情報セキュリティにおける学内固有内容
　小項目 5 : 大学が実施している取組
　小項目 6 : インシデント時の対処
　小項目 7 : 補足情報
　　方針 3 : フレッシュマン講習内容を踏襲

今回のポイントは，IPA の「情報セキュリティ 10 大脅威」を参考にしていることである．これにより，最新の情報セキュリティ情報の提供に加え，実施すべき対策・行動に対する根拠の確保，教材作成の効率化を可能にしている．

最後に，確認テスト作成においても 2 つの方針を定めた．一つ目は問題の難易度を一般的にするために，出典が可能な問題とすることである．今回，留学生等に対して未知の問題とさせないために，出典先となる教材とページ番号を解説に明示することとした．

二つ目は，問題数を 20 問に修正することである．今回，二者択一問題を 20 問とし，20 満点中 16 点以上で合格とした．出題範囲はフレッシュマン講習，フォローアップ講習で触れている内容のみとした．また，新規に追加した内容に関連する問題については必ず出題するものとし，過去に出題された問題を再度出題しても良いとするが，不正解率が高かった問題を優先して出題するものとした．

4. 2017 年度情報セキュリティ・コンプライアンス教育コンテンツの実装

設計で定めた内容をもとに 2017 年度情報セキュリティ・コンプライアンス教育コンテンツを再開発した．表 1 に 2017 年度情報セキュリティ・コンプライアンス教育の対応関係を示す．本章では，再開発したフォローアップ講習とフレッシュマン講習の教材内容について述べる.

4.1. 2017 年度フォローアップ講習教材

2017 年度の教材では，情報セキュリティ 10 大脅威 2016[5]の 1 位～5 位を参考に，身近な情報セキュリティの脅威としてフィッシング詐欺，ウイルス感染，不正アクセスの 3 つの内容を厳選した．加えて，情報セキュリティ対策の基本と情報セキュリティ船中八策を参考に，本学における 5 つの対策および 5 つの行動を定義した．以下に示す.

対策1. ウイルス対策ソフトを導入し，最新の状態に更新する
対策2. OS・ソフトウェアを最新の状態に更新する
対策3. ID・パスワードを適切に管理する
対策4. 定期的にバックアップをとる
対策5. 最新の脅威・攻撃の手口について知る
行動1. 添付ファイルやURLを安易にクリックしない
行動2. 怪しいアプリをインストールしない
行動3. PCやスマホの紛失・盗難に注意する
行動4. 身に覚えのない利用がないか確認する
行動5. 安全な通信路を使う

また，カード式の情報セキュリティクイックガイドも作成した．図6に情報セキュリティクイックガイドカードを示す．広島大学ではパソコンの必携化を進めていることもあり，インシデント発生時の緊急連絡先も携帯することが重要と考えた．情報セキュリティクイックガイドには，インシデントに該当する事案例と緊急時の連絡先が記載されている．学生証・職員証と同等のサイズであり，一緒に携帯することが可能である．現在，全構成員に配布している．

2017年度フォローアップ講習の教材内容のタイトルを以下に記す．なお，本教材のポイントは，フィッシング詐欺，ウイルス感染，不正アクセスの各々で求められる対策と行動を示すとともに，最終的に個人が実施すべき事として5つの対策と5つの行動にまとめられている点である．

1. 最近の情報セキュリティの脅威
　フィッシング詐欺被害
　　怪しいメールに気づくポイント（1）
　　怪しいメールに気づくポイント（2）
　　巧妙なフィッシングサイトの例
　　フィッシング詐欺の対策・行動
　ウイルス感染被害
　　ランサムウェアの事例
　　ランサムウェアに感染したら
　　ウイルス感染経路
　　ウイルス感染の被害に遭わないための対策・行動
　不正アクセス被害
　　不正アクセス被害に遭いやすいケース
　　不正アクセスの対策・行動
2. 日常的にたいせつなこと
　ウイルス対策
　ソフトウェアの更新
　パスワードは強固に
　定期的バックアップ

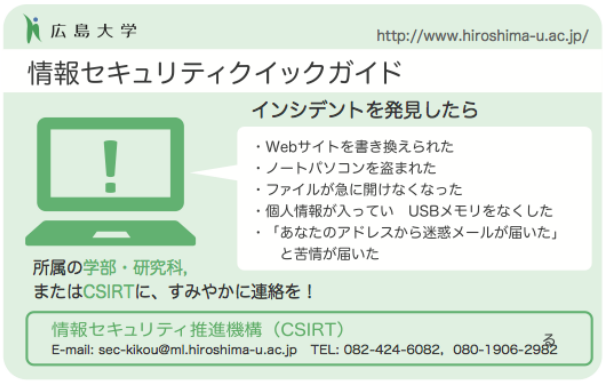


図 6　情報セキュリティクイックガイドカード

　最新の脅威・攻撃の手口を知る
3. さらにすると良い行動
　メールにファイル添付しない
　データのやりとりはクラウドを使う
　より強固な本人認証にする
　身近な人と情報共有する
　こんな症状はインシデントかも
　インシデントは早急に報告する
　その他の注意（1）
　その他の注意（2）
対策と行動
　5つの対策
　5つの行動

4.2. 2017年度フレッシュマン講習教材

2017年度フレッシュマン講習の教材内容のタイトルを以下に記す．下線はフォローアップ講習の教材開発にともない2016年度の教材から新たに追加した内容である．なお，脅威2：ウイルス感染における説明では，「メール経由によるランサムウェア感染の脅威」のサンプルムービー[6]を紹介している．

1. 身近な情報セキュリティの脅威
　脅威 1：フィッシング詐欺
　脅威 2：ウイルス感染
2. 広島大学の学生・教職員が取るべき対策・行動（個人の対策）
　対策 1：ウイルス対策を行う
　対策 1(2)：ウイルスを検知したら
　対策 1(3)：このような症状があったら・・・
　対策 2：ソフトウェアを更新する
　対策 2(2)：ウイルス対策との違いを理解する
　対策 3：ID，パスワードを適切に管理する
　対策 3(2)：推奨パスワードポリシー
　対策 3(3)：パスワードの変更方法

対策 3(4)：サービスごとに異なるパスワード
対策 3(5)：パスワード管理ツールの例
対策 3(6)：本人認証をより強固にする
対策 4：バックアップをとる
対策 5：ファイル共有ソフトを使用しない
行動 1：フィッシングメールに注意
行動 1(2)：怪しいメールの見分け方
行動 2：利用規約の確認
行動 2(2)：利用規約の更新も確認
行動 3：SNS を利用するときの注意
行動 3(2)：SNS を利用するときの注意
行動 3(3)：投稿をしても良い内容ですか？
行動 3(4)：匿名性について
行動 3(5)：SNS の適切な利用のために
行動 4：スマホの取扱いに注意
行動 4(2)：不正アプリに注意
行動 4(3)：アプリの導入時に気を付ける点
行動 4(4)：写真アプリの設定に注意
行動 5：公衆 Wi-Fi を利用するときの注意
行動 5(2)：公衆 Wi-Fi を利用するときの確認事項

3. 広島大学が実施している取り組み（組織の対策）
取組み 1：利用者認証・身分証の提示
取組み 2：パスワード強度メーター
取組み 3：多要素認証
取組み 4：ネットワーク監視
取組み 5：マイクロソフト包括ライセンス

4. コンピュータ関係のトラブルにあったら
学部・研究科の学生支援担当に相談！
情報セキュリティクイックガイド

5. 考察

2017年5月末時点で判明しているアカウント利用確認状況およびアカウント年度更新状況の結果を報告する．一年目の構成員としてアカウント利用確認を実施する必要がある対象は5,027名である．5月末の時点では3,449のアカウントが利用確認済みとなっているおり，既に68.6%が確認テストに合格している．なお，2017年度のフレッシュマン講習は，4月から5月末までに3名の教員が担当し，13回（東広島7回（うち英語1回，中国語1回），霞地区3回（うち英語1回（東広島からテレビ会議中継）），東千田地区3回）実施されている．また，6月末までには，残り6回（東広島5回，霞地区1回）の講習が実施される予定である．二年目の構成員としてアカウント年度更新を実施する必要がある対象は17,393名である．5月末の時点では12,616のアカウントが年度更新済みとなっているおり，既に72.5%が確認テストに合格している．

情報セキュリティ・コンプライアンス教育に対する意見については，2017年5月末時点で0件であった．昨年度なかなか合格できなかった利用者からは，今回は問題無く合格できたという連絡も頂いた．このように，短い期間ではあるものの2017年5月末時点までは，全構成員の7割が特に問題が生じること無く確認テストに合格することができており，今回の再開発によって課題を解決できる見込みを得ることができた．

一方，確認テストの作成方針については，再度見直しが必要と考えられる．今回，確認テストが既に公開され実施されている状況において，複数の解釈が考えられる問題文があることを内部関係者から指摘され，問題文の差し替えを議論することになった．このことから，より具体的な作成方針を定めておく必要があり，今後の課題になると考えられる．

6. おわりに

本論文では，全学構成員向け情報セキュリティ・コンプライアンス教育コンテンツの再開発に向けて，課題と原因を明確にし，設計内容と再開発した教材内容について報告した．教育コンテンツの統合化と教育コンテンツ作成基本方針の明確化によって，段階的な学習体系の構造を確立するとともに，最新かつ信頼性のある情報源からの情報提供，実施すべき対策・行動に対する根拠の確保，教材作成の効率化を可能にしている．IPAの10大脅威を用いることで，毎年度のコンテンツの改定がしやすくなったことは大きなメリットと考える．短い期間ではあるものの情報セキュリティ・コンプライアンス教育に対する意見については，2017年5月末時点で0件であり，今回の再開発によって課題を解決できる見込みを得ることができた．

今後の課題は，確認テストの作成方針の見直しならびに年間を通じて再開発の効果を定量的に評価することである．

参考文献

[1] 岩沢和男，吉冨健一，宮原俊行，“セキュリティ強化のためのアカウントへの制限，”平成20年度情報教育研究集会，基盤システム，p491-494，2008.

[2] 西村浩二，大東俊博，岩沢和男，隅谷孝洋，稲垣知宏，中村純，宮内祐輔，三戸里美，相原玲二，“広島大学における情報セキュリティ・コンプライアンス教育の取組み，” 情報処理学会研究報告

インターネットと運用技術（IOT），Vol.2012-IOT18，No.2，pp.1-6，2012.
[3] 天野由貴，隅谷孝洋，岩沢和男，西村浩二，“情報セキュリティ教育教材の改善検討～自由記述アンケートの分析から～，” 情報教育シンポジウム 2015 論文集，pp.133-140，2015.
[4] 天野由貴，隅谷孝洋，渡邉英伸，岩沢和男，西村浩二，“H28 年度学部新入生を対象とした情報セキュリティ教育の自由記述アンケート分析，”大学 ICT 推進協議会年次大会論文集 (2016)，WD26，pp.1-7，2016.
[5] IPA，“情報セキュリティ 10 大脅威 2016，” https://www.ipa.go.jp/security/vuln/10threats2016.html
[6] トレンドマイクロ，“メール経由によるランサムウェア感染の脅威，” https://www.youtube.com/watch?v=EK_UtE5RqAg