高知大学における情報セキュリティ教育の現状と課題

佐々木 正人, 石黒 克也, 佐々 浩司

高知大学学術情報基盤図書館

sasaki@kochi-u.ac.jp, ishiguro@kochi-u.ac.jp, sassa@kochi-u.ac.jp

The Current Status of information security education in Kochi University

Masato Sasaki, Katsuya Ishiguro, Koji Sassa

Library and Information Technology, Kochi University

概要

本学では，新入生に対する情報セキュリティ教育を，入学後履修登録前の「情報セキュリティ講習」と必須科目「情報処理」で行っている．情報セキュリティについてさらに学習したい学生を対象として 2016 年度より選択科目「情報セキュリティ入門」も開講している．本稿では，本学における情報セキュリティ教育の現状と課題について報告する．

1 はじめに

本学では，平成９年度よりノート PC 必携による情報教育を行っている．入学直後の Web 履修登録，授業レポートや卒論作成など，入学から卒業までの 4 年間各自のノート PC を使用している．情報セキュリティ教育は，Web 履修登録操作説明会前の「情報セキュリティ講習（全入学生対象)」と「情報処理（必須科目)」で実施している．さらに情報セキュリティについて学習したい学生を対象として 2016 年度より「情報セキュリティ入門（選択科目)」も開講している．情報セキュリティに関するアンケート調査や情報セキュリティポリシーに関する自己点検の試行結果から，現状と課題について報告する．

2. 情報セキュリティ教育の概要

本学では，全新入生を対象に以下の情報セキュリティ教育を実施している．

(1) 全新入生対象「情報セキュリティ講習」
(2) 必修科目「情報処理」
(3) 選択科目「情報セキュリティ入門」

なお，在学生については，新年度オリエンテーション時に全員に情報セキュリティに関するパンフレットを配布し，セキュリティ対策の確実な実施を指導している．

2.1 入学時のセキュリティ講習

学術情報基盤図書館(高知大学 CSIRT)では，Web 履修登録操作説明会の前に全入学生を対象として，「情報セキュリティ講習」を実施している．時間的な制約もあり，その解説のほとんどが「...をしなければいけない」，「...をしてはいけない」方式での説明（座学）となっている（表 1 左）．

なお，情報セキュリティに関するパンフレットに加え，全員に「IT パスポート」と「情報セキュリティマネジメント」試験のパンフレットを配布している．資格取得はもちろん，これらの学習を通じて，情報技術の向上や情報セキュリティに関心を持ってもらう狙いもある．

2.2 情報処理

基本的なパソコン操作や Web ブラウザ，ワープロやパワーポイントなどの使い方に加え，ネット利用時のマナーやモラル，著作権，パスワード管理，Windows Update 等脆弱性対策など情報倫理や情報セキュリティに関する解説も行っている（表 1 中）．「情報処理」では，実際にノート PC で実習しながら解説している．

2.3 情報セキュリティ入門

情報セキュリティに関してさらに学習したい学生を対象に，2016 年度より「情報セキュリティ入門（選択科目)」を開講している．この授業では，「情報セキュリティマネジメント」試験を受験することを想定した内容となっている（表 1 右）．ほぼ毎回，フィッシングメール，ウイルス検知，不正サイトへのアクセス，PC のセキュリティ設定の確認，HTTP 通信の盗聴など，各自のノート PC を使って実際に体験させている．さらに，高

知県警察本部サイバー犯罪担当者によるランサムウェアや携帯乗っ取り等の実演・解説，県内のサイバー犯罪事例の紹介なども行っている．

3. アンケート調査と自己点検の実施

多くの学生は，入学直後の「情報セキュリティ講習」と必須科目「情報処理」を受講しており，どの程度理解しているのかを把握するため，「情報セキュリティ入門」の受講生に対して授業アンケートを実施した．さらに，今年度より学部別に情報セキュリティポリシーに関する実施手順の自己点検が実施されるが，その試行結果も示す．

3.1 「情報セキュリティ入門」授業アンケート

「情報セキュリティ入門」では，最終授業時に 39 項目(表 2)についてアンケート調査を実施し，その内容を理解したのは「受講前」，「受講後」，「理解していない」で回答してもらった．

3.1.1 質問項目

質問項目は，どの講習・授業により解説したかにより以下の 3 つに分かれる．

(A) 「情報セキュリティ講習」で解説:16 項目
(B) 「情報処理」で解説:13 項目
(C) 「情報セキュリティ入門」で解説:10 項目

なお，「情報セキュリティ入門」では，(A),(B)のすべての項目についても解説している．

3.1.2 集計結果

設問別の回答を集計した結果(「授業前」の回答率をプラス，「授業後」をマイナスとして表示)は図 1 のとおり．

(A)の多くは，その後「情報処理」でも解説されているが，３割程度は理解していない．特に電子メールや高知大学 CSIRT については予想に反して低い結果となっている．また(B)については，「授業前」の回答を期待していたが，全体的にその割合は低い．(C)については，SNS に関しては予想以上に高かった．

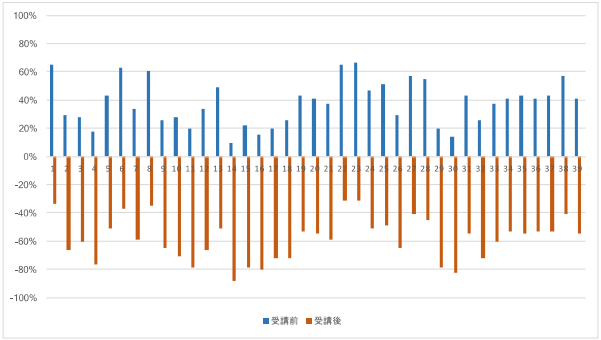

図 1 情報セキュリティ入門アンケート

3.2 「自己点検」の試行

今年度から，学内 e-Learning システムを利用して，学部別に情報セキュリティポリシーに関する実施手順の自己点検を行う予定である．この結果を元に，本人による改善はもちろん，情報セキュリティ教育の方法や内容について改善することを目指している．今回このシステムを使って，「情報セキュリティ入門」受講生および「情報処理」のみ受講している学生（2 クラス）を対象に試行した．

3.2.1 点検項目

点検項目は，数分で手軽に回答できるよう，最低限理解し実施すべき 10 項目(表 3)とした．

3.2.2 集計結果

「情報処理」のみ受講，さらに「情報セキュリティ入門」も受講に分けて集計した結果は図 2 のとおり．

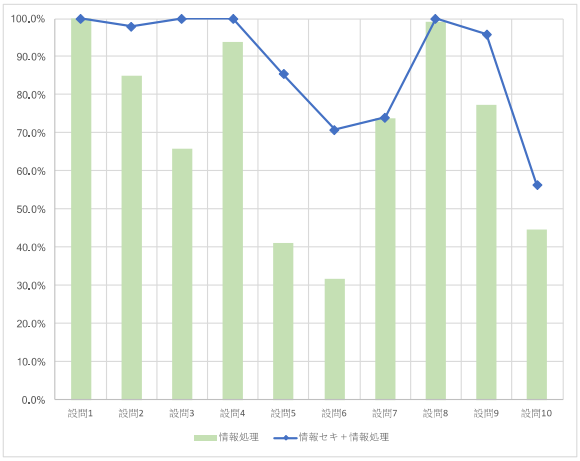

図 2 情報セキュリティポリシー 自己点検

確認 02,03 から Windows Update は実行しているが，実際に実行できているかどうかの履歴確認の方法を知らない学生が多い．確認 05,06 から，「情報セキュリティ入門」受講生を含め，ウイルスパターン更新確認やフルスキャン操作方法を知らないか，知っていても定期的に実施していない学生が多いことが分かる．また，確認 07 から新入生の場合初期パスワード変更後数ヶ月しか経過していないため，その後変更していない学生が未実施としたため 70%程度になったと考えられる．さらに，高知大学 CSIRT の存在や役割については，まだまだ理解されていないことは，自己点検からも分かる．

4. 情報セキュリティ教育の課題

「情報セキュリティ入門」受講生に対するアンケートと，「自己点検」の試行結果から，本学の情報セキュリティ教育の課題について考える．

なお，「情報セキュリティ入門」受講生は，「情報処理」も受講（1 回生は同時進行）している．

4.1 電子メールの署名に関する課題

電子メールには必ず署名を付加すること，必要な情報のみ（所属，氏名，電子メールアドレス）とすることを指導しているが，設問 15 から他にも情報を設定していることがうかがえる．「情報セキュリティ入門」中間レポート（電子メールで提出）では，全学認証 ID や回生を設定している学生がいた．個別ヒヤリングの結果，「情報処理」授業内で設定作業を行ったものであった．今後，「情報処理」授業担当者との意識合わせが必要である．

4.2 電子メールマナーと不正メール対策

電子メールのマナーについては，署名設定も含め「情報処理」で実習することになっている．設問 10 より，受講前（「情報処理」終了時）に，電子メールマナーに沿ってメール送信したことがあるのは 30%程度であることが分かった．不正メールのほとんどが，電子メールマナーに沿っていないことを考えると，常にマナーに沿って書くこと，マナーに沿っていないメールには注意すること（特に添付ファイルは開かない）が重要であり，そのためにもマナーに沿ってメールを送信する練習が欠かせない．現在，授業以外で署名やメールソフトの設定，メールマナーをチェックするサービスを検討している．

4.3 パスワードの扱いに関する課題

年に 1 回以上パスワードを変更すること，学外システムで使用しているパスワードは使用しないこと，以前使用したパスワードの使い回しは行わないことを指導している．新入生の場合，入学後全員パスワード変更を行っている．確認 07，設問 18 では，その後パスワードを変更していないため，未実施と回答したと考えられる．ただし，在学生の場合，3 割程度が 1 年以上変更していない．パスワードの有効期限設定することを含め，確実に変更させる仕組みを検討する必要がある．

4.4 ウイルス対策に関する課題

確認 04 から「ウイルス対策ソフトをインストールする」はほぼ全員理解し実施していることが分かる．しかし，ウイルス対策ソフトの仕組みやパターン更新の確認方法，フルスキャンの方法は十分に理解できていない．また，設問 02 より，ウイルス対策ソフトをインストールすればすべてのウイルスに対処できると考えている学生が多い．「...しなければいけない」方式ではなく，仕組みについて理解させる必要がある．

4.5 OS やアプリの脆弱性対応に関する課題

設問 06，08 より，Windows Update の実行やアプリの脆弱性対応が必要であることは，「情報セキュリティ入門」受講前に理解している．しかし，OS やアプリの不具合等に対する修正プログラムが提供されてることなど，その仕組みについては受講前には理解していない．ウイルス対策ソフトでの課題と同様，「・・・しなければいけない」方式での解説の限界と言える．

4.6 CSIRT への通報に関する課題

本学では，インシデント発生時に対応するため CSIRT を立ち上げている．学生に対しても講習やパンフレット配布等で周知しているが，まだまだ十分ではない．学部と協力して，情報セキュリティポリシーやその実施手順，自己点検と合わせて周知徹底する必要がある．

5. まとめ

入学直後の「情報セキュリティ講習」と，その後の「情報処理」授業による情報セキュリティ教育の現状と課題について述べた．「・・・してはいけない」，「・・・しなければいけない」方式だけでは不十分であり，仕組みなどさらに詳しく解説する必要がある．また，どのタイミングで，どのような事項を，どのようなやり方・内容で教育するのが効果的であるかを，今後も継続して検討・改善する予定である．

参考文献

[1] 沖野浩二，遠山和大，上木佐季子，黒田卓，富山大学の構成員に対する情報セキュリティ教育の実践と成果，第 21 回学術情報処理研究集会発表論文集, 2017

[2] 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，2016

表1　情報セキュリティ関連講習会および授業での主な内容

情報セキュリティ講習（全入学生対象）	情報処理（必修科目）	情報セキュリティ入門（選択科目）
1. 安全に利用するために 情報セキュリティポリシー 実施手順と自己点検　等 2. 具体的なセキュリティ対策 (1) 全学認証 ID とパスワードの 取り扱い説明と配布 (2) ウイルス対策ソフトの インストール，パターン更新， 定期的なフルスキャン等 (3) Windows Update の実施 (4) アプリのアップデート (5) ログインパスワードの設定 (6) メールマナーを身に付ける ことで不正メール被害を防止 (7) 学外から学内情報システムを 利用する際の注意事項 (8) 紛失・盗難防止 (9) その他のセキュリティ対策 3. 情報セキュリティに関する相談と 通報 CSIRT の役割，連絡先など	1. パスワード管理 パスワード変更 リスト攻撃等リスクへの対策 2. 電子メール メールソフトのインストール メールソフト・署名の設定 電子メールマナー解説・実践 フィッシングや標的型メール 3. ウイルス対策 ウイルス対策ソフトの導入 パターン更新確認 フルスキャン操作解説 ウイルス対策ソフトの限界 (ゼロデイ攻撃) 4. OS やアプリの脆弱性対策 Window Update の設定と 更新確認方法 アプリのバージョンアップ 脆弱性情報等の入手と対応 5. ノート PC の維持管理 ログインパスワード設定 定期的なバックアップ	1. インターネット社会と情報倫理 ネット社会の光と影，技術的・法的対策など 2. パソコンのセキュリティを確保するためには パソコン管理，OS・アプリに関するリスク等 3. 情報セキュリティとは 情報セキュリティの目的，考え方，対策など 4. コンピュータ・インターネットの仕組み （情報セキュリティ対策の視点からの解説） 5. 電子メールを安全に利用するためには フィッシング，標的型メール，ウイルス感染等 6. ケータイとネット スマートフォン・タブレットに関するリスク 7. サイバー攻撃の脅威と手口 8. 情報セキュリティとサイバー犯罪 サイバー攻撃 , 犯罪や脅威の行方 , 事例紹介など 9. コンピュータウイルス感染から PC を守るには マルウェアとは，ウイルス対策ソフトの限界等 10. サイトとパソコンのセキュリティを確保 ファイアウォール , IDS,IPS, 暗号化通信等 11. 組織的な情報セキュリティ対策と管理 情報セキュリティポリシー，ISMS など 12. 情報セキュリティと法整備 関連の法律，著作権保護の必要性と課題等

表2　2017年度　「情報セキュリティ入門」授業アンケート

設問 01　ウイルス対策ソフトではウイルスパターンを常に最新にしておくことが重要
設問 02　ウイルス対策ソフトではすべてのウイルスに対応できるわけではない (ゼロデイ攻撃など)
設問 03　ウイルス対策ソフトがウイルスを検知したらメッセージを出し動作を停止させる
設問 04　複数のウイルス対策ソフトを動作させてはいけない
設問 05　OS (Windows や MacOSX) に脆弱性や不具合が見つかった場合，修正プログラムが提供される
設問 06　OS は常に最新の状態（上記修正プログラムの実行 : Windows Update など）にすることが重要
設問 07　Thunderbird などのアプリ (フリーソフト) に脆弱性や不具合が見つかった場合，修正プログラムが提供される
設問 08　アプリも OS 同様に，常に最新の状態にすることが重要
設問 09　UAC(ユーザアカウント制御) 等により，管理者権限でプログラムを実行する際は警告が表示されるので，内容を確認してから実行しなければいけない
設問 10　電子メールマナーに沿ったメールとはどのようなものであるか知っていて，マナーに沿って送付したことがある.
設問 11　電子メール受信時，電子メールマナーに沿っていない場合は原則読まない（破棄する）.
設問 12　危機感を煽りパスワードの変更等を促す電子メール (本文に URL がある) が届いた場合，管理者に別途連絡し真偽を確かめる (マナーに沿っていない場合は破棄).
設問 13　電子メールに添付されているファイルは，開く前に来るべくして来たものであるかなどを確認する.
設問 14　電子メールを送付する際は，受信者は電子メールマナーに沿っていないメールは破棄していると考えて作成する
設問 15　電子メールの署名には，所属，氏名，電子メールアドレスを指定すれば良い.
設問 16　重要な情報（個人情報等）を電子メールに添付して送付する場合は，パスワード付圧縮ファイルに加工して送付する.
設問 17　パスワード付ファイルを電子メールで送付する場合は，ファイルを添付したメールとは別便でパスワードだけを送付する.
設問 18　全学認証 ID に対するパスワードは 1 回以上 / 年変更すること.
設問 19　パスワードは，以前使用したものを再度指定してはいけない（ローテーション禁止）.
設問 20　学外情報システムで使用しているパスワードと同じものを全学認証 ID に対するパスワードに使用していはいけない.
設問 21　全学認証 ID は，非公開とすること（学籍番号と同じため完全非公開とはならないが）.
設問 22　自分の全学認証 ID に対するパスワードを第三者に教えて使用させてはいけない.
設問 23　ノート PC やスマホなど，個人使用のデバイスには必ずパスワードを設定すること.
設問 24　離席時などは，盗難防止の策を講じた上でスクリーンロックすること.
設問 25　故障やランサムウェア等によりファイルにアクセスできなくなる恐れがあるため，定期的に USB メモリ等にバックアップを取る.
設問 26　電気屋，生協など修理依頼する場合は，事前に作業内容を確認しセキュリティ上問題が無いかチェックすること．原則ログイン可能な状態で渡さないこと.
設問 27　友達や先輩にノート PC やスマホを貸し出さないこと.
設問 28　自分の全学認証 ID で認証して，学内ネットワークに接続したノート PC や教育端末室周辺の PC を第三者に使用させない.
設問 29　ウイルス感染，情報流出などのトラブルが発生した場合は，高知大学 CSIRT に通報し，指示に従って対処する.
設問 30　トラブル発生時は，状況をメモすると同時にスクリーンダンプ（スマホで撮影も有効）を保存しておく.
設問 31　Web ブラウジング時，心当たりの無い請求等があっても，指定箇所に連絡したり画面上のボタンをクリックしないで無視する.
設問 32　Web ブラウジングした際（画面から個人情報を入力していない場合），サーバ側では接続者が誰であるか知るすべはない.
設問 33　リンクボタンをクリックする際は，Web ブラウザに表示される URL に気をつける.
設問 34　Twitter アカウント (約 3 億) の最大 15%はボットと言われており，情報操作されている可能性があることを前提に利用する.
設問 35　上記情報操作された内容を Twitter で入手し（信じて），Facebook 等の SNS に流している場合があることを前提に利用する.
設問 36　フェイクニュースを流したり，機械的に「いいね！」を行うサービスが存在することを前提に利用する.
設問 37　インターネット上の情報は，提供サイトの URL や提供者の所属や職業なども加味して真偽を判断する．また，複数の情報源から入手して真偽を判断する.
設問 38　必要以上にネットからアプリをダウンロードしてインストールしないこと．また，不要となったアプリは積極的に削除する.
設問 39　Windows 10 やスマホでは，アプリからカメラ，マイク等を操作する設定があるので，必要な範囲に限定して設定すること.

表3　情報セキュリティポリシー　自己点検（試行）

確認 01　PC にログインパスワードを設定していますか？
確認 02　PC の OS の更新 (Windows Update 等) は実行していますか？
確認 03　PC の OS の更新 (Windows Update 等) 履歴の確認方法を知っていますか？
確認 04　ウイルス対策ソフトをインストールしていますか？
確認 05　ウイルス対策ソフトのパターンファイルの更新履歴を月に 1 回以上確認していますか？
確認 06　PC の補助記憶装置（内蔵ディスクなど）に対して、ウイルス対策ソフトを使ったフルスキャンを月に 1 回以上実施していますか？
確認 07　全学認証 ID に対するパスワードを 1 年以内に 1 回以上変更しましたか？
確認 08　電子メールを利用する際、メールマナーに沿って利用していますか？
確認 09　離席等で PC から離れる場合、確実にスクリーンロック / ログアウト等の対策を実施していますか？
確認 10　高知大学 CSIRT の役割および CSIRT への連絡方法を知っていますか？