

大学間の情報セキュリティに関する連携体制の構築

中田 亮太郎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⁾, 長島 和平³⁾, 栴田 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 情報科学センター

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

Establishment of information security cooperation among universities

Ryotaro Nakata¹⁾, Koh Sugawara¹⁾, Hideaki Tsuchiya²⁾, Shunji Yazaki²⁾,
Takahiro Nemoto³⁾, Ryosuke Sato³⁾, Kazuhei Nagashima³⁾, Hideo Masuda⁴⁾

- 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 Information Science, Kyoto Institute of Technology

概要

大学運営や教育・研究活動で、多くの情報システムやインターネットの利活用が拡大する中、情報セキュリティに関するリスクも増加し、学内外で様々な対応が必要となっている。しかし、各大学で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、多岐に渡る業務の負担が拡大している。

大学の情報インフラやシステム・サービスは、一部で共同の取り組みや共通化されている例を除き基本的には個々の大学で独立して運用される中、情報セキュリティに関してはポリシーや方針の違いはあるもののその対象や目的は共通する部分も多く、かねてより大学間での情報共有や意見交換の他、様々な取り組みを通じたセキュリティの確保・向上の試みが行われてきた。

そこで今回、これまで情報セキュリティに関する共同の取り組みを行ってきた大学間で、今後さらに増加が懸念される情報セキュリティリスクへの対応やそれに伴う運用面の負荷を考慮し、さらに実運用レベルまで見越した協力を行うべく包括的な連携体制を構築することで合意を得た。情報セキュリティに関する施策・取り組みの共同実施や、システム運用・サービス提供・制度・人材育成・確保など様々な面において、効率的で実現性の高い情報セキュリティの連携体制構築を目指す。

1 はじめに

大学運営および教育・研究活動の中で、学内外のネットワークやさまざまな情報システム・サービスの利用が増加している。学術情報ネットワーク（SINET）の利用は国立大学で 100%、国公立大を合わせても 9 割近くに上っており、インターネットや各種クラウドサービスの利用も今や必須となっている [1]。

これらは業務の効率化や利便性の向上をもたらし、学生・教職員はもちろん、産官学の連携や地域との交流など学内外のあらゆる業務や教育研究活動等でメリットをもたらす一方、情報セキュリティリスクの増

加やインシデント対応の困難さなどへの懸念も高まっている。

大学等の教育機関は、一般企業と比較してセキュリティ体制・対策における課題の多さや、守るべき情報資産の多さが指摘されており、情報系センター等セキュリティ関連業務の主たる担当となる部局の負担は増加しているが、現行のシステムを維持しつつセキュリティ確保・向上のための新たなシステムやサービスの導入などに要するコストの確保や、専属で対応できる人員の配置および教育などを含む人的なリソースの不足は多くの大学で喫緊の課題となっており、効果的な施策が求められている [2]。

2 大学における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

国立大学において情報セキュリティが強く意識されたのは 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」に情報セキュリティ対策の強化が打ち出されたことが影響し、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、研修等の実施、自己点検・監査の実施、情報機器の管理状況の把握及び必要な措置の実施を対策として行うべきことが示された [3]。

2018 年には政府のサイバーセキュリティ戦略が改定され、新たな施策として大学等における安全・安心な教育・研究環境の確保が追加され、それを受け 2019 年には文部科学省から「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」が通知されており、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を保護が促されている [4]。

各大学でも増え続ける情報セキュリティインシデントの状況を鑑みて、サイバーセキュリティ基本計画等に基づきセキュリティポリシーや関連規定の整備、またそれに伴うさまざまな情報セキュリティ関連の施策・取り組みの実施や強化を進める中、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、サイバーセキュリティ対策にかかる実施すべき事項として、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示され、新たに対応すべき事項なども含め継続したサイバーセキュリティへの取り組みが求められている [5]。

2.2 国立大学の情報セキュリティ体制と課題

国立大学のセキュリティ体制の例を図 1 に示す。

CISO を中心とし、CSIRT が情報セキュリティインシデント発生時の連絡・報告・指示等を統括して各所との調整を行う。実動的な組織として学内の情報インフラや各種情報システム・サービスを運用管理する情報系センターやそれに準ずる組織があたり、平時を含めた情報セキュリティに関する対応や各種の取り組みを実施する。また、関連する業務として情報セキュリティ対策基本計画の策定、情報セキュリティインシデント対応体制及び手順書等の整備、情報セキュリティポリシーや関連規定の組織への浸透、情報セキュリ

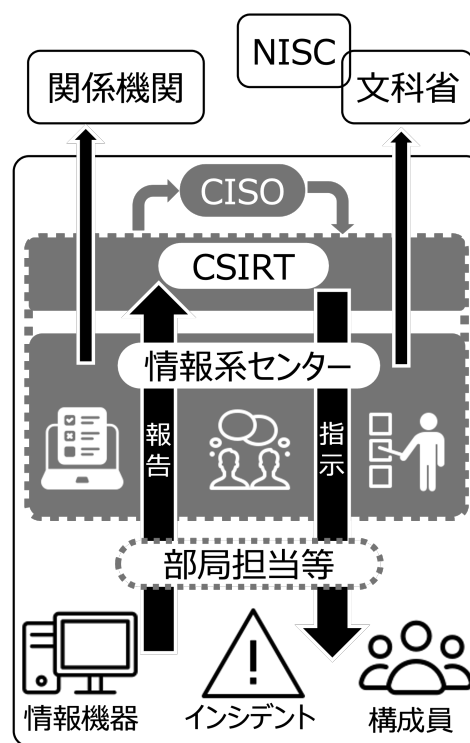


図 1 国立大学のセキュリティ体制の例

ティ教育・訓練や啓発活動の実施、情報セキュリティ対策に係る自己点検・監査の実施、情報機器の管理状況の把握及び必要な措置の実施など多岐にわたっており、実際の業務にあたる人員の不足や継続的な体制づくりへの負担が増加している [6]。

さらに、大学や教育・研究機関は一般企業とは異なる組織形態や構成員などの理由により、以下のような特有の対策や施策が求められる場合もある。

- 多様なユーザーと機器管理：学生、教職員、研究者、一時的な訪問者など多様なユーザーの存在や、個人所有のデバイスを含む多種多様な機器がネットワークに接続する。
- オープンな学術環境とセキュリティのバランス：学術の自由と情報共有の必要性、および研究データや個人情報の保護との両立。
- 予算と人材の制約：セキュリティ対策に割ける予算の限界や専門的な知識を持つ IT 人材・セキュリティ人材の確保の困難さ。
- 常に変化する脅威への対応：新たなサイバー攻撃手法への迅速な対策やセキュリティポリシー・関連規則等の定期的な見直し・更新。
- 教育・啓発活動：ユーザー（学生・教職員）のセキュリティ意識向上と定期的なトレーニングおよびベストプラクティスの共有。

大学の規模感やセキュリティに関する課題は共通している部分も多く、個々の大学間の取り組みだけで完結せず関係校全てで共通の目的に向かい、これまで行ってきた取り組みを拡大しつつ、さらに効率的で実

効性の高い体制づくりに向け活動を開始した。

3.2 連携体制構築に関する取り決め事項

本活動は現在のところ正式な協定として締結されたものではなく任意の取り組みとして進んでいるが、今後の継続的な体制維持のためにも一定のルールの下で合意形成しておく必要と、これまでの取り組みでも覚書という形で一定の取り決めを行っていたことから、同様に内容を各校で確認中の協定書を図3のように準備中である。主な内容を以下に示す。



大学間情報セキュリティ連携に関する協定書（案）

情報技術やインターネットの発展に伴い、情報セキュリティに関する脅威やその対応も増加する中、各大学で割ける人的・経済的リソースの停滞や低下が懸念されるなど多くの課題がある。一方で、各大学の情報セキュリティに関する取り組みや対応の目的は共通しており、情報共有や意見交換の他、さまざまな取り組みを通じた連携体制を構築し、実運用レベルまで様々な協力・協業が求められる。

そこで、趣旨に賛同する大学間において、情報共有/交換・システム運用・サービス提供・制度・人材育成/確保など様々な面において、効率性の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、次のとおり協定を締結する。

図3 協定書（案）

- 対象：協定の主体となる部署を情報系センター・CSIRT・DX推進組織など参加校の事情に合わせて柔軟に設定できるよう規定し、かつ他の大学の参加も検討できる内容。
- 目的：情報セキュリティに関して実施している各種対策・対応や制度、施策、取り組みなどを通じ参加大学全体で効率的・効果的な情報セキュリティの確保と管理・運用体制を築くこと。
- 実施方法：いくつかの取り組みについて具体例を示しつつ情報セキュリティに関する恒常的な協力体制を確立することや、記載されていない内容に関しても新たな活動の提案やその実施について積極的な連携を行うことを明記。
- 運用体制：各参加大学は本協定に関する運用責任者を1名選出し、各大学での活動と大学間の連携に関する責を負う。
- 費用負担：本協定に基づく各種活動について、費用負担が発生する場合は関係する大学間で協議の上で負担割合を決定するものとする。事前に費用負担に関する合意のない活動により発生する費用負担については活動主体となる大学で負担する。
- 秘密保持義務：相互の承諾なく、本協定に係る活動によって知り得た秘密を第三者に開示してはならない。

- 変更：本協定内容の変更については、既参加大学全との合意によって新たに締結を行うこととする。
- 期間：基本的に年度ごとの更新とし、破棄・解除に関する内容も明記。問題ない場合の自動更新についても規定。
- 協議解決：協定に定めのない事項が生じたときや協定書について疑義が生じた場合には参加大学間で誠意協議の上解決する。

また、協定書に明記はしていないが、この取り組みを継続的なものとするために3ヶ月に1回程度の定期的なミーティングの場を設け、今後の取り組み内容の検討や意見交換の場とすることとしている。なお、ミーティングその他の取り組み等で知り得た個人情報を含む各種情報の取り扱いについてはチャタムハウス・ルールを原則とし、知り得た情報に関しても個人や所属等の情報が特定されるような形での利活用はしないことで合意している。

4 取り組み内容

4.1 既存の取り組みの発展と共通化

これまで各大学間で行なってきた主な取り組みとしては、電気通信大学と一橋大学間で実施してきた相互監査がある。情報セキュリティ関連規則の整備状況や周知・遵守の状況などを文書の確認やヒアリング等を通じて確認するもので、昨年度はクラウドサービスの利用に関する部分を対象として、政府機関等のサイバーセキュリティ対策のための統一基準群にある内容を参考として双方合意の下でチェックリストを作成して実施している。

昨年度まで実施してきた2校がこれまでのノウハウをもとに監査側となり、今年度は電気通信大学→京都工芸繊維大学、一橋大学→東京農工大学の間で実施し、今後も監査・被監査側の交代やペアの変更、全体での実施などにより継続する予定である。

また、東京農工大学と一橋大学間で行われてきた情報交換会では相互の情報系センター教職員が訪問し合い、各校で運用中のシステムやサービス、各種取り組みに関して詳細な内容や導入の経緯、運用体制、稼働状況や効果などを忌憚なく情報交換・意見交換する場を設けることで相互の情報セキュリティに関する活動状況の確認や今後の参考とするもので、今年度は一橋大学を会場として全ての大学が参加可能な形で開催予定である。地理的に遠い京都工芸繊維大学の参加に関して課題はあるが、オンラインでの参加や今後の開催地

の検討なども含め継続的取り組みとする予定である。

4.2 新たな取り組み

これまでの取り組みのほか、現在新たな取り組みとして始めたものや、施行中のものについて述べる。

まず、これまで電気通信大学および一橋大学でそれぞれ実施されていた役員向け情報セキュリティ研修を合同開催として、協定参加校の関係者も含めて参加できるように実施する。各校はこれまで、それぞれ外部講師を招き内容の検討や調整を重ねた上で役員向け情報セキュリティ研修を実施してきており、各校での実施の際にオンラインでセンター関係者同士が参加するなど交流を行っていたが、今年度からは共催として各校の参加者（役員、および幹部職員）の予定を調整し、かつ協定の参加校の関係者も参加できるなど規模を拡大して実施予定である。内容の検討や各校の予定の調整、オンライン開催における機器設備の準備等の負担はあるが、参加校間で問題意識を共有し、効果的なセキュリティ対策に繋げるための重要な取り組みとして継続・発展させていきたい。

また既に前項で述べたが、これまで東京農工大学と一橋大学間で実施してきた情報交換会を発展的に継続し、協定参加校間の関係者に広く参加を募っている。これまでの情報交換会では、参加校から各校のセキュリティに関する状況やシステムの運用管理など多岐に渡る内容の情報交換とディスカッションを行っており、参加校を増やすことでより各校で参考となる事例等の共有やシステム・サービスの導入など、セキュリティを含めた広い範囲の情報交換が可能となる。なお、現地開催を原則することで話題の広がりやインタラクティブなやりとりの中でのより効果的な情報交換を促す形となっているが、本協定は全ての参加校が地理的に近いわけではなく、今後の開催形式やオンラインも含む効果的な開催方法などは検討課題である。

そして、新たな取り組みを検討する中で最も意見が多かったのが恒常的な情報交換についてである。各校の導入している情報システムや利用するサービス、セキュリティポリシーの内容や運営体制などに至るまで状況はさまざまであり、セキュリティインシデントの内容や状況も異なるため、本協定では試行的に図4のようなインシデント情報の交換が可能なプラットフォームを準備するとともに、今後各校の情報インフラやサービス導入・運用・維持管理に関するさまざまな情報の共有やデータベース化を検討している。

なお、現在は試行的に一橋大学の Slack ワークスペースを利用し、気軽な意見交換や質問・相談が行え

る場としているのと、活動内容がアーカイブとして残るようにしている。



図4 インシデント情報の共有例

5 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。

- 情報共有促進：インシデント情報の共有に加え、さまざまな内容や形式での情報共有が考えられる。たとえば各校のセキュリティ関連規則を常時共有することで、不足する内容の確認や修正・更新の検討を効率的に行うことや、システム・サービスの関連資料を共有することで各校が導入・更改の参考としたり、発展的に共通のデータベースとして整備し、それらを活用して共通モデル化したチャットボットや生成 AI の活用など、研究分野とも融合した利活用も考えられる。
- システム・サービスの共通化・共同導入：各校で共通化したシステムの導入・運用や、クラウドサービス等の共同調達・運用も検討できる。セキュリティ分野に限らず各校で導入している各種システム・サービスは、同等の目的や機能を持つものであったり、中には全く同じものを利用している場合もある。契約時期や形態、そして体制やコスト等さまざまな課題はあるが、一法人複数大学制度の例などを参考とし、情報セキュリティ面でも効果的・効果的な施策を検討する。
- 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。

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。しかし、一般的な情報セキュリティ対策の他、大学特有の事情にも対応する必要もあり、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喫緊の課題となっている。

情報セキュリティは社会全体のリスクとしても広く認識されており、NIIのように共同利用できるシステムやサービスを提供することで不足する人的・経済的リソースを全体で負担する試みや、シンポジウムの開催等によって意識の向上・共通化を促進し、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。

本体制は発足したばかりであり、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。

参考文献

- [1] 国立情報学研究所 (NII) . Sinet への加入機関数の推移 - sinet6 - science information network 6. <https://www.sinet.ad.jp/aboutsinet/document/count>. (2024/10/20 確認).
- [2] 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).
- [3] 石井徹哉. 「学術機関におけるサイバーセキュリティ」. デジタル・フォレンジック研究会コラム. <https://digitalforensic.jp/2020/11/30/column642/>. (2024/10/20 確認).
- [4] 文部科学省 高等教育局 私学部 私学行政課. 私学行政課説明資料. https://www.mext.go.jp/content/20210317-mxt_sigsanji-000013293_7.pdf, 3 2021. (2024/10/20 確認).
- [5] 内閣サイバーセキュリティセンター (NISC). サイバーセキュリティ 2024 (2023 年度年次報告・2024 年度年次計画). <chrome-extension://efaidnbmninnibpcajpcglclefindmkaj/https://www.nisc.go.jp/pdf/policy/kihon-s/cs2024.pdf>, 4 2024. (2024/10/20 確認).
- [6] サイエнтиフィック・システム研究会. 学術研究機関におけるサイバーセキュリティ・ガバナンスwg 成果報告書. サイエнтиフィック・システム研究会 WG 成果報告書, 10 2018.
- [7] 中西貴裕, 福岡誠, 金野哲士, 田頭徹, 鈴木健之, 田口慎, 大内慎也, 木村優太, 加治卓磨, 川村暁. 岩手大学における持続可能な情報セキュリティインシデント対応体制の構築. 学術情報処理研究, Vol. 22, No. 1, pp. 44-53, 2018.