

情報セキュリティポリシーの実質化に向けた取り組み

石黒 克也, 岡谷 英明

高知大学 学術情報基盤図書館

ishiguro@kochi-u.ac.jp

Initiatives to ensure the practical implementation of information security policies

Katsuya Ishiguro, Hideaki Okatani

Library and Information Technology, Kochi Univ.

概要

高知大学では情報セキュリティを確保するため、情報セキュリティポリシーおよび情報セキュリティポリシー実施手順を策定している。本稿では、研修および自己点検を通じた情報セキュリティポリシーの実質化に向けた取り組みを報告する。

1 はじめに

高知大学では、平成9年度(1997年度)よりノートPCの必携化を実施しており、学生は各自のPCを学内に持ち込んで授業や課外活動等に利活用している。[1-4] 大学では、必携化とともにPCを用いた情報教育を共通教育必修科目として開講しており、その中で情報セキュリティ教育も実施している。情報セキュリティ教育に関する大学全体の取り組みとしては、2004年に高知大学情報セキュリティポリシーの初版が策定されており、現在までに数回改定されている。また、2017年には高知大学情報セキュリティポリシー実施手順が学内の各部局ごとに定められている。

本報告では、高知大学で定められている情報セキュリティポリシーに基づいたセキュリティ教育に関する近年の取り組みについて報告する。

2 情報セキュリティポリシー

2.1 情報セキュリティポリシー

高知大学では情報セキュリティ対策を全学的に円滑に進めるため、全学情報セキュリティ委員会の承認のもと、高知大学情報セキュリティポリシーを策定している。初版は2004年に策定され、2025年現在は第4版に改定されている。ポリシー策定の主な目的は、情報セキュリティインシデントから大学の情報資産を守り、情報セキュリティを損ねる加害行為を防止し、情報倫理・情報セキュリティ教育を実施することで、大

学の情報セキュリティを確保し、社会的信頼を保つことである。

情報セキュリティポリシーは「基本方針」と「対策基準」から構成されている。「基本方針」は情報セキュリティに対する基本的な考え方を述べたもので、「対策基準」は「基本方針」に定められた情報セキュリティを確保するための判断基準を示したものである。

2.2 情報セキュリティポリシー実施手順

情報セキュリティポリシーの「対策基準」に定められた内容を具体的に実行していくために、情報セキュリティポリシー実施手順が策定されている。初版は2017年に策定され、現在は第4版となっている。情報セキュリティポリシーは全学で統一した内容となっているが、実施手順に関しては学部やセンター、事務局等の個々の事情を考慮して、各部局ごとに策定されている。策定主体は各部局の情報セキュリティ委員会である。

実施手順には、大学の情報資産をどのようにして守り、どのように社会的信頼を保っていくのか、それらを行うための教育をどう実施するのか、などの具体的な方法が記されている。

2.3 情報セキュリティ研修

高知大学では情報セキュリティ対策の一つとして、情報セキュリティ研修を行っている。研修の主なものとして

- 新入生情報セキュリティ講習会(4月)
- 新留学生情報セキュリティ講習会(4月、9月)

- 新採用職員情報セキュリティ研修（4月）
- 教職員情報セキュリティ研修（3月）
- 役職員情報セキュリティ研修（3月）

などが挙げられる。新入生向けおよび新留学生向けの情報セキュリティ講習会は、大学においてPCやスマートフォンを学内ネットワークに接続する上で守るべきあるいは知っておくべき事項について、入学直後に学ぶことでその後の利用がスムーズにできるように行うものである。これらの講習会では、大学の情報セキュリティポリシーおよび実施手順について解説し、実施手順に従ったPCの設定等についても各自のPCにて実施させており、これにより学生の持ち込みPCにおいても最低限のセキュリティ設定ができるようにしている。教職員・役員向けの研修では主に近年のセキュリティ業界の状況や大学におけるインシデント事例などを通じて、セキュリティ意識を啓蒙している。

2.4 自己点検

情報セキュリティポリシー実施手順では、様々なセキュリティ対策の具体例が示されているが、それと同時に実施手順が適切に実施されているかを確認するため、実施手順の評価をすることが定められている。その評価のため、大学の全構成員に対して自己点検を実施している。自己点検については、次節にて詳細を記す。

3 実施手順自己点検および情報セキュリティ研修

3.1 これまでの実施手順自己点検

情報セキュリティポリシー実施手順において、部局等情報セキュリティ委員会は実施手順が適切に実施されているかどうかを確認するため、定期的に実施手順自己点検を行うことが定められている。大まかな流れとしては、全学情報セキュリティ委員会とCSIRTにより自己点検の内容や実施方法が決められ、部局等情報セキュリティ委員会から各部局構成員に対して自己点検を行うよう指示がなされる。自己点検後には各部局での点検結果を部局等情報セキュリティ委員会にて考察し、全学情報セキュリティ委員会にてまとめた上で、次回以降の自己点検につなげていく。

第1回の自己点検は、情報セキュリティポリシー実施手順の初版が策定された2017年3月に実施された。自己点検には当時既に本学にて稼働していたLMS(moodle)を使用した。LMSには全ユーザが登録されており、集計のためのデータ取得も可能であっ

たためである。実施周知の際には、CISO名で各部局に通達を行い、同時に学生には教務システムにて通知を行った。第1回は周知方法や自己点検に使用するシステムの動作も含めて試行的に行ったため、全体の実施率がわずか5.7%であった。実施率は部局により異なり、教職員の場合には多い部局で約70%、少ない部局は15%程度にとどまった。学生には教務システムを用いた掲示のみであったことと、実施時期が春期休暇中の3月であったこともあり、どの学部でも1%に満たない実施率であった。

第2回の自己点検からは実施時期を変更し、教職員は5月に、学生は4月から5月にかけて実施することとした。特に新入生に対しては必修授業である情報処理の授業内で実施することとし、2年生以上の学生に対してはオリエンテーション等で周知を呼び掛けてもらうようにした。これらを実行したところ、第2回の全体実施率は31.6%に上昇した。特に新入生に対しては授業で周知したことにより、80%を越える実施率となった。しかしながら、2年生以上の在校生や教職員の実施率についてはまだまだの状況であった。

第3回（2020年度実施）から第7回（2024年度実施）までの結果を含めた実施率のデータを図1に示す。これを見ると、第3回実施時に教職員の実施率が急激

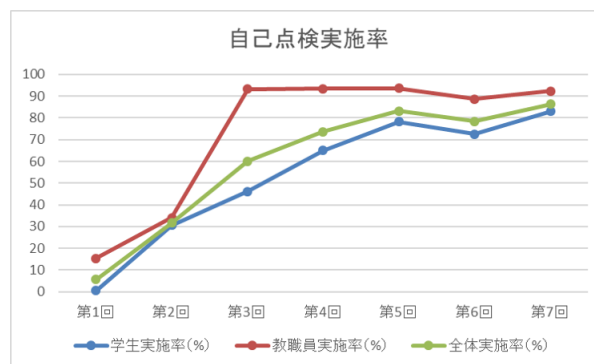


図1 情報セキュリティポリシー実施手順自己点検実施率

に上昇していることがわかる。各部局責任者からの通知がなされたことも原因のひとつであるが、さらに影響が大きいと思われるのがコロナ禍である。自己点検を実施するシステムとしてLMSを採用していたが、コロナ禍が起こる以前にはLMSを利用している教職員がそれほど多くはおらず、その存在自体があまり知られていないような状況であった。そのため、LMSで自己点検が行われても、システムになじみがなく、実施率が低くなってしまっていたと思われる。第3回はコロナ禍において最初の自己点検実施回であり、LMS

の存在が大きくクローズアップされた時期であったため、LMS での実施に違和感がなくなったものと推測される。学生の実施率が大きく変化していないのは、第 2 回と同様に 2 年生以上の学生の実施率が低いためである。第 4 回以降も周知方法に工夫をし、未実施者には各部局責任者からリマインダーを送付するなどして、実施率は徐々に高くなっている状況である。なお、自己点検実施システムとして、第 1 回から第 4 回までは LMS (moodle) を使用したが、第 5、6 回では Microsoft Forms を用いた。これは学内で Form の使用率が高まり、スマートフォンから手軽に実施できるのではと考えてのことである。しかしながら、Forms よりも LMS の方が集計しやすく、LMS の使用に不慣れなものも少なくなっているため、第 7 回からは再度 LMS にて実施をしている。

3.2 2025 年度の試み

第 8 回 (2025 年度) の自己点検は 2025 年 10 月 1 日から 11 月 30 日にかけて実施予定である。例年、自己点検は 4 月から 5 月にかけて行われていたが、これとは別に情報セキュリティ研修が 3 月に実施されていた。しかしながら情報セキュリティ研修と情報セキュリティポリシー実施手順自己点検は密接に関連しており、同時に実施することでより効果が上がると考えられるため、試行的に 10~11 月に実施することとした。2026 年度はこれまで同様、年度初めの 4~5 月に実施予定である。

第 8 回からの新たな取り組みとして、情報セキュリティ研修と自己点検の未実施者に対して学内システムの利用制限を課すこととした。自己点検はこれまで 7 回実施されており、必修授業内での実施やオリエンテーションでの周知、実施期間中の未実施者へのリマインダーなどを行うことで、実施率を向上させてきた。しかしながら、自己点検未実施者の中には自己点検が行われていることを知りつつも実施しないものが一定の割合で存在し、これにより本来 100% の実施率となるのが望ましいものの、未達成の状況が続いている。そのため、CISO を議長とした全学情報セキュリティ委員会の議論を経て、2025 年度より自己点検未実施者への学内システム利用制限を実施することとした。未実施者に対する利用制限の話自体は、最初の本格的な実施となった第 2 回の後の全学情報セキュリティ委員会にて既に話題になっていたものの、当時は実施率が低く、対象者に対する周知がまだまだ不十分であったこと、システム利用停止の仕組みがないことなどから実施が見送られてきた。自己点検の回数を経るにつ

れて徐々に実施率が高くなり、周知方法にも工夫をこらすことにより、現状のやり方で未実施のものはほぼ自己点検があることを知りつつ実施していないものと見なしてよいのでは、との合意が委員会にて得られたため、2025 年度より未実施者に対する学内システム利用制限のペナルティを課すこととなった。なお、これまでに実施されてきた情報セキュリティ研修は、新入生向けおよび留学生向けのものを除くと対象者は教職員であり、受講率は 70% 程度であった。

2025 年度の情報セキュリティ研修および自己点検は次の内容で実施する予定である。対象者は情報セキュリティポリシー適用者であり、本学構成員のみならず学外者も含めて本学の情報資産にアクセスするすべてのものとする。実施システムとして、研修および自己点検用の LMS(moodle) を構築している。具体的な実施内容は次の 3 点で構成される。

- 情報セキュリティ研修 (動画) の受講
- 各部局情報セキュリティポリシー実施手順の確認
- 情報セキュリティポリシー自己点検の実施

受講対象者が具体的に実施することを記載した情報セキュリティポリシー実施手順は、学内の各部局ごとに定められているため、多数の実施手順書が存在する。そのため、それらの実施手順をすべて LMS に掲載し、各自が遵守すべき内容を確認できるようにする。また、LMS 上に研修用動画および資料を掲載し、受講対象者はそれらを視聴することで、実施手順に書かれている内容の把握、および自己点検時に知っておくべき事項について学ぶことができる。自己点検は期間内であれば何度でも実施可能とする。前述したように、2025 年 10 月 1 日~11 月 30 日が研修および自己点検の期間であり、その間何度か受講状況を確認し、未実施者に対しては実施を促すよう通知を行う予定である。研修および自己点検の期間中に未実施のものについては、2025 年 12 月 1 日より学内システムの利用制限を開始する。利用制限の内容は次の通りである。

- 学内各種システム利用不可 (教務情報システム、学習管理システム moodle、e ポートフォリオなど)
- 学外契約サービス利用不可 (Microsoft 365、Google Workspace など)

利用者が学内ネットワークに接続する場合、まず最初にポータルサイトに入り、その後各種システムにアクセスをする。利用制限がかかっている場合には、ポータルサイトにて要研修・要自己点検の表示がなされ、

上記利用不可サイトにはアクセスできない。学生の場合、これらのサービスを利用できないと授業等で即支障のある状態になってしまうため、強めの制限と言える。教職員の場合は業務上の理由で一部利用できるシステムがあるものの、やはり普段よく使用するシステムが利用できないために苦慮する状況になってしまう。もし利用不可の状態になっても、研修と自己点検を実施すれば、1時間以内に利用不可は解除され各種システムを利用可能となるため、ペナルティ解除の壁は高くない。

3.3 情報セキュリティ研修

これまでの情報セキュリティ研修は、基本的な内容に時事的なものを含めて動画を作成し、オンデマンド形式で行っていた。2025年度は情報セキュリティポリシー実施手順自己点検に合わせて行うことにしたため、研修の内容も自己点検に合わせたものとした。動画の作成には国立情報学研究所の学認 LMS サービスのひとつである学認 PtM [5]を使用した。学認 PtM は合成音声付き動画教材作成システムで、パワーポイントを利用した教材にナレーション用のノートを書き込み、システムにアップロードするとナレーション付き動画を作成するものである。合成音声の調整には SSML タグと Speech Markdown を利用することができ、話す速度やアクセントなどを細かく調整可能である。また日本語だけでなく、英語にも対応可能なため、今回の研修では日本語版と英語版の両方を作成した。これまでの研修では、人力で音声入力を行って動画化していたため、英語版の作成まで手が回らなかったのだが、学認 PtM を利用することにより容易に研修動画を作成できるようになった。

3.4 実施手順自己点検

情報セキュリティポリシー実施手順自己点検の内容は、毎年の回答状況や情報セキュリティ委員会からの意見を参考にして見直しを行っている。また、実施手順の改定があった場合にはそれに合わせて自己点検の内容も変更している。自己点検は実施手順に書かれた内容を実施しているか確認するためのもので、特に難しいものではない。ただし、PC 関連の用語や設定方法に慣れていないものにとっては設問内容がわからないということも考えられるため、各設問に対してフィードバックにて説明を行い、設定が必要なものに対しては設定方法までフィードバックに付け加えた。自己点検は何度でも実施可能なため、設問内容がわからず不満足な回答となってしまった場合でも、フィードバックを読むことでそれが解消できるようになって

いる。自己点検に関しても、セキュリティ研修と同様に英語版を作成し、留学生等の便宜をはかっている。

3.5 2025 年度の状況

2025 年度の情報セキュリティ研修および自己点検は前述したように 10 月 1 日から開始されるため、本稿執筆時点ではまだ開始されておらず、データ等が得られていない。システム自体は moodle と ID 管理システムを連携することで作られており、動作確認中である。2025 年度 AXIES 年次大会の際には、実施状況を報告する予定である。

4 おわりに

本稿では、高知大学において実施されている情報セキュリティ研修および情報セキュリティポリシー実施手順自己点検について報告した。2024 年度までは研修と自己点検が別個に行われていたが、2025 年度からは内容も合わせて同時に実施することとした。また、研修および自己点検の未実施者には、学内システムの利用制限をかけることで、研修受講率・自己点検実施率の向上をはかることとした。これにより、情報セキュリティポリシーの実質化がなされることを期待している。今後は、同システムを用いて入学前情報セキュリティ研修などを行い、大学構成員が入口の段階で持ち込むセキュリティ上の危険性を軽減することができるよう検討している。

参考文献

- [1] 佐々木 正人、石黒 克也、佐々 浩司、“高知大学における情報セキュリティ教育の現状”、2017 年度大学 ICT 推進協議会年次大会論文集、WF2-4 (2018)
- [2] 佐々木 正人、石黒 克也、佐々 浩司、“高知大学における新入生に対する情報セキュリティ教育の改善”、2019 年度大学 ICT 推進協議会年次大会論文集、SF1-2 (2020)
- [3] 佐々木 正人、石黒 克也、佐々 浩司、“コロナ禍における新入生対象情報教育の取り組み”、2020 年度大学 ICT 推進協議会年次大会論文集、TA1-5 (2021)
- [4] 石黒 克也、佐々木 正人、岡谷 英明、“高知大学における新入生を対象とした情報セキュリティ教育”、2024 年度大学 ICT 推進協議会年次大会論文集、12AM2E-3 (2025)
- [5] 学認 PtM, <https://ptm.nii.ac.jp/>、(2025 年 9 月 23 日閲覧)