文部科学省　平成２８年度産学官連携支援事業委託事業

産学官連携リスクマネジメントモデル事業

（技術流出防止マネジメント）

成　果　報　告　書

平成２９年４月

委託者　　文　部　科　学　省

委託先　　国立大学法人　名　古　屋　大　学

様式第２０

本報告書は、文部科学省の平成２８年度産学官連携支援事業委託事業による委託業務として、国立大学法人名古屋大学が実施した平成２８年度産学官連携支援事業委託事業「産学官連携リスクマネジメントモデル事業（技術流出防止マネジメント)」の成果を取りまとめたものです。

目　　　次

図表一覧

第１章　事業の概要

1)-1　事業目的と事業内容

【目的】

本事業は、科学技術・学術審議会産業連携・地域支援部会に置かれた「大学等における産学官連携リスクマネジメント検討委員会」において提示された、「大学等における産学官連携活動の推進に伴うリスクマネジメントの在り方に関する検討の方向性について」に基づき、大学等が産学官連携リスクマネジメント体制を構築する際のモデルとなるような取組体制・システムを構築するとともに、この取組を全国的に普及させることを目的とする。

【事業内容】

平成２８年度は、学内外の調査で先進例や現状を把握し、技術流出防止マネジメントに関するガイドラインを策定し、実効的・効率的なマネジメント体制・システム構築した。学内の横断的組織のNU MIRAI WGでは、総長プラン「松尾イニシアティブNU MIRAI 2020」で謳う「世界で卓越した大学にふさわしい内部統制と新たなリスク管理体制の整備、構成員のコンプライアンス意識の向上」の実現に向け、内部統制・リスク管理担当理事の下、総務課、研究支援課、監査室、法務室等の関係者が、学術研究・産学官連携推進本部と連携して、学内外の現状調査と課題分析を実施し、名古屋大学にふさわしいリスクマネジメント、のあり方について検討した。

1)-2　名古屋大学の規模が分かる基本情報（研究者数、部局構成等）

名古屋大学の源流をたどれば、1871年（明治4年）に仮病院、医学校が設立されたことにさかのぼり、144 年の歴史を刻んでいる。この間にさまざまな変遷を経て、1939年（昭和14 年）には医学部と理工学部からなるわが国で7番目の帝国大学となった。第二次大戦後の学制改革により、1955年（昭和30 年）には8学部・研究科からなる総合大学となり、その後もさまざまな改革を経て、現在は学部9（文学部、教育学部、法学部、経済学部、情報文化学部、理学部、医学部、工学部、農学部）、研究科14、附置研究所3、共同利用・共同研究拠点2、学内共同教育研究施設19、中央図書館・分館（蔵書数323万冊余）、教員数約1,700名、学部学生10,200 名余、大学院学生6,300名余、留学生1,600名余、等を擁する中部圏の中核大学であるとともに、わが国屈指の総合大学に成長してきた。名古屋大学の卒業生からは、これまで特に学界、産業界において、輝かしい活躍をしている人材が数多く育ち、日本と世界を牽引するリーダーとして社会に貢献している。

第２章　モデル構築・実施について

2)-1　　モデル構築・実施担当者

・事業総括

学術研究・産学官連携推進本部　本部長　理事・副総長　財満 鎭明

・実施責任者

学術研究・産学官連携推進本部　副本部長　教授/総長補佐　一村 信吾（安全保障輸出管理責任者）

学術研究・産学官連携推進本部　知財技術移転グループリーダー　教授　鬼頭 雅弘(秘密情報管理責任者)

・実施担当者

学術研究・産学官連携推進本部　安全保障輸出管理担当　URA　石川 綾子（安全保障輸出管理・秘密情報管理担当者）

学術研究・産学官連携推進本部　安全保障輸出管理担当　URA　宮林　毅（安全保障輸出管理・秘密情報管理担当者・新規雇用）

学術研究・産学官連携推進本部　知財技術移転グループ　特任准教授　道井 敏（秘密情報管理担当者）

NU　tech(名古屋大学海外拠点)　特任教授　神山 知久

NU　tech(名古屋大学海外拠点)　岩倉 信弘

・事務担当者

研究協力部研究支援課　部長　吉野　明

研究協力部研究支援課　次長　加藤　滋

研究協力部研究支援課　課長　荒木 正寛

研究協力部研究支援課　課長補佐　山中 誠

研究協力部研究支援課　専門員　小出 信吾

研究協力部研究支援課　事務職員　中林 佑樹

研究協力部社会連携課　主任　柴田　健太郎

学術研究・産学官連携推進本部　安全保障輸出管理担当　事務補佐員　本髙聡子（新規雇用）

2)-2　　モデルの構築にあたって注意した点

・これまでの秘密情報管理等のリスクマネジメントの取組みは実効的といえない面もあり、実効的な仕組みとするため、まず学内外のリスクマネジメントの現状の課題を正確に把握し、学外の進歩的な取組の導入可能性を探る。

・名古屋大学だけのモデル構築とならないように、大学が置かれている環境と課題の因果関係を見極めてのモデル構築とする。

2)-3　　中間まとめにある５つの方向性への対応

産学官連携活動に関する明確なビジョンの下で、産学官連携リスクマネジメントを大学の経営上の重要事項として、過剰な負担をかけずに、適切に実行していくために、次の５

つの方向性が重要となる。

・実効的・効率的なマネジメント体制・システムの構築の必要性
・学長等のリーダーシップの下でのマネジメント強化の必要性
・研究者への普及啓発の必要性
・リスクマネジメント人材の確保・育成の必要性
・事例把握、情報共有の必要性

以下、上記５つの方向性ごとに項目を設けて、報告を行う。

2)-3-1　　実効的・効率的なマネジメント体制・システムの構築へ向けて

2)-3-1-1　学内外追加調査による実体把握

【課題】

実効的・効率的なマネジメント体制・システムの構築へ向けて、これまでの秘密情報管理等のリスクマネジメントの現状の課題を把握し、学内外の進歩的な取組み状況を参考にして、ベストプラクティス構築する。

【実施内容】

ⅰ）学外調査として、技術流出防止マネジメントについての国内外の企業や大学等での管理手法や課題等のヒアリングによる調査を行った。

ⅱ）学内調査として、産学官連携がさかんで、他機関情報と関連が深い研究活動を展開する教員等が多数所属する大学内センターにつき現状の秘密管理状況、学生のプロジェクト参加状態などの調査を行った。

ⅲ）安全保障貿易管理の学内調査として、教職員の保有する技術の機微度調査（理系部局）を実施し、併せて個々人の輸出管理の法令順守の意識度も調査し、教職員の保有する技術の管理区分の階層化を実施した。技術流出の潜在リスクを把握し、留学生等の受入れ手続きに反映させた。

ⅰ）学外の機関：「産学官連携リスクマネジメント（技術流出防止マネジメント）実務者研修会」全国 54 大学に向け実施した（11/1～11/2：三重大学と共催）。リスクマネジメントモデル事業の概要と本学のモデルについて説明し、参加機関の実情や課題など情報交換を行った（アンケート調査の結果は資料１）。

ⅱ）学内調査（大学内センター調査）≫：多数の共同研究等の産学連携活動が盛んな大学内センター（※）の教員や研究支援組織をヒアリング調査することによって、共同プロジェクトに関わる教員の現状の管理状況を把握することができた。また研究支援組織の現状のサポート状況や課題を把握することができた。

（※）本大学内センターは、多数の共同研究等の産学官連携活動が盛んであり、大学内で、特別の秘密管理の組織内規程をもち、運用のある特区である。企業等からの秘密管理の要望も多い。

秘密情報管理に関する学内外追加調査

学内のコンソーシアム、COI（Center of Innovation）、ベンチャーにおける秘密情報管理手法や課題等の追加調査を行った。その際、学生の取扱いについてもできるだけ詳細に情報収集した。得られた技術流出防止マネジメントの先進例や現状把握の結果は、ガイドラインの策定や、実効的・効率的なマネジメント体制・システム構築へ向けての基礎資料とした。

具体的には、以下の学内に設置された組織に対して、技術流出防止マネジメントに関して調査を行い、本学の技術流出防止マネジメントシステム構築の参考とした。

・コンソーシアム等：NCC（ナショナルコンポジットセンター）コンソーシアム、車載制御システム向け高品質プラットフォーム開発（コンソーシアム型）、中部先端医療開発円環コンソーシアム、GaN 研究 コンソーシアムの合計４拠点でのヒアリングを行った。

・COI ：未来社会創造機構（企業参画の COI）でヒアリングを行った。

・学内ベンチャー ：アフォーロ、Photo electron Soul（PES）、APTJ の合計３社でヒアリングを行った。

ⅲ）**安全保障輸出管理に関する学内外追加調査**

大学からの技術流出のパターンを以下の図１に示す。パターン A の教職員からと、パターン B の留学生等からの技術流出を防止することが課題である。そこで技術提供での実効的な管理方式モデルを構築するために、研究者ごとの研究内容の機微度（リスト規制技術の保有等）調査とリスク評価（図２）を行なった。具体的には、研究内容の機微度と輸出管理遵守意識に関するアンケート調査し、得られたデータに基づきリスク評価（図３）を行った。

図１ 大学での技術流出のパターン

図２　機微技術の把握と濃淡管理

具体的には、安全保障輸出管理関する機微技術の保有状況を把握するために、まず理系研究科所属の教員対象に「研究内容の機微度調査」を行った（資料２）。安全保障輸出管理に関する監査のなかで機微度調査について趣旨説明し、対象者約 600 名に調査票を一斉送付した。回収率 30%であるが、研究者の保有技術と輸出管理遵守意識の階層化を行った（図３）。

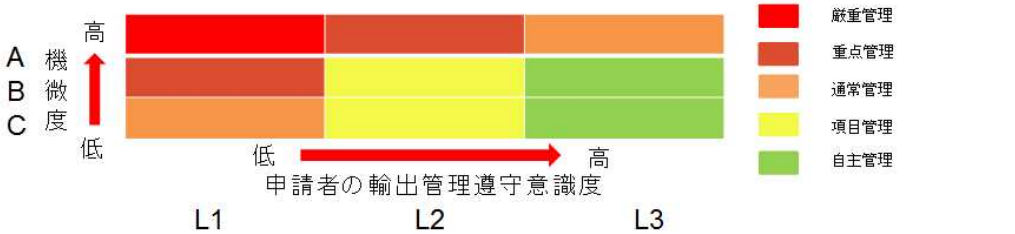
■ 機微度の階層化

レベル	判断基準	備考
A	1～4項該当品	大量破壊兵器関連
B	5～15項該当品	通常兵器関連
C	リスト規制関連技術はない	

管理区分を階層化するために、調査票を配布させて頂きます。

研究室	教員名	管理区分
×1研	Y1、	AL2
×2研	Y2	BL2
×3件	Y3	AL3

■ 機微度と管理意識で階層化



■ 技術提供を行う場合、管理区分により、電子申請を検討して頂きます。

機微度レベルＡに区分された場合、もしくは機微度管理区分に基づき、電子申請が必要（重点管理以上の区分）との連絡を部局等から受けたとき　電子申請を検討してください。

図３　保有技術と輸出管理遵守意識の階層化

2)-3-1-2　構築したルール（ポリシー、ガイドライン等）

ⅰ）「産学連携における秘密情報管理ポリシー」を制定した（資料３）。平成 27 年不正競争防止法改正による未遂行為の処罰、親告罪化等に加え、本事業での調査結果により、対象とする秘密情報の範囲、秘密情報の等級、学生の取扱いについて定めた。

ⅱ）また、学内外調査の結果を分析し、「産学連携における秘密情報管理ガイドライン」を制定した（資料４）。秘密情報の等級指定基準、等級ごとの管理方法、学生へのインフォームド・コンセントのインフォーム要件とプロセスを定めた。

ここで秘密情報管理に関する学内外調査の結果を反映させ、濃淡管理を基本とした三段階の管理等級の基準を策定し、等級指定のフローチャートを策定した。管理費用の負担少ない場合でも、共同研究・受託研究先の企業と協議し、秘密情報管理が行える仕組みとした。また、行政機関と情報交換を行い、他大学が参考とできる内容とし、濃淡管理モデルは、管理対象・管理水準ごとの対応を秘密情報の漏洩対策（2-3-1-6 表１）として明確化した。

2)-3-1-3　秘密管理すべき対象の明確化

【課題】

秘密管理すべき対象が明確化されなければ、研究者は管理対象が不明であり、秘密情報の管理が困難となる。保有する情報の把握・評価、秘密情報を決定する必要がある。

【実施内容】

大学が保有する情報の全体像の把握

まず、学内において「どのような情報を保有しているのか」を全体的に把握することから開始した。情報には、学内の運営情報や研究開発等の技術に係る情報などがある。

（情報の把握方法）例えば、以下のような方法が考えられる。

- 法人文書管理簿などが整備されていれば、その内容を活用する。
- 各部署や担当職員に対して直接ヒアリング等を実施することにより把握する。
- 各研究室等の教員（研究者）等に、所定の基準に則してそれぞれが有する情報を報告頂く。

（留意点）

- 保有する情報の全体像の把握といっても、学内に現在存在する書類や電子データ等の一つ一つを網羅的に確認するのではなく、情報の種類を明記し、一般化・抽象化した形で把握することがポイントである。

（保有する情報の評価）

- 大学が保有する情報のなかで、図４に示す棲み分けをおこなう。
  ここが最も重要なポイントであり、マネジメント体制・システムにも影響する。

保有情報の評価

図４　管理すべき秘密情報

（論点と課題）
- アカデミックフリーダムとアカデミックキャピタリズムのバランス
- 産学連携に影響のある情報に絞る
- 実効性

※運用マニュアル：秘密情報管理の方法を記載したマニュアル（表１に記載）

秘密情報の範囲の決定

・学内の運営情報は対象外とし、産学連携に資する研究情報を対象とする。

・今回のマニュアルにおいて対象範囲は、次に定めるところとする。ただし、臨床研究等に係る個人情報を含む秘密情報は、本ポリシーの対象範囲から除く。大学・公的機関のみとの共同研究等は対象には含めない。

具体的には

① 共同研究等（共同研究を前提とした秘密保持契約を含む）で相手先から取得した秘密情報

② 共同研究等において締結した共同研究契約書（「秘密」として取り扱うこととしたものに限る。）

③ 共同研究等で創出したもので、相手先から取得した秘密情報を含み、内容及び帰属を指定したノウハウ

・今回のマニュアルにおける対象範囲に含まれる秘密情報

例）共同研究契約書、NDA、研究情報、実験データ、実験方法、ロードマップ、事業戦略など

・今回のマニュアルにおける対象範囲に含まれない秘密情報

例）特許、MTA、大学独自のノウハウ等は既設の取り扱い規程を優先する。

2)-3-1-4　秘密情報の管理水準

【課題】

すべての秘密情報に一律に厳格な管理を行うことは、円滑な研究活動等の実施に支障を及ぼし、また管理コストの無用な増大を招く結果となる。そこで、取り扱う秘密情報の性質やその評価の高低、その利用態様等の事情に応じ、秘密情報を同様の管理水準であると考えられるものごとに分類したうえで、その分類ごとに必要な対策をメリハリつけて選択することが重要となる。

秘密情報の分類

（論点と課題）

- 現在ある秘密情報の分類との整合性
- 分類数をいくつにするのか？
- レベル基準の整合性（学内外基準との整合性）
- 実効性

【実施内容】

秘密情報の具体的な分類（名古屋大学の例）

秘密情報を管理するために，次の各号の等級を設け，本学及び秘密情報の開示元機関（以下「企業等」という。）との間で秘密情報として扱うことに合意した秘密情報については，レベル３，又レベル２に該当するものとして管理を行う。

レベル３

他に漏らすことにより本学若しくは企業等が極めて重大な損失若しくは不利益を受け、又はそのおそれがある秘密情報等であり、極めて厳格な管理を必要とするもの

【具体的には】

企業株価等企業の価値に著しく影響し、漏えいにより企業等が極めて重大な損失又は不利益を受けるとして企業等から指定を受け、極めて厳格な管理を必要とするもの

レベル２

レベル３ではないが、これを他に漏らすことで本学若しくは企業等が重大な損失、若しくは不利益を受け、又はそのおそれがある秘密情報等

【具体的には】

ア．企業等から受領した秘密情報で当該企業等から特定の制限が課されたもの（「秘密」である旨の表示が示され、かつ、秘密情報に相当する秘密レベルを示す情報マーキング、アクセス者の具体的な限定、配布先記録等を課された秘密情報）

イ．共同研究等で創出したもので、企業等から取得したアの秘密情報を含み、内容及び帰属を指定したノウハウで相手先から制限等が課されたもの（「秘密」である旨の表示が示され、かつ、秘密情報等に相当する秘密レベルを示す情報マーキング、アクセス者の具体的な限定、配布先記録等を課されたノウハウ）

レベル１

レベル３及びレベル２ではないが、漏えい等の事象が本学若しくは企業等に影響を及ぼすものであり、企業等との間で善良なる管理者の注意をもって厳重に秘密保持義務を課された情報

【具体的には】

企業等から善良なる管理者の注意をもって厳重に秘密保持義務を課されたもので次の情報のいずれかに該当するもの（レベル２に該当するものを除く）。

ア．企業等から受領した秘密情報（「秘密」である旨の表示が示された秘密情報）

イ．共同研究契約等の契約書（「秘密」として取り扱うこととしたもの）

ウ．共同研究等で創出したもので、企業等から取得した前号アの秘密情報を含み、内容及び帰属を指定したノウハウ

2)-3-1-5　秘密情報の等級指定

【課題】

秘密情報の等級指定にあたり、以下の３項目に関して検討を行う必要がある。

〇秘密情報として指定すべき情報か？

〇相手先から秘密等級指定、情報開示先、開示記録の指定がある？

〇秘密情報の相対的、絶対的な価値の評価？

秘密情報の等級指定

（論点と課題）

・誰が、いつ、どのように秘密情報の等級指定するのか？
・等級指定された秘密情報の届出、報告は誰にするのか？
・等級指定された秘密情報のアクセス権者の決定は誰がするのか？
・等級指定された秘密情報の管理は誰が、どのようにするのか？
・実効性

【実施内容】

秘密情報の具体的な等級指定方法

企業からの研究情報を入手する場合、図５のフォローチャートに基づき、５つの判断により、秘密情報の等級付を行う。

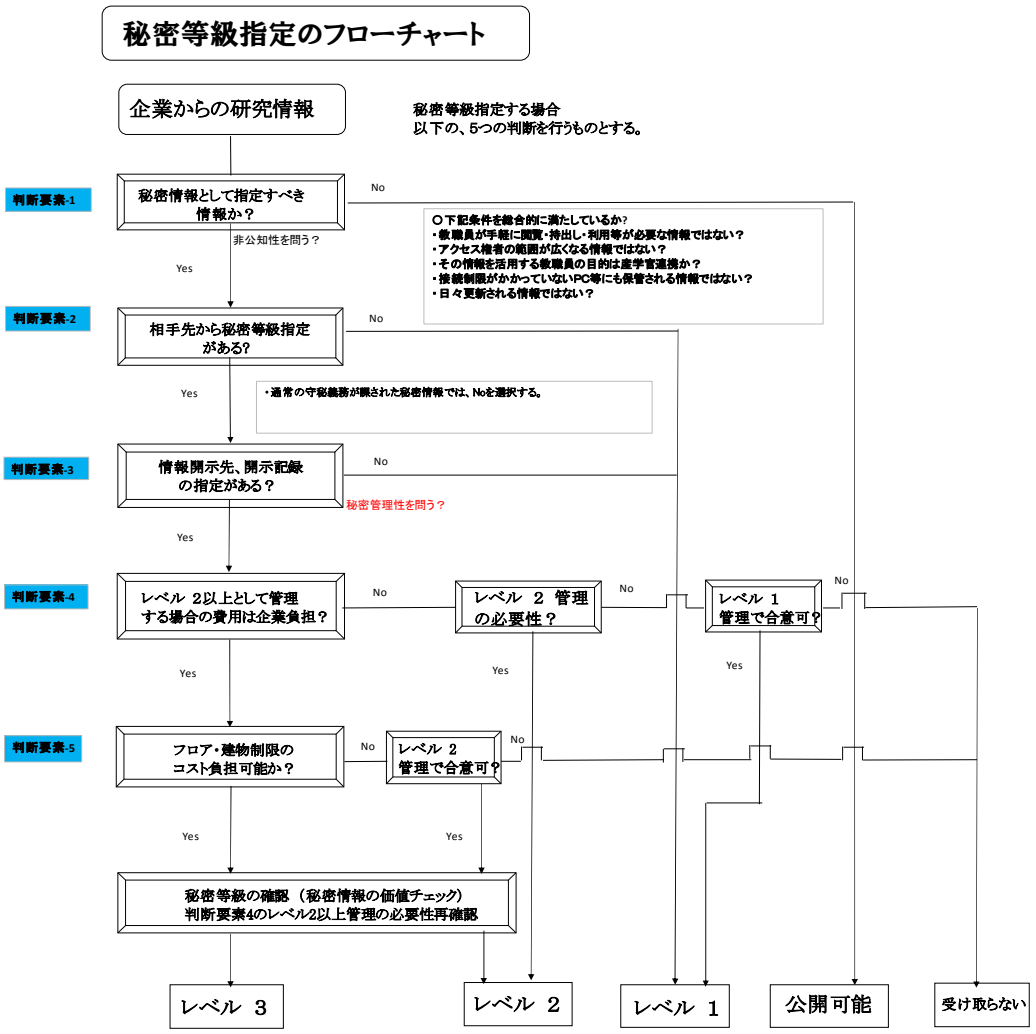


図５　秘密等級指定のフローチャート

2)-3-1-6　秘密情報の管理方法

【実施内容】

秘密情報の等級を、前述の等級指定フロー（図５）に基づき判断し、以下の図６に示すように研究者・秘密情報管理責任者・秘密情報統括責任者により届出・アクセス権者、管理方法を指定する。部局分散型の管理例とする。

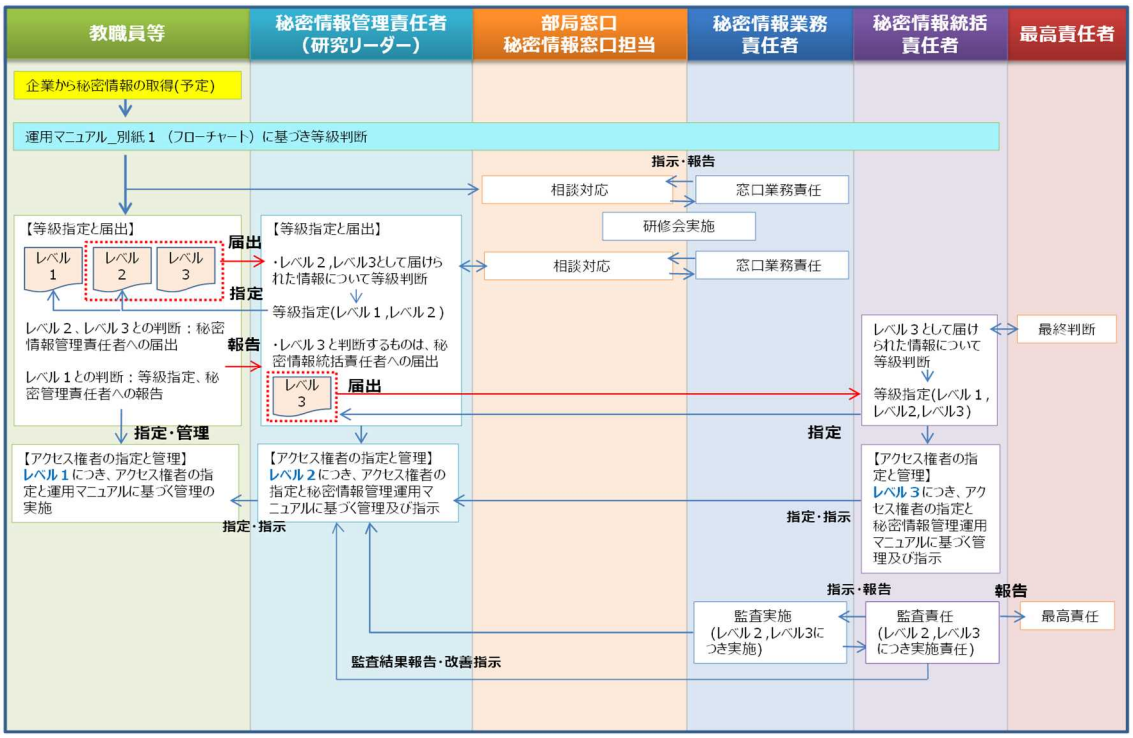


図６　秘密情報の等級ごとの管理プロセス

等級に応じた情報漏えい対策の選択

秘密情報の等級を、レベル１、レベル２、レベル３の３段階として設定して、以下の表にその指定基準、誰が何を決めるのか、どのように管理していくかを記載した。

表１　秘密情報の漏えい対策

区分	レベル３	レベル２	レベル１
指定基準	●極めて重大な損失もしくは不利益を受ける秘密情報等 例）企業の株価に影響する秘密情報、M&A、LBO　等	●重大な損失もしくは不利益を受ける秘密情報等 例）共同研究等で企業からの研究等秘密情報で相手先から制限等が課されたもの 例）共同研究等で創出したもので、企業から入手した秘密情報を含み、内容及び帰属を指定したノウハウで相手先から制限等が課されたもの	●企業等との間で通常の秘密保持義務を課された情報等 例）共同研究等で企業等からの研究等秘密情報 例）共同研究契約等の契約書 例）共同研究等で創出したもので、企業等から入手した秘密情報を含み、内容及び帰属を指定したノウハウ ●原則、学生がアクセスできる秘密情報のレベルはレベル１とする。
等級指定	●届出のあった秘密情報を秘密情報統括責任者が判断し指定 フローチャートに基づき等級判断し指定する ●レベル３と判断し指定した秘密情報は原簿管理	●届出のあった秘密情報を秘密情報管理責任者が判断し指定 フローチャートに基づき等級判断し指定する ●レベル２と判断し指定した秘密情報を原簿管理する ●レベル３と判断した秘密情報は秘密情報統括責任者へ届出	●取得等した秘密情報を管理する教職員が等級判断し指定 フローチャートに基づき等級判断し指定し、秘密情報管理責任者へ報告する。 ●レベル2以上と判断した秘密情報は秘密情報管理責任者へ届出
アクセス権者	●秘密情報統括責任者が指定 教職員等及び共同研究員	●秘密情報管理責任者が指定 教職員等及び共同研究員	●取得等した秘密情報を管理する教職員が指定 教職員等、共同研究員及び学生
表示	●企業から「機密」・「Top Secret」等と表示された秘密情報をレベル３の秘密情報である旨を表示	●企業から「厳秘」・「Secret」等と表示された秘密情報をレベル２の秘密情報である旨を表示	●企業から「秘」・「Confidential」等と表示された秘密情報をレベル１である旨を表示することが好ましい
入出制限	●秘密情報資料及び電子化情報を保管する 建物、もしくはフロアの入出制限する	●秘密情報資料及び電子化情報を保管する 部屋の入出制限をする	●秘密情報資料及び電子化情報を保管する 部屋の入出制限が好ましい
保管	●秘密情報資料（紙媒体等）は、 専用の保管庫等に施錠して保管する。 ●鍵は、 秘密情報統括責任者及び秘密情報統括責任者が指定する教職員等及び共同研究員が管理する。	●秘密情報資料（紙媒体等）は、 他の資料と区別し保管庫等に施錠して保管する。 ●鍵は、 秘密情報管理責任者が管理する。	●秘密情報資料（紙媒体等）は、 保管庫に施錠して保管する。 ●鍵は、 取得した秘密情報を管理する教職員が管理する。
	●電子化情報を情報機器（PC等）に保管する場合には、 暗号化等措置を講じた上で、 ネットワークに接続されていない専用情報機器に保存、 当該情報機器を入退室管理エリアに設置する。 当該情報機器にはパスワードによる認証をかける。	●電子化情報を情報機器（PC等）に保管する場合には、 暗号化等の措置を講じた上で、 情報機器を入退室管理エリアに設置する。 情報機器にはパスワードによる認証をかける。	●電子化情報を情報機器（PC等)に保管する場合には、 当該情報機器を原則として入退室管理エリアに設置する。 入退室管理エリアに設置することができないときは、 暗号化等措置を講じた上で情報機器に保管するか、 もしくは当該情報機器にパスワードによる認証をかける。
	●電子化情報を電子媒体（USB等)に保管しない。	●電子化情報を電子媒体（USB等）に保管する場合には、 暗号化等の適切な措置を講じた上で、 当該電子媒体にパスワードによる認証をかける。 当該電子媒体を保管庫等に施錠して保管する。 ●鍵は、 秘密情報管理責任者が管理する。	●電子化情報を電子媒体（USB等）に保管する場合には、 当該電子媒体を他の電子媒体と区別して 保管庫等に施錠して保管する。 ●鍵は、 取得した秘密情報を管理する教職員が管理する。
区分	レベル３	レベル２	レベル１
複製	●複製・印刷・撮影を行ってはならない。	●複製・印刷・撮影は、 秘密情報管理責任者又は秘密情報管理責任者の許可を得たアクセス権者のみが行うことができる。 ●電子化情報の印刷は、 原則として入退室管理エリア又は当該電子化情報の取扱者が占有する個室等に設置されたプリンタで、 アクセス権者以外に読み取られないよう注意して行う。 それ以外の場所に設置されたプリンタの場合には、 印刷中からプリンタの前に待機し、完了後直ちに回収する。	●複製・印刷・撮影は、 取得した秘密情報を管理する教職員又は取得した秘密情報を管理する教職員の許可を得たアクセス権者のみが行うことができる。 ●複製・印刷は、 アクセス権者以外に読み取られないよう完了後直ちに回収する。
閲覧	●アクセス権者以外のものに閲覧させてはならない。	●アクセス権者以外のものに閲覧させてはならない。 ●電子化情報の画面表示は、アクセス権者以外に読み取られないよう注意して行う。	●アクセス権者以外に閲覧させてはならない。 ●電子化情報の画面表示は、アクセス権者以外に読み取られないよう注意して行う。
配布	●配布・送付をおこなってはならない。	●文書等への「厳秘」・「Secret」等、レベル２の秘密情報である旨を表示し、取り扱い方法についての説明等、アクセス権者以外に情報が漏えいしないよう、必要な措置を講ずる。 ●文書等を会議等で配布する場合は、通し番号を付し、会議後回収する。 ●文書等の送付は、密封の上、必要に応じ親展扱いとする。 ●電子化情報をアクセス権者に対してメールで送信する場合には、暗号化した上で送信する。 ●FAXで送信する場合は、送信先FAX機の前での待機を要請。	●文書等への「秘」・「Confidential」等、レベル１の秘密情報である旨の表示を行うのが好ましく、取り扱い方法についての説明、資料の回収等、情報が漏えいしないよう、必要な措置を講ずる。 ●電子化情報をアクセス権者に対してメールで送信する場合には、暗号化、もしくは電子媒体にパスワード設定した上で送信する。
持出	●保管室外に持ち出し不可。	●保管室外に持ち出す場合は、秘密情報管理責任者の許可必要。 ●学外に持ち出す場合には、取扱者自らが携行し、滞在先では保管庫に保管する。 ●電子化情報が記録された電子媒体を保管室外に持ち出す場合には、暗号化等の適切な措置を行う。 ●電子化情報を電子メール等で送信する場合には、暗号化等の適切な措置を行う。	●保管室外に持ち出す場合には、アクセス権者自らが携行し、滞在先では保管庫に保管する。 ●電子化情報が記録された電子媒体を保管室外に持ち出す場合には、暗号化等の適切な措置を行う。 ●電子化情報を電子メール等で送信する場合には、暗号化等の適切な措置を行う。
廃棄	●秘密情報統括責任者の許可が必要。 ●統括責任者の責任の下で、第三者が残留情報を読み取ることができないように廃棄しなければならない。	●秘密情報管理責任者の許可が必要。 ●秘密情報管理責任者の責任の下で、第三者が残留情報を読み取ることができないように廃棄しなければならない。	●取得した秘密情報を管理する教職員の責任の下、第三者が残留情報を読み取ることができないように廃棄しなければならない。

2)-3-1-7　学生による秘密管理

【課題】

秘密情報管理における学生等の扱い

学生を共同研究に参画させる場合の基本的な考え方

大学の教職員と異なり、大学と雇用関係にない学生等には当該大学の教職員向けの学内規程を適用することはできない。したがって、学生等が学内の秘密情報に触れる場合に何らかの秘密情報管理を行わないと、当該秘密情報の漏えいが発生し、大学や共同研究先企業等にとって大きな損害が生じるおそれがある。そこで、学生等の基本的な立場を尊重し、アカデミックハラスメントにも配慮しつつ、適切な秘密情報管理を行うことが必要となる。その際、情報資産の活用と管理のバランスを考慮しつつ、大学、学生、共同研究先が得られるメリットを勘案しながら実施していくことが重要である。

例えば、産学共同研究の場において、学生等を雇用し秘密保持義務を課すことは、コストがかかる一方で、人的リソースを確保することによる研究成果のコミットや、意図せぬ情報漏えいの可能性の軽減などといった観点から、大学、共同研究先企業双方にとってメリットがある。

また、学生等にとっても、より本格的な産学共同研究活動に携わることが可能になるなどの教育・研究上の利点がある。研究活動へ学生等の参加を認めるに際して、学生等と取り決めるべき事項は、秘密保持の遵守、発明の取扱い等を含めて種々の事項があるので、それらを総合的に取り決めることが望ましい。

特に、学生等が参加する研究活動のうち、学外機関との連携による共同研究や、外部機関からの受託研究を行うケースでは、学生等の共同研究等への参加に先立って、学生等に対して、秘密保持に関する誓約書の提出や秘密保持契約の締結を行うこと等が考えられる。

このようなケースで、共同・受託研究終了後一定期間の守秘義務が課せられる場合、当該秘密保持期間中の教育や研究に関する活動を制約してしまう可能性があるため、研究に学生等が参加することで生じる学生等にとってのメリットと、学生等に課せられる義務とのバランスに応じて、研究への学生等の参加の是非について予め検討しておく必要がある。

秘密情報の管理方法

（議論と課題）

- 学生を共同研究に参画させる場合，どこまで秘密保持義務を負わせるか？
- 共同研究において，教育の自由と，学ぶ自由をどこまで考慮するのか？
- 学生への，インフォームド・コンセントはどのように行うべきか？
- 実効性

【実施内容】

インフォームド・コンセントの要件（名古屋大学の場合）

□　考え方

企業を含む共同研究に学生を参画させる場合、できるだけ学生が不利益を被らないように、企業等から学生に課される制限について調整・配慮のうえ，学生の了解を取ってから参画させる。

□インフォーム要件-１（テーマ選択時）

学生の研究テーマの選択種があることを説明する。

・共同研究のテーマを選択しない場合でも、選択種により不公平感が生まれないよう配慮することを説明する。

学生にとって共同研究のメリットを知らせる。

・研究成就の暁には、企業の研究者と協働して製品化・事業化の醍醐味を味わえ、研究開発のモチベーションがあがることを説明する。

学生にとって共同研究の以下のデメリットを知らせる。

・守秘義務を負う可能性があること。
・秘密保持契約に署名を求められることがあること。
・研究成果の学会発表、論文投稿で制限が係る場合もあること。
（共同研究契約時に企業と要調整）
・研究過程で生じた知的財産の帰属は大学と企業になる場合もあること。
・就職時に同業他社への就職が制限される場合があること。
（共同研究契約時に企業と要調整）

□インフォーム要件-２（共同研究テーマを選択し、同意書の署名に当たり）

研究情報の守秘義務を説明する。

・秘密情報管理のポリシー、ガイドラインを説明する。
・秘密保持契約の内容を説明する。
・在籍時に限らず、他機関へ転出した場合でも、一定の期間守秘義務があることを説明する。
・守秘義務を怠ると、民事・刑事の処罰対象になりえることを説明する。

共同研究体制と遂行上のルールを説明する。

・対象となる共同研究を遂行する上での体制を説明し、学生個人の立場を理解してもらう。
・共同研究に係る業務は研究責任者の承認を得たうえで、その指示に従うことを説明する。

□インフォーム要件-３（RA 等に採用され、契約書を結ぶ場合）

RA 等の業務を説明する。

・RA 等に採用された場合、共同研究費から雇用費用の一部が支払われることを認識させる。
・RA 等に採用された場合、教職員同様に、守秘義務を負うことを認識させる。
・RA 等に採用された場合、契約書記載事項で拘束されることを認識

させる。

・秘密情報の取り扱いについて、再度説明する。

・記載事項を遵守しない場合はペナルティーがあることを説明する。

□インフォーム要件−４

教育、啓発活動について説明する。

・共同研究遂行上のルール（秘密情報管理のガイドライン等）を周知徹底するための教育、啓発活動について説明し、参加義務があることを説明する。

具体的なインフォームド・コンセントの例

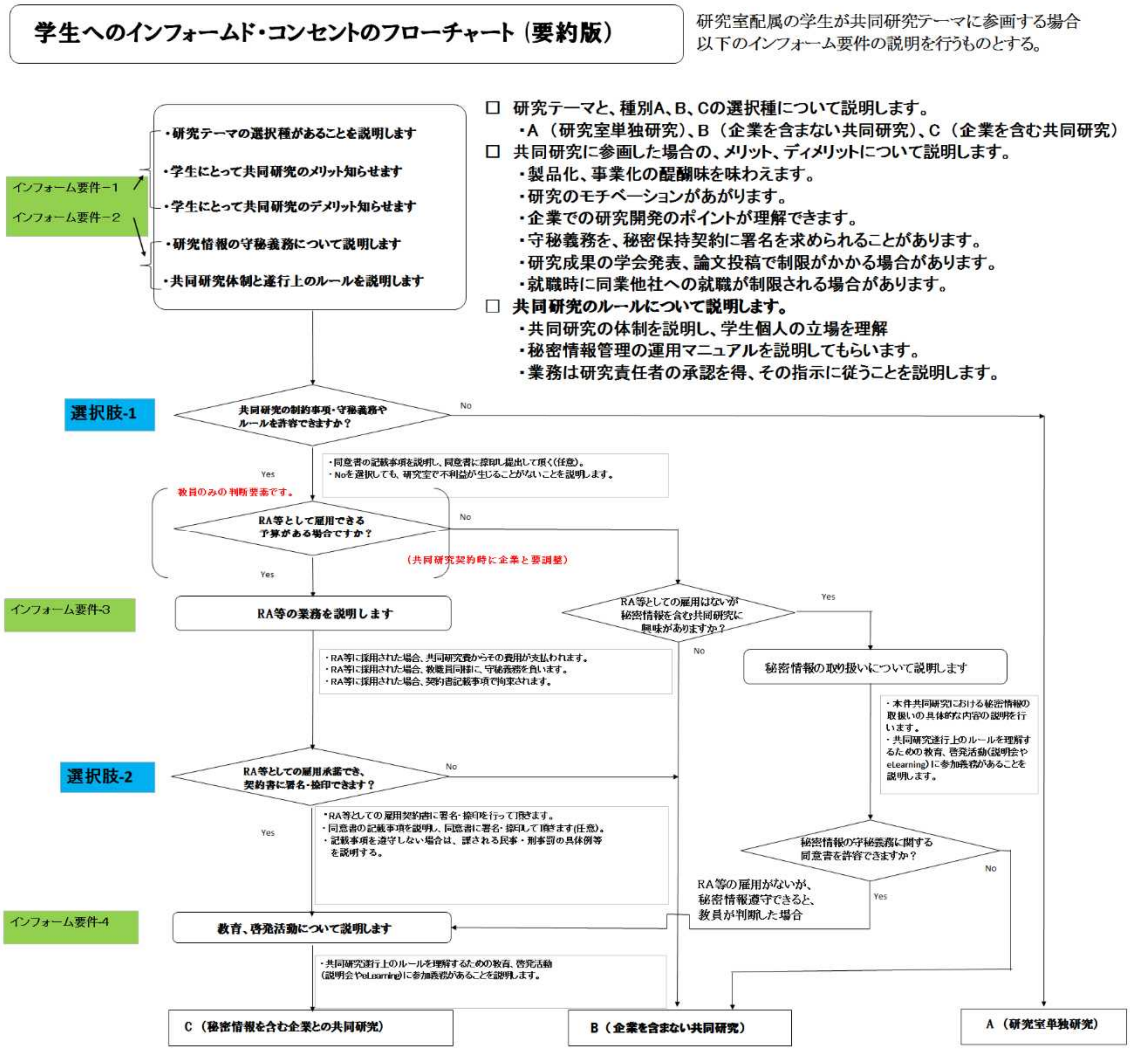


図７　インフォームド・コンセントのフローチャート

2)-3-1-8　リスクマネジメントに関する学内体制とシステム

2)-3-1-8-1　リスクマネジメントに関する学内体制

【課題】

ⅰ）秘密情報管理については、知財関連業務の担当者が付帯業務として業務遂行しており主導的なシステム運用が困難である。秘密情報管理実施体制として、学術研究・産学官連携推進本部に、「秘密情報管理担当者」を配置しシステム構築や相談対応を主導する。

ⅱ）安全保障輸出管理については、留学生等増員（2020年留学生3000人等）、国際連携増加から、今後業務量とリスクの増大が予想される。安全保障輸出管理について、現行の管理体制で引き続き推進するが、秘密情報管理担当者と協働により事業を実施する。

ⅲ）技術流出防止マネジメント活動のためのリソースの確保

【実施内容】

ⅰ）秘密情報の管理に係る学内体制のあり方

秘密情報の適切な管理を継続するため、定期的な管理状況のチェックと、適宜見直しを行うことができる学内体制を整えることが重要である。また、コンプライアンスの観点からも、経営層が、率先して、内外に向け、秘密情報の管理に取り組む姿勢（ポリシー）を明確に示し、組織内の個々人すべてが、秘密情報の管理の当事者であるという意識を持って、継続的に対策を講ずることができる体制を整えることが重要となる。では、どのような組織体制が望ましいのかは、事業の規模や性質によって異なるが、例えば、総合大学の場合、一般に、大学では学部や付属機関ごとで事情が異なり、独立性の高い運用をしているケースが多い。そのため、部局間の調整を行うための横断的な組織（例えば「秘密情報管理委員会」という。）を設置し、全学的な権限をもつ当該組織の責任者（例：副総長、担当理事等）の指示に従って、学内規程の整備や見直し、各部門の役割分担の決定、漏えいに対応するルールの策定といった情報管理を行うことが適切と考えられる。

学術研究・産学官連携推進本部長のもと、知財技術移転グループに、責任者としてグループリーダー、「秘密情報管理担当者」としてリサーチ・アドミニストレーター（企業出身・秘密管理・知的財産関係の業務経験あり）を専任にて配置のうえ秘密情報管理実施体制を構築し、事業を推進した。

（議論と課題）

- 主管部門をどこにするのか？
- 本部集約型、部局分散型どちらの管理体制とするか？
- 外部委員会を設置するのか？
- 役割分担をどうのようにするか？
- 実効性

学内体制と本部・各部局の役割分担

（1）最高責任者

秘密情報の管理における重要事項の最終的な決定を行うため、本学に秘密情報管理の最高責任者を置き、総長をもって充てる。

（2）秘密情報統括責任者

秘密情報の管理を統括するため、秘密情報統括責任者（以下「統括責任者」という。）を置き、国際的な産学連携又は国際的な学術交流分野を担当する理事又は副総長のうちから総長が任命する。

（3）秘密情報管理委員会

秘密情報管理の重要事項の審議を行うため、本学に、秘密情報管理委員会を置く。委員長は、リスク管理を担当する理事又は副総長のうちから総長が任命する。

（4）秘密情報業務責任者

秘密情報を管理するため、秘密情報業務責任者を置き、統括責任者が指名する。秘密情報業務責任者は、統括責任者の指示、連絡、要請等の周知徹底に関する業務及び秘密情報管理遂行上における教職員等からの相談への対応業務等を行う。

（5）秘密情報管理責任者

教職員等から届出のあった秘密情報を管理するため、秘密情報を扱う部局に秘密情報管理責任者を置く。秘密情報管理責任者は、本学の各研究室又は研究グループの責任者（教授又は准教授等）を充て、部局の長の指名により決定する。

秘密情報の管理に関する重要事項の審議を行うため、秘密情報管理委員会を置き、秘密情報委員会の所掌事項は、運用マニュアルの改廃の審議に関する事項、秘密情報の管理についての教育及び監査の実施に関する事項、その他秘密情報の管理についての重要事項の審議であり、秘密情報統括責任者は、秘密情報管理委員会発足前に、運用マニュアルの暫定版を定めることができる。

秘密情報管理委員会は、各部局の長又は部局長が指定する者を委員とする。

同メンバーと本事業の進捗について情報共有・意見交換のうえ、秘密情報管理に関して、全学的な体制・システム構築について検討した（5回）。

月１度以上、学術研究・産学官連携推進本部会議にて技術流出に関する情報共有を行い、経営層に秘密情報管理等の技術流出防止マネジメントが経営上の重要事項であることを日常的に喚起した。

以下に、秘密情報管理に関する運営体制を図８に示す。

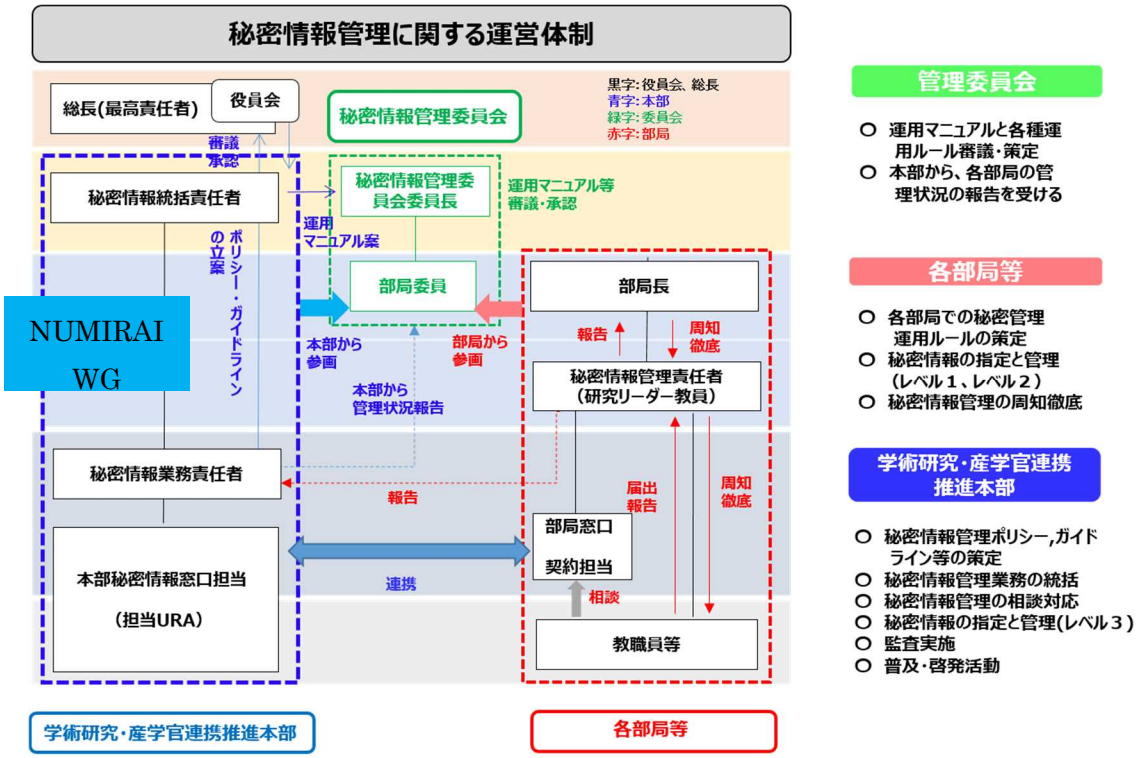


図８　秘密情報管理の運営体制

ⅱ）安全保障輸出管理について、現行の管理体制で引き続き推進するが、秘密情報管理担当者と協働のうえ事業を実施した。

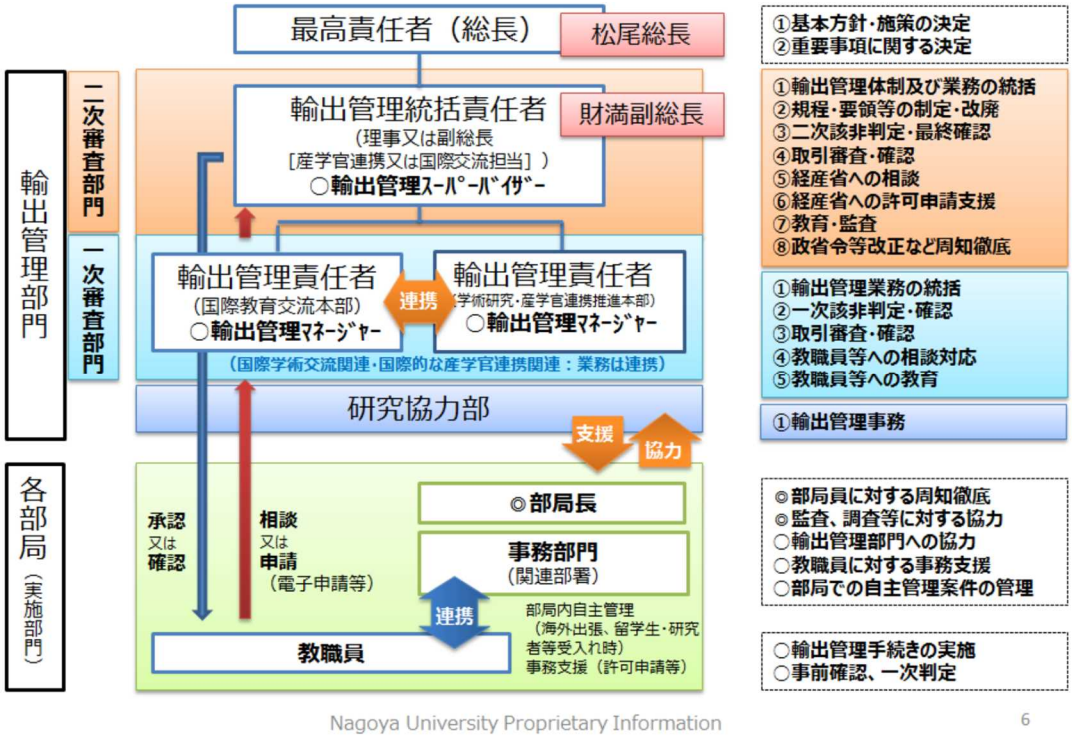


図９　安全保障輸出管理の運営体制

ⅲ）技術流出防止実施体制の人員は、秘密情報管理担当：5 名（兼任）、輸出管理担当：6 名（兼任）である。本事業予算で不足する分は、安全保障輸出管理の予算を充当した。

2)-3-1-8-2　構築したシステム（業務フロー等）

【実施内容】

ｉ）秘密情報管理担実施体制においては、図８の左の青色破線で囲ってある部分が学術研究・産学官連携推進本部で、ここに秘密情報統括責任者（学術研究・産学官担当の理事もしくは副総長）を置き、秘密情報業務責任者と秘密情報窓口担当を配置する。役割は、図の左端に水色で示す NU MIRAI WG の内部統制管理のもと、ポリシー・ガイドライン等の策定、相談対応業務、監査、普及活動等を実施する。図の右の赤色破線で囲ってある部分が各部局で、部局長のもと、秘密情報管理責任者（教授もしくは准教授）、部局窓口担当を任命する。役割は秘密情報の取得、指定、届出、管理を実施する。図の中央上部緑色破線で囲ってある部分が秘密情報管理委員会（学術研究・産学官連携推進本部とは独立の立場）で、秘密情報管理委員長（リスク管理の理事もしくは副総長）を置き、役割は運用マニュアルや各種ルールの審議・策定を実施し、監査等の報告を受ける。業務フローについては、図８の中で各担当

の業務内容を示しアクション先を矢印で示した。

ⅱ）安全保障輸出管理においては、図８、図９に示すように、最高責任者の総長のもと、輸出管理部門と秘密情報管理部門を配置。輸出管理部門は、輸出管理統括責任者の下、輸出管理責任者を配置されている。実務担当は、スーパーバイザーと、マネージャー、事務局（研究協力部）とが連携して、部局事務部門と教職員からの学内申請に対する審査承認、相談、経産省への許可申請手続きの支援をおこなった。

図１０の輸出管理システムで、縦コラムが職制階層ごとの担当業務、横コラムが黄色枠で示した事前検討/相談、電子申請/審査判定、許可申請・輸出手続/支援業務である。これらがリンクして、一気通貫のシステムとして実効的・効率的なマネジメントとなる。

マネジメント体制・システム（名古屋大学の例）

□輸出管理システム

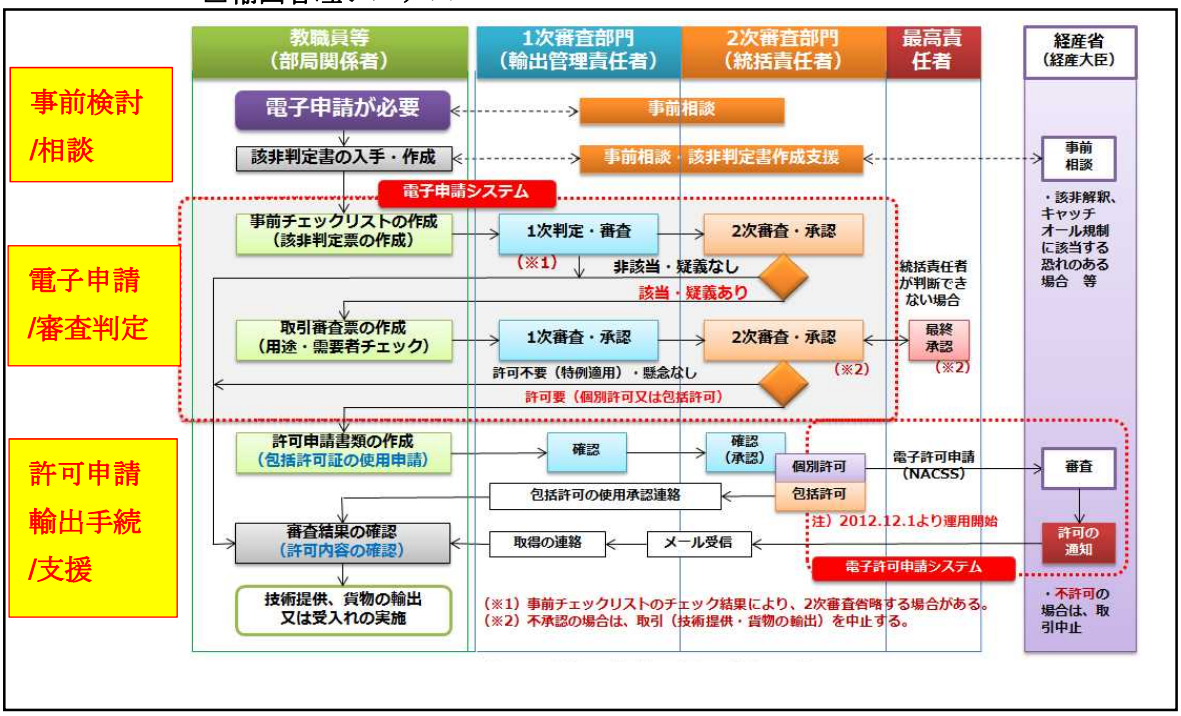


図１０　輸出管理システムフローチャート

電子申請システムの構築

平成２７年度導入した汎用的な新電子申請システム（図１１）では、教職員向けの利用マニュアルを作成、輸出管理のホームページ上に掲載し、部局別の説明会等を実施した。また、導入に積極的な他大学等に、デモや説明等を実施して、輸出管理システムへの考え方を説明した。さらに、「経済産業省主催の大学等向け安全保障輸出管理説明会」

（12 月）等で、新システムの特長や導入効果を紹介し、システムの普及促進を行った。

図１１　新電子申請システムのトップページ

2)-3-1-8-3 モデルにより運用された件数（手続きを行った件数、マネジメント件数）

ｉ）１．未来社会創造機構（ＣＯＩ拠点）

多数機関と産学共同講座を実施するＣＯＩ拠点において、秘密情報管理を行う手段として、今回制定された産学連携における秘密情報管理ポリシー等を参考に、退職者、学生に対する守秘義務に関する同意書の提出を義務づけ、秘密情報管理ルール内容を遵守する内容とされた。

２．産学共創プラットフォーム（ＯＰＥＲＡ）

ＯＰＥＲＡでは、博士課程学生を雇用したうえ本格的共同研究プロジェクトを実施するための仕組みが求められている。この仕組みとして、「学生雇用のためのチェックシート（学生用・指導教員用）」に、今回制定された産学連携における秘密情報管理ガイドライン等で規定するインフォームド・コンセントを盛り込み、ルール内容を遵守するシステムが導入された。

３．地域連携・情報発信グループ支援実施の大型共同研究プロジェクト

地域連携・情報発信グループにて現在取りまとめが行われている数件の大型の共同研究プロジェクトにおいて、企業側から、締結の前提として大学側の秘密管理が

求められている。今回制定された産学連携における秘密情報管理ポリシー等を参考に、そこで用いる秘密管理ルールを検討された。

ⅱ）手続き・マネジメント件数　（平成 28 年 4 月～平成 29 年 3 月末）

①　秘密情報管理：相談・質問対応件数 10 件

②　安全保障輸出管理：事前チェックリスト 621 件　取引審査票 45 件　相談・質問対応件数 179 件

2)-3-2　　大学のビジョンと学長等のリーダーシップ下でのマネジメント

2)-3-2-1　モデル構築の基となった大学のビジョン

ⅰ）名古屋大学松尾総長イニシアティブ（NU MIRAI 2020）では、「名古屋大学を世界屈指の研究大学に」というスローガンのなか「イノベーションへの貢献と社会的価値の創出」、「幸福に貢献する「勇気ある知識人」の育成」等掲げている。

本イニシアティブのひとつに「シェアドガバナンスをふまえた総長リーダーシップによる自律的なガバナンス改革」をあげ、「世界で卓越した大学にふさわしい内部統制と新たなリスク管理体制の整備、構成員のコンプライアンス意識の向上」を謳っている。これをうけ、NU MIRAI WG では全学的な立場から、適切なリスクマネジメント・ガバナンスを再検討・新たな協働の方法を模索している。技術流出防止マネジメント等の産学官連携推進に関するリスクマネジメントについても、本ビジョンのもと学長のリーダーシップにより強化される。

2)-3-2-2　学長等のリーダーシップ下でのマネジメント強化

【課題】

ⅰ）松尾総長プランであるNU MIRAIビジョン反映のためのWGでは、リスク管理強化・体制再構築を行う予定である。）においては、WGメンバーとリスクマネジメントについての学外調査を協働して行うことや、情報交換を行うことによって、技術流出防止マネジメント等のリスクマネジメントに関連する事例や課題の共有を行う。

ⅱ）学術研究・産学官連携推進本部会議で技術流出の事例や情報共有を行い、経営層に秘密情報管理等の技術流出防止マネジメントが経営上の重要事項であることを日常的に喚起していく。

ⅲ）総長がリーダーシップを発揮してトップマネジメントを実施できるようにするために、リスクマネジメントの制度を構築する、そしてこの制度に担をいれるべく関与する集団を活性化させるための、啓発教育活動が最も重要となる。

【実施内容】

ⅰ）NU MIRAI WG では、総長プラン「松尾イニシアティブ NU MIRAI 2020」で謳う「世界で卓越した大学にふさわしい内部統制と新たなリスク管理体制の整備、構成員のコンプライ

アンス意識の向上」の実現に向け、現在、内部統制・リスク管理担当理事の下、総務課、研究支援課、監査室、法務室等の関係者により WG が立ち上げられ、名古屋大学にふさわしいコンプライアンス体制のあり方について検討している。NU MIRAI WG メンバーと協働による事業実施を行い、技術流出防止マネジメントについて、全学的なリスクマネジメントのあり方を検討した。

ⅱ）毎月開催される学術研究・産学官連携推進本部会議や産連 WG 等において技術流出防止マネジメントの報告と情報共有を行った。

ⅲ）関与する集団を活性化させるための、啓発教育活動を進めている。具体的には産学官連携担当の URA・事務職員は関連知識や実務能力の習得のため、ケーススタディーを主体とした URA 研修（※）を行った。

2)-3-3　研究者等への普及啓発

【課題】

ⅰ）本学は、輸出管理での普及活動に特に力を入れており、多数の啓発活動を行っている。しかし濃淡管理モデルを漏れなく実効的に行うには、さらに関係者、特に研究者への啓発が重要である。現在の輸出管理e-Learningを改訂し、技術流出防止e-Learning（日本語版）留学生等用の同e-Learning（英語版）を作成する。

ⅱ）年に 1 度以上、部局等の輸出管理事務手続き等の関連教職員への研修会を行う。

【実施内容】

安全保障輸出管理の監査等で部局等意見聴取し、技術流出防止 e-Learning の再リリースを行った。秘密情報管理の e-Learning についてもガイドラインの内容を反映させ再構築した。教職員向けに技術流出防止マネジメントに関する説明会を部局単位で行い教職員の技術流出防止に関する意識と理解を向上させ、研究者の役割分担を明確させた。

ⅰ）情報セキュリティ面については、情報統括本部にて「情報セキュリティ自己点検」（全構成員受講必須）を行った。電子情報の電子メールの取扱い、本学管理の PC の持出し、サイバー攻撃等の問題顕在化の発見と対処法等についての質問形式の e-Learning である。

また、技術流出防止 e-Learning について、次の①～③を作成した。

① e-learning_秘密情報管理_text（和）（資料５）

② e-learning_輸出管理（和）（資料６）

③ e-learning_輸出管理（欧文）（資料７）

技術流出防止 e-Learning を日本語版と英語版にて作成した。テキストとチェックテストのコンテンツをもつが、その内容は、安全保障輸出管理及び秘密情報管理の基本的な知識や注意点を習得できるものである。

2)-3-4 リスクマネジメント人材の確保・育成

【課題】

ⅰ）現状からすれば関連業務の増大と適切な専門家の配置が必要となる。本業務は、法令知識、産学官連携の専門性が要求されるため、専門人材は不可欠である。

本事業で技術流出マネジメント担当者(URA) 1名雇用し、学内での相談対応や研究室調査等全般的な技術流出マネジメントに携わる専門家として確保する。

ⅱ）本モデル事業実施担当者は、関連知識や実務能力の習得のためURA研修(※)等を受講することによって、専門知識を育成し、また産学官連携関連知識を習得する。それにより、産学官連携推進の観点を含めて技術流出防止マネジメントによる研究支援を行う。

(※)URA研修：本学独自でURAとして必要な知識・スキル・ネットワーク涵養のため月１回定期的に実施。H24年度から大学経営・知財・リスク管理等多様なテーマにて全49回実施。東海地区の大学・研究機関にも開放している。

【実施内容】

秘密情報管理に関する学内の専門家人材育成、部局との窓口対応人材育成を目的に、URA及び実務担当職員向けの研修会を開催し（学外者にも開放)、秘密情報管理に関する情報の共有化と実際の秘密情報管理の場面を想定したケーススタディーを受講頂いた(平成29年1月)。

この他、学外との情報共有を目的に、技術流出防止マネジメントの取組みや学内外調査の結果について、東海地区知財実務者情報交換会（10月、2月）において学内外に情報発信、共有を行った（資料８)。リスクマネジメントの体制・システムづくりで直面した問題点とマネジメント事例について、普及展開を想定する大学等に向けて情報提供し、学外シンポジウム等で情報発信を行った。また、実務者研究会（11月）に開催し、全国から54大学の実務担当者に現在抱えている課題について議論いただき、モデル的な対応方法について学習いただいた（資料９)。加えて、利益相反マネジメントの受託機関と連携し普及活動できる仕組みを構築する目的で、ネットワーク構築連絡会を開催した（11月)。

2)-3-5　事例把握、情報共有（マネジメントのノウハウ等の整備）

【課題】

ⅰ）特別な状況化における技術流出防止マネジメントについての事例を収集し、平成28年度特殊事例を含め収録する。

ⅱ）技術流出防止マネジメントについて、学内の関係者、NU MIRAI WGメンバーにおいて情報共有を行う。定期的に打合せ（連絡会）をし、案件整理を行い、課題を十分に把握しながら、具体的な管理手法等の事例の蓄積と情報共有を行う。

ⅲ）技術流出防止マネジメントの取組みや、学内外調査の結果について東海地区を中心にURA研修等によって学外も含めて情報発信、共有を行う。

【実施内容】

ⅰ）国内外調査を実施し特別な状況化のマネジメントについて事例を収集した。具体的には、学内のコンソーシアム、COI（Center of Innovation）、ベンチャーにおける秘密情報管理手法や課題等の追加調査を行った。管理レベルごとの具体的なマネジメント手法の例を集積することができた。

ⅱ）学内の関係者、NU MIRAI WG メンバーにおいて、秘密情報管理委員会（学術研究・産学官連携推進本部とは独立の立場）を検討した。秘密情報管理委員長（リスク管理の理事もしくは副総長）を置き、役割は運用マニュアルや各種ルールの審議・策定を実施し、監査等の報告を受けるシステムとした。

ⅲ）東海地区知財実務者情報交換会（10 月、2 月）において学内外に情報発信、共有を行った。リスクマネジメントの体制・システムづくりで直面した問題点とマネジメント事例について、普及展開を想定する大学等に向けて情報提供し、学外シンポジウム等で情報発信を行った。

第３章　モデルの改善について

3)-1　実践して得られた課題と解決方法

3)-1-1　実践して得られた課題

（１）課題の概要

名古屋大学では「産学連携における秘密情報管理ポリシー」、および「産学連携における秘密情報管理ガイドライン」は制定された。秘密管理すべき対象の明確化と秘密の区分に応じた管理手法も明示され、管理レベルごとの具体的なマネジメント手法の例示を含んだルールの設定もなされた。URA 及び事務職員の秘密管理教育も実践形式のケーススタディーで実施され、教授会等で教職員への説明会も実施された。しかしながら、実際の共同研究開始時に URA が同席しての秘密管理マネジメントの蓄積例は少なく、これから課題抽出となる。

産学官連携リスクマネジメント（技術流出防止マネジメント）実務者研修会で情報取集した大学のほとんどが、研究情報管理に関するポリシーやガイドラインが策定されておらず、秘密管理すべき対象の明確化と秘密の区分に応じた管理手法を示したルールが明示されていないため、教員一人一人の常識での対応に任せている状況である。実効的・効率的な教職員の秘密管理の実施が困難な状況である。まずはガイドライン策定、啓発活動、濃淡管理の DNA 転写が課題となる。

（２）秘密管理に必要な費用の捻出

大学内センター（学内特別区）の多数の研究者については、共同研究等では、基本的に、企業の要求に即して十分に秘密管理を行っていることがわかった。しかし、全学的に同様のルールで実施することになる場合、建屋や IC カード等の情報セキュリティ設備等が必要となり、その費用の捻出をどのように行うかが課題となる。

（３）学生の取扱いの困難さ

研究室内で、複数の企業の共同研究が実施され学生が関与する場合、もしくは異なるレベルの秘密情報に学生が触れる場合、秘密情報のコンタミネーション、秘密管理が複雑となる。本年度確立したモデルだけでは、指導教官が学生への秘密管理教育を行うのは難しい。

（４）学内の情報セキュリティ部門との連携の強化

情報連携統括本部が行う情報セキュリティのうち、全学的セキュリティレベルが未だ十分でないということがわかった。また、現状研究情報の秘密管理について、技術的管理は、情報セキュリティ関連部署と協働のうえ実施すべき部分が多い。

3)-1-2　　課題への解決方法

（１）解決方法の概要

学内での事例集を充実させURAや教職員にわかりやすい教材を作成し提供する。学外対応については、技術流出防止マネジメントの取組み、学内外調査の結果・事例集など、ユーザーニーズに合わせた教材を作成し、全国レベルでの研修等によって情報発信、

共有を行う。

（２）秘密管理に必要な費用の捻出への解決方法

共同研究等において、秘密管理のために必要な建屋や設備費用・学生の雇用費用について企業側の負担や、研究プロジェクト直接経費から捻出できることの制度化が望ましい。

また、企業との共同研究等における秘密管理のための費用（学生を RA として雇用する費用・秘密管理のための IC カードや設備等）を企業側で負担することを制度化することが望ましい。特に、企業との共同研究等において、企業側からの秘密の管理について、特殊かつ厳格な要求がある場合、その負担（例えば PC、施設）を大学負担にて行うには限界がある。

そこで、共同研究開始時に URA が仲介し、個別の秘密情報の等級指定、費用対効果が良い秘密情報管理方法について提案させて頂き調整する必要がある。

（３）学生の取扱いの困難さの解決方法

共同研究等において、秘密管理のために必要となる費用（学生の雇用費用・秘密管理のための設備や PC 等）について企業側の負担や、研究プロジェクトの直接経費での捻出が制度化されることが望ましい。海外調査の結果にあるように、学生の意思尊重のため、インフォームド・コンセントの手続きを採用することで学生の自主的な意思を確認する。

（４）学内の情報セキュリティ部門との連携の強化への解決方法

情報連携統括本部と協働のうえ、全学的情報セキュリティレベルの向上、研究情報の秘密管理における技術的管理の実施を行う。具体的には、全学的な情報セキュリティレベルの向上の取組みを推進するため、現在全学的な情報セキュリティレベルの向上のための取組みを継続的に実施し、また、「名古屋大学情報セキュリティガイドライン」や「情報セキュリティ自己点検」への秘密情報の重要項目の追加、反映を行い、組織としての適切な監視活動を行う。

3)-2　得られた知見、ノウハウ（例えば有識者からの知見等）

リスクマネジメントを検討予定の大学で、リスクマネジメントに取り組む場合の自校の課題を明確にしておいてほしい。リスクマネジメントが本部集約型、部局分散型の情報以外に、例えば、アカデミックフリーダムを重視し秘密情報管理の推進がうまくいかないケースをモデル A、企業を含む大学等複数の参画機関が関与する研究を行っている大学内特区のセンターと大学本部との間でリスク管理に対する温度差が大きいケースをモデル B、財源がない・人がいないケースをモデル C などとし、事前調査により明確にしておいてほしい。この情報があれば各大学への普及活動の効率が向上する。

3)-3　次年度に向けた改善点

本年度、名古屋大学が策定したリスクマネジメントモデルから、モデルA、B、Cに対応できるようなリスクマネジメントモデルを、参画大学の力を結集して情報収集や共有化を図っていく。

第４章　　モデルの普及について

4)-1　モデルの普及のための取組状況

【課題】

ⅰ）技術流出防止マネジメントの取組みや、学内外調査の結果について全国レベルでURA研修等によって学内外に情報発信・共有を行う。

ⅱ）現在運用中の安全保障輸出管理の電子申請システムについて、他大学においても効率的な輸出管理を普及すべく、「汎用的な新電子申請システム」を他大学においてもシステム導入しやすくするために、複数の大学で共同利用できるシステム機能の考案を行う。

【実施内容】

ⅰ）「経産省　大学等向け安全保障輸出管理説明会」にて本学の輸出管理の取組みについて情報発信を行った。「アジア地域向け輸出管理セミナー」や「産学官連携リスクマネジメント事業シンポジウム」にて事業担当者が本学の事業の取組み内容について発表を行った。

・経済産業省主催「平成28年度　大学等向け安全保障貿易管理説明会」
発表者：石川綾子（12／6）
・「アジア地域向け輸出管理セミナー」発表者：石川綾子（2／23）
・文部科学省主催「平成28年度文部科学省委託事業『産学官連携リスクマネジメント事業』シンポジウム」発表者：鬼頭雅弘（3／2）

ⅱ）「汎用的な新電子申請システム」について、近畿経済産業局に11大学を集めて説明会を行った（12/2）。また、5大学においては本学にて運用中の電子申請システムについての打合せのうえシステムのデモを行い、意見交換を実施した。

4)-2　次年度以降のモデルの普及のための取組状況

図１２に、全国の大学等へのリスクマネジメントモデルを普及していくプロセスを示す。提示するモデルは、類型とリスクに応じた濃淡管理モデルであり全国展開を図っていく。

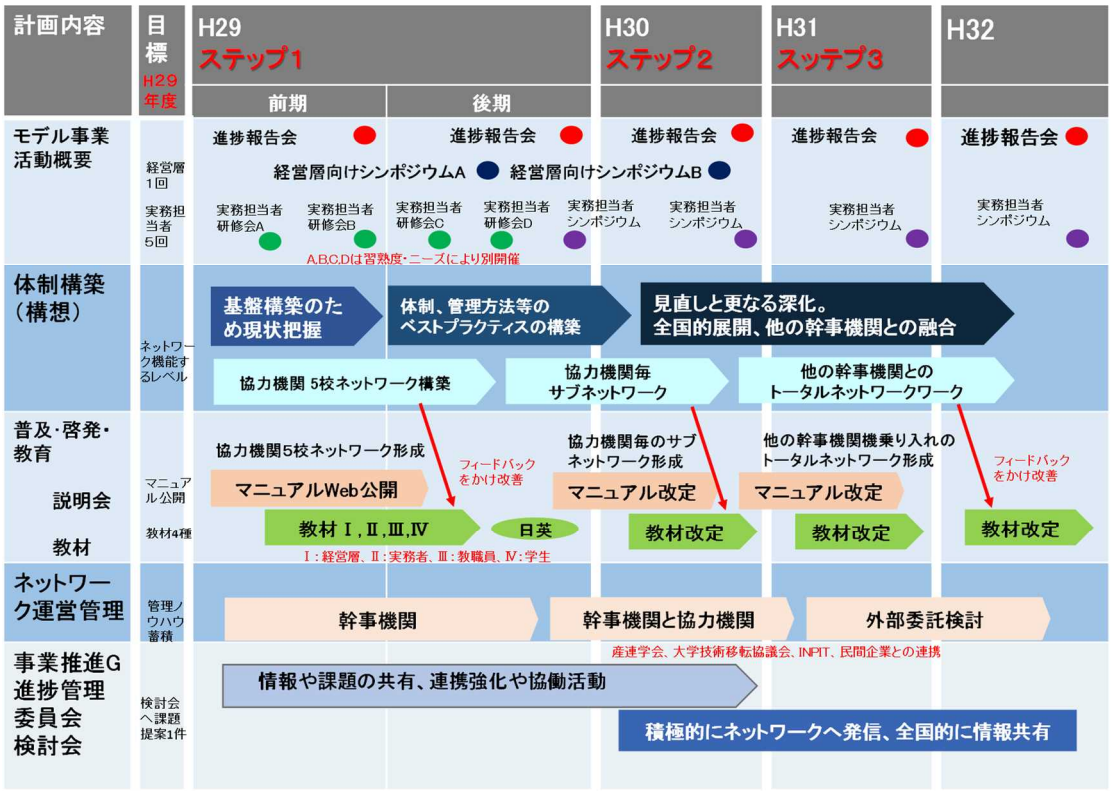


図１２　技術流出防止マネジメントモデルの普及計画

第５章　全体総括

１．実効的・効率的なマネジメント体制・システムの構築

① 秘密情報管理に関するベストプラクティス構築のため学内外調査と先進例の導入可能性の検討

秘密情報管理に関する学内外追加調査として、学内のコンソーシアム、COI（Center of Innovation)、ベンチャーにおける秘密情報管理手法や課題等の追加調査を行った。その際、学生の取扱いについてもできるだけ詳細に情報収集した。得られた技術流出防止マネジメントの先進例や現状把握の結果は、ガイドラインの策定や、実効的・効率的なマネジメント体制・システム構築へ向けての基礎資料とした。

安全保障輸出管理に関する学内調査として、留学生の受入れの際のシステムに組み込むため、理系部局において研究内容の機微度調査とリスク評価を行った。この結果を、マネジメントシステムの構築の参考とした。

② 学内体制の構築

秘密情報管理について、学内外調査の結果を踏まえて「名古屋大学 産学連携における秘密情報管理ポリシー」を改訂した。併せて「名古屋大学産学連携における秘密情報管理ガイドライン」を策定し名古屋大学のホームページに掲載した。

統括責任者、管理責任者を配置のうえ、秘密情報管理マネージャーにて、ワンストップで相談対応できる体制を構築し、NU MIRAI WG 部署や情報統括本部等と協働にて秘密情報管理の実施を検討した。まず、学術研究・産学官連携推進本部で秘密情報管理の試行を行い、次に各部局等への説明会を実施し、学内ルールの周知徹底を行うとともに、各部署で異なる運用とならないよう、秘密情報管理にかかる情報共有のフローを明確化した。また情報セキュリティ部門と情報共有のうえ、セキュリティレベルの向上、「情報セキュリティ自己点検」への秘密情報管理の重要項目の追加・反映を行った。

③ リスクに応じた管理水準設定　【濃淡管理モデルの構築】

学術研究・産学官連携推進本部会議や秘密情報連絡会・輸出管理連絡会などで、対応案件を整理・分析することでリスク顕在化させ、管理方針決定した。学内外機関や海外大学での秘密漏洩リスクや、国内大学で学生雇用する場合の秘密管理の在り方、学内組織において複数の競合企業と共同研究実施する場合の秘密管理の在り方など、特別な状況化の事例等の収集を行った。

④ 新規の電子申請システム導入

平成２７年度導入した汎用的な新電子申請システムについて、教職員向けの利用マニュアルを作成、輸出管理のホームページ上に掲載し、部局別の説明会等を実施した。また、導入に積極的な他大学等に、デモや説明等を実施して、輸出管理システムへの考え方を説明した。さらに、「経済産業省主催の大学等向け安全保障輸出管理説明会」（12 月）等において、新システムの特長や導入効果を紹介し、システムの普及促進を行った。

２．学長等のリーダーシップの下でのマネジメント強化

松尾総長プラン（NU　MIRAI2020）では、「世界で卓越した大学にふさわしい内部統制と新たなリスク管理体制の整備、構成員のコンプライアンス意識の向上」を謳う。NU MIRAI WG（法務室、学術研究・産学官連携推進本部、監査室、総務部総務課文書法規係）では、全学的な内部統制の立場から、適切なリスクマネジメント・ガバナンスを再検討・新たな協働の方法を検討した。その結果として、秘密情報管理体制の最適化、協働関係を構築した。さらに、推進本部会議で技術流出の事例や情報共有を行い、経営層にリスクマネジメントが経営上の重要事項であることを日常的に喚起した。

３．研究者等への普及啓発

安全保障輸出管理の監査等で部局等意見聴取し、技術流出防止 e-Learning の再リリースを行った。秘密情報管理の e-Learning についてもガイドラインの内容を反映させ再構築した。教職員向けに技術流出防止マネジメントに関する説明会を部局単位で行い教職員の技術流出防止に関する意識と理解を向上させ、研究者の役割分担を明確させた。

４．リスクマネジメント人材の確保・育成

本事業費で雇用した技術流出防止マネジメント担当者を、学内での相談対応や研究室調査等全般的な技術流出防止マネジメントに携わる専門家として育成した。

産学官連携担当の URA・事務職員は関連知識や実務能力の習得のため、ケーススタディーを主体とした URA 研修（※）を行った。その他のリスクマネジメントに係るセミナー・講習会にも参加することで継続的な人材の確保育成に繋げた。

(※)URA 研修：本学独自で URA として必要な知識・スキル・ネットワーク涵養のため月１回定期的に実施。平成 24 年度から大学経営・知財・リスク管理等多様なテーマにて全 49 回実施。東海地区の大学・研究機関にも開放している。

５．事例把握、情報共有（マネジメントのノウハウ等の整備）

技術流出防止マネジメントの取組みや学内外調査の結果について、東海地区知財実務

者情報交換会（10 月、2 月）において学内外に情報発信、共有を行った。リスクマネジメントの体制・システムづくりで直面した問題点とマネジメント事例について、普及展開を想定する大学等に向けて情報提供し、学外シンポジウム等で情報発信を行った。また、リスクマネジメント実務者研究会（11 月）に開催し、全国から 54 大学の実務担当者に現在抱えている課題について議論いただき、モデル的な対応方法について学習いただいた。加えて、利益相反マネジメントの受託機関と連携し普及活動できる仕組みを構築する目的で、ネットワーク構築連絡会を開催した（11 月）。

添付資料

１．産学官連携リスクマネジメント（技術流出防止マネジメント）実務者研修会_事前アンケート集計
２．機微度調査票（回答用）_2017
３．産学連携における秘密情報管理ポリシー
４．産学連携における秘密情報管理ガイドライン
５．e-learning_秘密情報管理_text（和）
　e-learning _秘密情報管理_check test(和)
６．e-learning _輸出管理（和）
７．e-learning _輸出管理（欧文）
８．第 19 回東海地区知財実務者情報交換会_秘密情報管理
９．産学官連携リスクマネジメント（技術流出防止マネジメント）実務者研修会の概要