参考資料３

豪州の大学セクターにおける外国の干渉に対抗するためのガイドライン

外国の干渉タスクフォース
University Foreign Interference Taskforce
November 2019
※下線は訳者

声明

豪州の大学システムが世界トップクラスの実績と評価を得ている要因は、世界に対して開かれていることにあり、それが大学の競争力の基盤でもある。

このグローバルな取り組みにより、豪州では、世界トップクラスの研究者が世界中の最先端の研究者と協力して最先端の研究を行うことができている。また、世界の優秀な学生を教育することで、彼らは卒業後、豪州に対する知識と愛情をもって帰国することができる。

これは豪州にとって強力なソフトパワーとなる。また、豪州は、世界の優れた専門家を採用して、豪州の大学で教えたり研究することができ、豪州の国力を競合国よりも飛躍的に向上させることができる。国際経験とコラボレーションは世界中のアカデミック・キャリアパスにとっての不可欠である。グローバルなアイデアの交換は人々の多様な交流によって可能になる。

豪州政府は、グローバル人材ビザ、国際教育を促進するための豪州貿易委員会の包括的なプログラム、新コロンボ・プラン、外国人研究者の豪州国内の競争的補助金制度への参加資格、豪州／中国科学研究基金や豪州／インド戦略研究基金などの対象研究基金の提供、豪州の学生や教職員の海外渡航の支援など、幅広いイニシアチブやポートフォリオのプログラムを通じて、このような国際的な協力関係を支援している。

このような重要なグローバルな取り組みは、これまで以上に複雑化した世界で行われている。それに伴い、知的財産やITシステムなど、新たな課題や脅威が発生している。2018年に発生したオーストラリア国立大学へのサイバー攻撃は、こうした脅威の顕著な例である。何十年もの間、豪州の大学は、セキュリティ問題に関して政府機関と強固な協力関係を築いており、人材、研究、システム、知的財産を保護し、セキュリティを破ろうとする試みを阻止するために、定期的にアドバイスを求めてきた。大学と政府は、リスクを管理して利益を実現するため

には、強固で信頼できる国際協力システムが必要であることを理解している。

豪州のダン・テハン教育大臣は、国内の大学と政府が外国からの干渉に対する既存の安全策を強化するための共同タスクフォースを設立した。より複雑なリスクが存在する世界において、私たちは、豪州の世界的な大学システムの成功に欠かせない開放性と協力関係を維持しつつ、現行の保護機能を強化するために協力している。

この作業は、大学セクターと政府機関が意見を出し合いながら進められており、国際的に展開する大学の専門知識と、新たな脅威に対応する安全保障機関の知見を利用している。

豪州の大学セクターの知的財産権を強化するための４つのガイドライン

タスクフォースは、「文化とコミュニケーション」「海外との連携」「研究と知的財産」「サイバーセキュリティ」の４つの戦略分野に焦点を当てた。その目的は、大学がグローバルな活動を行う上でのリスクを評価し、人材やデータを保護するための指針を提供することにある。大学と政府が共有する目的は、豪州の大学セクターの安全性を守る一方で、コミュニティの利益を最大化する開放性というかけがえのない資産を損なうことのないようにすることにある。

タスクフォースにとっての包括的な原則は以下である。

- セキュリティは、学問の自由、価値観、研究上の協力関係を守るものであること。
- 国益に配慮した研究、協力、教育活動であること
- セキュリティは個人の説明責任を伴うものであること。
- セキュリティは組織のリスクに比例すべきであること。
- 大学コミュニティの安全が最も重要であること。

このガイドラインは、大学に新たなコンプライアンスや規制上の負担を強いるものではない。また、外国からの干渉のリスクに関する大学の検討事項をすべて網羅することも意図していない。本ガイドラインの目的は、大学が既存のツールを検討することを支援し、意思決定者が外国からの干渉によるリスクを評価することを支援し、大学全体のガイドラインの一貫性を高めることにある。

脅威

2019 年 10 月、豪州のマイク・バージェス安全保障局長は、豪州の利益に対する外国の干渉が前例のない規模で行われていることを指摘した。現在、特定の外国アクターは大学や研究分野を含む豪州社会の様々な分野において豪州の意思決定者に干渉する機会を探っている。

「外国の干渉」と「外国の影響力」

外国の干渉

外国の干渉とは、外国の行為者によって、または外国の行為者の代わりに強制的、隠密的、欺瞞的、または腐敗的な活動が行われ、そのことが豪州の主権、価値、国益に反する場合に起こるものである。

外国の影響

豪州を含むすべての政府は、自国にとって重要な問題について影響を与えようとしている。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ている場合には、国際関係と外交の正常な側面であり、公共の議論に積極的に貢献することができる。

外国の干渉の脅威に対して大学が積極的に対応することは、豪州の大学のレピュテーションを守り、学問の自由を保護し、学術機関と豪州経済が研究活動の成果を最大限に発揮できるようにすることにつながる。このような対応は、外国政府が豪州で外国からの干渉を行う際のコストを高め、利益を減らすことを目的とした豪州の外国からの干渉対策（CFI）戦略と一致している。

国際的な交流の大部分は歓迎されるものであり、豪州の利益となっている。しかし、以下のような方法で、大学部門に干渉しようとする外国のアクターがいるかもしれない。

- 研究テーマを変更したり、またはそれに対する指示を行う
- 経済的圧力
- ポスドクやアカデミック・スタッフの勧誘・採用
- サイバー攻撃など

外国からの干渉による未曾有のリスクのため、2019 年に大学と政府機関がさらなる連携を協議した。2019 年 8 月、教育担当大臣は、大学セクターにおける

外国からの干渉に対抗するためのガイドラインを策定するため、「外国からの干渉タスクフォース」の設立を発表した。

このガイドラインは、豪州の大学セクターにおいて、グローバルな連携を損なうことなく、これらの脅威に対するレジリエンスを高めることに貢献するものである。

はじめに

大学は、新たな知識の開発や技術革新において重要な役割を果たしている。大学の自治には、国益を考慮し、政府や安全保障機関の支援を受けて、リスクを管理し、それに対処するための積極的なアプローチが含まれる。本ガイドラインは、時間の経過とともに発展・変化する新たな脅威や圧力に対して、レジリエンスと対応力を兼ね備えた方法で、大学をさらに強化することを目的としている。

豪州の大学は、国際的な活動に深く関わっており、世界中の優秀な人材と知識を共有し、発展させている。豪州の人々は、情報や知的財産から著しい恩恵を受けている。国際的な協力関係は、世界をリードする研究の創出に不可欠である。われわれは外国からの干渉のリスクを防ぐための大学の方針を策定する一方で、そのことと自由な意見交換、開かれた研究文化、学問の自由を促進することとの間に、潜在的な緊張関係があることを懸念している。

大学は、芸術、社会科学、医学、工学、情報技術など、幅広い分野の研究を行っている。多様な研究分野においては、リスクの比例原則、ならびに対応の規模を考慮することが重要である。リスクの比例原則はガイドラインの下敷きになる。国際的な交流の大部分は豪州の利益につながるものであり、本ガイドラインは、リスクの低い学術活動の大部分を阻害することを意図したものではない。

大学の自治という基本原則を堅持しつつ、外国からの干渉に対するレジリエンスを強化するために、いくつかの重要なテーマを掲げている。大学は、国際的な共同研究や関与に関連するリスクの管理を含め、リスク管理のフレームワークや関連するポリシー、プラクティスの開発にすでに多大な投資を行っている。本ガイドラインで示されているリスクを管理するための主要なテーマや目的、ベストプラクティスの検討は、こうした基盤の上に構築されるものである。

主なテーマは以下の通りである。

ガバナンスとリスクフレームワーク

- 外国からの干渉に対する抵抗力を高め、積極的な安全・セキュリティ文化を促進・強化する構造を確保する。
- 既存のリスクフレームワーク、ポリシー、手続きに外国からの干渉リスクを含め、人、情報、資産のセキュリティに貢献する大学の能力を構築する。

デューディリジェンス

- リスクに見合ったデューデリジェンスを適用する。
- 研究テーマと潜在的な研究パートナーの機密性に基づいて、慎重にリスク評価を行う。
- 内部のガバナンス要件に加えて、大学の方針と手続きでは、2012 年国防貿易管理法（DTCA）や Foreign Influence Transparency Scheme Act 2018 などの法的枠組みが適用されるかどうかを考慮する。
- 潜在的な外国からの干渉や風評被害のリスクを考慮し、適切なデューデリジェンスを行うことでパートナー、研究協力者、スタッフを保護する。

コミュニケーションと教育

- コミュニケーション戦略と教育プログラムにより、外国からの干渉のリスクに対する認識を高める。
- 意思決定者に、リスクに見合った警戒レベルを可能にする知識を提供する。

コミュニケーション戦略、教育および専門能力開発プログラムは、大学のセキュリティ文化へのコミットメントを促進し、リスクとその影響についての認識を高めるものである。

知識の共有

- 新たなリスクや外国からの干渉の経験について、部門全体および部門と連邦の間での知識共有メカニズムを強化する。
- 安全保障機関が、リスクと適切な対応を設定するために、大学への支援を強化する。ただし、重要な情報はこれまでもすでに大学に提供されている。

サイバーセキュリティ

- 堅固なサイバーセキュリティ戦略の開発と実施、英連邦機関との連携、ベストプラクティスの共有、サイバー脅威のモデル化を通じて、ICT システム上の情報を保護する。

本ガイドラインの使用方法

本ガイドラインは、大学の自主性を尊重するものであり、規制を目的としたものではない。外国からの干渉に対するレジリエンスを高めるために、リスクを管理し、それに対処するための主要なテーマと目的が設定されている。ベストプラクティスは、意思決定者のリスク管理を支援するために、主要なテーマと目的を補足するものである。

大学はすでに、積極的なセキュリティ文化を確保するためのポリシー、フレームワーク、システム、仕組みを持っている。本ガイドラインの目的は、意思決定者が外国からの干渉によるリスクを評価し、リスク軽減戦略を推進するのを支援するための、教育上そして政策上の対応を示すことにある。

本ガイドラインは、国際的な経験に基づき、豪州の大学がすでに実施しているリスク管理方針やセキュリティ対策を参考にしている。本ガイドラインは 2 つのセクションで構成されている。

- 大学が外国からの干渉のリスクを管理し、対処するためのな主要テーマと目的
- 意思決定者を支援するためのベストプラクティスの検討

ガバナンスとリスクのフレームワーク

目的

大学が、外国からの干渉に対するレジリエンスを促進・強化するための方針、構造、フレームワークを備える。

責任ある大学当局

■ 説明責任を有する者がセキュリティ・リスクを監督し、リスク軽減戦略に責任を持つ

学内のセキュリティ文化は、適切に配置された人員による積極的なリーダーシップ、コミュニケーション、決意に依存しており、それは決して短期的なプロジェクトにはならない。説明責任のある当局とは、説明責任を果たす上級管理職または執行部のことを指し、彼らは人員、情報、資産のセキュリティに責任を有する。

説明責任者は、外国からの干渉のリスクを評価、監視、軽減するためのポリシー、構造、フレームワークの継続的な開発と見直しを監督し、そのようなリスクを管理する個人の責任を育むセキュリティに対する土壌を発展させる。

意思決定の指針となる質問

- 貴学では、誰が外国からの干渉や保護措置の運用責任を負っているか？
- 外国からの干渉を防ぐために、安全とセキュリティに対する意識を高めるための大学の方針、慣行、仕組みは何か？
- 外国からの干渉を防ぐために、安全性とセキュリティに対する意識を高める大学の方針や実務、仕組みは何か？
- 外国からの干渉や保護措置に対して責任を持つスタッフは誰か？
- 法規制の遵守と外国からの干渉に関して、連邦政府の関連機関との連携のための方針はあるか？

外国からの干渉に関するリスク・プランニング

■ 大学は、既存のルール枠組みに、大学の人材、情報、資産に対する外国からの干渉の脅威と脆弱性に関する事項を組み込み、その対応策を説明する。

これには、人員、情報、資産のセキュリティに貢献する大学の能力の特定が含まれる。既存のリスク・フレームワーク、ポリシー、手続きに外国からの干渉リ

スクを統合することで、強固なセキュリティを促進し、不必要な重複を避けることができる。一貫した内部通報メカニズムにより、必要に応じてセキュリティ情報を政府機関と共有し、大学のセキュリティ環境に対する理解を深めることができる。

意思決定の指針となる質問

- 外国からの干渉をリスクとしてどのように認識しているか？
- スタッフや学生が特定のセキュリティリスクの影響を受ける人物を把握するための方針や手続きはどのように決められているか？
- セキュリティポリシーおよび手続きにおいて、ステークホルダーの範囲はどのように考慮されているか？
- セキュリティ・インシデントへの対応を管理するポリシーは何か？
- エスカレーション経路はどのようになっているか、またこれらのリスクに対する適切な対応はどのように明確化されているか？
- 内部の評価と外部のステークホルダーとのコミュニケーションをサポートするために、内部の報告メカニズムは一貫性を有しているか？
- 防衛省の輸出規制、外国からの影響の透明化スキーム、自立的制裁の遵守を確実にするために、連邦政府機関と連携するタイミングについて、大学全体の役割と責任はどのように明確化されているか？
- 特定の研究プロジェクトのリスクレベルと、当該リスクを軽減するために適用できるガバナンス、ならびに監視の程度を検討しているか？
- 研究活動の遡及的評価が行われた場合、どのような文書やテンプレートを用いて、これらの検討事項を記録し、参照できるようになっているか？

■ 大学の方針と手続きは、スタッフ、学生、契約職員、名誉教授等が国際的な共同作業に従事する際の要件をリスクに応じて説明するものである。

国際共同研究におけるあらゆるレベルの管理者の役割、責任、説明責任は、内部の利害関係者にとって明確である。方針や手続きが明確な言葉で書かれており、実施が容易である。方針には、外国からの干渉によるリスクを軽減し、大学の中核的価値を守り、必要に応じて DTCA やその他の規制の遵守を支援するためのガイドラインが含まれている。

意思決定の指針となる質問

- スタッフが起こりうるリスクを特定し、軽減するためにどのようなメカニズ

ムがあるか？

- スタッフの任用に大学の理事会や執行部はどの程度関与しているか？
- 職員が大学における権利と義務を認識していることを保証する仕組みはあるか？
- 外国からの干渉の可能性を特定する能力を高めるために、職員にどのような研修を行っているか？ 大学のリスク軽減戦略を遵守する必要性を理解するために、研究者や高等学位（HDR）学生にどのような研修を行っているか？
- 研究者が大学のリスク軽減戦略を遵守する必要性を理解するために、どのようなトレーニングや戦略が必要か？
- 研究者とその海外パートナーは、研究活動における利益相反をふくむ法的義務をどの程度認識しているか？

■ 明確な大学のリスク評価と報告の枠組み

外国からの干渉を管理する上で重要なのは、リスクを特定して管理することである。大学は、非公式および公式の研究活動、そしてそれによって創出される知的財産に対する外国からの干渉の影響を最小限に抑えるために、リスクベースのアプローチをとっている。リスクベースのアプローチとは、すなわち、以下を決定することである。

- 特定の研究プロジェクトに関わるリスクのレベル、および当該リスクを軽減するために適用可能なガバナンスおよび監督の性質を決定すること。
- 研究活動を遡って評価する際に使用できるよう、考慮すべき事項を確実に文書化すること。

意思決定の指針となる質問

- 外国からの干渉に対処するためのリスク・フレームワークはどの程度強固か？
- リスクに関する取り決めを維持、促進、適用する責任者は誰か？
- リスクに関する取り決めは、大学で行われている研究の範囲や関連するリスクのレベルにどのように対応しているか？
- 内部通報制度から収集した情報を分析し、それに対応するための能力はどの程度か？
- 海外からの投資やパートナーシップに対して、どのようなレベルの内部通報が適用されているか、それは説明責任とリスク管理に役立っているか？

■　透明性が高く、かつ明確な報告要件の策定、そしてその文書化

研究活動を妨害したり、不当な影響力を行使しようとする者は、研究アジェンダを不適切に変更したり、特定の研究分野に誘導しようとすることがある。これはセンシティブな形での不当な影響力や関与、将来的な価値の喪失や知的財産の管理につながる可能性のある資金提供の取り決めを通じて起こる可能性がある。

組織レベルでは、研究や潜在的なドナーとしての国際的なコンタクト（少なくとも国際的な共同パートナー）について内部通報を行うことで、大学のステークホルダー間で早期にそれを認識し、透明性を確保する能力を高めることができる。

意思決定の指針となる質問

- 内部通報制度から得られた情報を分析し、それに対応するために、大学にはどのような能力があるか？
- 名誉職や兼任職などを含む職員の任用について、どの程度の監視が行われているか。
- 外国からの投資やパートナーシップには、どの程度のデューデリジェンスが適用されるか？

■　大学は、利益相反ポリシー／利益開示ポリシーを有しており、このポリシーでは、外国との提携、関係、経済的コミットメントを特定し、豪州の大学に対するスタッフの責任を定めている。

大学は、国際的な機関との提携を含め、国際的な経済的利害関係を持つスタッフを特定するために、既存の利益相反契約に報告義務を含めることができる。

意思決定の指針となる質問

- 大学の共同研究ポリシーには、国際的な経済的利害やその他の利害がどのように含まれているか？
- 大学の利益相反ポリシーには、名誉職や非常勤職員などの雇用はどのように含まれているか？
- 紛争がどのように取り扱われ、報告されるかを監督する仕組みは何か？ これらには、潜在的なリスクを軽減し、学問の自由と言論の自由を守り、輸出管理法やその他の規制を確実に遵守するための施策が含まれる場合がある。

■ 大学は、外国からの干渉に関連したセキュリティ戦略、ポリシー、手続きの成熟度を定期的に評価し、リスク報告サイクルに組み込む。

大学のリスク管理戦略とツールは、学んだ教訓を定期的に見直し、安全保障環境を理解し、適応することで改善される。

意思決定の指針となる質問

➢ 内部評価や外部のステークホルダーとのコミュニケーションをサポートするための内部通報の仕組みは、どの程度一貫しているか？

デューデリジェンス

目的

大学は、外国からの干渉リスクについての適切なデューデリジェンスを通じて、パートナーをよく理解する必要がある。国際的パートナーとの契約は、豪州の法律を遵守し、大学の研究とレピュテーションに対する潜在的な脅威に対処し、外国からの干渉や安全保障上のリスクなど、新たなリスクや潜在的なリスクを特定するものでなければならない。

パートナーを理解する

■ 海外のパートナーと共同作業を行う際、大学スタッフは外国からの干渉のリスクを念頭に置くことができるようサポートされている。

豪州の大学が関与する国際的な共同研究の多くは、個々のスタッフ間の対話や協力などの非公式なパートナーシップで構成されている。このようなパートナーシップは、学問の自由などの中核的な価値観に依拠したものである。

豪州の大学の教員やその他の職員には、倫理的かつ誠実に行動する責任がある。外国からの干渉のリスクについて職員に周知する仕組みは、職員がその責任を果たすのに役立つものである。

意思決定の指針となる質問

- 非公式な共同作業やコミュニケーションにおいてスタッフが外国からの干渉のリスクを認識するための仕組みはあるか？
- 必要に応じて、これらの方針に対するスタッフや学生の理解をサポートするガイドラインはあるか？
- 教職員、専門職従事者、研究生は、日常業務、通信、海外渡航における外国からの干渉リスクを認識するためのトレーニングをどのように受けるか？

■ 正式なパートナーシップ契約を締結する前に、パートナーが誰であるかを確認するために、リスクと情報源に応じたデューデリジェンスを行う。

豪州の大学における国際共同研究には、他の大学や企業などのパートナー企業との正式な取り決めが必要となる。

デュー・デリジェンスには、パートナーの過去の活動、研究分野や関連分野、研究室の実質的な所有者、運営組織の商業的・倫理的地位などの調査が含まれ

る。

意思決定の指針となる質問

- パートナーやその関係者は関連する研究経歴を持っているか、そのパートナーはレピュテーションが高いか、プロジェクトに従事する人物に対して妥当な身元調査が行われているか。
- デューデリジェンスを支援するために政府からどのような情報や助言が得られるか。
- パートナーシップの利点はリスクを上回るか。
- パートナー企業の外国政府、政党、関連団体、個人との関係はどうなっているか？これらは適切に開示されているか。

■ 制度的なリスク管理の枠組みは、連邦および州の法律、規制、行動規範の対象となる活動を認識し、それに対応している。

一部の活動は特定の法律、規制、行動規範によってカバーされている。

意思決定の指針となる質問

- パートナーまたは後援団体は何らかの公的登録簿に掲載されているか、またパートナーは所属と意図について透明性の高い対応をしているか。
- 申請されている研究活動は、国防戦略物資リストに記載されている品目に関連しているか？提案されている研究活動は DTCA に含まれるか？

■ 長期にわたって継続する共同研究は、パートナーのデューデリジェンス評価に基づいて再検討し、定期的に契約を見直す。

長期にわたって継続する協力関係については、リスクに見合った情報源に基づいて、パートナーのデューデリジェンス評価を再検討し、契約を定期的に見直す。外国からの干渉のリスクは、パートナー自身や外部の状況の変化に伴って時間とともに変化する可能性があるからである。

意思決定の指針となる質問

- 共同研究者の行動、関心事、外部との関係が、時間の経過とともに大学や個人にとって好ましくないものに変化していないか？
- 政府の助言や評価はその間、変化したか？
- 共同研究者からの外国からの干渉リスクを特定するために、スタッフをサポートする仕組みはあるか？長期滞在したり、適切な経歴を持たなかったり、

異常な行動をとったりする共同パートナーからの干渉リスクを特定するために、スタッフをサポートする仕組みはあるか？

■　研究スタッフと学生の、研究プロジェクトにおけるリスク評価能力

大学は、国際的な共同研究者や資金提供者に関連する財務リスクやその他のリスクを評価する方針や仕組みを持っているが、研究者は、潜在的な貢献者、従業員、パートナーが風評被害やセキュリティ関連のリスクをもたらすかどうかを検討し、この評価に基づいて意思決定を行うための合理的なステップを踏むべきである。

外国の共同研究者が公開していない何らかの関係を持っている可能性や、貿易管理などを遵守する必要性を認識していない可能性があることを考慮に入れる必要がある。

意思決定の指針となる質問

- 研究者が大学のリスク軽減戦略を遵守する必要性を理解するために、どのような研修および戦略があるか？
- 研究者とその外国人パートナーは、利益相反を含め、特定の研究における法的義務を認識しているか？

明確な契約

■　国際的な組織や個人と正式に協力、契約、パートナーシップ、アライアンスを結ぶ場合、大学は対象となるパートナーのデューデリジェンスを行い、協力分野を明確にする。

外国の機関や個人との正式なやりとりについては、契約メカニズムとポリシーについてのベストプラクティスを参照することで、外国からの干渉のリスクを軽減することができる。契約条件や覚書には、活動の完全性を保護する条項が含まれている。

意思決定の指針となる質問

- パートナーのバックグラウンドをどの程度、知っているか、またパートナーから報告されている利益に疑わしい点はないか。
- パートナーの提携関係や意図について、パートナーはどの程度率直で透明性があるといえるか？ これらには、既存のベンダー関係、調達パートナー、主要パートナーと利害関係のあるアライアンスなどが含まれる場合がある。

- 提携先が学問の自由や研究倫理に反したり、輸出規制の対象であることが判明した場合に、契約から離脱する明確な権限を有しているか？
- 契約では豪州の法律が優先されることが規定されているか？

■ 寄付について

外国の団体は、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ことがある。

意思決定の指針となる質問

- 寄付の受け入れを検討する際、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？

研究と知的財産

研究は経済成長の強力な原動力である。そのため、研究システムを損なわせるような試みがなされる可能性がある。

大学には、知的財産を特定、開発、管理するための研究室が存在する。国際的な研究システムに参加している豪州の研究者を教育し、政策的に対応することは、研究者の育成にとって重要である。

外国からの干渉を管理する上で核となるのは、リスクの特定と管理である。大学は、非公式および公式の研究活動や、それによって生み出される知的財産に対する外国からの干渉の影響を最小限に抑えるために、リスクベースの管理アプローチを採用している。

意思決定の指針となる質問

- 研究への外国からの干渉に対処するためのリスク・フレームワークはどの程度強固であるか？
- これらの取り決めを維持、促進、適用する責任者は誰か？
- これらの取り決めは、大学で行われている研究ないし関連するリスク・レベルとどのように対応しているか？

■ 研究契約について

研究契約を結ぶ外国企業は、様々な形態の資金提供の取り決めや、個人を対象としたその他の誘引を通じて、研究契約の特定の分野にアクセスしようとする。

意思決定の指針となる質問

- 研究の性質および／またはパートナーシップの種類により、追加的な監視が必要となる可能性のある研究契約を特定するために、大学にはどのようなガイドラインがあるか？
- 国際的な共同研究プロジェクトの開始時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。
- 大学の研究支援室やセキュリティ・オフィスは、研究者のデューデリジェンス活動をどのように支援できるか？
- 研究者が学内または学外でさらなる助言を求めるべき際に、どのような指針があるか？

■　最終用途の潜在的可能性を検討する

研究の最終用途の可能性をすべて予測することは不可能である。しかし、リスク管理戦略のなかには、潜在的にセンシティブな技術や研究を特定し、保護するための早期に対策を講じることが含まれる。

■　デュアルユース技術と研究

1901 年関税法とその規制は、有形財や技術の移転を規制している。これらの取り決めにより、豪州は財や技術の輸出を管理し、それらが不適切な者の手に渡るリスクを最小限に抑えることができる。豪州の法律の枠組みは、国際的なベストプラクティスに沿ったものとなっている。

意思決定の指針となる質問

- 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考慮しているか？
- 防衛貿易管理体制およびその他の関連する法的枠組みの遵守を確実にするために、どのような仕組みがあるか？

■　潜在的にセンシティブな技術や研究成果

研究には、開発の初期段階では特定できない多くの最終用途がある。デュアルユース技術の最終用途については、研究者や組織にとってグレーゾーンとなることがある。

意思決定の指針となる質問

- 研究者は、自分の研究が、豪州国民の経済的、社会的、安全保障上の利益を促進することと矛盾する目的で使用される可能性を考慮しているか？
- リスクが高いと思われる分野での研究開発をどのような戦略で監視しているか。
- 政府からどのような情報や助言が得られるか？

■ IP パートナーへの積極的なアプローチ

商業的な利益をもたらす可能性のある研究は、外国企業の関心を引くことがあるが、多くの研究は保護する必要がなく、共有されている。しかし、研究の盗用や流用は、研究プロセスのどの段階でも起こり得る。

また、商業的に価値のある研究を保護するためには、知的財産権が制限される場合がある。リスクマネジメントシステムは、盗用や不正使用に対する脆弱性を特定するのに役立つ。

意思決定に役立つ質問

- 商業的に価値のある研究を特定し、保護するために、大学はどのような仕組みを持っているか？
- 商業的価値のある研究に携わる研究者に対して、どのような追加的または対象的な研修を行っているか。

コミュニケーションと教育

目的

研究や学問の性質上、外国からの干渉はさまざなきっかけで起こりうる。大学は、政府機関の支援を受けて、職員や高等学位学生（HDR）に対して、外国からの干渉行為がどのような形で現れるかについてのトレーニングを行う。また、外国からの干渉を認識した場合のサポート体制について情報を提供する。

コミュニケーションと教育的プログラムの推進

■ 大学のコミュニケーションプランや教育プログラムにより、外国からの干渉リスクに対する意識を高める

セキュリティに対する文化は、大学のスタッフや学生に組み込まれた責任と共有された知識から生まれる。コミュニケーションプランと教育プログラムは、外国からの干渉のリスクに対する認識を高めるものである。

意思決定の指針となる質問

- 外国からの干渉リスクに対する認識を高めるために、大学ではどのようなトレーニングを行っているか？
- スタッフや学生が外国からの干渉に関する報告義務に従うことをサポートする連絡手段や手続きはあるか？
- 人に対する倫理、安全な渡航の手配、施設へのアクセス、イベント管理などに関する現行のガイドラインは、潜在的なリスクを特定し、リスクの高い研究分野やセンシティブな研究分野の研究者による積極的なリスク管理を支援するために、どのように発展していけるか？

■ 研究者、専門スタッフ、高等学位（HDR）の学生は、外国からの干渉の可能性があることを認識している

研究の性質上、外国からの干渉を受ける可能性のある入口は複数ある。大学は、スタッフや高等学位学生に対して、どのようにして外国からの干渉行為が起こるかについてのトレーニングを行い、外国からの干渉に気づいた場合のサポート体制について情報を提供する。大学のコミュニケーションプランや教育プログラムは、外国からの干渉リスクに対する意識を高めるものである。研究者、専門スタッフ、高等学位学生は、外国からの干渉が起こりうる方法を認識している

必要がある。

研究者は、外国からの干渉が発生した場合、意図的または非意図的な影響について考慮しておく必要がある。重要な質問としては、次のようなものがある。

- この研究によって誰が影響を受けるのか。それは良い影響か、悪い影響か？
- どのようにして影響を受けるのか？
- この研究は何に影響を与えるのか―そのプラス面とマイナス面は？

意思決定の指針となる質問

- 現在どのようなトレーニングがあるか？
- 外国からの干渉のよりセンシティブな形態についての情報を提供するために、どのようなトレーニングが行われているか？

知識の共有

目的

大学と政府は、大学セクター間で事例を共有することにより、新たな脅威や外国からの干渉の経験に対する認識を高めることができる。これには、外国からの干渉、不当な影響力を行使しようとする試み、学術的な自由や価値を損なう試みなどが含まれる。

大学はすでに他の大学との間や政府とのあいだで干渉に関する情報を共有している。外国からの干渉の事例、不当な影響力を行使しようとする試み、学術の自由や価値観を損なうような試みなどを含め、新たなリスクや外国からの干渉の経験に対処するために、追加の知識共有メカニズムを開発することができる。

大学間および英連邦との情報共有

■ 複数の大学に悪影響を及ぼす可能性のある干渉のリスクを、高等教育セクター全体で共有する。

大学セクターは、すでに大学間および豪州政府と干渉に関する情報を共有している。大学はより広範なセクターに影響を及ぼす可能性のあるリスクがある場合、必要に応じて他のセクターのパートナーと知識やリスク軽減の機会を共有することを検討する。パートナーシップに関する情報や、干渉や不当な影響が確認された事例は、他の機関にとっても参考になる。

政府機関の存在は、大学が外国からの干渉の事例や試みを特定する際に、役立つかもしれない。大学は、キャンパス内で不当な影響力が行使されていないかどうかを検知するのに有利な立場にある。政府と連絡を取るための通報制度、そしてそれを担当するスタッフがいれば、リスクについての双方向のコミュニケーションが可能になる。

意思決定の指針となる質問

- どのように部門間で協力し、情報を共有しているか？
- スタッフは、過去に大学と協力関係にあった可能性のあるパートナーについての情報を入手しているか？
- スタッフは懸念事項がある際、いつどこでアドバイスを求めたらよいかを知っているか？
- いかにして経験を共有し、他の人の助けになっているか。どのような機会に

フィードバックを提供し、学んだ教訓を共有しているか？

■ 干渉に関連した外国との共同研究のリスクが新たに確認された場合、その知識は関連する政府機関と共有される

政府機関は、大学が外国からの干渉の脅威を特定するのに役立つ可能性があるため、外国からの干渉の脅威や発生を適切に報告することが重要である。セキュリティに関する大学と政府機関との連絡は、通常、執行部の中の指定されたメンバーが行う。

意思決定の指針となる質問

- どのようなリスクを政府機関と共有すべきか。それについては職員はどのように理解しているか？
- スタッフは、政府機関との連絡を担当する大学の担当者をどのように把握しているか？

サイバーセキュリティ

目的

本ガイドラインは、大学がネットワークを管理・保護し、サイバー・セキュリティ・インシデントが発生した場合に、それを検知し、適切に対応するためのものである。

■　大学のサイバー・セキュリティ戦略の実施

サイバー・セキュリティ戦略は、大学が情報システムを保護するためのリソースと能力を確保するのに役立つ。

■　大学間および政府とのサイバーインテリジェンスの共有

大学間や政府とサイバー情報を共有することは、大学全体の脅威の共通認識を構築するのに役立つ。これにより、大学はサイバー脅威によるリスクの変化に対応し、対策を共有することができ、政府はタイムリーに個別の支援を提供することができる。また、各省庁が、大学の運営実態や高等教育・研究システムの発展に資する具体的な実務を深く理解することにもつながる。

■　組織全体の「人」の問題としてのサイバーセキュリティ、積極的なセキュリティ文化の重視

強靭なサイバーセキュリティ文化を育むには学生、スタッフ、研究者、執行部の積極的なサポートが必要である。これは、サイバーセーフな行動と意思決定を大学全体に浸透させ、サイバーセキュリティを学問の自由、学生とスタッフのセキュリティ、そして大学の目標を実現するための不可欠な要素とみなすことを意味する。

■　ビジネスリスクを理解し、軽減するためのサイバー脅威モデル

脅威モデリングは、潜在的な脅威とそれが大学にもたらすリスクを事前に特定するための手法である。

ベストプラクティス

このセクションは主要なテーマや目標を達成するために、意思決定者が状況に応じて参照できる具体的な検討事項を提供することを目的としている。

ベストプラクティスの検討は、継続的な改善を前提としている。本セクションは、追加のコンプライアンスや規制を課すことを企図したものではない。大学は、その業務とリスクの比例原則に応じて、ベスト・プラクティスをどのように適用し、組み込むかを検討できるだろう。

ガバナンスとリスク・フレームワーク

ガバナンスとリスク・フレームワークに関する 2 つの重要な分野は次である。

- 説明責任を有する大学執行部
- 対外的なリスク計画

説明責任のある大学執行部

説明責任者は、以下の事項について責任と説明能力を有する。

- 外国からの干渉に対抗するための人員、情報、資産のセキュリティ
- 大学のセキュリティ戦略を反映したリスク報告の枠組みを監督し、外国からの干渉を含む脆弱性と関連するリスク分野にどのように対処しているかを詳細に説明すること。
- 既存のリスクフレームワーク、報告体制、レビュー、評価に基づいて、大学の運営組織に報告すること。

大学によっては、これらの責任を安全・セキュリティ最高責任者に帰している場合もあるが、他の機関ではさまざまなポートフォリオにまたがる理事やその他の上級スタッフに帰している場合もある。彼らの役割には、以下のような責任が含まれる。

- セキュリティに関する大学と政府機関との間の連絡調整
- 人員（スタッフ、学生、請負業者、visitors、顧客を含む）、情報、資産の安全とセキュリティを確保するため、大学の説明責任者をサポートする。
- 外国からの干渉を防ぐために、安全・セキュリティ管理の意識を高め、リスクを軽減する方法を導入する。

- 海外在住者や海外出張者を含むスタッフや学生を対象とした情報の安全性とセキュリティ意識向上のためのトレーニングプログラムを監督する。
- 関連部署（人事部など）と協力して、大学の安全・セキュリティ関連のインシデントへの対応を、大学のセキュリティ・インシデントおよび調査手続きに従って管理し、外国からの干渉を防ぐために大学全体のモニタリング・メカニズムを監督する。
- 要求される保護レベルの維持、リスクへの対応、許容できない安全・セキュリティリスクへの対策、セキュリティ成熟度の向上のための手続きの整備
- スタッフや政府機関からのアドバイスを受けて、学内の関係者に情報や脅威の情報を発信し、管理する。

干渉リスクに関する計画

以下は、既存の制度枠組みに外国からの干渉リスクの計画と緩和策を組み込む方法の例である。

- 職員と学生が外国からの干渉を報告するための明確な仕組みを構築し、それを責任ある機関が監督する。
- 外国からの干渉のリスクを念頭に置いた、海外渡航のための人員、情報、資産のセキュリティに関する仕組み、ガイダンス、連絡経路の定期的な見直し。
- 人、情報、および物理的資産を保護するための施設の計画
- 外国からの干渉のリスクを念頭に、スタッフや学生が大学を離籍した後に学内システムへのアクセスを防ぐための仕組みづくり。
- 以下のリスクを最小化または除去するためのセキュリティ対策。人への危害、および情報および物理的資産が動作不能またはアクセス不能になったり、許可なくアクセス、使用、除去されたりするリスクを最小化または除去する。

以下は、大学の方針や手続きが、リスクに見合った形で、職員、学生、請負業者、名誉職員が国際的な共同作業に従事する方法を説明するための例である。

- 職員が、名誉職や兼任職などを含む職員の任用について、大学のルールに従うこと。
- 海外のパートナーと共同研究契約を結ぶ予定のある研究者を対象としたデ

ューデリジェンス・チェックリストなど、国際共同研究を検討しているスタッフ向けのテンプレートを用意する。

- スタッフが問題を通報したり、懸念を共有するための方針と仕組みの策定。
- 学問の自由と価値、および大学の利益に反する可能性のある外国機関の行動を職員に認識させること。
    - ✧ 外国の政治的、宗教的、社会的アジェンダに基づいて、科目の内容を変更するよう要求、または誘導すること。
    - ✧ 外国の政治的、宗教的、社会的なアジェンダと対立すると考えられる場合に、訪問や活動を中止するように要求したり、誘導したりすること。
    - ✧ 大学の情報システムへの不必要に広範なアクセスを許可するような要求を行ったり、または誘引したりすること。
    - ✧ 取得したアクセス権を使って、承認されていない第三者にアクセスを提供すること。
    - ✧ 外国の利害関係者がデリケートだと考えるテーマについて、教職員、管理者、学生、visitors の立場を調査するための監視。
    - ✧ 外国の政治的、宗教的、または社会的なアジェンダと対立する問題についての立場をもつアカデミック・スタッフ、アドミニストレーター、学生、または visitors に対する嫌がらせ、敵意、脅迫、またはその他のネガティブな行為。
    - ✧ 特に批判や反対意見を抑圧する目的でキャンパス内の生活に侵入すること。
    - ✧ 外国の利害関係者がセンシティブだと考えるテーマの講義やその他の活動に、見知らぬ人物が参加すること。
    - ✧ スタッフがそのような活動（ソーシャルメディアやその他のフォーラムを通じたオンライン活動を含む）に気付いた場合は、説明責任のある執行部または関連する上級ラインの管理者に通報される。

以下は、リスク評価および報告の枠組みのために考慮すべき事項である。

- 対外的な干渉に関する研修。これには、さまざまな方法で発生する可能性のある干渉に関する情報を含めることができる。例としては、ソーシャルメデ

ィア、サイバー活動、関係構築を通じた監視および情報収集などが挙げられる。

- 国際的な組織体が関与する契約、資金提供契約、金融投資、パートナーシップの構築に関する内部のガイドライン。
- 外国からの干渉に関する懸念を研究者が報告するための明確な取り決め。
- スタッフと学生のために、以下のようなさまざまな分野でアドバイスを実施。
    - ✧ アカデミックフォーラムなどのイベントの管理
    - ✧ 安全な渡航の手配
    - ✧ リスクの高い研究活動を管理するためのヒト研究倫理ガイドライン
- 第三者の研究パートナーとの研究費の取り決めに関する内部記録。

以下は、大学が利益相反と利益開示を管理する方法の例である。

- 国際的な提携、関係、財務上の取り決めを明らかにする。
- 風評被害を回避し、不当な影響や干渉を管理するために、資金源について適切な内部通報を行う。
- 国際企業や豪州に拠点を置き、海外とのつながりが強い企業からの寄付が、大学の方針と一致しており、学術プログラムに不当な影響を与えていないことを確認し、必要に応じて「外国からの影響」透明化スキームを含めて適切に開示する手続き。
- 大学の方針には、海外渡航、スタッフの任命や契約、贈収賄、汚職、外国人からの寄付に関するアドバイスが含まれる。

外国からの干渉に関連して、大学がセキュリティ戦略、ポリシー、手続きの成熟度を定期的に評価する方法は以下のとおりである。

- 外国からの干渉に関する大学のセキュリティ戦略、方針、手続きに基づくリスク計画と対応策の成熟度を定期的に評価する。
- 外国からの干渉に関するコミュニケーション計画や教育プログラムを定期的に見直す。

デューディリジェンス

デューデリジェンスのための３つの重要な領域は次の３つである。

- パートナーの理解
- 明確な契約
- 研究と知的財産

以下では、大学がこれらの分野をどのように管理するかのについて、いくつか例を示す。

パートナーの理解

- 申請された活動が、大学の学問の自由、監査とリスク、研究倫理とインテグリティに関する方針、および関連する法律を遵守しているかどうかを確認するためのデューデリジェンス活動。
- デューデリジェンスのレビューと定期的なリスク保証の更新。
- 特にセンシティブな分野での研究を含む海外パートナーとの共同研究は、より詳細なデューデリジェンスの対象となる。
- 関係する倫理的、安全保障的、法的、風評的リスクを検討するよう大学を指導する仕組み。
- スタッフが海外にいる間に生じるリスクについてのデューデリジェンスを支援するために、機密性の高い海外出張を可視化する。
- エンゲージメント活動に関するアドバイスやサポートを求めるための連絡先の確保。

明確な契約

以下は、国際的な協力関係、契約、パートナーシップ、アライアンスにおけるデューデリジェンスの例である。

- 外国との共同研究における倫理的、安全保障的、風評的なリスクを、上級スタッフの会議の重要かつ定期的な議題とする。
- 共同研究契約を可視化することで、上級管理職によるガバナンス、監督、デューデリジェンス、リスク評価を合理化する。
- 協定は、MoU、国際協力協定、その他の形式の契約など、法的拘束力のあるものか、拘束力のないものかを考慮する必要がある。
- 海外のパートナーとの契約では、豪州で行われるすべての関連活動について、海外のパートナー機関の法律よりも、豪州の法律と大学の書面による方針が優先されることを確認する。

- 大学は、国際共同研究中に発生した新たなリスクや潜在的な脆弱性を評価するために、定期的に契約書を見直す。
- 学内での研修や意識向上のための話し合いは、外国人代表団などが訪問した際の国際的な活動の管理に役立つ。

以下は、大学が寄付に関連したリスクを管理する方法の例である。

- 研究の性質やパートナーシップの種類によって、追加的な監視が必要な研究を特定する。
- 大学の研究インテグリティ・オフィスやセキュリティ・オフィスが、研究者のデューデリジェンス活動を支援する方法を検討する。
- 研究者が学内または学外でさらなる助言を求めるべき場合には、明確な指針を示す。

研究と知的財産

研究と知的財産に関連するデューディリジェンスの例は以下である。

- 一部の研究分野と将来のデュアルユース技術との間の潜在的な関連性のリスクを評価するための方針と仕組み。
- 国際的な企業との共研究の下流における応用可能性を特定するため研修。
- 外国からの干渉や不正利用の対象となりうる特定の研究分野の評価。
- 防衛省との定期的な協議により、機密技術やデュアルユース技術に関するアドバイスを求め、輸出規制の遵守を徹底する。

コミュニケーションと教育

- 大学のセキュリティに対する意識向上のための取り組みを促進し、リスクとその影響についてのコミュニケーション戦略。
- 対外的な干渉のリスクとその軽減に関する認識を高めるための教育および専門的なプログラムの開発。
- 外国からの干渉を防ぐために、人、情報、資産のセキュリティに貢献する主要な人材を対象としたトレーニング。
- 外国からの干渉に関するコミュニケーションプランと教育プログラムの定期的な見直し。

サイバーセキュリティ

- 大学のサイバー・セキュリティ戦略の実施
- 大学全体および政府とのサイバー情報の共有
- 積極的なセキュリティ文化を重視した、組織全体の「人」の問題としてのサイバー・セキュリティ。
- ビジネスリスクを理解し、軽減するためのサイバー脅威モデル

以下では、大学がこれらの分野をどのように管理するかの例を示する。

《大学のサイバー・セキュリティ戦略の実施》

大学のデジタルシステムは、教育、研究、管理、活動を可能にし、サポートするためのプラットフォームを提供しているが、不正なアクセスを阻止するために設計・運用されている。

サイバー・セキュリティ戦略は、大学が情報システムを保護するためのリソースと能力を確保するのに役立つ。

1. 大学が直面する可能性のあるリスクを理解した上で、サイバー上の脅威や潜在的な脆弱性に見合った対策を講じる。
2. 情報セキュリティマニュアル（ISM）や国立標準技術研究所などの既存の枠組みを活用して、一貫性のある保護措置を開発する。
3. 各セクター間の戦略と専門知識の共有を強化する。
4. 設計・運用文書、方針、手続きの中核となるものの開発を支援する（リスク識別と管理の指針となる）。
5. 学内の機運と受容性を高めるために、サイバーセキュリティ戦略をどのように伝えるのが最善かを検討する。
6. セキュリティについての文化、ガバナンス、サプライチェーン、技術的コントロール、データなどの側面を包含する。
7. 大学のサイバーセキュリティ戦略の進捗状況と効果を追跡する方法を検討する。

以下は、大学がサイバー・セキュリティ戦略を実施する方法の例である。

- 各大学がサイバー・セキュリティ戦略を持っている。
- 各大学は、個々のサイバーセキュリティ戦略の実施を支援するための基礎的な資料集を整備している。

- 大学は知見、ポリシー、専門知識を共有するためのメカニズムを特定する。
- 大学は、サイバーセキュリティ戦略の構成要素として、一連の方針と手続きを策定する。ただし、各大学が独自にカスタマイズすることに留意する。
- 大学は、政府や大学の専門的な知識を持つスタッフの人材育成と確保を強化する方法を検討する。

《大学間および政府とのサイバー・インテリジェンスの共有》

大学間および政府とのサイバー・インテリジェンスの共有は、大学間での脅威の共通認識を構築するのに役立つ。また、豪州政府の各省庁が、大学の運営実態や、高等教育・研究システムの成功に貢献している実務をより深く理解することにもつながる。

大学には以下のことが推奨される。

1. センサーデータやその他の脅威情報を共有する（ただし、共有するかどうか、どの程度共有するかは、常に各大学の判断に委ねられる）。
2. 豪州サイバーセキュリティセンターや他のセキュリティ機関が開催するセクタ ーブリーフィングやフォーラムに参加する。
3. 他大学との共同インシデント管理を検討する。
4. サイバーセキュリティ関連技術の選択についての知見を共有する。
5. 共有可能なサイバー情報の安全な保存・送信方法を検討する。
6. 政府安全保障機関の連絡先の最新リストを更新する。

大学がサイバー・インテリジェンスを部門間や政府と共有する方法の例としては、以下のようなものがある。

- 政府による大学へのサイバー・セキュリティの脅威に関する定期的なブリーフィング。
- 大学が必要に応じて関係省庁に連絡するための連絡先の登録。
- 技術取得のためのセクターのサイバーセキュリティパネルの形成可能性を含め、サイバーセキュリティ関連技術の選択に関する知見の共有。
- サイバーセキュリティ関連問題の調整窓口
- 各大学の判断により、ネットワーク・センサー・データと分析結果を部門間および政府と共有する。
- 大学間でのインシデント共通管理プロトコルを開発する機会を探る。

《セキュリティに関する文化を育む、組織全体の「人」の問題としてのサイバーセキュリティ》

サイバーセキュリティに関する文化を育むには、学生、スタッフ、研究者、経営者の積極的な支援が必要である。これは、サイバーセーフな行動と意思決定を大学全体に定着させ、サイバーセキュリティを学問の自由、学生とスタッフの安全、大学の目標を実現するための不可欠な要素とみなすことを意味する。

これには次の検討が必要である。

1. 研究者、スタッフ、学生、執行部のように、異なるユーザーグループの固有の課題と期待に合わせて、サイバーセキュリティのメッセージとプログラムを調整する。
2. サイバーセキュリティに関する文化を定着させ、推進させるために、評議会を含む大学のあらゆるレベルの組織を巻き込む。
3. サイバーセキュリティに関する文化プログラムを、大学のサイバーセキュリティ戦略の他の要素と連携させる。
4. サイバー・セキュリティの課題と解決策を、技術だけでなくユーザの視点から捉える。
5. 成熟したサイバー・セーフ・カルチャーにおいては、集団責任と個人責任の包括的な原則を強調する。
6. 学問の自由を保護するものとしての、サイバー・セキュリティ能力を推進する。
7. いくつかの文化的課題の共通性とキャンパス間の人材の移動を念頭に、サイバー・セーフティ・メッセージの作成と実践に関するアプローチを共有する。

以下は、大学が組織全体の問題としてサイバーセキュリティを奨励する方法の例である。

- 技術的・文化的教育のための短期コースを大学内部で運用する。これには、サイバーセキュリティをゲーム化する可能性も含まれる。
- メッセージングを調整し、サイバーセーフな行動と意思決定を支援するために、研究者とユーザーの行動特性を理解するための学際的なユーザー研究を共同で行う。
- 様々なユーザー層向けのサイバーセーフポケットガイドを作成する。

- 物理的・仮想的なサイバーセキュリティ・シミュレーションにより、侵害された USB など、脅威の主体がどのように行動するかを示す。
- 海外の大学からのゲストスピーカーによる、サイバーセキュリティに関する経験やアプローチの紹介。
- 評議会、経営陣、教員等の意思決定者が、サイバーセキュリティガバナンスに関与する。

《ビジネスリスクを理解し軽減するためのサイバー脅威モデル》

脅威モデルは、潜在的な脅威とそれが大学にもたらすリスクを特定するための積極的な手法である。

優れた脅威モデルを構築することで、各セクターや個々の大学がビジネスリスクを明確にし、戦略に反映させたり、投資のケースを構築することができる。

強力なモデルの枠組みには、以下のような要素がある。

1. 直面する脅威の性質についての理解を深めるため、ACSC やその他のセキュリティ機関から定期的に指導を受ける。
2. 脅威モデルを脅威の情報源とし、現在および将来の脅威に合わせて定期的に更新する。
3. 脅威モデルを大学同士や政府機関と共有し、共通の脅威像を構築することを奨励する。
4. 大学のサイバーセキュリティ戦略の指針となり、投資の可能性を高める脅威モデルを構築する。

以下は、大学がビジネスリスクを理解し軽減するためにサイバー脅威モデルを使用する方法の例である。

- 他大学の有用な事例や ACSC のガイダンスを活用した、個々の大学の状況に応じた脅威モデル。
- 政府と共同で開発し、定期的に更新している、大学の脅威モデルの共通フレームワーク。
- 脅威モデル作成能力を高めるためのトレーナー/実務者ワークショップ
- 脅威モデルの思考と実践を強化するための脅威モデルゲストスピーカー
- 個人および部門の脅威モデルを用いて、戦略の改良、情報の共有、部門全体の能力の構築を行う。

付録 1：外国からの干渉タスクフォース

2019 年 8 月 28 日、豪州の教育担当大臣は外国からの干渉タスクフォースの設立を発表した。タスクフォースは、大学セクターと豪州政府機関を集め、大学セクターに対する外国からの干渉に対抗するためのガイドラインを策定した。

タスクフォースを主導するためのワーキング・グループも設立された。ワーキング・グループには、政府高官と関連する専門知識を持つ大学の上級代表者が参加した。具体的には、4 つのワーキンググループが設置され、それぞれが重要な戦略分野に焦点を当てた。ワーキンググループは、大学セクターと政府が共同議長を務め、政府と大学セクターの両方から関連する専門家が参加した。

焦点となった主要戦略分野は以下の通りである。

- 文化とコミュニケーション
- 海外との連携
- 研究と知的財産
- サイバー・セキュリティ

豪州の大学は、研究協力や教育コミュニティなど、広範に国際的な活動を行っており、その成果は豪州社会に大きな利益をもたらしている。大学は、国家資産としての責任を重く受け止めると同時に、学問の自由を守ろうとしている。

タスクフォースの基本原則は以下の通りである。

- セキュリティは、学問の自由、価値観、研究協力を守るものであること
- 国益を意識した研究、協力、教育活動であること
- セキュリティは個人の責任を伴う、集団的責任であること
- セキュリティは組織のリスクに比例すべきであること
- 大学コミュニティの安全が最優先であること

付録 2：政府機関と連絡先

豪州政府の様々な機関が、国際教育、高等教育、国家安全保障、規制などの分野で、サービス、指導、助言、支援を提供し、大学部門を支援している。

国家対外連絡調整官（National Counter Foreign Interference Coordinator）

国家海外干渉対策調整官は、外国からの干渉行為に対応するための豪州の政府全体の取り組みを調整している。

- 豪州の国家情報機関と協力して、外国からの干渉の脅威、脆弱性、もたらさ

れた結果についての評価を行う。

- 外国からの干渉活動に対応する国内および国際的な統合調整プログラムを構築する「CFI 戦略」の運営。
- 外来の干渉を受ける恐れのあるセクターやシステムに対する支援活動や助言の調整。
- 文化的、言語的に多様なコミュニティとの連携を強化し、外国人による操作や強制に対抗する能力の向上。

教育省

教育省は、豪州国民が質の高い幼児教育、学校教育、高等教育、国際教育・研究を受けられるようにするための国家政策やプログラムを担当している。

高等教育と研究は、即応性のある労働力と強力なイノベーションシステムを構築・維持するために不可欠であり、学部教育から上級研究者までを対象としている。また、強力な高等教育部門は、豪州の大学の世界的な評価と国際的な実績を支え、留学生や研究者を豪州に惹きつけ、産業界との協力関係を構築している。

高等教育局は、政策、資金、プログラムを通じて、高等教育と研究を支援している。

高等教育局は、高等教育セクターと協力して、大学全体の革新と専門分野を推進し、入学希望者や在校生が公平に大学にアクセスできるようにし、大学が財政的に持続可能で長期的に利用できるようにしている。

また、豪州政府の「国際教育国家戦略 2025」を推進し、国内外の関係者と協力して、豪州の教育サービス貿易の持続的な拡大を支援している。同省は、外国政府や各分野の関係者との国際的な協力関係やパートナーシップを促進し、国際的な教育活動を拡大する機会を見極め、教育機関間の学生や研究者の移動を促進し、知識のグローバルな交換を促進している。

豪州安全保障情報機関

ビジネス・アンド・ガバメント・リエゾン・ユニット（BGLU）は、豪州・セキュリティ・インテリジェンス・オーガニゼーション（ASIO）と政府および産業界のステークホルダーとの間の主要なインターフェースである。

BGLU は、閲覧者が管理するウェブサイト、ASIO 主催のブリーフィング、政府と産業界の合同フォーラムへの参加など、さまざまな手段で情報を提供して

いる。BGLU の目的は、政府や産業界のリスク管理の意思決定者に、最新のセキュリティ情報やセキュリティに関するアドバイスを提供し、以下のことを支援することである。

- 国家安全保障上の脅威の認識と対応
- 適切なリスク軽減戦略の策定
- 役員やスタッフへの情報提供

このレポートは、ASIO が保有するすべての情報と専門知識、および一部の外国情報機関のレポートから作成されている。

豪州・シグナルズ・ディレクター

豪州信号総局（ASD）内の豪州・サイバー・セキュリティ・センター（ACSC）は、国家的なサイバー・セキュリティを主導している。このセンターは、豪州政府全体のサイバーセキュリティ能力を結集して、豪州社会のサイバーレジリエンスを向上させ、デジタル時代における豪州の経済的・社会的繁栄を支えている。

ACSC は、国益に関わる重要なインフラやシステム、連邦政府、州政府、地方政府、中小企業、学界、非営利セクター、豪州のコミュニティなど、経済全体のサイバーレジリエンスを推進している。

ACSC は、サイバーセキュリティの脅威を防ぎ、対処し、すべての豪州人への被害を最小限に抑えるための、官民の協力と情報共有のハブとなっている。

より具体的には、ACSC は

- 豪州のコンピュータ緊急対応チーム（CERT）として、サイバーセキュリティの脅威や事件に対応し、民間および公共部門と協力して脅威に関する情報を共有し、回復力を高める。
- 政府、産業界、地域社会と協力して、サイバー・セキュリティに対する意識を高める。
- すべての豪州人に情報、アドバイス、支援を提供する。

検察庁

検察庁の目的は、豪州の法律、司法、セキュリティ、インテグリティの枠組みを維持・改善することで、公正で安全な社会を実現することである。検察庁は、豪州の法と司法の枠組みを維持・改善し、政府の公正性と透明性を促進・保護し、

法の支配を維持するためのプログラムと政策を提供している。この部門の業務は、すべての豪州国民の生産性、自由、福利の中心となっている。安全性と整合性の機能の一環として、検察庁は「安全保障政策フレームワーク」と「外国からの影響の透明性スキーム」を管理している。

セキュリティ保護政策フレームワーク（PSPF）は、豪州政府機関が国内外で国民、情報、資産を保護することを支援するものである。PSPF は、特定の政府機関に義務づけられているが、その原則と指針は、すべての機関や組織にとってのベタープラクティスを示している。

PSPF は、セキュリティ・リスク管理のアプローチを通じて適用され、組織内および政府全体にお いて積極的なセキュリティ文化を醸成することに重点が置かれている。組織は、フレームワークの指針を考慮し、独自のセキュリ ティ・リスク環境に対処するためにセキュリティ対策を適切に行うことで、PSPF の成果を実現する。

The Foreign Influence Transparency Scheme は、2018 年 12 月 10 日に開始された。この制度の目的は、豪州の政府や政治プロセスに対する外国の影響力の性質、レベル、程度を一般市民や政府の意思決定者に可視化することである。

この制度では、外国人代表者と取り決めを行い、その代表者のために特定の活動を行う個人や団体に登録義務を課している。個人や団体に登録義務が課されるかどうかは、外国人代表者が誰であるか、実施される活動の性質、活動の目的、場合によってはその人が豪州で公的な上級職に就いていたかどうかによって決まる。

防衛省

国防省の防衛輸出管理局は、防衛大臣に対して、防衛・戦略物資や技術の輸出を規制する責任を負っている。

これらの物品および技術には以下が含まれる。

- 軍事目的のために設計された軍事品目、または本質的に致死性、無力性、破壊性のあるもの。
- 軍事計画に使用されたり、適用されたり、化学・生物・核兵器システムの開発・生産に貢献する可能性のある品目と技術。

豪州の輸出規制は、豪州の国益と国際的な義務に合致する場合に、防衛および戦略物資と技術の輸出を可能にしている。

産業・イノベーション・科学省(Department of Industry, Innovation and Science)

産業・イノベーション・科学省は、世界的に統合されたデジタル・テクノロジー主導の経済を促進する上で中心的な役割を果たしている。豪州の産業界、企業、研究機関が、市場の混乱を回避し、デジタルトランスフォーメーションを含む新たな機会を模索するための支援を行っている。

このような支援は、世界的に競争力のあるビジネスの成長につながり、雇用の創出と強固で安全な経済を支えている。

DIIS はまた、新しい発見を支える科学研究、インフラ、スキル開発、コラボレーション、エンゲージメントにも投資し、支援している。このポートフォリオは、研究機関が豪州のために質の高い研究を行うための体制を整えられるよう支援している。

DIIS は、豪州の革新的な起業家や研究者が協力して国際的な機会を活用できるようにすることを目的とした、グローバルイノベーション戦略に基づく様々な競争的補助金プログラムを管理するだけでなく、彼らの努力を支援するための追加リソースを提供している。

特に、ファクトシート *A guide to undertaking international collaboration* は、豪州の研究者や機関が国際的な共同研究を行う際に考慮すべき主要な課題と戦略をハイレベルでまとめている。