大学間の情報セキュリティに関する連携体制の構築と深化

中田 亮太郎 [1)], 大足 恭平 [1)], 松村 芳樹 [1)], 菅原 光 [1)],
土屋 英亮 [2)], 矢崎 俊志 [2)], 根本 貴弘 [3)], 佐藤 亮介 [3)], 桝田 秀夫 [4)]

1) 一橋大学 情報基盤センター
2) 電気通信大学 情報基盤センター
3) 東京農工大学 総合情報メディアセンター
4) 京都工芸繊維大学 情報基盤センター

nakata.ryotaro@r.hit-u.ac.jp

Establishing and Further Developing for Information Security Cooperation Among Universities

Ryotaro Nakata[1)], Kyohei Oashi[1)], Yoshiki Matsumura[1)], Koh Sugawara[1)],
Hideaki Tsuchiya[2)], Shunji Yazaki[2)],Takahiro Nemoto[3)], Ryosuke Sato[3)], Hideo Masuda[4)]

1) Center for Information and Communication Technology, Hitotsubashi University
2) Information Technology Center, The University of Electro-Communications
3) Information Media Center, Tokyo University of Agriculture and Technology
4) Center for ICT Services, Kyoto Institute of Technology

概要

大学における情報システムや各種サービス、インターネットの利活用が引き続き拡大している。これに伴い情報セキュリティ対策の重要性は年々高まっているが、各大学が情報セキュリティの維持・管理に割ける人的・経済的リソースの停滞や低下が顕在化しており、多岐にわたる業務の負担が拡大している。特に、高度な専門知識を持つIT 人材やセキュリティ人材の確保や各種施策を実施するためのコスト確保は多くの大学で喫緊の課題となっており、新たな施策の必要性によるシステムやサービスの導入に要するコストの確保も課題となるなど、各大学の情報セキュリティ施策の限界を浮き彫りにしている。こうした背景から、一橋大学、電気通信大学、東京農工大学、京都工芸繊維大学の 4 大学は、共通するセキュリティ課題への効果的な対応と運用負荷の軽減を目指し、2023 年より情報セキュリティに関する包括的な連携活動を開始した。昨年度の AXIES2024 では、本連携体制の構築と初期成果について報告を行い、大学間連携の概要を示している。本稿では、連携開始から 2 年目となる活動成果を整理し、持続可能な大学間情報セキュリティ連携モデルの確立に向けた知見を提供する。

1 はじめに

大学におけるデジタルトランスフォーメーション（DX）の推進が加速する中、情報システムやインターネットの利活用範囲は飛躍的に拡大している。文部科学省の学術情報基盤実態調査によると、大学における情報システムのクラウド化は継続的に進展しており、2021 年度時点で 93.2% の大学が導入しているなど、システムやサービス、およびネットワークへの依存度が高まり、同時にセキュリティリスクの増加も課題となっている [1]。

このような情報化の進展に伴い、情報セキュリティ対策の重要性が年々高まっている中、各大学が対策の維持・管理に割ける人的・経済的リソースには深刻な制約が生じている。国立大学法人情報系センター協議会（NIPC）の 2023 年〜2025 年資料分析では、情報セキュリティを課題として認識する大学の割合が 74.6% から 83.1% に増加する一方で、「専門人材の確保困難」を挙げる大学は 41.8% から 62.3% に急増するなど、深刻さを増している [2]。

現在の大学情報セキュリティを取り巻く課題は、(1) 人材確保の困難さ、(2) 予算制約と費用増加、(3) 技術的複雑化、(4) 組織的ガバナンスの課題など多岐にわたっている。情報セキュリティに限ったことではない

が、情報システム・サービスの運用全般に関して専門人材の絶対数不足や大学と民間企業との待遇格差などの人的リソースの問題や、円安と物価高騰などに起因するシステム導入・更新費用の増加など経済的リソースの問題があり、大学内でこれらの対応を担う部局（主に情報系センター）の運営は厳しさを増している。

こうした課題への対応として、複数大学間での連携による活動が行われ、情報セキュリティに関する活動も地域での小規模なものから国立情報学研究所のNII-SOCS[3] 等、国レベルの取り組みまで存在するが、本活動は、中規模専門大学間での新たな連携モデルとして位置付け、2023 年より活動を行なっており、密度の濃い情報共有と迅速な意思決定を両立できる適正規模と位置付け活動を進めている。

本稿では、連携開始から 2 年目となる活動成果を整理し、持続可能な大学間情報セキュリティ連携モデルの確立に向けた成果を述べる。

2 大学における情報化と情報セキュリティの状況

2.1 国立大学の情報セキュリティに関する経緯

国立大学における情報セキュリティ対策は、2016 年の文部科学省通知「国立大学法人等における情報セキュリティ強化について」を起点として段階的に強化されてきた。同通知では、中長期的な視点による情報セキュリティ対策基本計画の策定とその組織的・計画的な実施、インシデント対応体制及び手順の整備、情報セキュリティに関するポリシー及び関連規程の周知等が対策として示された。

2018 年の政府サイバーセキュリティ戦略改定を受け、2019 年には「大学等におけるサイバーセキュリティ対策等の強化について」が通知され、大学等に対し一定レベルのサイバーセキュリティ対策の実施が求められるとともに、科学技術競争力や安全保障等に係る技術情報の保護が促進された。

2022 年には「大学等におけるサイバーセキュリティ対策等の継続的な取り組みについて」が通知され、リスク管理体制の構築やサプライチェーンリスクへの対応、インシデント対応体制の構築などが新たに示され、継続的なサイバーセキュリティへの取り組みが求められるようになった。

2024 年 12 月 25 日には「大学等におけるサイバーセキュリティ対策等の継続的な取組について（通知）」が改めて発出された [4]。この通知では、大学等から報告されたインシデントの約半数が「メール誤送信や情報の意図せぬ公開など、基本的な情報セキュリティ対策の未実施や意識の欠如に起因する」ことが示され、人為的ミスを防ぐ組織体制の重要性が強調されている。また、ランサムウェア等による情報流出被害の増加が指摘されており、サイバーセキュリティ対策が重要な経営課題として位置づけられている。

同通知では、サイバーセキュリティ対策において考慮すべき事項として、CISO（最高情報セキュリティ責任者）の役割強化、経営判断体制の整備、ゼロトラストアーキテクチャの検討、生成 AI 利用に関するガイドライン策定などの新たな要求事項が提示されている。

これらの政策変遷は、大学を取り巻くサイバーセキュリティ環境の急速な変化と脅威の高度化を反映している [5]。特に最新の通知では、従来の技術的対策に加えて、経営層のコミットメント、組織的な意識向上、新技術（生成 AI 等）への対応、ゼロトラストアーキテクチャの検討など、多岐にわたる要求事項が示されており、大学におけるサイバーセキュリティ対策の複雑化・高度化が進み、対策の重要性が増していることがわかる [6]。

2.2 国立大学の情報系組織の運用と課題

国立大学を取り巻く情報化や DX の推進においては、セキュリティに限らず多くの課題を抱えている。大学現場が実際にどのような課題に直面しているかを近年の国立大学情報系センター協議会（NIPC）資料をもとに表 1 の通り分析した。

- **情報セキュリティ**
  情報セキュリティに関しては以前から多くの大学が課題として認識をしており、基本的な体制構築や人材確保の面から、規定等の制定、大小インシデント対応、最新動向や技術の確認など、多岐にわたる業務の負担が顕在化している。サイバーセキュリティ対策基本計画などにより大学全体の方針・取り組みとして位置付けられていても、実業務の大半が情報系センターに集中するなどの場合も多く、大学特有の事情も相まって多くの大学で人的・経済的なリソース不足が顕著になっている。
- **人的リソース**
  情報セキュリティや DX といった情報分野・情報系センターに直結する業務は増加の一途をたどっているが、そこに対する人的補償多くの場合十分に行われておらず、多くの大学で専門人材の不足、育成の困難さ、業務の属人化、または人員配置に

表 1 国立大学の情報系センターにおける課題項目の分類とその言及割合

課題	2023	2024	2025	主な内容
情報セキュリティ	74.6%	82.1%	83.1%	CSIRT体制構築・運用/CS対策基本計画改訂/インシデント対応の増加/ゼロトラスト対応
人的リソース	41.8%	53.7%	62.3%	IT専門人材・セキュリティ人材の確保困難/技術職員の慢性不足/業務範囲拡大と人員削減のギャップ
予算制約・物価高騰	22.4%	38.8%	53.2%	調達価格の2-3倍増や保守・運用費の増加/MSライセンス値上げ/VMwareライセンス高騰による仮想基盤見直し
技術的複雑化	52.2%	56.7%	58.4%	生成AI利活用への対応/研究データ管理（RDM）構築/DX推進への対応/システム統合
組織的ガバナンス	26.9%	32.8%	45.5%	持続可能な運用体制構築/DX推進組織の統合/情報システム整備方針の策定/全学的ICT戦略の高度化
調達・運用面	52.2%	56.7%	57.1%	入札参加ベンダーの減少/仕様書作成人材の不足/調達期間の長期化/システム分離調達の増加

関する課題を報告している。この問題は、技術職枠での採用がないため一般事務職員が情報システム業務を担当せざるを得なかったり、任期つきの教職員のみによる運用や定期的な人事異動により知識・技術の継承が滞るという構造的な問題が根底にあり、人材不足の深刻度は年々増している。また「国立大学法人と民間企業との待遇の差は大きく、IT スキルを有する人材の確保が難しい」との状況が報告されており、人材確保の困難さがより広範な大学に波及していることがわかる。

- **予算制約・物価高騰**
  物価高騰と円安の影響が継続的に大学財政を圧迫しており、とくにここ数年でシステム導入や更改が不調に終わることも見られ、急激に課題として認識が大きくなっている。具体的な影響として、システム構成の大幅な見直しやサービスの縮小、セキュリティレベルの低下が避けられないとの報告や、パソコン実習室廃止、オンプレミス全学メール廃止といった運用変更を迫られている事例も報告されている。システムの導入や更改・運良等にかかる費用は 1.5〜2.0 倍が当たり前になるほどとの具体的な数値も示されており、この傾向は継続している。
- **技術的複雑化**
  技術的課題は以前から多くの大学が認識しているが、特に近年注目すべき変化は生成 AI 関連課題への言及の急増である。NIPC2024 総会のテーマとして取り上げられたこともあるが、課題意識としては年度ごとに倍増する保ペースで増加しており、情報漏洩リスク、著作権侵害、教育における評価方法など、より具体的な課題認識が示されている。また、Microsoft 365 や Google Workspace などのクラウドサービス運用では、機能の過多、管理の複雑さ、容量逼迫による追加費用の問題が多数報告されている。ある大学では容量逼迫により卒業生へのサービス提供終了を検討せざるを得ない状況となっており、これまで拡大してきたサービス範囲の見直しや変更が現実的課題となっている。
- **組織的ガバナンス**
  情報セキュリティにも関連するが、組織的ガバナンスに関する課題も増加している。運用体制を構築しても、一時的で持続的な体制がとられていなかったり、DX 推進等による組織の変化・統合やそれに伴う対応の増加・高度化等、組織全体の ICT 推進等の変化が生む負の効果も報告されている。個々のインシデント対応においてはユーザの無理解や誤解、当該部局の対応により、法人としての定型化した措置を講じにくい状況や、部局間の縦割り意識が連携を阻害するといった組織文化に起因する課題が広く報告されている。
- **調達・運用**
  予算制約や物価高騰による調達・運用の困難さもあるが、要求事項の複雑化・高度化に伴い、入札に参加する（できる）ベンダーの減少や仕様書の策定が可能な人材の不足、調達期間の長期化などによる制約など、直接的なコスト以外の面でも課題が多くなっており、業界的にも大きな課題になっている。

表 2 連携を推進する各大学の概要

大学	教職員数/学生数（概数）	教育研究分野	キャンパス	担当部局
一橋大学	700/6000	社会科学	東京都千代田区/国立市/小平市	情報基盤センター
電気通信大学	500/5000	情報理工	東京都調布市	情報基盤センター
東京農工大学	650/6000	農学・工学	東京都小金井市/府中市	総合情報メディアセンター
京都工芸繊維大学	400/4000	工芸科学	京都府左京区/右京区福知山市	情報基盤センター

多くの課題が顕在化しているが、情報セキュリティに関しては特に課題があると認識する大学が 8 割に上っており、全体でも突出している。各大学の要望について詳しく確認すると、小規模〜中規模大学間での CSIRT 連携体制の構築や、セキュリティ知見の共有を支援する仕組みの整備が具体的に要望されていたり、これまでの連携事例を見ると 15 大学以上が他大学・外部機関との連携に言及しているが、小規模な相互監査や情報交換に留まっている。大規模な協議会等への参加困難さについては多くの大学が人的リソースの不足と業務負担の増大を訴えており、大規模連携への参加阻害要因となりうることも示唆されている。

地理的要因については、課題の傾向に顕著な違いは見られず、情報セキュリティ課題が特定地域に限定されない全国共通の構造的問題であることが確認された。地域をまたいだ連携事例も報告されており、地理的距離を超えた連携の実現可能性も示されている。

これらの内容から、特に類似の規模感と特性を持つ中規模専門大学にて、密度の濃い情報共有と迅速な意思決定を両立できる適正規模で連携する新たな連携モデルを検討した。単独対応の限界と大規模連携の実効性の課題を踏まえ、中小規模大学に持続可能な連携体制の構築を目指し、大学における情報セキュリティ課題解決へ向けた方法の一つとして連携活動を開始した。

3 情報セキュリティ連携体制の深化と制度化

3.1 連携体制の発展経緯と 2 年目の活動

本連携活動に参加している各大学の概要を表 2 に示す。各大学ともに学生数 4,000〜6,000 名程度、教職員が概ねその 1/10 程度となっており、学問領域も専門性をもった中規模大学と分類できる。情報セキュリティやシステム運用など、情報系センターが関連する業務等での課題や取り組みの内容も類似しており、もともと教員間での交流も盛んであった。

情報セキュリティに関する連携活動としては 2023 年の発足から 2 年目を迎え、当初の実験的な取り組みから持続可能な連携モデルへの発展を目指し活動を継続している。発足当初の背景として、各大学が従来より行なっていた相互監査や情報交換会等の個別連携を実施してきたが、前章で示したような構造的課題の深刻化により、より多角的で継続的な協力・連携体制の構築は共通の課題として認識されており、特に共通の特性を持つ 4 大学が、個別の課題解決から共通課題への組織的対応へと連携の質的転換を図ることに現場レベルで合意し、活動を開始した。

連携活動の 2 年目までの成果として、連携活動の範囲拡大と深化が挙げられる。当初の個別大学間の相互監査や情報交換から、役職者向け研修の共同実施、外部機関との連携強化、技術課題への共同対応等、より包括的な連携活動へと発展している。また、日常的な情報共有の場を設けることにより、脅威情報共有や技術的課題の相談のみならずそれぞれの大学の組織面やガバナンス、監査体制などさまざまな相談・質問等が常態化し、連携の実効性が向上している。

3.2 協定書の正式化と運用原則の確立

2 年目の重要な成果として、連携活動の制度的基盤の確立が挙げられる。発足当初から正式に協定の締結に向けて準備を進めていたが、昨年も示していたこれまでの案（旧案）では以下のような課題があり、特にセンター間の現場レベルでの合意よりもさらに進んだ大学間での合意として進める際に課題として浮き彫りに

なったため、内容を見直した上で新たな協定書案（新案）として確認を行なっている。

- **各大学の負担**
  本活動はもともと各大学で実施していたことや大学間で既に実施していたことを、4 大学間での相互実施に拡大するものであり、新たな人的・経済的リソースの負担を極力抑えた形で進めることを目指していたが、明確な各大学のメリットや負担がわかりにくく、学内での確認において懸念が示されることがあったため、本活動そのものによる新たな金銭的負担を設けないことと、個別の取り組みにおいて負担が必要な場合は事前の合意のもとで実施することを明記した。なお、本活動で発生する各大学の人的・経済的負担は、本来の情報セキュリティ関連活動において必要な業務の範囲を逸脱しないことを基本としており、本活動によって本来発生しないはずの過度な費用負担を求めるものではない。
- **機微情報の扱いとチャタムハウスルール**
  旧案においては、各大学の情報セキュリティやインシデントに関する情報も含めて共有可能とすることのみに触れており、その方法や内容については明記せず、通用ルールとしてチャタムハウスルールを適用することで担当者間で確認していたのみであった。しかし、この点も各大学での確認で大きな懸念点となったため、原則として各大学の情報セキュリティポリシーや関連規定等が優先されることを明記し、各大学の情報セキュリティ関連活動の延長線上として協定/活動を進めることを明確化した。
- **持続可能性の検討**
  本活動は情報セキュリティの向上という共通目的のための協働活動であり、増加・高度化を続けるさまざまな脅威やリスクに対応するため今後も継続した体制の維持が求められるが、前章で示したように情報系センターや CSIRT など、大学の情報セキュリティを担う部門における人材の確保や育成および体制確保・維持は大きな課題となっており、参加大学間でも大きな差があるため、発足時のメンバーの維持はもちろん、継続的な協力体制確保も大きな懸念点となっている。そのため、CISO を含む経営層レベルでの合意を基本とし、かつ各大学で運用担当者を 1 名以上指名することで、協定の継続性の確保と現場レベルでの活動の推進を促すこととした。

これらの内容を検討し、新案として表 3 の通りの内容を定義した。

表 3 新たな協定案の内容

条項	内容	詳細
1条	趣旨	協定の趣旨・目的
2条	基本原則	活動に関する基本原則
3条	運用の主体組織	各参加大学における 本活動の主体組織・部局等
4条	活動内容	現在の活動および想定しうる 今後の活動や情報交換範囲
5条	機微情報の扱い	各大学の関連規定の優先と チャタムハウスルールの適用
6条	秘密保持義務	秘密保持義務の範囲と 終了後の効力継続義務
7条	他大学・機関協働	参加大学の他大学・機関との 協働・協力・各種活動等
8条	運用体制	本協定に関する活動の運用
9条	費用負担	費用負担の原則
10条	責任制限	活動に起因する損害発生の 場合の責任範囲
11条	協定内容の変更	協定内容の変更可否と方法
12条	脱退	脱退の場合の方法や手続
13条	有効期間	協定の有効期間と延長
14条	協議解決	定めのない事項の解決

この新案は今年度中の締結を目指して現在各大学にて内容に問題がないかを確認中である。

4　情報交換会の開催

今年度の特筆すべき活動として、2025 年 6 月 27 日に開催された「情報セキュリティに関する情報交換会」がある。

発足当初より、参加大学の関係者で集合した情報交換会の開催を模索していた。以前から一橋大学と東京農工大学間では教職員同士がそれぞれの大学を訪問してセンター運営や情報セキュリティに関する情報交換・意見交換を行なっていたが、それを発展させつつ参加大学全体での積極的な情報交換の促進のため、かつ地理的に離れた京都工繊大へ不利にならないことも考慮し、当初は京都での情報交換会開催に向けて検討を行っていた。

図 1: 情報交換会の内容（プログラムより抜粋）

しかし、それぞれの予定を合わせることの困難さや、本活動のみに割ける人的・経済的リソース確保の困難さもあったことから、関係者が多く集う予定であった国立大学情報系センター協議会（NIPC）総会の機会を利用し、今年度開催地であった広島大学周辺で NIPC 総会の翌日に集合し、来られない方もオンラインで参加してもらう形で進めることになった。

NIPC 総会は本活動の中心となる各大学の情報系センター関係者が多く集う場であり、かつ全国の大学の活動状況や課題が共有できる場であり、セキュリティに関する連携活動を進める上でも重要な情報収集の場でもあるため、その翌日の情報交換会の開催は各大学の負担を最小限にしつつ、最大限の効果を得られる場としても有効であると考えられる。

なお、本来情報交換会で想定していた内容は各大学の取り組みや課題の共有、この後の共通した取り組みや運用体制に関することなどであるが、AXIES2024 年次大会の際に NII-SOCS の方々にお声がけいただき、ヒアリング会の開催も模索していたことから、この機会に実施できないかとお声がけしたところ広島まで来ていただいての開催が実現することとなった。

また、筆者が別途交流のあった国立高専機構や、NICT の CYDER ご担当者の方々にセキュリティ関連での最新動向・情報交換として有用な情報をいただけないかお話している中で、セキュリティに関する取り組みには積極的に協力したいとのありがたい申し出をいただき、それぞれ広島まで来ていただいてご講演いただくことになるなど、当初の予定を大幅に変更して急遽他の大学の方々も参加可能なシンポジウム形式の情報交換会の形式を取ることとなった。

会場の確保や時間調整、オンライン配信の準備等実施に関する調整は一橋大学で担当した。予定外、かつ急遽の開催決定であったため、連携参加校はじめ NIPC 総会の運営側にもご迷惑をかけることとなった部分もあったが、さまざまな組織のセキュリティへの関心の高さを感じることができ、多くの方々から快い協力をいただけたことに感謝するとともに、セキュリティに関する取り組みの必要性も改めて認識できる機会となった。

多くの方から今後の予定についての問い合わせをいただいたこともあり、今後も何らかの形で連携参加校以外も含めた情報交換の場を設けることも考えられる。

5　今後の計画と課題

5.1　今後の計画

今後の計画としてこれまでの打ち合わせの中で提案されたものや話題にあがったものを示す.

- **人的リソースの確保・共有化**
  大学における情報セキュリティの維持向上に関しては人的リソースの不足が重要な課題となっている．特に情報系センターの負担は継続して増加傾向だが，専門家の確保や専門技術を持つ者の不足・育成はより困難となっており，最近ではセン

ター教員の公募も不調に終わることも多くなっている．各校の体制や制度の違いも多いが，例えば情報セキュリティを担う組織の共同での設立やセキュリティベンダーとの協業・共同体等の検討など，人的リソースを継続的に確保し，かつ学内のシステムやサービスの状況にも精通できるような施策を検討する．

- **外部発信と活性化**
  現在 4 大学で始めた協定だが，目的を共にする他大学や各種組織・企業等との協業も検討している．まずは 4 大学で可能なことから始めているが，今後の計画を含め未定のものも多く，より効果的で実効性の高い体制づくりのため，活動内容の外部への発信や他大学・他組織も巻き込んだ活動も検討する．

- **CSIRT 共通化**
  大学のインシデント対応は基本的に CSIRT やそれに準じる組織での対応となるが，対応時間や人員不足など多くの課題を抱４えており，大学間で共通で利用できる機能や組織として制度化・体制づくりの検討が必要である．

- **他組織連携**
  大学のみで可能なことから連携活動を行っているが、外部の専門組織や警察等、平時から有事まで連携・協力体制など関係を構築しておくことはセキュリティ分野では非常に有効性が高いと考えられる。近年では大学と各県警等が協力して情報セキュリティに関する活動を行っていたり、分野を超えた協力活動も積極定に行われていることから、多方面と協力体制を整えることも検討できる。

5.2 現状の課題

- **大学間の体制格差**
  参加大学は類似する特色や規模感を持ち、共通の課題の解決に向けて活動を推進しているが、それでも各大学における情報セキュリティに割ける人的・経済的リソースの違いや情報系センターの体制・位置付けなどはかなり異なっており、専任教員数や技術職員の配置状況が異なることで、連携活動への参加度に影響が生じる可能性がある。各大学の実情に応じた柔軟な参加形態の確保が課題である。
  また、各大学の体制の違いにも関連して、職員の積極的な参加も必要である。具体的な活動に際してはそれぞれの大学で情報関連部局の職員の参加も進んでいるが、実際の運用や各種取り組みの実施・施策の実行などには職員の意見や各大学でのディスカッションも重要な要素であり、個別の活動だけではなく連携活動そのものへの積極的な関与のための施策も検討したい。

- **地理的条件の違い**
  京都工芸繊維大学が関西に位置することによる地理的な面の違いへの対応も重要な課題である。元々京都工芸繊維大学と電気通信大学は情報セキュリティに関しての協働を行っており、相互監査等の具体的活動も行なっていたため、4 大学間の連携活動においてもそれまでの知見を活かしつつ発展的活動への昇華を進めているが、当然ながらさまざまな活動における移動の発生など不利な面も考えられる。
  先述した情報交換会のように、他の予定と合わせたりオンラインツールの活用・工夫によって過度な負担がかからないようバランスをとった活動を進めていくとともに、例えば災害等有事の際の対応や相互バックアップなど、地理的に離れているからこそ実現可能な施策やメリットも考えられるため、連携モデルの重要なテーマの一つとして検討を進めていく。

- **運用コスト**
  連携活動そのものには新たなコストを求めるものではなく運用を進めているが、各大学のそもそもの情報セキュリティに関する活動やその予算が適切に維持されていないと、参加大学間での格差や活動への支障が発生する可能性もある。本活動はあくまでそれぞれの大学で必要な情報セキュリティ活動の延長線上に位置しており、新たな負担を求めるものではないという理解のもと、本活動を通して情報セキュリティの必要性を各大学での周知啓蒙にも活用し、共通の目標に向かって一体となって推進するとともに、効率的・効果的な施策を検討していく。

- **新たな技術への対応**
  生成 AI の急速な普及に伴う新たなリスクへの対応や、ゼロトラストアーキテクチャへの移行など、技術的課題への共同対応体制の構築が求められている。文科省通知等でもこれらの内容は触れられており、多くの大学で課題となっていることではあるが、まだ前例がなかったりコストがかかって

しまうなどの理由から新たな技術等への対応は後手に回ってしまうことも多い。

積極的な情報交換や外部組織との連携なども含め、連携活動を行なっているからこそのメリットを見出しつつ、大学が取り組むべき情報セキュリティのベストプラクティスを見出せるよう、協力体制を発展させていく。

6 まとめ・展望

大学の情報セキュリティを取り巻く状況は，情報技術の発達やインターネットの普及，およびサイバー攻撃の高度化・巧妙化によって負担が増加している中であるが，情報セキュリティ関連規則など制度面の充実や，その運用管理のため CISO や CSIRT などの体制整備を行なっている．

2024 年 12 月の文部科学省通知には、セキュリティ・バイ・デザインやゼロトラストなど情報セキュリティの重要度のさらなる高まりや、より高度なセキュリティ施策の必要性が謳われており、大学組織のガバナンスやマネジメント面からも情報系センターやセキュリティ担当部局の果たす役割は極めて重要なものとなっている。

しかし，実務を担う情報系センターを中心として人的・経済的リソースの不足はますます顕在化しており、サイバーセキュリティ対策等基本計画や各種セキュリティ関連規定の整備を進めても、それに基づいた活動を十分に行える人的・経済的リソースの確保は困難になっている。そうした課題を解消するため、さまざまな連携活動や協働・協力体制の構築や推進が進んでおり、新たな施策に繋げるなど大学を含む情報セキュリティに関する協働の取り組みもかねてより実施されている中，もともと相互に関係性のあった 4 大学間で情報セキュリティに関する連携体制を構築することで合意し、効率的で実現性の高い情報セキュリティ維持のための連携体制を整えるための活動を開始した．

活動は 2 年目を迎える中、具体的な活動を継続的に進めるとともに、より持続可能な体制の構築を進めるため正式に大学間での協定としての合意を目指し、現在協定内容の最終的な調整を進めている。

，具体的な活動内容として決定していることも少なく情報発信としても十分とは言えなが，大学の情報セキュリティ体制や情報系センターの維持管理への懸念が高まる中で，気軽に相談できる仲間の輪を広げるという意味でも極めて重要であると考えている．

情報セキュリティを取り巻く状況は今後もさまざまな課題や懸念が考えられるが，この活動を通して参加各校の情報セキュリティの向上や情報システム・サービスの運用・維持管理に寄与し，関連する組織や他の教育・研究機関なども含めた情報セキュリティ・エコシステムとしての一助となるよう，活動を継続していく．

謝辞

本活動の推進にあたり、参加大学の関係者はもちろん多くの方々にご協力いただきました。特に、NIPC 総会において広島大学近堂先生、静岡大学長谷川先生に情報交換会開催について急な話でご迷惑おかけしつつも周知等ご協力いただき、また高専機構 CSIRT 長の伊藤先生や木更津高専の歸山先生、齋藤様、NICT ナショナルサイバートレーニングセンタのセンター長園田先生や五十里様、NII-SOCS の高倉先生、長谷川先生、田中先生、小薗先生には事前の調整や遠方までご足労いただくなど多大なご協力をいただきました。この場を借りて感謝申し上げます。

参考文献

[1] 文部科学省．R3 年度学術情報基盤実態調査報道発表資料．https://www.mext.go.jp/content/20220318-mxt_jyohoka01-000010395_1.pdf．(2024/10/20 確認).

[2] 国立大学情報系センター協議会 (NIPC). 総会資料（会員大学活動報告および要望書 2023〜2025 分）.

[3] 大学間連携に基づく情報セキュリティ体制の基盤構築（nii-socs: Nii security operation collaboration services）. (2025/9/20 確認).

[4] 文部科学省． 大学等におけるサイバーセキュリティ対策等の継続的な取組について（通知）. (2024/12/25).

[5] 国家サイバー統括室サイバーセキュリティ戦略本部． サイバーセキュリティ 2025（2024 年度年次報告・2025 年度年次計画）. https://www.nisc.go.jp/pdf/policy/kihon-s/250627cs2025.pdf, 6 2025.

[6] KDS 国大協サービス． 特集テーマ：大学へのサイバー攻撃． 国立大学リスクマネジメント情報. https://www.janu-s.co.jp/mail_magazine/backnumber_202404.html, 4 2024. (2024/10/20 確認).