参考資料２

国際化におけるリスク管理：セキュリティ関連の問題

イギリス大学協会
October, 2020

定義

- セキュリティ関連の問題：「セキュリティ関連」という用語は、国際化に関連する幅広い問題やリスクを表す包括的な用語である。本ガイドラインで言及している安全保障関連のリスクは、以下の 2 つのカテゴリーに大別される。海外・敵対的・外部の関係者やその代理人が、学術的な研究や専門知識を不正に取得しようとすること、および学術的な言説を妨害しようとすることである。大学は、セキュリティに関する問題やリスクを管理しなければならない。これらのリスクを管理せずに放置すると、英国高等教育セクターの評判や価値観、人材、キャンパス、教育・研究のパートナーシップに影響を及ぼす可能性がある。

要旨

概要

教育機関の運営組織および経営陣は、本ガイドラインに示された脅威やリスクから教育機関を守ることに責任と説明力を有する。この責任を果たすために、教育機関の運営組織は、教育機関が直面しているリスクと、そのリスクがどのように軽減されているかを記述した年次報告書を受け取るべきである。

ガイドラインの構成

本ガイドラインは 4 つの章で構成されている。

1. 機関の評判と価値を守る - ガバナンス、プロセス、ポリシー
2. 人材の保護 - 機関で働くまたは学ぶ人々の役割と責任、スタッフ、学生、visitors を保護するための対策、オンラインでの接触のリスク
3. キャンパスの保護 - サイバーセキュリティと英国のキャンパス
4. パートナーシップを守るために-研究の安全性とトランスナショナルな教育

1: 評判と価値を守るために

1.1: セキュリティ関連の問題に対するレジリエンスの構築

貴機関のリスク・エクスポージャーは独自のものであり、様々な要因に依存している。貴機関や環境の変化に伴い、かつ時間の経過とともに変化する。

セキュリティ関連のリスク管理を、重要かつ継続的な優先事項として確立する。これには以下が含まれる。

- 機関のリスクプロファイルに合わせたポリシーと仕組みの策定
- 個人がセキュリティ関連のリスクを特定し、報告することを支援し、権限を与える
- リスク・フレームワークを定期的に見直し、目的に合っているか、ベストプラクティスに沿っているかを確認する

1.2: デューディリジェンス

貴機関はデューディリジェンスのプロセスを実施していると思われるが、それはおそらく以下のようなものだろう。

主に財務リスクや風評リスクに焦点を当てていると思われる。貴機関は、デューデリジェンスのプロセスを再度検討し、以下の点を確認する必要がある。

- 公式的な手続きに従って、風評リスク、倫理リスク、セキュリティリスクを検討している。
- 政府からの情報を含め、公的に入手可能な情報を有効に活用している。
- 職員が潜在的または現在のパートナーシップについて懸念を提起できるような学内風土を構築し、維持している。
- 現在および将来のパートナーは、学問の自由と言論の自由に対する貴機関の誓約と、協力関係を築く上での影響の問題を認識している。

1.3: 英国高等教育の価値の促進

厳密で十分な情報に基づいた議論は、質の高い高等教育と知識の向上の基盤である。干渉のリスクを特定し管理するために、以下のことを行うべきである。

- 学問の自由と言論の自由という基本的価値観を明確にした行動規範、方針、法的合意を策定し、推進する。
- 干渉がどのようなものであるかについて、オープンで透明性のあるコミュニ

ケーション、議論、研究、調査を推進する。

- スタッフと学生が、それぞれの活動において、これらの干渉から自らを守る責任を負うことを支援する。
- スタッフや学生が、学問の自由や言論の自由に関連する問題について懸念を報告し、支援を受けることができる仕組みやメカニズムを開発する。

2: 構成員を守るために

2.1: 学内外のコミュニケーションと知識の共有

組織の方針や制度は、組織を守るために役立ちうる。しかし、それらは、個人がセキュリティ関連のリスクを特定し、報告し、管理する責任を理解するという意識をもたなければ効果を発揮しない。

透明性を高め、そうすることで、相互に有益な国際共同研究を行うことができるというスタッフの自信を築くべきである。

2.2: 海外に渡航・勤務するスタッフと学生の保護

仕事や学業のために渡航する学生やスタッフは、特定の、場合によっては深刻な個人的リスクにさらされる可能性がある。教育機関は、すべての海外渡航に適用される適切なプロセスを用意しておく必要がある。これには、学生やスタッフに対する適切なトレーニングが含まれ、関連するポリシーや行動規範を確実に理解し、リスクを自己管理できるようにサポートする必要がある。

3: キャンパスの保護

3.1: サイバーセキュリティ、施設、visitors

英国の大学は、ダイナミックで多様性に富み、国際的な機関であることを誇りとしており、年間を通じて世界中から研究スタッフ、学生、visitors を集めている。大学は、コミュニティを支援し、共同スペースやオープンスペースを提供するなど、重要な市民的役割を果たしている。

教育機関は、この市民としての役割と、教育機関とその資産を保護する必要性とのバランスを取る必要がある。そのためには、施設と visitors に関する統合的なポリシーを策定し、サイバーセキュリティ戦略の策定と実施を徹底する必要がある。

4: パートナーシップの保護

4.1: 研究のセキュリティ、知的財産、輸出管理のコンプライアンス

世界をリードする研究は、いよいよオープンで協力的になっている。これは英国の成功の基本であるが、リスクと課題もある。大学は、個人や組織が研究や知的財産（IP）に不正にアクセスしようとする者の標的になっている。

貴機関は、主なセキュリティ上の脅威と課題を認識し、以下のような方法でリスクを軽減するための行動をとる必要がある。

- あらゆる種類の共同研究において、すべての海外パートナー候補について、相応のデューデリジェンスを行う。
- 知的財産を保護するための方針や契約を実施する。
- 管理されている技術の輸出管理法およびその他の法的要件を遵守する。

4.2: トランスナショナルな教育パートナーシップ

英国の大学はトランスナショナル教育（TNE）の世界的リーダーとして評価されており、英国のプログラムに登録している学生は海外で 70 万人近くに上る。トランスナショナル教育の手配は、現地の規制の対象となり、現地当局の指示に従わなければならないが、これは大きなリスクをもたらす特徴である。

教育機関は、海外のパートナーに異なる影響を与える可能性のあるリスクの存在を認識し、評価するリスク軽減方針を持つ必要がある。特に、以下の点を確認されたい。

- 海外のパートナーについて徹底した定期的なデューデリジェンスを行う。
- 海外における組織の自立性および学問の自由に関するリスクを、リスク登録およびリスク・ステートメントの中で認識する。
- 現地の自治に対する要求と、一元的なリスク管理とのバランスをとる。
- 現地のステークホルダーとのコミュニケーションにおいて、明確な報告ラインを確立する。
- 包括的なルールベースの取り決めとハイレベルな原則に支えられた出口戦略を策定する。

その他のリソース

本ガイドラインに記載されているリスクを理解し、管理するために、機関や同僚を支援するための様々なリソースが用意されている。さらに、サイバーセキュ

リティ、輸出規制、学問の自由の保護などに関する資料も作成中である。本ガイドラインは、これらの追加リソースが利用可能になった時点で、定期的に更新される。

Centre for Protection of National Infrastructure（CPNI）および National Cyber Security Centre（NCSC）は、Trusted Research2 など、機関の意思決定およびリスクの軽減を支援する資料を公開している。これらのリソースは、本ガイドラインの関連セクションに記載されている。言及されているすべてのリソースのリストは、このガイドラインの最後にある「参考文献」に記載されている。

概要

本ガイドラインの使用方法

本ガイドラインの実施には、大学関係者全員の賛同が必要であるが、本ガイドラインに記載されているリスクや脅威から大学を守る責任を誰かに委任することはできない。統治機関と上級責任者チームは、明確な統治構造を確立し、本ガイドラインに記載されているリスクを管理する責任を負うスタッフを特定しなければならない。上級責任者チームは、教育機関が適切に運営されている効果的な仕組みを持っているという適切な保証を統治機関に提供しなければならない。これには、組織のシステム、プロセス、ポリシーの変更だけでなく、改革や文化的な変容も含まれると思われる。

我々は、教育機関が国際化に伴うセキュリティ関連のリスクをどのように管理しているかについて、教育機関が直面しているリスクとそのリスクがどのように軽減されているかについての年次報告書を、教育機関の運営組織が受け取ることを強く推奨する。この報告書には、教育機関の自治と学問の自由を守りつつ、セキュリティ関連のリスクを管理するために導入されているシステムとプロセスの概要に加え、教育機関のスタッフと学生の間でこれらの問題に対する意識をどのように高めているかを示す情報が記載されている。

英国大学協会の活動の目的

英国大学協会（Universities UK：英国大学協会）は、高等教育におけるセキュリティ関連の問題について、以下の 3 つの長期目標を実現するための作業プログラムを策定している。

1. 英国の大学は、国際的な安全保障上の脅威を管理・緩和するための一貫した、

積極的かつ戦略的な運用方法を有していることを証明する。
2. 英国の大学が自信を持って、持続可能で安全な国際的パートナーシップを追求することができる。
3. 英国の高等教育機関と政府が、安全保障上の課題において、研究・イノベーション（R&I)、機関の自立性、学問の自由の保護と促進に向けて、明確かつ協力的で建設的なアプローチをとっている。

これらの目標を達成するために、英国大学協会は以下の 3 つの中間目標を設定した。

- セキュリティ関連の問題について、スタッフと学生を問わず、個人の認識と理解の向上
- 組織のシステム、仕組み、行動様式の強化
- 大学と政府の間の接点を含むエコシステムの変化、およびシステムのレジリエンス。

このガイドラインの目的は、機関が最初の 2 つの成果に向けて前進するのを支援することである。このガイドラインを使用し、配布することで、このガイドラインが対象としている問題についての認識と理解が深まると考えている。その結果、システム、仕組み、行動に変化がもたらされる。このような変化は、国際的な協力関係や、所属機関の安全性、繁栄、継続的な成功のために役立つ。英国大学協会と政府は、このような活動を支援する役割を担っているが、最終的には、各教育機関が以下を確実に実行することが重要である。

大学と政府の接点を含む、高等教育セクターの広範なエコシステムに求められる変化は重要であるが、本ガイドラインでは直接取り上げていない。政府と高等教育セクターは、より広範なエコシステムが、大学が本ガイドラインに示された課題に対応できるよう支援するために協力している。本ガイドラインで検討されているリスクは、ダイナミックかつ複雑なものである。本ガイドラインで検討されている問題についての議論は現在進行中のものであり、アドバイスやガイダンスを含むより多くのサポートが今後、各機関に提供される予定である。

1 評判と価値を守る

概要

英国の大学の成功は、英国の高等教育セクターのレピュテーションや、学問の自由、言論の自由、機関の自立性といった共通の価値観によって支えられている。

本章は、英国の大学のレピュテーションと、英国の高等教育セクターの成功を支える価値観を守るために、貴機関を支援することを目的としている。シニア・リーダーであるあなたのリスク認識は、機関内の他の多くの人々よりも進んでいるはずである。国際的な共同作業に対する安全なアプローチを目に見える形で支持することは、機関内での実施とコンプライアンスの成功に不可欠である。

セキュリティ関連の問題に対する組織のレジリエンスにかかっている。本章では、以下の方法で組織のレジリエンスを強化する方法を詳述する。

- 堅牢なガバナンス、報告、およびリスク管理構造に支えられた、積極的でリスク情報を重視する文化の構築
- 特に、国際的な契約やパートナーシップを結ぶ際に、英国の法律・規制上の要件を包括的に理解するために、セキュリティ関連の問題をデューデリジェンスの手順に組み込む。
- 学問の自由、言論の自由、組織の自立性、学生と職員の保護という価値観を守るために、集団的責任を負う文化を構築する明確な方針と仕組みを確保する。

統治機関の監査委員会は、リスク登録にセキュリティ関連のリスクに関する常設項目を含めるべきである。

1.1: セキュリティ関連の問題に対するレジリエンスの構築

リスクリテラシーとリスクアウェアの文化を醸成する

シニア・リーダーは、積極的でリスクリテラシーが高く、リスクを認識する文化の構築を優先し、英国の高等教育の強みと価値を促進する明確なガバナンス、報告、およびリスク管理構造を実施することで、セキュリティ関連の問題に対する組織のレジリエンスを高める。

国際的な共同研究を成功させるために、シニア・リーダーシップ・チームがと

るべきステップがある。それは、セキュリティ関連のリスクを特定し、管理することである。これは高等教育機関のシニアリーダーにとっての戦略的優先事項である。

リーダーはリスク管理に高い技能を持ち、国際的な協力関係が高品質であることを保証するために、デューデリジェンス、ガバナンス、報告仕組みの開発と維持に多大な投資を行っている。

国際的な協力関係の大部分は歓迎され、相互に利益をもたらすものであるが、教育機関の安全と地位を脅かす可能性のある活動に常に注意を払うことが重要である。このような活動には、機密情報の入手、学問の自由の抑圧や操作、英国の高等教育セクターの優越性の利用などを目的として、貴学のような機関を標的としたものが含まれる。これらの活動は、関係する機関や個人にとって、財政的、法的、風評的な影響を及ぼす。したがって、以下のことが重要となる。

自身の機関がこれらのリスクにさらされていることを理解し、その保護に優先的に取り組むことが、機関の継続的な成功、そして英国の安全と繁栄のために不可欠である。

セキュリティ関連のリスクを効果的に管理することを妨げている課題は以下のとおりである。

- セキュリティ関連のリスクの性質と規模、およびそれらを管理する責任について、上級責任者チームと主要なスタッフの間での理解が不十分である。
- スタッフがリスクを認識していなかったり、リスク管理制度において特定したリスクに対処する権限が十分に与えられていない可能性がある組織文化
- リスク管理、ガバナンス、および報告の仕組みが定期的に更新されておらず、これらのリスクの性質の変化に対応する能力を備えていない。

セキュリティ関連リスクの特定と管理

セキュリティ関連のリスク管理を怠ると、財務的、法的、風評的に深刻な結果を招く可能性がある。場合によっては、その影響は所属機関を超えて、英国の国家安全保障と繁栄に影響を及ぼすこともある。

輸出規制、ATAS（Academic Technology Approval Scheme）、GDPR（General Data Protection Regulation）など、関連する法律や規制、契約上の取り決めに従わない場合、あなたや貴機関、あるいは貴機関内の個人が刑事責任を問われたり、訴訟を起こされたりする可能性がある。共同研究の性質と条件、注意義務、

および個人がアクセスできる情報によって、具体的かつ発展的な法的義務が生じる。

セキュリティ関連のリスクを不適切に管理した結果、風評被害が生じ、質の高いサービスを維持し、資金、学生、スタッフ、認定を獲得・維持する能力に影響を及ぼす可能性がある。

要するに、自らの機関の地位や英国の安全と繁栄に影響を及ぼす可能性のあるセキュリティ関連のリスクについて、積極的に検討する必要がある。

上記の説明はすべてを網羅しているわけではなく、追加情報は以下のセクションにある。

- サイバーセキュリティ、不動産、visitors
- 研究の安全性、知的財産、輸出管理の遵守
- 海外に渡航・勤務する職員・学生の保護

このようなリスクに直面しているのは、貴機関だけではない。知識の共有と関与（法律によって関与が求められる場合を含む）については、「内部および外部のコミュニケーション」で詳しく説明している。

セキュリティ関連のリスク管理を重要かつ継続的な優先事項として確立する

貴機関は、リスクを管理するために、さまざまなリスク管理、ガバナンス、報告の枠組みと能力を備えている。学問の自由や言論の自由に関連するものを含むリスクは、これらの仕組みでカバーされ、教育機関全体に広く公表されるべきである。

セキュリティ関連のリスクを積極的に報告し、エスカレーションする個人の責任を含め、これらのリスクを管理するために設けられた方針と仕組みについての理解を共有することは、認識とセキュリティに関する風土を醸成するために極めて重要であり、その点は、「内部および外部のコミュニケーション」の項で詳しく説明する。

方針と仕組みは、機関のリスクプロファイルに沿ったものでなければならない。リスクプロファイルが高ければ、より強固なデューデリジェンスの仕組みや監視が必要となり、機関はさらなる精査を受けることになる。リスクプロファイルの評価は、法的な義務をしっかりと理解した上で行われなければならない。

機関に属する個人が、報復や検閲の恐れなしに、セキュリティ関連のリスクを特定することができると感じ、それをサポートすることが不可欠である。

各機関は、スタッフが問題や懸念を報告する方法を熟知するような、適切なポリシーとプロセスを導入する必要がある。これは、宗教的、国民的、人種的、社会的なアイデンティティーと交差していると思われる場合や、偏見や人種差別と混同される場合には、特に問題となる可能性がある。しかし、教育機関はこれらの問題に対処し、適切なポリシーと仕組みを確立する必要がある。

これらのリスクは動的なものである。脅威が変化するにつれ、それらを管理するためのシステムや仕組みも変化する必要がある。リスク・フレームワークは、目的に合っているか、ベスト・プラクティスに沿っているかを確認するために、定期的に見直されなければならない。ある場合には、外部の独立機関が、実施されている管理についての保証を提供する必要があるかもしれない。

ケーススタディ：　ガバナンス

英国のある高等教育機関のシニア・リーダーシップ・チームは、同機関の国際的な協力関係に関するガバナンス・プロセスの見直しを要請した。このレビューは、同機関の国際的なパートナーシップの規模、範囲、種類が増加したことを受けたもので、安全で持続可能なパートナーシップを促進するための方針を特定することを目的としていた。

レビューの結果、以下のような「重要な国際的な共同研究やパートナーシップ」には、副学長の明確な許可が必要となった。

- 海外にジョイント・キャンパスを設立したり、教育機関を代表することになる可能性のあるすべてのプロジェクト
- 全面的または部分的に海外のパートナーから資金提供を受けているベンチャー企業や団体
- スタッフを長期間海外に派遣するプロジェクト
- 経済的価値に関わらず、風評被害やセキュリティ、法的リスクを伴う可能性のある新規性の高いプロジェクトや論争の的となるプロジェクト

副学長を補佐するために、国際担当副学長を議長とし、関連する専門サービスと上級教育スタッフで構成される国際グループが結成された。この方針変更は大学全体に伝えられた。

シナリオ

あるコラボレーションの機会が国際グループに提示された。ある研究者が海外の大学に招かれ、自分の専門分野（植物生物学）に関する一連のゲストレクチャ

ーを行い、研究施設の設立に関する一般的なアドバイスを行う。彼らの旅費と宿泊費は国際協力者が全額負担するが、それ以上の報酬は受け取らない。

海外グループは、この協力関係に最初は不安を感じていた。海外の大学をウェブで検索しても成果は限られており、またその大学の代表者は積極的に情報を開示していたが、連絡は途絶えていた。海外大使館への問い合わせを含め、さらに調査を進めると、提案されたパートナー機関は設立から1年が経過しており、英国をはじめとする海外の多くの機関や組織に支援や協力を求めていた。これらの協力関係の多くは問題なく行われていた。

国際グループは、適切な保護措置さえ講じられていれば、このプロジェクトは有益なものであると判断した。大学にとっては経済的な利益にはならないものの相手国にとっては、地元の農業技術を向上させることができ、大学が海外市場で存在感を示すことができるというメリットがあった。

関連するアドバイスを検討した結果、英国の教育機関は以下のことを確認した。

- 出張中の研究者は、必要な情報のみを持ち出し、アクセスできるようにし、英国外では一時的に共同データや所属機関のイントラネットにアクセスできないような安全策を講じる。
- 研究施設に関連して計画されたアドバイスは、一般的でハイレベルなものであり、英国の戦略的輸出規制に抵触しないものであった。
- 研究者は、海外の機関からのいかなる寄付や申し出も受け取らないことを理解し、受け入れ側の気分を害さないよう、文化的に配慮した方法で申し出を断る方法をアドバイスした。
- 渡航前に法律相談を受け、共同研究契約には問題がないことを確認したが、仮想プライベートネットワーク（VPN）が海外では違法であることを確認し、サイバーセキュリティ担当者の意見を聞くことを勧めた。

研究者たちはこの渡航が有益であったと感じ、国際グループは有益で必要なサービスであると同僚に勧めている。

1.2: デューディリジェンス

たいていの国際的なパートナーシップはすべての当事者に利益をもたらすものであるが、重大なリスクを伴うケースも少なからず存在する。場合によっては、当事者が不誠実な行為を行ったり、契約の条件を超えた利益を求めたり、契

約に定められた範囲を超えた活動を行ったりすることがある。したがって、相互に利益のある国際的なパートナーシップを促進し、機関、部門、英国の利益への損害を最小限に抑えるためには、定期的な見直しを前提とした強固なデューデリジェンスが不可欠である。

上級管理者は、パートナーシップの包括的な理解を促進し、英国やその他の関係国の立法・規制上の要件を認識するために、セキュリティ関連の問題がデューデリジェンスに完全に組み込まれていることを機関の運営組織に保証する必要がある。

英国の大学は、将来のパートナー候補について、定期的にデューデリジェンスを行っている。これまでのところ、この活動は主に財務リスクと風評リスクに焦点を当てている。我々は、政府やその他のガイダンスを考慮して、各機関が既存のデューデリジェンスプロセスを再検討し、デューデリジェンス・プロセスの有効性、風評リスク、倫理リスク、セキュリティ・リスクの評価方法を検討することを推奨する。

大学は自立的な機関であり、関連する法律や規制に基づいて、どのようにリスクを軽減するのが最善か、また、どの程度のリスクが適切かを判断するのは、各大学に委ねられている。この評価は比例原則に基づくべきで、計画されている共同研究の規模や性質、パートナーの所在地や地位に基づいて決定されるものである。

このセクションでは、機関がセキュリティ関連のリスクを評価し、潜在的な損害を軽減するデューデリジェンス・プロセスを開発するのに役立つ情報とガイダンスを提供する。

このセクションは、「パートナーを知る」、「明確な契約を締結・維持する」、「スタッフの明確な役割と責任を確立する」という 3 つのパートに分かれている。

パートナーを知る

英国の大学は、個々のスタッフ間の対話や協力などの非公式な協力関係から、トランスナショナル教育などの公式なパートナーシップまで、複雑な国際関係のネットワークを持っている。このような協力関係の中には、大学が安全保障上の脅威にさらされるものもある。これらの協力関係は、パートナーが拠点を置く国の事情によって個別に形成される。そのため、ガバナンスやデューデリジェンスもそれに合わせて行う必要がある。例えば、地域によっては公文書が制限され

ており、詳細な記録を入手することができない場合がある。

非公式な共同研究は、教育機関の正式な方針や手続きの対象にはなりにくいが、リスクは残る。貴機関は、可能な限りパートナーシップや共同研究を開示するようスタッフに求めることを含め、正式な方針や手続きにもとづかない情報に依拠し、意思決定を行うスタッフをどのようにサポートするかを検討する必要がある。これにより、非公式な共同研究に関連する利益相反やその他の法的、風評的、または経済的なリスクを可視化することができる。

リスク情報に基づいた意思決定

正式なデューデリジェンスのプロセスを経てない情報に基づいた意思決定を行うために、貴機関はどのようなサポートをしているだろうか。海外の大学、企業、政府機関との正式なパートナーシップの場合、デューデリジェンスには、パートナーの過去の活動、事業分野、運営組織の商業的・倫理的地位、パートナーの法的・規制的環境などを調査する必要がある。

一般的に大学は、パートナー企業にアンケートの回答を求めたり、書類や証拠の提出を求めたりするが、これらはパートナー企業との協力関係に伴うリスクのレベルを評価するために使用される。また、大学は、所属機関で雇用されている専門家、ウェブ検索、コンサルタント会社などを利用する。貴機関は、パートナー、他の活動や国とのつながり、パートナーが活動する法律上の背景についての理解を深めるために、公開されている情報をどのように利用しているだろうか。貴機関は、民間企業と同様に、パートナー候補やその従業員の身元調査をどの程度まで行うことができるだろうか。

どのようなパートナーシップにおいても、リスクは提案されている共同活動の内容に大きく左右される。一部の活動は、ATAS（Academic Technology Approval Scheme）や輸出管理法など、特定の法律、規制、行動規範によってカバーされている。貴機関のリスク管理フレームワークは、関連する法律、規制、行動規範を認識し、それに対応しているだろうか。機関は、意思決定を行う際に、英国政府の助言や専門知識をどの程度活用しているだろうか。

明確な契約の締結と維持

海外のパートナー候補に対するデューデリジェンスは、適切かつ関連する法律や規制の規定を参照する必要がある。また、国際的なパートナーシップに関連す

る学問の自由へのリスクを含め、セキュリティ関連のすべてのリスクを考慮する必要がある。モニタリングデータ、および誰が誰に何を報告する責任があるかを明確にする。

パートナー組織または個人とのあらゆる公式のやりとりについては、セキュリティ関連のリスクを管理するために、ベストプラクティスの契約メカニズムおよびポリシーを活用する。契約書や覚書の条件には、学術活動の完全性を守るための条項を含めるべきである。

専門的なサービスを提供するスタッフを含む学内の関係者は、訪問や委任を含む関与活動を管理するために、トレーニングや意識向上のためのワークショップ、および簡単なリスク評価ツールを利用するとよい。

セキュリティ関連のリスクを軽減するためのデューデリジェンスを定期的に実施し、研究提携を含む国際的なパートナーシップやプロジェクト、投資、寄付、慈善活動、商業化、設備投資、授業料収入、スタッフの名誉職やコンサルタント職などの収入源についても定期的に見直すべきである。最もインフォーマルな協力関係から最もフォーマルなパートナーシップまで、あらゆる関係において、セキュリティ侵害の可能性を十分に考慮しなければならない。

英国の機関は、何がきっかけで撤退するのかを理解した上で、適切な撤退戦略を策定し、規定を設ける必要がある。最終的には、継続的なデューディリジェンスの結果、海外の組織や研究者がもはや適切なパートナーではないことが判明した場合、何の責任も負わずに契約から離脱したり、契約を早期に終了したりする権利も含まれる。例えば、継続的なデューデリジェンスの結果、学問の自由を維持するという大学の法的義務が脅かされていることが判明した場合などが挙げられる。契約の設計や適切な保護の確保に関しては、具体的な法的助言を求める必要がある。

パートナー組織や個人は、様々な形の資金提供の取り決めや、個人を対象としたその他の誘因を通じて、特定の活動分野にアクセスしたり、影響を与えようとする可能性がある。これを緩和するために、個人や組織は資金源について透明性を保つべきである。デューデリジェンスでは、潜在的な収入源を検討する際に、セキュリティ関連のリスクを管理するためにどのような仕組みが存在するかを確認する必要がある。

スタッフの役割と責任を明確にする

大学はすでに、国際的な活動に伴うリスクを特定し、管理するための手順や方針を持っている。セキュリティ関連のリスクに対する認識は高まっており、大学はスタッフがこれらのリスクを特定し、それに基づいて行動することを支援すべきである。

主な成果

- デューデリジェンスのプロセスにおいて風評被害、倫理的リスク、セキュリティリスクを確実に考慮する。
- 公開情報を利用して、パートナーや、他の国家とのつながりについての理解を深める。必要に応じて、英国政府にさらなる情報を求める。
- スタッフが懸念事項を提起できるような学内風土を構築・維持し、その活動が風評被害や倫理的・安全保障上のリスクをもたらすかどうかを機関が検討できるような仕組みを導入する。
- 学問の自由や言論の自由に対する英国の教育機関の取り組みや、これが共同研究やパートナーシップに与える潜在的な影響について、パートナーが理解していることを確認する。

ケーススタディ：多機関共同パートナーシップ

英国の 2 つの大学が、基礎研究プログラムでの共同作業を模索していた。これらの機関は、研究評議会とのパートナーシップのもと、英国政府の特定の資金調達プログラムに入札し、資金を確保することに成功した。入札プロセスでは、資金提供プログラムの国際的なパートナーが、英国の大学とその国の 2 つの組織と提携した。英国の大学は、その国の 2 つの組織と提携することになった。

シナリオ

学術コミュニティでは、この資金提供プログラムについて、海外側が資金提供を受けるべきと判断した団体をテーブルに持ち込むという理解がある。英国のコンソーシアムは、助成金が資金調達プログラムと研究評議会によって承認されたため、海外の団体が適切であると考えていた。その結果、英国の協力大学は十分なデューデリジェンスを行うことができなかった。

このプログラムは支援を受け、その後、共同研究プログラムを成功裏に完了させ、研究成果の一部は研究誌に掲載された。

大学側は、このプログラムが輸出管理規制に違反している可能性があることを指摘された。両大学のパートナーは、デューデリジェンスを怠ったことと、自分

と機関の評判に影響を与える可能性について、同等の責任を負っていた。

教訓

- 海外のパートナーは、新技術や研究が輸出規制法の対象となる前に、その開発初期段階にアクセスしようとする可能性がある。
- 共同提案における英国のパートナーは、デューデリジェンスと継続的な監査に責任を持たなければならず、それは上級スタッフによって監督されるべきである。
- 徹底したデューデリジェンスは、UKRI、英国研究評議会、その他の政府部門が資金提供するものを含め、すべての国際的なパートナーシップや共同研究に必要である。
- 他の機関や政府と情報を共有し、デューデリジェンスや監査のプロセスを担当する担当者を各大学において任命することで、こうした事態は回避されたかもしれない。

1.3: 英国高等教育の価値の促進

教育機関は、明確な方針と仕組みを持ち、学問の自由、言論の自由、機関の自立性という価値観を守るための連帯責任の文化を築いている。

情報に基づいた厳格な議論は、学問の自由と言論の自由という価値観に裏打ちされた、質の高い高等教育と知識の進歩の基礎となるものである。われわれは、英国の高等教育の重要な価値が、教育機関のあらゆるレベルで理解され、保護され、支持されるよう、積極的に協力しなければならない。

しかし、国際的な政府や組織が、英国の大学に公然と、あるいは密かに干渉し、個々の大学や高等教育機関全体の評判を貶めようとしている例が、いくつか報告されている。

干渉と影響

「干渉」と「影響」の概念は、ここでは重要な意味を持ちうる。干渉とは、他国または他国に代わって行動する何者かが、英国の利益に有害な影響を与えることを目的とした悪意ある活動を行うことを指す。このような活動には、欺瞞的なもの、強制的なもの、腐敗的なものがある。これには、影響力を持つエージェントの活用、投資のレバレッジ、経済的な誘導、偽情報、破壊的または悪意のあるサイバー活動が含まれる。

英国の高等教育部門の文脈では、干渉には、英国の高等教育機関の価値や利益

に反する悪意のある活動が含まれる。これには例えば、コースの内容やカリキュラムを変更しようとする行為などが挙げられる。また、研究においては、研究成果やデータの盗用などが考えられる。場合によっては、妨害の対象者が、自分が妨害の被害者であることを認識していないこともある。

英国政府を含むすべての政府は、自分たちにとって重要な問題の審議に「影響」を与えようとする。このような活動は、オープンで透明性のある方法で行われる場合、国際関係と外交の正常な側面であり、公的な議論に積極的に貢献することができる。英国の高等教育セクターの文脈では、影響には、開かれた国際協力と大学の利益を促進することを意図した活動が含まれる。これには、例えば、文化交流会の開催、相互に有益な国際的な協力関係やパートナーシップなどが含まれる。

上記の例は明確なものである。しかし、干渉と影響の区別は曖昧な場合がある。影響は、自己検閲や、透明性やスタッフへの説明責任という点で閉鎖的な環境を生み出す可能性がある。機関内のオープンで透明性の高い議論は、これらのリスクを管理するための効果的な方法である。

妨害行為に対抗するためには、学問の自由、言論の自由、機関の自立性に及ぼすリスクを考慮し、潜在的な侵害に対するレジリエンスを高める必要がある。

イングランドとウェールズの 1986 年教育（No.2）法第 43 条は、教育機関の運営に関わるすべての個人および団体に、会員、学生、従業員、訪問研究者の法に定められた範囲内での言論の自由を確保するために、合理的に実行可能な措置をとる義務を課している。また、プロバイダに対して、言論の自由に関する行動規範を付し、常に最新の状態に保つことを求めている。教育機関のガバナンスに関わるすべての個人および団体は、行動規範の要件が遵守されるよう、合理的に実行可能な措置（適切な場合には懲戒措置を含む）を講じなければならない。

学問の自由、言論・表現の自由は、英国の学術文化の中心的な信条となっている。これらの概念は微妙で複雑なものであり、大学には、訪問するスタッフや学生を含む大学コミュニティのすべてのメンバーがこれらの概念をよりよく理解できるようにする責務がある。大学は、これらの概念に対する大学の立場を明確に示した行動規範や方針を策定するとともに、これらの概念に関連する法的保護や法律を明確に区分することで、これらの概念に対する理解と合意を得る必要がある。

大学は、干渉に関する明確な声明を示し、これらを確実に守るための方針や手

順を策定する必要がある。

重要な行動

- 学問の自由や言論の自由といった基本的価値観に加え、干渉の回避を明記した明確な行動規範、方針、法的合意を策定し、推進する。
- 学問の自由、言論の自由、組織の自治への干渉がどのようなものであるかについて、オープンで透明性のあるコミュニケーション、議論、調査、探求を促進し、スタッフや学生が自らの関わりや活動を通してこれらの侵害から守る責任を負うことを支援する。
- 干渉から生じる問題を含め、学問の自由や言論の自由に関連する問題について、スタッフや学生が報告、懸念の提起、支援を受けられるようなプロセスや仕組みを構築する。
- われわれが共有する価値観について、オープンで透明性のあるコミュニケーション、議論、調査、探求を促進し、スタッフや学生がその価値観を損なおうとする試みから身を守る責任を負うことを支援する。

オープンで透明性のある議論を奨励する

英国の高等教育機関の健全性とアイデンティティに関わる学問の自由と言論の自由の重要性について、オープンで透明性のある議論を促すために、上級スタッフは所属機関全体でこれらの問題についての議論、研究、調査を促進すべきである。また、外国からの干渉によって学問の自由や言論の自由が損なわれる可能性があることを認識させるべきである。大学は、労働組合や学生団体、専門的なサービスを提供するスタッフ、学識経験者、名誉職、契約者、キャンパスを訪れる人々など、幅広いスタッフや学生を対象にトレーニングなどを実施することが望ましい。

懸念事項を提起するためのプロセスとメカニズムの開発

教育機関は、学問の自由や言論の自由と同じように、干渉に関する懸念をスタッフと学生の両方が提起できるように、機密性の高いメカニズムを開発すべきである。

このようなケースがタイムリーにシニアリーダーの注意を引き、必要に応じてエスカレーションされるように、明確で透明性のある報告ラインを設定する必要がある。

英国の大学が海外で事業を展開するようになると、差別禁止政策や個人の権利の保護などについて、他国の法律や社会的枠組みが必ずしも英国のそれと一致しないことに気づくかもしれない。これらは、通常のリスク管理の枠組みの中で評価されるべきである。

学問の自由や言論の自由といった英国の規範が他国では法的に支持されない可能性があることを認識しながらも、大学は、平等や多様性といった中核的価値観が大学の範囲や職場環境の中で尊重されるように対策を講じることができる。例えば、海外で働くスタッフのために価値観に関する憲章を発行し、その国の法律や文化的規範を認識しながら、平等、多様性、尊重の価値観に対する大学のコミットメントの意味を明確に示すことができる。

域外管轄権の問題を考慮する

英国の個人は、他国で制定された域外管轄権が適用される場合がある。これらの法律は英国内では強制力を持ちないが、将来の海外渡航、海外での活動、あるいは留学生や学者の場合は特定の国への帰国に支障をきたす可能性がある。域外管轄権は、英国での活動を萎縮させる可能性がある。学者や学生は、他の国ではデリケートであるとみなされ、法的規制の対象となる可能性がある特定のトピックについて、学術的な議論に参加したり、研究を進めたりすることが難しくなると感じるかもしれない。

教育機関は、域外管轄権的に適用される法律が学生、スタッフ、visitors に与える影響を考慮しなければならない。域外適用の法律に対応して、一部の教育機関では学生の保護を導入している。これには、例えば、特定の州で政治的にデリケートとみなされる可能性のあるコース教材を修正せずに学生に提供することなどが含まれる。また、セミナーやその他の口頭での議論にチャタムハウス・ルールを導入したり、学生がコースワークを匿名で提出できるような手段を導入したりすることで、学生を保護する措置をとることもできる。

録画される可能性のあるオンラインプログラムの配信には、考慮すべき特定の課題がある。教育機関は、このような状況下であるタッフや学生を保護する方法を慎重に検討する必要がある。

2　構成員を守るために

概要

本章は、貴機関が、学生やスタッフ、そして貴機関を訪れる人々を保護することを目的としている。これを達成するための最良の方法は、全員がセキュリティ関連のリスクを認識し、自分がどのような状況に置かれているかを理解する文化的土壌を育成し、支援することである。英国の大学は多様性に富み、世界中の市民がコミュニティに参加している。そのため、このような文化を育むことはこれまでは必ずしも容易ではなかったかもしれない。

コミュニティのメンバー全員が、セキュリティ関連のリスクを特定し、報告し、管理する役割を担っている。本章の第 1 部では、これらの責任を学内外のコミュニケーションのなかでどのように明確化するかを検討する。

第 2 部では、海外に渡航・勤務しているスタッフや学生の保護と、それらの人々をサポートするために貴機関が取るべき手段について解説する。

内部コミュニケーションは、セキュリティ関連のリスクを特定、報告、管理する個人の責任を強化するために使用されるべきである。対外的なコミュニケーションは、透明性を促進し、相互に有益な国際的な協力関係やパートナーシップを構築する機関の能力を高める。各機関はベスト・プラクティスを特定し、レジリエンスを高めるために、相互に情報を共有し、それを政府と共有すべきである。

シニア・リーダーは、安全保障上のリスクに対処し、スタッフと学生の安全と福祉を促進するために、短期および長期の海外活動を保証するプロセスと手順があるという確信を持つべきである。

2.1: 学内外のコミュニケーションと知識の共有

内部コミュニケーションは、意識の高い文化を促進し、セキュリティ関連リスクを特定、報告、管理する個人の責任を強化するために用いられるべきである。外部とのコミュニケーションは、透明性を促進し、相互に有益な国際的な協力関係やパートナ ーシップを構築する能力に対する機関の信頼を築く。各機関は、ベスト・プラクティスを特定し、レジリエンスを高めるために、相互に情報を共有し、それを政府と共有すべきである。

このセクションでは、互恵的な国際協力やパートナーシップを促進するために、既存のコミュニケーション・チャネルをどのように利用すべきかを概説している。また、セキュリティ上の課題に対する各部門の対応を強化するために、各機関が相互に、また政府とどのように関わるべきかを説明する。このセクションは、内部コミュニケーション、外部コミュニケーション、知識共有の 3 つのパートに分かれている。

内部コミュニケーション

リスク情報に関する文化は、リスクに対する共通の認識と評価から生まれる。内部コミュニケーションは、リスクに対する共通の理解を築く上で非常に重要であり、多様な学生やスタッフに対応するために様々なフォーマットで提供されるべきである。そうしたコミュニケーションにおいては、海外からの学生やスタッフを含むすべての人が、安全なキャンパス環境を維持し、同僚や仲間を守るために果たすべき役割があることを強調する必要がある。また、不適切なリスク管理がもたらす結果についても詳しく説明する必要がある。

学生やスタッフが国際的な共同研究やパートナーシップに関連するリスクを理解し、特定の義務を管理するための最善の方法を理解するのを支援するためのリソースを用意する必要がある。補足的なトレーニングや教育機関固有のリソースを教育機関が開発する必要がある場合もある。補足的な研修や機関固有のリソースは、教育機関が開発する必要があるかもしれない。

外部コミュニケーション

外部とのコミュニケーションは、教育機関がセキュリティ関連のリスクを管理・軽減するために強固な対応をとっていることを示すために利用できる。ガイダンスにおいて推奨される事項、方針、プロセスを公開することを推奨する。

知識の共有

セクター間や政府とのあいだで情報や経験を共有することで、問題の性質や規模、ベスト・プラクティスに関する共通の理解を深めることができる。活動を調整し、機関を支援するために連絡窓口を設置し、そこの担当者を英国大学協会に紹介する。これにより、部門間および部門と政府間の連携が容易になる。

貴教育機関やスタッフは、すでにセクター団体や専門的な会員組織と関わって

いるはずである。これらの組織は、ベストプラクティスやアイデアを共有する上で重要な役割を果たす。英国大学協会は、今後各セクターおよび専門家組織と体系的に関わり、必要な情報、助言、指導を確実に提供していく。

各機関はセクター横断的な対話に参加し、各自の経験を強調し、ベストプラクティスを共有し、共通の問題に対するレジリエンスを構築することが重要である。また、必要に応じて、政府との対話も行うべきである。リスクの性質、頻度、範囲を理解することで、政府が外交手段やその他の手段を用いて効果的に対応することができる。

ケーススタディ：内部コミュニケーション

シナリオ1

あるスタッフが、既存の研究提携について懸念を抱いている。そのパートナーは、本学の機密性の高い研究にアクセスするための隠れ蓑として利用されている疑いがある。パートナー組織の代表者は、契約上の範囲を超えた資料へのアクセスを何度も要求してきた。スタッフはパートナーの要求をすべて拒否しているが、パートナーが他の大学職員にも同じ要求を出していることを知った。そのスタッフは貴機関でどのように懸念を表明するべきか。大学では以下の問題を考慮する必要がある。

- 現在の枠組みの中で、通報がどのように機能するか
- どの個人またはグループが通報を最終的に監督するか
- 不適切なアクセスを防ぐためにどのような保護措置をとっているか。

このシナリオでは、スタッフは懸念される行動を認識していた。資料にアクセスしようとするさらなる試みも拒絶した。貴機関では、潜在的なリスクについてスタッフを教育し、対応の一貫性を確保するために、どのようなプロセスおよび手順を実施しているだろうか。

シナリオ2

ある大学院生が、英国外の研究者からメールを受け取った。そのメールには、学生が最近共著で発表したジャーナル論文についてお祝いの言葉が書かれており、研究内容や論文についてもっと詳しく話してみないかと尋ねられた。学生は、メールの送信者の名前も出身大学も知らなかったが、自分の研究について喜んで議論したいと返信した。

学生の指導教官は、論文が注目されていることを喜び、可能であれば電話会議

に参加すると言った。学生の上司は、国際的な活動を行う前に、学部で定められている簡単なオンラインフォームに記入することを提案した。その学生はフォームを提出したが、翌日、ミーティングを断るように言われた。彼が受け取った電子メールは、機関内の複数の研究者に送信されており、研究テーマも多岐にわたっていたため、疑わしく、本物である可能性は低いと判断された。

このシナリオでは、学生は学部のプロトコルに従い、研究についての話し合いの要求を最終的に断った。このような状況や似たような状況において研究スタッフの意思決定をサポートするために、どのような内部プロセスを導入しているだろうか。これには次の点を検討する必要がある。

- 内部の手続きが目的に合致しているか、またスタッフがその手続に従う可能性があるか。
- 学生、研究者の意思決定をサポートし、内部プロセスへの賛同を得るにはどうすればよいか。

2.2: 海外に渡航・勤務するスタッフと学生の保護

シニアリーダーは、セキュリティ関連のリスクに対処し、海外に渡航するスタッフと学生の安全と福祉を促進するためのプロセスと手順があることを確認すべきである。

渡航の手配

大学のスタッフや学生の多くは、仕事や勉学のために定期的に海外へ渡航する。ほとんどの場合、このような短期出張は、目的にかかわらず、英国内での同様の活動と同程度のリスクエクスポージャーを伴いうる。しかし、特定のケースでは、個人や大学が著しく高いリスクにさらされる可能性がある。例えば、先端技術や新技術に携わる学生や研究者は、地元や国の当局から大きな関心を寄せられる可能性がある。

デューディリジェンスとリスク評価の実施

海外への渡航には、異なるリスク環境、海外における法的・社会的・文化的規範の違い、海外の事業環境の変化を考慮した特別なプロセスが必要である。

学内にその地域の専門家がいる場合には、リスクレベルに関する大学の意思決定や職員への情報提供のために、専門家として関与すべきである。

一貫性のある安全な渡航方針は、海外への渡航や関連する活動を安全に管理するために必要なステップを概説し、リスクがエスカレーションして機関の承認

を得るプロセスなど、明確な承認プロセスを明らかにしていなければならない。また、渡航方針では、それぞれの状況において輸出規制やその他の英国の法律がどのように適用されるか、また、海外に渡航する個人に対する現地の法律の影響を考慮する必要がある。

各機関は海外渡航の記録を保持し、特定の国や地域への渡航に伴う特定のリスクに関する内外の知識を活用すべきである。さらに、教育機関は仕組みや手続きを、事故後だけでなく、定期的にモニタリングし、見直すための正式な方法を確立すべきである。

特定の国への渡航には、特別な配慮と準備が必要である。セキュリティ関連の特定のリスクについて学生やスタッフを教育するための仕組みを設けるべきである。これには、学生とスタッフが、関連するポリシーや行動規範、海外渡航前に求められることやその他の義務を確実に理解するための、適切なトレーニングが含まれるべきである。

ケーススタディ：海外でのデータ消失

ある海外の大学が、英国の教授を VIP 待遇で招待し、彼らの国で開催される国内会議で基調講演を行った。これは、教授にとって、自分の研究を紹介し、上級レベルの人脈を作り、権威ある国際会議で学部を紹介する絶好の機会だった。教授とゲスト 1 名には、ビジネスクラスの航空券、高級ホテルの宿泊費、滞在費など、すべての参加費用が提供された。これらの費用については渡航前に大学に申告した。教授は以前にもこの国を渡航したことがあり、リスクは無視できると感じていたため、渡航リスク評価は行わなかった。教授は到着後、ホスト機関との参加同意書に署名した。

シナリオ

学会で発表するために、教授は大学のノートパソコンを持っていった。彼女はホテルの部屋で定期的にデバイスを充電し、会議の主催者がプレゼンテーションを円滑に進めるためにポータブル・ストレージやその他のデバイスを接続することを許可した。彼女の基調講演と訪問は成功し、好評を博した。

それから数ヶ月後、その教授は、自分が基調講演を行った国の大学で、自分の未発表の研究が発表されているのを見て非常に心配になった。会議の参加契約書を確認したところ、教授は自分が会議で発表された資料の権利放棄にサインしてしまったことに気付いたが、その中には講演中にプレビューした未発表の

資料も含まれていた。

教訓

- この機関は、すべての海外出張に先立って、スタッフ、学生、研究者の責任を明確にするための適切なリスク評価とガバナンスの仕組みを欠いていた。
- すべての海外出張には、適切な出張承認とリスク評価が必要である。
- ある国やパートナーが教育機関や海外渡航者にとって既知のものである場合には、過信がプロトコルの信頼性に影響を与える可能性がある。
- 渡航する学者や研究者には、データの盗難や漏洩の可能性を含め、関連するセキュリティポリシーに関するトレーニングが必要である。

3 キャンパスを守る

概要

本章は、潜在的な敵対行為に関連するセキュリティ関連のリスクからキャンパスと資産を守るために、貴機関を支援することを目的としている。この章では、貴機関の国際的なパートナーシップや協力関係の中で、サイバーセキュリティ、施設、visitors に焦点を当てている。

3.1: サイバーセキュリティ、施設、visitors

英国の高等教育機関は、ダイナミックで多様性に富み、国際的であることを誇りとしており、一年を通して世界中からスタッフ、学生、visitors が集まってくる。キャンパスとその関連施設へのオープンアクセスは、学術活動の重要な側面であり、それは必然的に安全なサイバーネットワーク、物理的資産、キャンパスという基礎の上に成り立っている。

大学への脅威は、デジタルネットワークへの計画的で巧妙な攻撃から、個人のサイバーセキュリティに対する意識の低さや、気まぐれな侵入まで多岐にわたる。このような侵害がもたらす影響は、所属機関にとどまらず、英国の安全と繁栄を脅かす可能性がある。

サイバーセキュリティ戦略の策定と実施

シニアリーダーは、サイバーセキュリティ戦略の策定と実施を確実に行う必要がある。これと並行して、サイバーセキュリティ情報共有パートナーシップなどの仕組みを通じた脅威のモデル化や政府・業界との情報共有など、サイバーセキュリティ・リスクに対する効果的な監視・報告プロトコルを策定する必要がある。

教育機関は、ソフトウェアやハードウェアへのアクセスを管理するために、さまざまなサイバーセキュリティポリシーや手順を持っているはずである。しかし、パートナーシップや共同研究がより厳しく監視されるようになると、サイバー攻撃の頻度と巧妙さが増してくると考えられる。機関は以下のことを確認する必要がある。

- NCSC が毎週発表している脅威評価など、公表されている脅威評価を利用し

て、起こりうるサイバー脅威を予測する。

- NCSC のサイバーセキュリティに対する 10 のステップを理解し、実行している。
- NCSC Cyber Essentials スキームによる認証を検討する。

より大きなリスクにさらされる可能性が高い特定の価値を持つ情報の保護に特に注意を払う必要がある。これには、例えば、潜在的な経済的価値のある研究、政治的・商業的にセンシティブな資料、センシティブな企業データ、スタッフや学生のデータなどが含まれる。

学内のサイバーセキュリティ・リスク対応プロセスを定期的に見直し、可能であればその結果を他の機関や政府と共有することで、今後のインシデントへの対応を強化することができる。このような情報交換は、機関、セクター、政府の対応能力を高めることになる。

適切なトレーニングは、安全性の高い問題、規制された技術、輸出規制の対象となるその他の研究分野に従事する研究者にとって特に重要である。教育機関は、研究資料を分離し、機密データや情報へのアクセスを制限・監視する必要性を強調したポリシーやトレーニングパッケージを開発する必要がある。そのような方針には次のようなものがある。

- 機密性の高い研究の分離 ： 研究の異なる分野を分離し、物理的にもオンラインでもデータや情報が一箇所に集中しないようにする。
- アクセス制御 ： データやネットワークにアクセスできるのは、正当な要件を満たすユーザーおよびパートナーのみであり、可能な場合は 2 段階の本人確認を行う。
- IT プラットフォームのセキュリティ ： 共同で使用する IT プラットフォーム（特に第三者が使用するもの）のセキュリティについて、スタッフや学生が理解できるようなポリシーを策定する必要がある。
- 域外管轄権の問題からの保護 ： 一部の国家が機密性を有するとみなす問題についてオンラインでの議論に参加する研究者や学生が直面するリスクを慎重に検討し、これらの個人に通知するための手段を講じる必要がある。

意思決定者を支援するため、JISC と英国大学協会は、2013 年に発行したガイダンス *Cyber Security and universities: Managing the Risk* の最新版を発行する予定である。このセクションは、更新されたガイダンスが利用可能になり次第、更新される。

施設と visitors に関する統合的な方針の策定

セキュリティ関連の問題に対する認識を、既存の施設および visitors に関する方針に組み込む必要がある。スタッフと学生の両方を対象とした、visitors に関するポリシーと手順が必要である。

データの損失に関するケーススタディが示すように、デジタル及び物理的なインフラは、セキュリティ侵害に対して脆弱である。キャンパスのインフラを保護するためのすべての組織のポリシーとフレームワークは、特定の物理的なセキュリティリスクをカバーする必要がある。

キャンパスへの visitors に関連して、これらのポリシーには以下が含まれる。

- 異なるタイプの visitors を明確に区別する枠組み、ポリシー、リスクアセスメント（例えば、専門職と研究職、学部生と大学院生、短期滞在と長期滞在など)。
- 身分証明書の確認、ビザ要件の遵守状況の確認、アクセスが承認された訪問期間に限定されていることの確認など、キャンパスの制限区域への visitors の事前、到着時、滞在中の適切なチェック
- すべての visitors およびビザ契約に対する監督および説明責任
- ビザまたは ATAS 申請で許可されていないコースまたはプロジェクトへの visitors のアクセスに関する制限、および訪問中にこれらを変更するための監督と説明責任の明確なプロセス
- visitors およびスタッフに対して、キャンパス滞在中に適切なプロトコルを遵守する必要性を伝えるための明確なアドバイス、情報、ガイダンス。

ポリシーをどのように設計し、実施するかについては、教育機関が個別に判断する必要がある。キャンパスへのアクセスレベルは、実施される活動の種類に応じて異なると思われる。

ケーススタディ：スタッフの訪問

シナリオ

英国を拠点とする外国人大学院生が、母国の大学の研究グループとのつながりを維持していた。その学生は、2 つの研究室間でより正式なパートナーシップを結ぶ許可を求め、それを促進することを申し出た。当時、この研究は輸出規制の

対象ではなく、また当初、研究の規模が小さかったため、この新しいパートナーシップは高度な学内デューデリジェンスや監督の対象外だった。

パートナーシップの確立後、学生は海外の研究室の同僚を英国の研究機関に招待し、旅費などの手配や滞在中の通訳のサポートを行った。提携開始から約１年後、英国の研究代表者は、この関係が非常に一方的であることを懸念した。海外の研究室は非常に資金力があるにもかかわらず、新しい研究や技術のフォローアップが遅れていたのである。また関係を再評価した結果、代表はは研究が輸出規制の対象になる可能性が高いことに気づき、パートナーシップを解消した。

その後、訪問中に代表団が英国の大学で研究室を再現する目的で、研究室の設備を詳細に撮影していたことが明らかになった。

教訓

- 海外のパートナーは、技術や研究が輸出管理法の対象となる前の初期段階の開発にアクセスしようとする可能性がある。
- すべての国際的なパートナーシップには徹底したデューデリジェンスが必要であり、提案されたパートナーとその識別可能な関連団体をさらに調査して、その事業の規模とスケールを確認する必要があるかもしれない。
- 訪問するスタッフや学生に対しては、キャンパス訪問やツアーの前に厳格な手続きを行う必要がある。
- ビザの招待状は、学生ではなく、適切な上級スタッフのみが権限を持つべきである。

4　パートナーの保護

概要

本章は、貴機関が国際的なパートナーシップを維持するための支援を目的としている。本章は 2 つのセクションに分かれている。まず、関連する法律を参照しながら、大学が研究パートナーシップを保護するために必要な措置について考察する。次に、大学が国境を越えた教育パートナーシップを保護する方法について考察する。

ケーススタディでは、研究サイクルのすべての段階において、予想される課題と、知的財産（IP)、研究の完全性、関連法の遵守を守るための実践的な行動を示している。

シニアリーダーは、国際的なパートナーシップにおいて知的財産を保護し、輸出管理法を遵守し、倫理を促進するプロセスを、研究スタッフと学生が理解し、遵守することを確実にするための対策を講じる必要がある。

4.1: 研究の安全性、知的財産、輸出管理の遵守

世界をリードする英国の研究は、いよいよオープンで協力的になっている。これは、重要で刺激的な機会をもたらすと同時に課題も生み出す。英国の高等教育機関は、研究や知的財産への不当なアクセスを求める海外の個人や組織による定期的かつ標的的な試みにさらされている。

NCSC と CPNI は、各機関が国際的なパートナーシップについて十分な情報を得た上で意思決定を行い、かつ研究者や学術的価値を保護するためのガイダンス、*Trusted Research* を開発した。このガイダンスは、STEM 科目、デュアルユース技術、新興技術、商業的にセンシティブな研究分野における研究に特に関連するものである。

研究者が管理・軽減すべき主なセキュリティ上の脅威・課題には以下のようなものがある。

- 正式な資金提供を受けた研究プロジェクトの一部ではないものも含め、国際的な研究パートナーシップに関する不十分なデューデリジェンス
- 研究パートナーシップおよびプロセスの不適切な監視とモニタリング
- 契約段階および研究パートナーシップ全体において、知的財産が適切に保護

されず、知的財産が流出すること。

- サイバー攻撃や個人的な財産の窃盗など、敵対的な行為者による知的財産の窃盗
- 輸出管理およびデュアルユース技術に関する法的枠組みの不遵守

海外との共同研究パートナーシップに関するデューディリジェンスの実施

共同研究に関して、各機関は正式なパートナーシップや非公式な共同研究、資金提供の有無を問わず、すべてのタイプの海外パートナー候補に対して、リスクに見合ったデューデリジェンスを行わなければならない。輸出規制の対象となるものを含む機密性の高い研究分野では、たとえそれがその場限りの非公式なものであっても、研究に関するあらゆるやり取りや議論が必然的に含まれることになる。場合によっては、これらのプロセスは、United Kingdom Research and Innovation (UKRI)などの資金提供組織によって監査される。

知的財産を保護するための方針と契約の実施

研究や知的財産の盗用や悪用は、研究サイクルのどの段階でも起こり得る。前述の「信頼される研究」ガイダンスを含め、このような事態から保護するためのツールやフレームワークが存在する。このガイダンスは、研究者、英国の大学、産業界のパートナーが国際的な活動に自信を持ち、研究とスタッフを潜在的な盗用、誤用、搾取から保護することを目的としている。

所属機関は、名誉職員や英国人・非英国人を含むすべてのスタッフが、所属機関との直接的な雇用関係にない利益相反やその他の職業上の義務、関連する所属や法的な契約を申告するために、外部業務や利益相反に関する方針を持たなければならない。

輸出管理法を確実に遵守する

研究者および研究スタッフは、規制されている技術に関連する法律および規制の枠組みを認識する必要がある。代表的な例としては、輸出規制と ATAS（Academic Technology Approval Scheme）がある。

英国の戦略的輸出規制は、大量破壊兵器（WMD）の拡散を防止することを目的として、機密技術、情報、戦略物資の輸出および移転を制限することを目的としている。

所属機関で行われる研究またはその他の活動に、輸出規制がどのように適用されるかを理解することは、所属機関の責任である。輸出管理法を遵守しないことは、犯罪行為であり、重大な法的結果を招く可能性がある。

重要な点は、「技術」および「情報」という用語は、通常または一般的に理解されているよりもはるかに広範な定義が法律において定められているということである。

輸出管理法を最大限に遵守するために、個人は以下を行う必要がある。

- 技術の潜在的な用途の可能性を考慮する：研究のライフサイクルを通じて、研究の潜在的な最終用途を監視することは、研究者とその所属機関の義務である。場合によっては、開発の初期段階では特定できない最終用途を持つ研究もあり、継続的な監視が必要である。
- 研究者に無形の技術移転の意味を伝える：研究者は、電子的（ソーシャルメディア、ファックス、電子メール、ビデオ会議、遠隔地での画面共有など）および口頭（電話や対面での議論など）で伝達される管理された機密情報が、依然として輸出規制の対象となる可能性があることを認識する必要がある。

ATAS は、英国の入国管理局の管理下にあり、特定の機密性の高い科目で大学院レベルの学習をしようとするすべての留学生に、ATAS 証明書の申請を義務付けている。申請は、英国での学習を開始する前、あるいは大学のシステムにアクセスする前に行わなければならない。機密性の高い科目とは、大量破壊兵器やその運搬手段を開発するためのプログラムに使用される可能性のあるものを指す。ATAS は Foreign, Commonwealth & Development Office（FCDO）によって運営されており、国籍が欧州経済領域（EEA）およびスイス以外にあるすべての学生に適用される。

ケーススタディ ケーススタディ：海外政府との契約および任命

ある教授が英国の大学に着任した。大学側には知らされていなかったが、この教授は、応用軍事研究のための国立研究所を率いるなど、多くの海外政府プロジェクトに有給で関わっていた。定期的な出張をせずにこの仕事を進めるために、教授は海外の研究室から客員研究生を受け入れた。この研究生は、デュアルユースの研究や技術を海外の研究所に移転するために働いた。

シナリオ

同僚が教授の仕事量と体調不良を心配した。教授は学外の役職に就き、シャド

ーラボを運営していることを告白した。教授は、海外での契約により、法的にも倫理的にも危うい立場に置かれていたこと、海外政府の雇用主の同意なしに関係を開示することができないこと、年に何ヶ月も追加で働く必要があることを認めた。さらに、翌年には英国での雇用を縮小し、既存の契約に沿って母国と研究室に戻るように指示されていた。資金提供を受けた客員研究生の大半は、海外の国の軍事開発活動に直結していることが判明した。

教訓

- 教育機関のスタッフや学生が、輸出管理規制を回避し、認可を受けずに技術を移転するために採用されることがある。
- この機関では、海外からの任命や利益相反を特定するための方針が定められていたが、これらの手続きは適切かつ強固なものではなかった。教育機関は、特にリスクの高い研究分野に関連して、警戒、リスクの最小化、および脆弱性を特定するための支援の文化を促進すべきである。
- 大学の方針は、すべてのスタッフに、海外での任用、コンサルタント、名誉職などをすべて開示することを求めなければならない。大学は、独立した学術研究が確実に守られるよう、ゲスト研究者の経歴の確認に積極的に取り組まなければならない。

4.2: トランスナショナル教育パートナーシップ

英国の大学はトランスナショナル教育（TNE）の世界的リーダーとしての評判が高い。英国の教育機関には、海外で英国のプログラムに登録している学生が70万人近くおり、「国際教育戦略」では、この活動の成長を支援する目標を掲げられている。このような活動は、教育機関に大きな機会をもたらすが、同時に、認識すべき様々なリスクも存在する。

英国のプロバイダーがTNEの取り決めを行う場合、現地の規制の対象となり、現地当局の指示に従わなければならない。TNE事業は、セキュリティ関連の問題のリスクが高くなる可能性がある。大学にとって重要な問題は、現地の要求に応じて、大学の中核的価値を確実に守ることである。大学は、海外政府の要求に従うか、活動を中止するかの選択を迫られることがある。

多くの大学はリスク管理において大きな進歩を遂げており、拠点間でのリスクの評価、ランク付け、軽減を可能にする統合管理モデルを採用している。しかし、こうしたシステムでは、海外のパートナー組織に影響を与えるリスクを外部の

ものとして扱い、統合できないことがある。健全なリスク軽減方針は、海外のパートナーに異なる影響を与える可能性のあるリスクの存在を認識・評価し、可能な限り、海外の多国籍パートナーと残存リスクを共有する枠組みを構築するべきである。

海外パートナーに対する徹底した定期的なデューディリジェンスの実施

TNE 活動によって、リスクのレベルは異なる。研究活動を行うスタッフがいるブランチ・キャンパスは、海外のプロバイダーが教えるプログラムを検証するためのパートナーシップよりも、受入国政府の高等教育政策の影響を受ける可能性がある。デューデリジェンス・プロセスの中でリスク軽減戦略を策定するシニアリーダーは、以下のことを行う必要がある。

- 特定の TNE の取り決め（科目や関連する要因など）に照らして、スタッフ、学生、研究、知的財産、その他のリソースがどの程度干渉を受けるかを検討する。
- 多様なリソースからの情報を活用し、海外で事業を行う際の潜在的なリスクを総合的に理解する（FCDO、関連する英国大使館または領事館、ブリティッシュ・カウンシル、海外の英国商工会議所、信頼できるパートナーなどを利用する）。
- 海外の TNE パートナーが、英国の教育機関の目的と互換性のある学術的・組織的な目的を持っていることを確認する。
- 出身国における国際機関の研究パートナーシップや関係性を理解する。例えば、パートナーが政府や軍事研究機関とのつながりを持っているかどうか。
- どのような研究を行うことができるか、どのような関係を結ぶことができるかについて、枠組みやガバナンスを構築する。

大学の自立性や学問の自由に対するリスクをリスク・レジスターやリスク・ステートメントに含める

大学の自立性に影響を及ぼすリスクや、国と高等教育機関との関係に対する異なるアプローチは、特に学問の自由の侵害を通じて、英国高等教育の中核的価値を脅かす可能性がある。教育機関は以下のことを確認すべきである。

- 海外の大学自治や学問の自由に関連するリスクがリスク・レジスターやリスク・ステートメントに含まれ、統治機関の監督のもとで適切に監視されてい

ること。

- 海外の政府当局との関係について、その自主性、独立性、透明性の度合いを含めて、将来のパートナーや既存のパートナーがそれを十分に理解していること。

TNE 活動を監督するシニア・リーダーには、現地の価値観、法律、慣習、期待を理解するとともに、海外における英国の高等教育の価値を守るための方針や手続きを策定する責任がある。こうした配慮は、大学の自立性や、国と高等教育機関との関係にも関連している。例えば、多くの地域では、大学は公的機関であり、政府によって任命された職員や事実上の公務員を抱えている。このこと自体がコラボレーションやパートナーシップを阻害するものではないが、大学はこの関係がリスクになるかどうかを考慮しなければならない。

シニアリーダーは、外国の管轄区域を拠点とする TNE 事業に関連する緊張や対立に対してオープンで透明性を保ちつつ、相互に尊重してトレードオフを管理することを目指すべきである。

強固で中央集権的なリスク管理と現地の自主性とのバランスを維持する。

TNE 事業の大半は、海外のステークホルダーとのパートナーシップによって成り立っている。多くの場合、これは現地当局や規制当局からの要請であり、TNE 事業の正式なパートナーとなることもある。教育機関は、これらのパートナーシップが、強固な中央集権的リスク管理と十分な現地における自治のバランスを保つようにしなければならない。シニアリーダーは以下を行うべきである。

- 関連する方針や手続きが、海外のパートナー機関で使用されているものと比較し、そのバランスを検討する。また、発生した問題を早期に提起し、解決するための強固なガバナンス体制を構築する。
- セキュリティ関連のリスクを、ガバナンスプロセス、リスクポリシー、英国および海外のリスクレジスター、保証・監査プロセス、緊急事態に対応した事業継続計画など、リスク管理フレームワークに組み込む。
- 英国の大学に雇用されている、または登録されている、海外に拠点を置くスタッフや学生の利益が適切に保護されていることを確認する（例えば、英国のプロバイダーに登録している学生に 対しては、大学の学生保護計画を利用すること）。

- 無形資産を含む適切で安全なアクセスプロセスと手順が実施されており、リソースの機密性に適しており、誰がそれらのリソースにアクセスできるかを中央で監視していることを確認すること。
- CPNI の資料に概説されているように、あらゆるサイバー・ネットワークの安全性を維持するために、関連する適切な措置が講じられていることを確認すること。

現地の利害関係者とのコミュニケーションのために、明確な報告ラインと安全な空間を共同で確立する。

最も成功している TNE パートナーシップは、相互の信頼関係と強固な監視メカニズムを兼ね備えている。現地のパートナーは、TNE に影響を与える規制、経済、社会の変化を認識し、それに対応するのに最も適した立場にあるだけでなく、英国の大学が活動する地域で教育活動を行うために不可欠な特定の法的行為を行う権限を持っていることが多い。

海外の利害関係者（学生とその家族、スタッフ、提携プロバイダ、現地当局、規制当局）からの信頼を獲得し、維持することは、大学が TNE 事業におけるリスクを特定し、管理し、軽減するためには極めて重要である。海外事業に適用される明確な報告ラインと安全なコミュニケーションの場（内部告発ポリシーを含む）を共同で確立することで、セキュリティ関連のリスクを早期に発見することができる。しかし、現地のパートナーがより多くのリスクにさらされているにもかかわらず、共同でリスク評価を行うことはまれであることに留意すべきである。シニアリーダーは下記のことに留意しなければならない。

- 現地の教育機関、当局、企業、雇用者、労働組合、非政府組織、市民社会、英国大使館、領事館、専門機関など、教育パートナーシップに関与する主要な関係者を把握する。
- 地域の利害関係者との関係、および地域の利害関係者同士の関係に影響を与える可能性のある力関係やその不均衡を認識する。
- 可能であれば、干渉の伝播のリスクを高める可能性のある、現地パートナーの組織構造および財務構造の脆弱性を評価する。
- 現地のステークホルダーが、特に不正行為、知的財産権の盗難、汚職行為に関連するリスク管理システムを構築し、共同で所有するための支援体制を確保する。

- 現地のパートナーが適切なレベルの機密性とデータおよび個人情報のセキュリティを確保した上で懸念を提起できるよう、適切なコミュニケーションチャネル（内部告発ポリシーを含む）を確立する。

包括的なルールベースの取り決めとハイレベルな原則に支えられた出口戦略の策定

TNE パートナーシップは時間とともに変化するため、教育機関はその範囲を定期的に見直す必要がある。パートナーシップを終了する必要がある場合には、出口戦略を用意しておくことが重要である。この戦略は、すべての TNE パートナーに伝達されたハイレベルな原則に支えられていなければならない。

この戦略は、すべての TNE パートナーに伝えられたハイレベルな原則と、学問の自由、知的財産、資産などの問題に対処する包括的なルールベースの取り決めによって支えられるべきである。シニアリーダーは以下を行うべきである。

- TNE パートナーに伝達された一連のハイレベル原則を明確に定義する。
- 学問の自由、知的財産、資産、人員配置などの重要な問題を保護するための規則に基づく取り決めを行う。
- パートナーシップの取り決めが終了した場合には、適切な移行措置やその他の取り決めにより、学生が保護されるようにする。

ANNEX 2:

サイバーセキュリティ、エステ、ビジターのポリシーに関する指針となる質問

1. セキュリティ関連のリスクや海外からの脅威は、サイバーセキュリティ戦略、施設ポリシー、visitors 向けの手順やプロトコルに十分に組み込まれているか。
2. キャンパスとインフラの保護に関する戦略を監督・実行する責任者間では、デジタルシステムの保護、物理的資産の保護、visitors の手続きやプロトコルの保護のすべてにおいて十分な連携が取れているか。この連携をサポートするために、どのような仕組みがあるか。
3. 秘密保持契約（NDA）があるものを含めて、キャンパス内で行われている研究活動の種類、visitors の範囲、建物への出入り等の複数の要因を考慮して、各建物のリスクを評価するための定期的なリスク・アセスメントが実施されているか。
4. リスク評価は、デジタルシステムの保護、物理的財産、visitors の手続きやプロトコルなど、関心のある様々な分野の専門知識と責任を有する者によって行われているか。
5. 機密性の高いデータや施設へのアクセスを、アクセス権を持つ者が定期的に確認する手順が確立されているか。

ANNEX 3:

研究の安全性、知的財産、輸出管理のためのチェックリスト

《研究セキュリティのチェックリスト》

国際的な研究パートナーシップのデューデリジェンス

1. 国際的な研究協力を開始する前に、相応のリスク評価を行うための要件はどの程度明確か。
2. 海外の研究プロジェクトのリスク評価を行う責任者は誰か。
3. 研究の性質やパートナーシップの種類によって追加的な監督が必要な研究契約を特定するために、学内にはどのような方針があるか。
4. 新たな研究パートナー候補が行っている研究事業の規模や種類を、学内でどのように調査しているか。

5. 個々の研究者や研究責任者によって設立された小規模または非公式の研究提携を監視するための機関内プロセスはあるか。
6. リスクの高い国際的な研究提携について継続的にデューデリジェンスを行うために、どのような追加資源や支援が必要か。
7. 契約書の翻訳版に同一の条件が正しく含まれていることを確認するための措置をとったか。

知的財産を保護するための方針と契約上の合意

1. 貴機関では、知的財産（IP）を保護するためにどのような方針、ツール、フレームワークを使用しているか。
2. 共同研究の契約書に署名し、監視する責任を持つのは誰か。
3. 英国と海外の研究者間の 1 対 1 の共同研究など、資金提供を伴わない研究プロジェクトの契約や合意のプロセスはどのようになっているか。
4. 契約上の研究合意に対する違反や変更に対処するプロセスはどのようなものか。
5. 英国を拠点とする研究者と海外を拠点とする研究者の両方が、外部での仕事の義務や利益相反を定期的に開示するよう求められているか。
6. サイバーセキュリティの侵害や個人所有物の盗難による知的財産の盗用やレバレッジド・トランスファーから研究者を守るための対策を支援するために、どのようなトレーニングが用意されているか。

デュアルユース技術と輸出管理法

1. 研究者は「デュアルユース」という言葉を理解し、それが自らにどのような影響を与えるかを知っているか。
2. 研究者は自分の研究がデュアルユースになる可能性をどのように合理的に判断することができるか。
3. 研究者は、自分の研究が、英国の経済的、社会的、安全保障上の利益の促進と矛盾する目的のために使用される可能性を、どのような方法で考慮できるか。
4. 輸出管理法やその他の関連する法律の枠組みを確実に遵守するために、どのような戦略があるか。研究者が学内・学外を問わず、どのような場合にさらなる助言を求めるべきかについての指針があるか。

5. 投資家が英国の戦略的輸出規制や同様の措置を弱めたり、回避しようとしたりするリスクはあるか。