サイバーセキュリティ・情報倫理 e ラーニング教育の課題解決 WG 報告書

2021 年 1 月 8 日

目次

1　はじめに

サイエンティフィック・システム研究会において，サイバーセキュリティ・情報倫理 e ラーニング教育の課題解決の WG を立ち上げようという話が出たのが 2018 年秋頃のことである．近年，全国の大学，研究機関（以下「大学等」という．）は，高度で悪質なサイバー攻撃の脅威にさらされ，組織内サーバー

への不正アクセスやメールシステムへの不正侵入や研究データ，機密データの流出といった事故が相次いでいる．大学等では，企業のような経営陣等のトップダウンでコンプライアンス・ポリシーを徹底する画一的な運用が難しい．さらに，国立大学法人においては運営費交付金が毎年度減額され，情報担当部署の多くは，その役割（情報セキュリティ強化など）増大にも係わらず少人数で構成されていることも少なくない．情報担当部署の人員や予算が増えることはほとんど期待できないだけでなく，一部の大学では情報担当部署の予算と人員の削減が行われている．また，大学等では，国内外を問わず一時利用者（非常勤講師，非常勤職員，海外研究者など）も多く，構成員によって，情報セキュリティやコンプライアンスに対する意識レベルが，差異がある点も課題の一つであり，組織全体のシステム整備だけではなく，構成員のセキュリティに対する意識レベルの向上が必要不可欠である．現在，大学等では，講義形式や e ラーニングを活用した情報セキュリティ教育，研修が行われているが，その反面，次のような課題を抱えている．

1. 受講率のみで評価するアリバイ作り的運用：著者らの所属機関では，サイバーセキュリティの e ラーニングコースについて，その教育的効果を評価することなく，受講者が何名で，受講率が低迷しているのが問題だという議論を数多く見てきた．e ラーニングによるサイバーセキュリティ教育には，少なくないコストが必要であるにも関わらず，アリバイ作りになっていると言わざるを得ない．
2. 受講者に合わせることが困難：大学生は初・中等教育においてある程度のサイバーセキュリティに関する教育を受けているはずであるが，その習熟度合いは一定ではなく，前提知識が一定ではない．受講者に合わせた e ラーニングを実現すること，それが適切かどうかの評価が困難である．
3. 継続的な更新が必須：毎日のように情報セキュリティインシデントが報告されているため，コンテンツの継続的なアップデートが必須となっている．このような取り組みを始めることじたい簡単ではないが，継続するのはさらに困難である．したがって，コンテンツの更新に関するワークフローを確立することが課題である．これを敷衍し，コンテンツの開発の前提となる，学習設計を含めた取り組みが必要であると考える．
4. テストが適切がどうか判断ができない：e ラーニングを用いて情報リテラシーなどを理解しているかを判断する手法として，確認（試験）を行うことが多いが，そのテストが適切かどうかについて，誰も判断基準を持っていないのが現状である．それにもかかわらず，毎年度，確認（試験）に合格することをアカウントの利用条件としているところも少なくない．さらには，e ラーニングに合格していることを卒業条件として設定しているところもある．本当に，これらの確認（試験）で罰則を設置しても良いか，その適切な判断がなされていないのが実情である．

このような問題意識のもと，サイバーセキュリティ e ラーニングの問題解決 WG では，より良いサイバーセキュリティ教育のためのテスト問題を作成し，「知識」の有無ではなく「態度」の習得を意識した．このテスト問題作成には，インストラクショナル・デザイン（Instructional Design: ID）の考え方を取り入れている．作成したテスト問題を格納するためのシステムとして，e ラーニングリポジトリを構築した．

本 WG での提案の利点は，大学等の事情に応じて問題を取捨選択できること，各大学のプラットフォームを活用でき責任分界点が明確であることが挙げられ，より持続的な取り組みを目指すものである [1]．

2 WG 概要

2.1 活動方針

近年，大学等を狙ったサイバー攻撃は深刻化，年々増加している．現在，大学等ではサイバーセキュリティ・情報倫理 e ラーニング教育が実用的に行われている反面，その実施のための課題も多い．例えば，受講率を向上させる方法，コンテンツの最新化，国際化，多様性の対応は多くの組織で抱えている課題で，また，e ラーニング教育と他の ICT システムの連携といった新しい取り組みが模索されている．本 WG では，これらの課題に対して e ラーニング実施者の立場から取り組み，組織で持続的にサイバーセキュリティ・情報倫理 e ラーニング教育を実施できるための提言を行う．

2.2 WG メンバー

2.2.1 学術界

- 上田浩 （法政大学　情報メディア教育研究センター）まとめ役
- 岡村耕二（九州大学　情報基盤研究開発センター）担当幹事
- 後藤田中（香川大学　情報メディアセンター）
- 平岡斉士（熊本大学　教授システム学研究センター）
- 金子晃介（九州大学　サイバーセキュリティセンター）
- 中村誠　（東京大学　情報システム本部）
- 松本多恵（総合地球環境学研究所　研究基盤センター）

2.2.2 富士通

- 田口 雅晴（富士通 文教・地域ソリューション事業本部）まとめ役
- 井上 俊治（富士通 文教・地域ソリューション事業本部）

---

[1] 本報告書は，情報処理学会研究報告[1]を加筆したものである．

- 中尾 礼文（富士通 文教・地域ソリューション事業本部）
- 石田 亮介（富士通 文教・地域ソリューション事業本部）

※所属は 2020 年 12 月末時点のもの

2.3 WG 検討経過

	日時	場所	活動内容
第1回	2019 年 2 月 26 日（火）14:00～17:00	富士通汐留本社	活動メンバーの確認活動方針/活動内容/活動の進め方の検討メンバーからの情報提供（島根大学　松本多恵）所属は当時
第2回	2019 年 4 月 24 日(水) 13:00～17:00	香川大学 幸町キャンパス	情報提供 （香川大学　小野 滋己）(熊本大学　平岡斉士) 現状の問題に対するディスカッション
第3回	2019 年 6 月 19 日(水)　13:00～17:00	富士通汐留本社	現状の問題と課題解決について（宿題） 現状の問題点のディスカッション 最終成果物の検討
第4回	2019 年 9 月 24-26 日(火-木)	熊本大学	リポジトリシステムの各個人の課題(宿題) リポジトリシステムに対するディスカッション最終成果物の検討
第5回	2019 年 12 月 18 日(水) 13:30～17:30	富士通汐留本社	リポジトリシステムの各個人の課題(宿題) リポジトリシステムに対するディスカッション
第6回	2020 年 5 月 14 日(木) 14:00～17:00	リモート	作問／リポジトリシステムに対するディスカッション 最終成果物の検討
第7回	2020 年 8 月 20 日(木) 14:00～17:00	リモート	最終成果物の検討
第8回	2020 年 12 月 14 日(月) 14:00～17:00	リモート	最終成果物の検討

3 情報セキュリティ教育・研修

3.1 現状の問題点

現在，国立大学法人等では，講義形式や e ラーニングを活用した情報セキュリティ教育，研修が行われている反面，その実施のための課題も多い．例えば，受講率を向上させる方法（罰則規定），コンテンツの最新化，国際化，多様性の対応は多くの組織で抱えている．現状の問題点を把握すべく，多くの機関で

実施している情報セキュリティ教育・研修を事例として紹介し，その内容を比較・検証していく．

3.2　事例紹介

3.2.1　大学共同利用機関法人人間文化研究機構の取り組み

大学共同利用機関法人人間文化研究機構は国立歴史民俗博物館，国文学研究資料館，国立国語研究所，国際日本文化研究センター，総合地球環境学研究所，国立民族学博物の 6 つの機関で総合的研究拠点として構成されている(図 1).

図 1 人間文化研究機構を構成する機関

本事例の紹介として，平成 30 年度の情報セキュリティ研修について述べていく．研修の実施時期は，平成 30 年 10 月 24 日～平成 30 年 11 月 28 日（平成 30 年 11 月 30 日まで延長）で，使用教材は，パナソニックソリューションテクノロジー株式会社製「大学向けテストで学ぶ情報セキュリティ」を用いている．全 40 コマで構成され，ケーススタディーによるテストがある． 8 割（32 問）以上を合格ラインと設定した.

受講対象者とは，機構本部及び機構が設置する大学共同利用機関（以下「機関」という．）の情報システム（PC 等）を使用する 機構本部及び機関に所属する者を対象とした．全体で 1,170 人である．合格ラインの 8 割以上を実施期間以内に終了した受講者は 1093 人で受講率は 93%である．平成 29 年度は，受講対象者は 1,165 人で，8 割以上で終了した受講者は 947 人で受講率の 81%であった．受講率が上昇した理由の一つとして，平成 30 年度より，各機関の状況に応じて，フォローアップ期間中に受講しない者には，受講が完了するまでの間，機関等は情報システムの使用を制限することもできるものとしている点が要因として考えられる．また，実施期間中には，機構本部及び機関の情報システム担当部門より再受講を促すメールや個別の連絡等を行った点も効果的であった.

令和 2 年度も令和 2 年 10 月 1 日～令和 2 年 11 月 30 日まで実施した.使用教材は、パナソニックソリューションテクノロジー株式会社製「大学向けテストで学ぶ情報セキュリティ」を用いている．全 40 コマで構成され，ケーススタディーによるテストがある． 8 割（32 問）以上を合格ラインと設定した.

3.2.2　香川大学における取り組み

香川大学では，2015 年度より，教職員を対象とした情報セキュリティの教育活動をオンライン（e ラーニング）の形式で実施している．教員が授業等で活用可能な Moodle 上でコンテンツの提供を行い，受講期間は，基本的に 1 ヵ月程度としてスタートした．なお，e-Learning 受講では，FD（Faculty Development）の一環とし，ペナルティ(強制力)は設けない形でこれまで実施している．

開始当初の 2015～2016 年度では，IPA が制作・提供する映像を視聴する形式であった．例えば，2016 年度は，当時，喫緊の課題として，日本年金機構の事案に代表される標的型メール攻撃の対応に加え，情報漏洩の抑止対応が必要との担当部局の見解から，それらに関連する動画[2-4]を視聴教材とした．視聴後は，映像テーマに紐づいたいくつかのキーワード（例：情報漏洩の防止，標的型攻撃メール対策，同メールのだましのテクニック等）の理解度を自己申告で問う形でのアンケート回答する形で行った．

しかしながら，この理解度を自己申告で問う形式においては，情報セキュリティ脅威の多様化に伴い，対策知識・判断・姿勢がより幅広く・深く求められるようになる中で，そもそも理解度の自己判定を行うこと自体が，より困難な状況となる予測から，2017 年度には，回答選択肢式の小テストへ移行することになった．

この方針に従い，2017 年度からは，情報資産の重要度に関わる情報セキュリティポリシーの規定内容や学内基準のパスワードルールの把握等を中心として，本人が，Yes/No（知っている/知らない，満たしている/満たしていない等）で回答可能と思われる点検については自己申告として新たに追加する一方で，先述の理由で自己申告が困難になりつつあると思われる情報セキュリティ対策に関わる知識を問う内容については，いわゆるクイズ形式の小テストと出題した．なお，自己点検後でなければ，小テストを受講できない形とした．狙いとしては，自己点検を行ってから小テストの回答が行うことで，例えば，規則を理解している(Yes)と回答しても，小テストの成績が思わしくない場合，規則の理解とは別に，情報セキュリティ対策に関わる知識等は別途獲得が必要あるという点を本人に意識させる警鐘の意図も含んでいる．

2017 年度からの小テスト教材は，既存の教材[5-10]を基に大学教職員にとって有用と思われる内容を抽出し，大学組織の特徴に合わせ本学内部で修正したオリジナル教材である．2017 年度は，計 51 題を用意し，一部必須出題も含みランダムに約半数の 25 題を出題する形で提供した．なお，2018 年度においては，より業務等に即した形でカバーする範囲と複数年利用できるコンテンツ見直し，計 81 題から 25 題する形へ変更し，問題バンクとしてのコンテンツの蓄積を図っている．

小テストについては，Moodle の機能である多肢選択式問題と自動採点機能を利用し，回答に対して判断の正誤および詳細な解説が提示されるようにしたことにより，単なるチェック機会だけではなく，学習機会としても機能するようにし，正答率が 80%を超えることを修了条件とし，正答率が下回る場合には，再受講が必要とした．なお，別途学内で実施している標的型攻撃メール訓練との連動性を意識し，例えば，2018 年度標的型攻撃メール訓練の結果を受けて香川大学の正規 Web サイト URL と不審な URL リンクを見分ける設問を必須問題としている．

このような変遷を経て，受講率は，2016 年度の 45%ほどから 2017 年度，2018 年度は，約 60%，約 55%と，形式変更前と比較すると大幅に受講率が改善している．また，2019 年度は，これまで，約 1 ヵ月という受講期間が短いという学内構成員も本 WG の意見や 4 月や 10 月などの入職者の教育機会に即時的に対応するため，通年でのコース開講とし，CISO からの再周知（受講リマインド）も適切に組み合わせながら 68%へ受講率の向上を図ることができた．

一方で，受講期間を広げたにも関わらず，学部間において受講率の差が見られ，特に，Moodle の利用方法がシンプルなマニュアル等で通知されつつも，一度も利用したことがない Moodle 利用の精神的ハードルを依然抱える構成員もいることが推測された．2019 年度の時点で，教員の Moodle の授業利用率については，学部間差があり，一概にその要因だけではないが，e-Learning システムを本人が利用したことがあるかどうかも影響している可能性が示唆された．

なお，2020 年度は，問題バンクの各問題文や回答選択肢等の文言を一部見直し，差し替えた上での公開を予定していたが，新型コロナウイルス影響とその対応[11]により，学生のオンライン受講用途で共用している Moodle の負荷増等を避けるため，2020 年 7 月まで，一時的にコース公開を中止し，受講時期を遅らせて 8 月より同コースの公開を再開している．これについて，今年度の受講開始が遅れた一方で，教員や一部の職員は，オンライン授業対応のため，強制的にではあるが，Moodle の利用がほぼ必須となったことにより，今後，「システムの利用法を知らない&操作したことがない」という構成員の割合が低下することにより，受講率にどのような影響を与えるか，分析を行う予定である．

3.2.3　九州大学における取り組み

九州大学では，2017 年度から九州大学の全教職員を対象に情報セキュリティ教育の e-learning を実施している．受講者の人数は，約 10,000 人程である．e-learning の実施期間は 3 ヶ月である．本 e-learning では，文章を読んで設問に答えるという方式をとっている．受講時間は 30 分～60 分程度を想定して文章と設問の内容を制作している．本 e-learning の教材制作は，九州大学情報統括本部の情報セキュリティ基本計画事業室で担当し，九州大学のセキュリティポリシーに合わせてオリジナルの教材を制作している．本 e-learning は Moodle を使って提供しており，九州大学情報統括本部の九大 CSIRT が実行主体として

実施している．これまでの情報セキュリティ教育の e-learning の取り組みから見つかった課題を以下に挙げる．

3.2.3.1 受講率に関する課題

九州大学の 2017 年度と 2018 年度の情報セキュリティ教育の e-learning の受講率は，それぞれ 45.5%と 51.1%になっており受講率はかなり低い状況であった．しかし，2019 年度の受講率は 77.1%と劇的に向上した．この受講率向上の理由は，2018 年度の e-learning 終了後に，受講率向上の取り組みに本格的に取り組んだことによるものである．具体的には，e-learning の実施期間中に，各部局の部局長が集まる会議において，部局毎の受講率の割合を提示した．さらに，部局長が受講率の向上を望む場合は，その部局の未受講者のリストを提供するようにし，部局長が未受講者に受講を促せる仕組みを用意した．また，受講率向上の取り組みを実施する中で，未受講者に罰則を設ける案も出たが，九州大学の CISO のポリシーにより，ネガティブな方法での教育は良い効果は得られないということから九州大学では罰則を設けなかった．未受講者への罰則を設けていないにも関わらず，部局長への通達を行うことで，8 割近くの受講率を達成できているので，情報セキュリティ教育の e-learning に取り組まれている組織で，罰則を設けずに受講率をあげたいと思われている方には，本学で実施した方法を実施してみる価値はあると思われる．また，2019 年度までの九州大学の Moodle は，通常の講義のコースと研修のコースが掲載されており，研修用のコースが閲覧できにくい状況にあった．そこで 2020 年度からは，教職員の研修専用の Moodle を新しく用意することになったため，このような研修専用の Moodle がどのような受講率向上の効果をもたらすのか注目している．

3.2.3.2 教材制作者の負担に関する課題

前述の通り，e-learning の教材の制作は，九州大学情報統括本部の情報セキュリティ基本計画事業室が担当している．作業の内情としては，1 人の教員が教材と設問の叩き台を作り，情報セキュリティ基本計画事業室の教育・訓練のワーキンググループで議論し内容を改善していく．その後，情報セキュリティ基本計画事業室と九大 CSIRT で，更に内容を議論し，最終的に統括本部全体の会議で内容を確認してもらう流れで進めている．また，教材は日本語版と英語版との両方を制作している．教材を制作するための時間的，労働的コストは非常に高く，教材の制作負担の課題は大きい．現時点で，九州大学での画期的な課題解決方法はないが，本 SS 研の e ラーニング課題解決 WG が提供している設問のリポジトリなどは，制作者の負担を軽減する可能性を有していると思われる．

3.2.3.3 受講者の受講負担に関する課題

受講者は，通常の業務に追われているため，情報セキュリティ教育の e-learning に取り組む時間を確保できにくいという問題はある．加えて，あまり

にも時間がかかるような e-learning は，受講負担の点から敬遠される可能性もある．前述の通り，九州大学では情報セキュリティ教育の実施時間を 30 分〜60 分で想定している．また，九州大学では，2018 年度まで，情報セキュリティ教育の e-learning に加えて，セキュリティに関する項目として，e-learning とは別に ISMS に基づく自己点検のアンケートなども全教職員を対象に実施していた．しかしながら，受講者から負担が大きいとの声も上がっており，2019 年度からは，情報セキュリティ教育の e-learning の中で自己点検も行うようにした．受講者が，Moodle 上のコースに入ると，まず自己点検のアンケートに回答する．その後，e-learning として，自己点検の内容を踏まえた教育の文章や設問が提供される流れをとっている．しかしながら，通常の e-learning に自己点検の内容も加えたことで，情報セキュリティ教育の実施時間が大幅に増え，余計に受講者へ負担をかける可能性が高まった．そこで，Moodle の機能を使って，情報セキュリティ教育の内容毎に章分けを行い，途中でやめても，中断したところから再び実施できるようにした．章訳の具体的な例としては，各章の最後に設問を設けて，設問を全問正解すると次の章に進めるという仕組みにしている．最後の章の設問に全問正解すると，受講完了証明書が提供されるという流れにしている．このような章分けを行い，いつでも中断箇所から実施できるようにすることは受講者の負担を軽減できる可能性があり，実際に受講者から負担が減ったという意見も頂いている．

3.2.3.4 教材の設問の内容に関する課題

2019 年度までは，設問の内容に関して，知識を問う問題を出していた．しかしながら，知識があるからと言って，実際に行動に移せるとは限らないと言う点は，本本 SS 研の e ラーニング課題解決 WG でも指摘されていた．そこで，本 WG でのインストラクショナル・デザインの考え方や議論を通じて，2020 年度からは，知識を問う問題から態度や行動を促すような問題を出すように方針を変更している．具体的にパスワードに関する設問として，2019 年度と 2020 年度の内容を記す．

3.2.3.4.1 2019 年度版

質問：パスワードの管理について，正しい選択肢を全て選んでください．

選択肢：

- パスワードには，英小文字や英大文字，数字，記号などをランダムに含めて，8 文字以上の複雑なパスワードを設定している．
- 教授の先生から，「私の SSO-KID とパスワードを教えるので，私の代わりにシステムにログインして事務的な手続きを処理して欲しい」と言われたので，そのまま従った．
- パスワードを他人に教える事は非常にまずいことではあるが，SSO-KID は他人に教えても問題ない．

- 様々なサービスで，同じパスワードを使うと，パスワードを効率的に管理できるので，同僚にも仕事のコツとして伝えている．

3.2.3.4.2 2020 年度版

質問：あなたは，「SSO-KID」と「業務用パソコン」と「私用の SNS（Facebook 等）」の 3 つのサービスで，パスワードを使って認証を行っています．あなたが，この 3 つのパスワードを設定する際に，やってはいけないと思われるパスワードの組み合わせを全て選択してください．

選択肢：

	（SSO-KID）	（業務用パソコン）	（私用の SNS）
	19701010	20150401	20100618
	7@bB	1We#	R^a7
	#qwTDF56&&%	$34^{r}TYbg$%6	76$#Dkau%
	Sso-Kid	Qdai	MyFacebook

これらの効果がどう現れるかは，今年度の情報セキュリティ教育の e-learning を実施して確認したい．

3.2.4 熊本大学における取り組み[12]

熊本大学では平成 22 年度に「熊本大学情報セキュリティポリシー」が制定されたが，このポリシーが十分に生かされているとは言いがたい状況であったため，情報セキュリティ意識の啓発と情報セキュリティ対策の拡充を図り，「安全・安心な情報環境の構築」を図る活動の強化を開始した．

3.2.4.1 これまでの取り組み

平成 24 年度までの情報セキュリティ対策は，年 1 回の集合研修，熊大ポータルへの情報掲示及びセキュリティ事案の対応等を行ってきたが，情報化社会の進展の中で，情報セキュリティへの関心が高まり，本学においても本格的な情報セキュリティ対策を行うことが必要になってきた．そこで，平成 25 年度から「熊本大学情報セキュリティ行動計画書」を策定して具体的セキュリティ対策を実行することとし，上段の取組概要にある各種事業を実践した．しかし，平成 25 年度の実績を検証した結果では，教職員向け e ラーニング研修の受講率が 17.6%，学生向け e ラーニング研修の受講率が 2.5%と低い結果となり，一方向的な情報の発信及び教育啓発では，教職員・学生の関心を高めることに限界を感じ，本学の情報セキュリティ対策の進展が危ぶまれる結果となった．

3.2.4.2 令和元年度の取り組み

平成 28 年度に策定した「熊本大学情報セキュリティ対策基本計画」について，平成 30 年度までの 3 ヶ年の取組の自己評価を行うとともに，新たに「サイバーセキュリティ対策等基本計画」を令和元年 9 月に策定した．

1. 情報セキュリティ管理体制調査(全部局対象)
2. 情報セキュリティ教育（全教職員・全学生対象） a 情報セキュリティ研修(e ラーニング利用) b 情報セキュリティ自己点検(e ラーニング利用) c 啓発ビデオ教材の配信(e ラーニング利用)
3. 情報セキュリティ監査(準拠性監査・技術監査・妥当性監査・フォローアップ監査)
4. 部局情報セキュリティ責任者向け研修
5. 部局システム管理責任者向け集合研修
6. 事務系課長，副課長向け集合研修
7. 留学生を対象とした情報セキュリティ研修
8. 教育系職員を対象とした標的型メール攻撃訓練
9. CSIRT 訓練（研修形式として）の実施
10. 情報セキュリティ対策ポスターの作成

今回の取り組みでは，「教育・啓発活動」では，28 年度に続き，30 年度に発生した留学生によるソフトウェアの不正利用の事案が発生したことから，新入留学生向けの研修内容にも著作権に関する内容を充実させた．また，階層別の集合研修及び教職員・学生向け e ラーニング研修では，前年度の監査の結果及び学内で発生したインシデントの再発防止に向けた内容を取り入れた．3 月には情報セキュリティ対策についてのポスターを作成し，4 月に配布する予定である．

また，「情報セキュリティ監査（準拠性監査）」では，これまでの準拠性監査，技術監査及び妥当性監査を実施し，さらに前年度指摘を受けた組織のうち，3 組織に対し，フォローアップ監査を実施し，是正後のセキュリティ状況を確認した．平成 25 年度から実施している情報セキュリティ監査は 2 巡目が終わり，3 巡目となるが監査対象を選定や実施方法の再検討を行う必要がある．次年度には大分大学及び宮崎大学との相互監査の試行を予定しており，今年度は実施に向けた検討を開始した．

3.2.4.3 取り組みの効果

令和元年度は，平成 30 年度の結果を踏まえて「情報セキュリティ行動計画」を策定し，「教育・啓発活動」においては，経営層主導のセキュリティ強化を目的として，部局情報セキュリティ責任者向け研修を計 11 回実施した．また，部局システム管理責任者等向け集合研修を部局系と事務系に分けて実施し，全体の受講率は 97%であった．一般には，教職員向け，学生向けに「自己点検」

を含む e ラーニング研修を実施した．受講率は教職員が 97.8%で高い受講率を維持しているが，学生は前回の 63.6%から 46%と低下したため，令和 2 年度以降の受講率アップに向けた対応策の検討が必要である．その他の強化施策として，教育系職員等を対象とした標的型メール攻撃対策訓練を実施し，標的型メールへの的確な対処方法を身につけさせると共に，IT・セキュリティ人材育成の一環として，総合情報統括センター教職員及び病院医療情報担当者の学外での受講促進を図り，また，次年度には事務システムに対する相互監査を他大学と連携して行うことにしている．これらの活動により，大学全体の情報セキュリティ対策および意識を向上させることができた．

3.2.4.4 まとめ

令和元年では学生向けの e ラーニング研修においては受講率が 46%と低下し，目標の約 6 割を達成できなかった．しかし，まだ不十分とは言えず，次年度は更に留学生を含む学生の受講率をアップさせ，学生の情報セキュリティに対する意識を高める必要がある．また，令和 2 年度はサイバーセキュリティ対策等基本計画として策定した各取組事項の実施に向けた検討を行う．

3.2.5 国立情報学研究所と連携した京都大学における取り組み

京都大学では，2012 年度まで日本データパシフィック社「INFOSS 情報倫理」と独自コンテンツによる e ラーニングを学内 CMS で提供していたが，2013 年 4 月より国立情報学研究所が運用する「学認連携 Moodle 講習サイト」を利用した学生向けの情報セキュリティ教育を行っている．具体的には，＊りんりん姫と学ぼう!情報倫理＊京都大学における情報セキュリティ の 2 つのコースによるもので，前者は NII が提供しているコースであり，後者は大学独自のコースとなっている．

学認連携 Moodle の利用にあたり，未受講学生に対するペナルティを課すことをアナウンスした結果，2013 年度は 78%，2014 年度は 81%の学部，大学院新入生が受講したことが報告されている．一方で，ブラウザによっては受講履歴が記録されない不具合，認証連携からログインまでの手順がはじめての利用者には分かりにくいといった問い合わせが多数寄せられた．

学認連携 Moodle では受講履歴を大学等の機関ごとにフィルタリングしてダウンロードできる機能を開発している．京都大学の大学コース管理者から，受講履歴のダウンロードに非常に時間がかかることが報告された．調査の結果，受講履歴の取得にはユーザ数と SCORM パッケージの章立てに依存した多数のクエリが発行され，それが高いシステム負荷となっていることが分かった．[13]

コンテンツの利用拡大に伴い，その分析に基づいて改善を行おうとするのは自然な流れである．しかしながら，「りんりん姫と学ぼう!情報倫理」をはじめとする学認連携 Moodle 講習サイト上のコースは，コース設計という概念がなく開発を行ったため，分析を行うための評価基準を定めることができず，正当

率，受講率のみの評価しか行うことができなかった．これではサイバーセキュリティ教育の改善につなげることは困難であると考える．[14]

3.2.6　東京大学での取り組み

2017 年度より情報セキュリティ対策に関する基本計画に基づき情報セキュリティ教育・訓練及び啓発活動の一環として，本学の情報システムを利用する全構成員を対象に e ラーニング形式の情報セキュリティ教育を毎年実施している． 当初は教材および確認テストを独自に開発したが，コンテンツ開発の業務負担を軽減するため 2019 年度より外部機関が開発したコンテンツを導入し効率化を図った[15].

コンテンツはマンガによる情報セキュリティで起こりがちな状況を提示し，その状況に対する判断や対応に関する 2 つの選択肢の正誤の組み合わせを答えるクイズ形式をとっており，その中から教職員であればメールの注意点やセキュリティ更新，学外での情報の取り扱いなどを中心に，学生であればメールの注意点や SNS の注意点などを中心に 10 数問を選定した． 学内 LMS のテスト機能を用いて選定した問題を 10 問ランダムに出題し全問正解するまで繰り返し受講させている．未受講者には全学無線 LAN サービスの利用を一定期間制限するとし 1,2 カ月の受講期間を設け期間中に定期的に総務や教務担当を通じて受講を促しており，2020 年度の受講率は教職員 94%，学生 82%であった．

3.2.7　富士通グループにおける情報セキュリティ e-learning 取り組み事例

3.2.7.1 実施概要

富士通グループにおいては，情報セキュリティに関する e-learning として以下のようなコースを運用している．

- 従業員が守るべきセキュリティ上のルールを学ぶことを目標とした，全従業員約 12 万人を対象としたコースを年 1 回実施．
- その他，部門ごとにセキュリティ意識の底上げをするためのコースが 24 コース．具体的には，マイナンバーや個人情報保護を対象にしたような，個別業務に応じたコースも含む．

これらのコースは，広く社員にとって必要な情報セキュリティ知識の底上げを図り，最低限の価値観を合わせるような入門・基礎的な内容がほとんどである．費用対効果の面で，受講者数を一定数確保する必要があるため，高度なセキュリティ技術者育成に関する e-learning は基本的に実施していない．

3.2.7.2 受講率

全従業員を対象としたコースの受講率は 98%以上である．休職中，海外出向中など物理的に受講できないケースもあるため，必ずしも 100%にはならないが，ほぼ全員が受講完了している．この受講率を達成している背景としては以下のとおりである．

- 未受講だと人事評価につながる可能性があるため，社員として自発的に受講する傾向にある．
- 業務の一環であるため，就業時間中に受講している．
- 上司は部下の受講状況を Web で確認することが可能であり，自身のチーム評価につながる可能性があることから，受講率が 100%になるように部下を確実にマネジメントする．コースに応じて，部署ごとの受講状況ランキング情報も提供されており，この情報を確認するたびに上司から部下への受講催促の頻度があがっていく．
- システム上からリマインドメールを 4 回(初日，期間中の中間地点，締切の 1 週間前，締切当日)にわたって送付している．フォローアップメール送信後にアクセス数が増加する傾向が顕著であり，3 割程度の受講率向上に寄与しているとの分析結果がある．

3.2.7.3 コンテンツの作成方法

グループ会社内には全社向け e-learning や集合教育等を企画，推進する専門部署（関連会社）が存在し，その部門が中心となって推進している．e-learning コンテンツは基本的には『学習』＋『小テスト』の形式が多く，最短で 2 か月程度かけて開発する．コンテンツ作成の流れとしては以下のような形である．

3.2.7.3.1 企画

まずはどのようなコンテンツを作るかの企画を行う．ここでは，Instructional Design の考え方を用いて，この e-learning を受ける前の受講者の状態と受けた後の受講者の状態を定義する．この定義を行ったうえで，学習目標とコース概要を明確化する．Instructional Design は正解のない教育に対しては適用し辛い傾向にあるが，情報セキュリティ e-learning で学ぶ内容は正解があることがほとんどであり，Instructional Design を用いることが有効である．

3.2.7.3.2 原稿作成

企画を踏まえて，原稿作成を行う．教材としては PowerPoint のスライドをそのまま使うものもあれば，音声解説を付与したり動画を埋め込んだりするものもある．それらの情報を整理し，文字起こしをしてレビューを行う．特にテストの設問は原稿作成者の個性に依存しがちであるため，特に入念なレビューを実施し，学習目標に到達したかどうかを測る問題になっているかどうかを確認する．

3.2.7.3.3 コンテンツ化

最後に，e-learning システムに搭載可能な状態にする．PowerPoint ファイルであれば，e-learning システム用のフォーマットに変換し，音声や動画であれば専門業者に依頼して，音声ファイルや動画ファイルを制作してもらう．

3.2.7.4 工夫しているポイント

教材やテストに取り込むコンテンツとしては「いかにして自分事として考えられるか」という点を重視している．そのため，教材にできるような実際の事例を汎用化することがポイントである．教材に取り込めないような事例であっても，教材の合間にコラムとして事例紹介をすることも効果的である．ただし，受講者自身が「自分事としてとらえようとする」ための努力も合わせて必要であり，受講者に対して意識付けを行うことも重要である．

また，一部のコースではアウトプットとしてレポートや報告書を義務付けている．教材の内容を踏まえて自らの言葉で理解した内容を表現することで，その理解度をセルフチェックできるのがポイントである．アウトプットの評価は受講者の上司が行う必要があり，上司自身のスキルも問われることとなる．

3.2.7.5 課題や改善したいポイント

e-learning において，課題や改善すべきと考えているポイントは以下のとおりである．

- 作りこんだコンテンツ(アニメーションの多用やシミュレーションなどを含む教材)へのニーズが高いが，実際はコンテンツの見た目を工夫しても受講者の理解度向上にあまり寄与しないことがわかってきている．コンテンツのアップデートや e-learning 環境の変化に柔軟に対応し，短時間で受講するためにも，シンプルなコンテンツ作りをすることが望ましいため，コンテンツの派手さを重視しない風潮を作っていく必要がある．
- 多様性に対する対応をどのレベルまで実現するか考える必要がある．たとえば言語は日本語と英語でよいか他の言語にも対応すべきか，あるいは目や耳の不自由な方に対する e-learning 作成おいて，自動読み上げ機能の活用の検討などを進める．
- マイクロラーニング(学習目標に対する教材全体ではなく，一部分だけを切り取って学ぶこと)の効果的な使い方を定義していく必要がある．現在は動画コンテンツで検索してその箇所にジャンプできる，あるいは倍速で聞けるなどの仕組みを持つプラットフォームも用意されており，マイクロラーニングの考え方で受講者自身が活用できる手法はある．ただし，本当に部分的な学びだけで効果があるのかどうかは評価できない点もあるため，検討する必要がある．
    - 短時間で学習する需要があると考えられるため
- 「よいコンテンツ」の定義が人によって違うことに対して，多くの人に有効な e-learning コンテンツを開発するために，わかりやすく統一していくことが必要である．この統一基準の検討においては，Instructional Design における「入り口と出口」の考え方，あるいはレイヤーモデルを活用するのがよいと考える．

- インフォーマルラーニングを e-learning 上で実現する手法の検討が必要である．学習効果を高めるためには，自分の考えと他者の考えをミックスして新たな価値観を作っていく，あるいは自分の悩みを解決した先人とのディスカッションが有効であるため，人と人をつなぐプラットフォームによって学びの場を提供できることが望ましい．
- アフターコロナにおける，あらゆる教材を e-learning 化すべきという風潮に対して，具体的な方針を決める必要がある．PowerPoint をスライドショー化する，あるいは講師の講義を撮影して動画で配信する，という従来の手法にとらわれない，ICT を活用したニューノーマル時代にふさわしい e-learning を模索していく必要がある．

4 インストラクショナル・デザインの基礎

e ラーニングによるサイバーセキュリティ教育にインストラクショナル・デザインを導入する．インストラクショナル・デザイン(Instructional Design: ID)は，日本語では「教授設計」と言われ，教材設計・開発へのシステム的なアプローチを取るものと定義される．さらに ID による教材設計・開発へのシステム的なアプローチは「Plan-Do-See」の 3 つの段階に分けることができる[16]．これを e ラーニングにおけるテストの作問にあてはめると，「学習目標の明確化(Plan)」の後に作問(Do) し，学習目標を達成できたかどうかの評価を行い，改善(See) することになる．すなわち，我々の行うサイバーセキュリティ教育は単にオンラインコースやテストを受講したという履修主義ではなく「何を学んだか」という習得主義への転換が必要となる．そのためには図 2 に示す通り，評価方法と学習目標，教育内容を一致させることになる[17]．

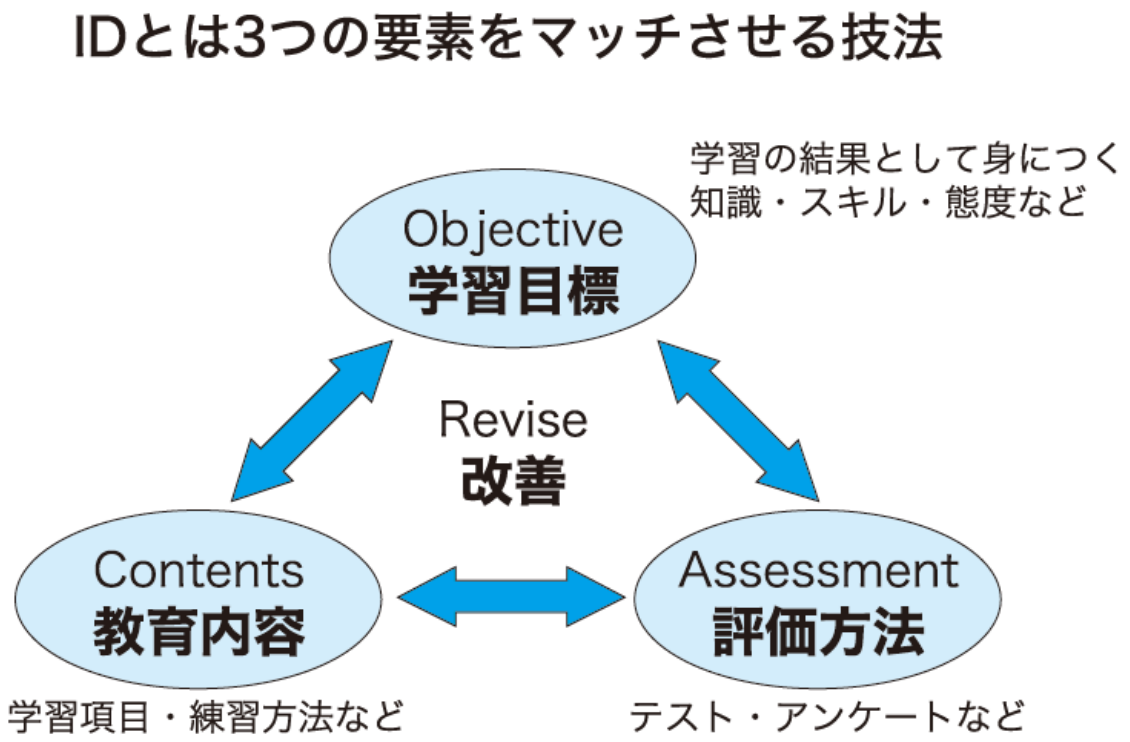

図 2 ID の 3 要素（参考文献[17]より著者の許諾のもと転載）

多くのサイバーセキュリティ・情報倫理 e ラーニング教育では，用語や事例についての解説に終始し，それらについて「理解」すれば目標を達成したとしている．しかしながら，サイバーセキュリティ・情報倫理 e ラーニング教育の本来の目的は，問題が発生したときに適切な行動を取れるようになること，また問題が発生しないようにそれを予防する行動を取れることである．ある行動を取れるようになることは，ID の道具の一つである「学習目標の 5 分類（ガニェ）」では「態度」の学習目標として分類される．態度の学習目標の達成は，学習者が実際にその態度を選択する（つまり，実際にその場面に遭遇し，適切な行動を行うこと）までは確認できないため，通常はアンケートなどで「こういうときにあなたはどう振る舞いますか」などと質問することで評価する．この場合，学習者は「正解」を推察できてしまうため，実際に態度の学習目標の達成をしたかしていないかに関わらず，正解ができてしまう．

そこで ID では態度の学習目標の評価自体はアンケートなどに委ねるとしても，その態度を取るための前提となる知識とスキルを習得することを目指した設計を行うことが一般的である．たとえば「重要文書にはパスワードをかけますか？」は態度の学習目標の達成を確認するための質問と言えるが，これに正しく答えられない人はいないだろう．しかし，この質問に対しては「望ましい回答」を推測することが容易であるため、正答したからと言って態度の学習目標の達成をしたとは言えない。本来，この学習目標の達成には，その前提として「どういう文書が重要なのかを判断できる」，「適切な暗号化の方法を選択できる」，「適切にパスワードを伝える方法を選択できる」などのスキルが必

要となり，さらにその前提として「重要な文章とは何か」，「暗号化の方法にはどのようなものがあり，それぞれの特徴は何か」，「パスワードを伝える方法としてどのようなものがあり，それぞれの特徴は何か」という知識が必要となる．その他，「パスワードをかけなかった場合に起こり得る被害」の知識も必要となる．さらに関連して「被害が発生した場合に適切な対処ができる」というスキルを学習目標とすることも考慮する必要もありそうである．

このような前提知識やスキルを習得しないまま「重要文書にはパスワードをかける」という知識だけに基づいて行動すると，本来パスワードをかける必要がない文書にパスワードをかけて無駄な手間を増やしたり，パスワード付き文書をメールで送り，直後に同じ経路でパスワードを送ったりすることが起こってしまう．実際，筆者が体験したこととして，「超極秘文書を送ります．パスワードは次のメールで」というメールに超極秘文書が添付されておらず，パスワードのメールが届いた後に，その「パスワードのメールを引用」した状態で「超極秘文書を添付し忘れましたので再送します」というメールが届いたことがある．

このようなスキルの学習目標のトレーニングでは，「重要文書にはパスワードをかけるべきです」と言う知識をただ提示するのではなく，現実に起こり得る問題場面を示し，それぞれにおける適切な行動を答えさせる練習させることが一般的である．たとえば，複数の文書の例を提示し「これらの文書のうち，どれにパスワードを掛けるべきか」などを問うのである．そうすることで，パスワードをかける必要がある文書とそうでない文書を判断できるスキルが身につく．そのようなスキルが身につけば「パスワードをかける必要」についても認識され，本当に必要なときにパスワードをかけるという態度につながる．

なお，スキルの前提となる知識については，無理に習得させる必要はなく，必要なときにアクセスできればよいと位置づける．むしろ，固定された知識を暗記するよりも，その時の最新の情報は何かを確認して行動を取れるようになることが重要だからである．また，何でも参照できる環境下で受講する e ラーニングでは，知識の評価ができないという実際的な問題もある．

以上のように本 WG においては，サイバーセキュリティ教育においては知識ではなく態度の学習目標を設定すべきであり，その学習目標の達成のために，前提となるスキルを習得することを推奨する．e ラーニングでは知識を確認する問題を出すのではなく，事例に対して知識を応用するスキルを確認する問題を出すことを推奨し，具体的な事例としてのテスト事例をテストリポジトリにて提案する．

5　問題解決のための具体的提案: 共有リポジトリの構築

これまで述べた問題意識と事例を踏まえ，サイバーセキュリティ e ラーニングのための共有リポジトリの構築を提案する．筆者らは所属機関，企業におい

てｅラーニングコンテンツの開発にかかわっており，共通の問題意識を持っている．組織の壁を越え連携することでより良い取り組みが行えるのではないかと考えた．さらに，連携を具現化するプラットフォームとして，次の要件を満たす共有リポジトリの構築を提案する(図 3).

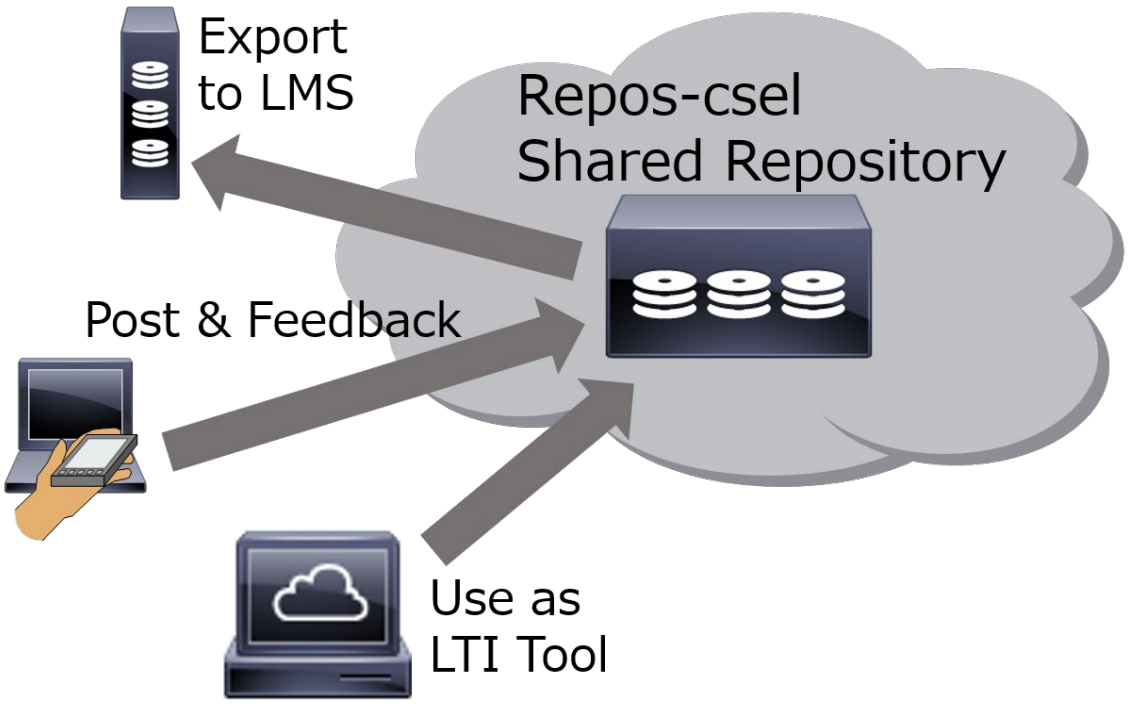

図 3 Repos-csel: Repository for cyber security e-learning 共有リポジトリの概念図

1. サイバーセキュリティ教育に関連するテスト問題を公開・共有する
2. 各組織の事情に合わせテスト問題を選びエクスポートあるいは利用する
3. 実運用の結果をフィードバックする

これらを満たすことができれば，1 章で述べた「受講者に合わせる」ことは各組織の責任において行うことができる．また，同「継続的な更新」という課題についても，複数の組織の作問を集約することにより，有用なリポジトリとなりうる．

6 成果

6.1 共有リポジトリの構築

前節で述べた要件について以下の通り検討を行い， Moodle 3.8 に StudentQuiz プラグインを導入し共有リポジトリ Repos-csel (https://csel.media.hosei.ac.jp) を構築した．

1. テスト問題の管理に適しているのは LMS
2. Moodle は様々な形式で問題をエクスポート可能であり，コース，アクティビティを LTI Tool[18] として利用することも可能
3. Moodle にはコース管理者でなくてもテスト問題を作成，相互評価できるプラグイン(StudentQuiz)[19] が存在する

同リポジトリは次のような運用を想定し，本 WG で作問を行った成果を公開している．

- 各機関のサイバーセキュリティ教育実施者が参加し作問する
- 作成した問題は参加者間で共有し，相互に評価する
- 各機関の事情に合わせ問題をエクスポートする，または LTI Tool として使用する

6.2 テスト問題の公開

同リポジトリに 2021 年 1 月 8 日時点で登録されている全ての問題をエクスポートした Moodle XML ファイル(Moodle_XML.zip)，XHTML ファイル(XHTML.zip)を本報告書とともに公開する．以下，カテゴリ別に問題の例を示す．

6.2.1 ID とパスワード

判断スキル：多要素認証(パスワード認証を複数行うことではない)，すなわち別の認証方式の組み合わせで認証することの有用性を認識する．

問題：職員(学生)A さんは，ある外部の Web システムにおいて，ログイン時に ID とパスワードだけでなく，家族の名前等を質問設定する多段階認証(複数の認証を組み合わせる)を用いていた（SMS・特定のメールアカウントへのワンタイムパスワードも利用できるが，最初の設定が，面倒に感じたので，そちらは利用していない）．ある時，何者かに，ID とパスワードの組み合わせが漏れ，さらに，公人である父親の名前を答えにしていた質問も突破され，Web システム内の情報を閲覧されてしまった．こうした経験に基づき，A さんがとるべき対策について，認証の組み合わせとして，より堅固な多段階認証はどれだと考えられますか？(単一選択)

1. 公人としての父親の名前がバレてしまったので，公人ではない母親の名前をヒントの答えとして設定する．ワンタイムパスワードへの切り替えまでは不要である．

2. 家族の名前は容易に推測されてしまうので，質問設定を「好きな親友の名前」に変更し，さらに，本当の親友の名前でなく，好きな車の名前を答えとして設定する．（断固，ワンタイムパスワードの利用は拒否する．）

3. A さんは，家族想いで，かつ複数の認証を使っていると何となく不安な気もするので，家族も共有しているメールアドレスへ，ワンタイムパスワードが届く認証方式に変更する．

4. 指紋認証のある本人が所有している携帯電話へ SMS でワンタイムパスワードが届く認証方式に変更する．(正解)

6.2.2 e メール

判断スキル：フィッシングかもしれない e メールを処理する際に適切な判断ができるようになる． 問題：情報センターから大学メールサービスの障害通知の連絡メールが届いていた．メールには URL が記載されていた．フィッシング詐欺メールは不安を煽ってパスワードや個人情報を不正に入手するために悪意ある人物が不特定多数に対して送信しているメールだという事実を踏まえて，以下の行動のうち問題があると思うものを選んでください．(1 つまたはそれ以上を選択)

1. URL をクリックするとパスワードを入力するよう表示されたので ID とパスワードを入力した(正解)
2. ブックマークしていた大学メールサービスのリンクをクリックして詳細を確認した
3. 大事なメールが届いていないか心配だったので，メールに記載された URL をすぐにクリックして確認した(正解)

6.2.3 著作権

判断スキル：情報発信時において（資料を参照しながら）法的根拠に基づいて，その行動が適切である理由を述べられる．不適切な場合はどうすれば適切となるかを提案できる．

問題：教員太郎さんはこれまで教室で紙でプリントを配布し授業をしていたが，同じ内容をオンライン型の授業で実施することとなった． 彼の授業では他者が権利を有する著作権を使う必要がある．次の彼の行動として適切なものを全て選びなさい．(1 つまたはそれ以上を選択)

1. 著作権者の許諾を得ずに，自分の自宅から授業時間に著作物の一部を投影した映像を授業の受講者に送信した．(正解)

2. 著作物の一部を投影した授業映像を録画し，著作権者の許諾を得ずに，オンデマンドで受信できるよう URL を学内に公開した．

3. 著作権者の許諾を得ずに，著作物の一部を抜粋して掲載した教材ファイルを LMS 上にアップし，受講者のみがいつでも参照できるようにした．(正解)

6.2.4 Wi-Fi

判断スキル：接続している Wi-Fi ネットワークの暗号強度が低い場合にリスクを踏まえた行動ができる．

問題：太郎君は学会に出席するためにホテルに宿泊した．ホテルの WiFi に接続しようとしたところ，暗号強度の低いサービスであることが分かった．適切な行動を次の選択肢からすべて選択してください．(1 つまたはそれ以上を選択)

1. 学会で発表する資料を教授にレビューしてもらうため，パソコンをホテルの Wi-Fi に接続して，自分の Gmail アドレスから資料を添付してメールを送信した．
2. 学会会場付近の天気が気になったので，スマートフォンをホテルの Wi-Fi に接続して，天気予報サイトを閲覧した．(正解)
3. 学会発表の質疑応答に備えて，大学のサーバに格納している研究データを確認するため，パソコンをホテルの Wi-Fi に接続して学内 VPN に接続した上で，研究データを閲覧した．(正解)
4. 学会会場の場所を確認するため，タブレットをホテルの WiFi に接続し道順を確認した．(正解)

7 おわりに

本 WG は，国立大学法人で進められているセキュリティ基本計画の一環であるセキュリティ e ラーニングの受講率が，全国的に低い傾向にあることに起因し，経験豊富な WG メンバーの知見をまとめて受講率をあげるためのノウハウを集め会員に提供するという目標からスタートした．WG 開始当初は，よくある，飴と鞭方式の是非や，企業である富士通の上長の決め細かいリマインド方式を参考にしたり，文字通りノウハウを集める議論が中心であった．しかし，ある時，e ラーニングの実施方法よりも，設問のクオリティの問題の方の話題になった時に，構成員にとってよい e ラーニングとはという議論の後，単に受講率をあげるノウハウの蓄積よりも，役に立つ e ラーニング，特に設問の作り方に方向が変わった．この時，日本にコロナ禍が来るとは夢にも思っていなかった頃である．その後，単なる記憶に頼らない，実践的な e ラーニングの設問の作成について議論が進んだ．そこで，急に来たコロナ．コロナのおかげで，各組織でオンライン授業が急速に普及した．オンライン授業の実施で苦労する点の一つが，オンラインでの試験である．その中には設問の作成も含まれる．コロナによるオンライン授業，在宅化によって，本 WG 開始時の時と比べてオンラインでの試験受験の敷居はぐっと下がった．現在，各組織でのセキュリティ e ラーニングの受講率はどのようになっているでありうか．受講率よりも，数多くあるオンラインコンテンツの 1 つとして，品質のよいもの，構成員の役に立つものを作成しようとしている組織は多いのではないか．本 WG は，設置

当初よりも少し方向性が変わってしまったが，結果的に現在の状況に役に立つ報告書ができたのではないかと考えている．本報告書がセキュリティにとどまらず，多くのオンラインテスト作成のために役に立てば幸いである．

8 参考文献

1. 上田 浩, 後藤田 中, 平岡 斉士, 金子 晃介, 中村 誠, 松本 多恵, 岡村 耕二, 田口 雅晴, 井上 俊治, 中尾 礼文, 石田 亮介, Repos-csel: サイバーセキュリティ e ラーニングリポジトリの構築の提案, 情報処理学会研究報告教育学習支援情報システム（CLE）, vol. 2020-CLE-30, no. 3, pp. 1–7, http://id.nii.ac.jp/1001/00203613/, 2020
2. IPA，そのメール本当に信用してもいいんですか？, https://www.youtube.com/watch?v=5K9U0-ASQM8, 2017
3. IPA，デモで知る！標的型攻撃によるパソコン乗っ取りの脅威と対策，https://www.youtube.com/watch?v=dSWrKh5FHKA, 2016
4. IPA，情報を漏らしたのは誰だ？ ～内部不正と情報漏えい対策～, https://www.youtube.com/watch?v=5Z_10h2aA8c, 2015
5. IPA，ここからセキュリティ！：セキュリティチェック, http://www.ipa.go.jp/security/kokokara/quiz/, 2020
6. 内閣官房情報セキュリティセンター，情報セキュリティ自己診断チェックリスト，http://www.nisc.go.jp/security-site/files/checklist_20120417_02.pdf, 2012
7. TREND MICRO，is702：クイズで判定あなたのセキュリティレベルは？，https://www.is702.jp/special/1314/partner/12_t/, 2013
8. MOTEX，セキュリティ 7 つの習慣・20 の事例, http://www.motex.co.jp/vision/enlightenment_activity/education_book/, 2017
9. 日本ネットワークセキュリティ協会，知っておきたい情報セキュリティ理解度セルフチェック，https://slb.jnsa.org/slbm/, 2020
10. JPCERT コーディネーションセンター，新入社員等研修向け情報セキュリティマニュアル, https://www.jpcert.or.jp/magazine/security/newcomer.html, 2014
11. 米谷 雄介，後藤田 中，末廣 紀史，小野 滋己，國枝 孝之，八重樫 理人，林 敏浩，香川大学の学内情報基盤に基づくオンライン教育体制の構築と運用，教育システム情報学会誌, vol. 37, no. 4, pp. 308-316, https://doi.org/10.14926/jsise.37.308, 2020
12. 熊本大学総合情報統括センター，熊本大学総合情報統括センター年報 R0/H31(2019)年度暫定版，http://www2.cc.kumamoto-u.ac.jp/koho20xx/main_2019r2.pdf, 2020
13. H. Ueda and M. Nakamura, “GakuNinMoodle: Toward Robust E-Learning Services Using Moodle in Japan,” Procedia Computer Science,

vol. 96, pp. 1710–1719, http://dx.doi.org/10.1016/j.procs.2016.08.219, 2016

14. H. Ueda and M. Nakamura, “Data Analysis for Evaluation on Course Design and Improvement of “Cyberethics” Moodle Online Courses,” Procedia Computer Science, vol. 112, pp. 2345–2353, http://doi.org/10.1016/j.procs.2017.08.204, 2017

15. パナソニックソリューションテクノロジー株式会社. 大学・学校の教職員向けに最適化した「情報セキュリティ教育」, https://www.panasonic.com/jp/business/its/hrd/education/security.html, 2020.

16. 鈴木克明. 教材設計マニュアル: 独学を支援するために. 北大路書房, 2002.

17. 鈴木克明. インストラクショナルデザインの基礎とは何か: 科学的な教え方へのお誘い. 消防研修（特集：教育・研修技法）, Vol. 84, pp. 52–68, 2008.

18. IMS Global Learning Consortium. Learning tools interoperability, https://www.imsglobal.org/activity/learning-tools-interoperability, 2019.

19. Frank Koch. StudentQuiz - Empowering Students, MoodleMoot Global 2019, https://moodle.com/wp-content/events/mootglobal19/StudentQuiz-EmpoweringStudents.pdf, 2019.