

大学における秘密情報の保護ハンドブック

平成16年4月

平成18年5月改訂

平成23年3月改訂

(全部改訂：平成28年10月)

経済産業省

目 次

本書の構成.....	1
第1章 目的及び全体構成	2
1. はじめに	2
2. 本書策定に係る調査、検討委員会	3
3. 本書の位置づけ	3
第2章 保有する情報の把握・評価、秘密情報の決定	5
1. 大学における「秘密情報」と秘密情報管理の必要性	5
2. 保有する情報の把握・評価、秘密情報の決定	8
(1) 大学が保有する情報の全体像の把握	8
(2) 保有する情報の評価	9
(3) 秘密情報の決定	9
第3章 秘密情報の分類、情報漏えい対策の選択及びそのルール化.....	12
1. 秘密情報の分類、情報漏えい対策の選択及びそのルール化	12
(1) 秘密情報の分類	12
(2) 分類に応じた情報漏えい対策の選択.....	13
(3) 秘密情報の取扱い方法等に関するルール化の考え方	14
(4) 大学において合わせて考慮すべき事項.....	16
2. 具体的な情報漏えい対策例	17
第4章 秘密情報の管理に係る学内体制のあり方.....	18
(1) 学内体制構築に当たっての基本的な考え方	18
(2) 各部局の役割分担の例	19
第5章 秘密情報管理における学生等の扱い	21
1. 研究活動に参加する場合	22
2. インターンシップへ参加する場合	27

本書の構成

本書の構成は以下のとおりです。

なお、本書は経済産業省が別途公表している

「秘密情報の保護ハンドブック～企業価値向上に向けて～」¹

(以下、「企業向けハンドブック」という。)と併せて参照することを前提に作成しておりますので、予めお手元にご用意いただけますと幸いです。

第1章 目的及び全体構成

本書の改訂の背景と意図、本書の位置づけについて説明します。

第2章 保有する情報の把握・評価、秘密情報の決定

秘密情報を管理する重要性和、大学が扱う情報の中からどのように秘密情報を選別して管理するかについて説明します。

第3章 秘密情報の分類、情報漏えい対策の選択及びそのルール化

秘密情報管理に関するルール策定の必要性について説明するとともに、企業向けハンドブックの内容について補足します。

第4章 秘密情報の管理に係る学内体制のあり方

企業向けハンドブックで説明している内容をもとに、大学向けの補足を行います。

第5章 秘密情報管理における学生等の扱い

学生等が秘密情報を扱う場合の対策と、対策の実施にあたって留意すべき事項について説明します。

¹ <http://www.meti.go.jp/policy/economy/chizai/chiteki/trade-secret.html>

第1章 目的及び全体構成

1. はじめに

近年、イノベーション創出を目的として、大学、高等専門学校、大学共同利用機関等の教育研究機関（以下、「大学」という。）と企業との産学連携活動が盛んになっています。この結果、共同研究等を通じて企業から秘密として保持すべき情報（以下、「秘密情報」という。）が大学に持ち込まれるなど、大学が企業等の秘密情報を保有し、これを取り扱う可能性が従前よりも増大しており、大学における適切な秘密情報管理への要請は年々高まっています。こうした情報が教職員等（大学に所属している（大学と雇用関係にある）教職員、学生（社会人学生を含む）、派遣職員等が含まれる。なお、教職員等に含まれる者の範囲は個々の事案によって異なるため、具体的な事案に基づきそれぞれ判断することを要する。以下、同じ。）により不正使用された場合等には、教職員等が責任を問われるのみならず、大学の責任が問われたり大学の社会的信頼も損なわれたりする可能性があります。

一方で、大学は「その成果を広く社会に提供することにより、社会の発展に寄与するもの」²などとされており、大学が保有する情報には、何らかの形で社会に対して公表されることを前提としたものが多くあります。こうした環境の中で、例えば、共同研究の相手先企業から取得した情報を秘密として保持しようとするとき、新たに管理の方法をルールとして定めたり、そのルールを守るための体制を整備したりするといった取組が必要になる場合があります。企業等から秘密情報を受け取ることを過度に回避したり、あるいは受け取っても必要以上に厳格な管理をしたりするのでは、新たなイノベーションを生み出すことはできません。そのため、大学に対して、情報の管理と有効利用とのバランスを考慮しながら、日々の業務や研究活動等の中で秘密情報を積極的に活用し、当該秘密情報の価値を発揮させていくことが求められています。

経済産業省は、平成16年4月に、大学が自ら主体的に営業秘密管理指針を作成する際に留意すべき点を示すことを目的とし、平成15年1月に策定した「営業秘密管理指針」（以下、「指針」という。）を基に、「大学における営業秘密管理指針作成のためのガイドライン」（以下、「ガイドライン」という。）を策定しました。その後、平成27年1月に指針の全部改訂を行い、不正競争防止法によって差止め等の法的保護を受けるために必要となる最低限の水準の対策を示しました。また、営業秘密としての法的保護を受けられる水準を超えて、漏えい防止ないし漏えい時に推奨される（高度なものを含めた）包括的対策を示すため、平成28年2月に「秘密情報の保護ハンドブック ～企業価値向上に向けて～」（以下、「企業向けハンドブック」という。）を策定しています。

一方、指針や企業向けハンドブックは、主に企業を念頭においたものであり、学生が企業との共同研究に参加し当該企業の秘密情報を取り扱う場合における対策などの、大学特

² 学校教育法第83条、第115条

有の事情に配慮した記述がないことなどから、前述のガイドラインを新たに「大学における秘密情報の保護ハンドブック」（以下、「本書」という。）と改題の上、全部改訂を行うこととしました。

本書が、各大学における関係規程の整備や適切な秘密情報管理の一助となり、結果として産学共同研究をはじめとした産学連携等が一層推進されることを強く期待しております。

2. 本書策定に係る調査、検討委員会

経済産業省では、平成27年度産業技術調査事業（大学における営業秘密管理に関する実態調査）において、大学・産業界の有識者から成る検討委員会（委員長：飯田 香緒里・国立大学法人東京医科歯科大学 研究・産学連携推進機構教授 兼 産学連携研究センター一長）を設置し、ガイドラインの再改訂の是非及び改訂内容について検討を行いました。同調査事業では、改訂に係る検討に先立ち、大学における営業秘密情報の管理に関する実態についてアンケート（注）及びヒアリングによる調査を実施しています。実態調査の結果、営業秘密情報管理に関する規程等自体を策定していない大学が多く存在することが明らかになりました。

経済産業省では、こうした実態及び検討委員会における議論の内容を踏まえ、

- i 指針の全部改訂内容の適切な紹介
- ii 企業向けハンドブックとの整合性の確保
- iii 秘密情報管理における学生等の扱いについての留意点等を示す

等の方針に基づき、大学が企業向けハンドブックを活用して秘密情報の漏えいを防止するための対策を検討する際、特に考慮すべき事項を示すことを目的として、本書を策定しました。

（注）「大学における営業秘密情報の管理に関する実態調査」アンケート調査 実施概要

調査期間	平成27年12月4日から平成28年3月18日まで
調査対象	全国立大学並びに検討委員会において推薦のあった公立及び私立大学 計157機関(国立86、公立24、私立47)
調査方法	各大学総務・財務担当理事宛て、調査票(大学全体の取組に係るもの(機関全体編)1部、部局・研究科単位での取組に係るもの(個別編)複数部)を発送し、郵送等による回答を依頼
調査事項 (設問例)	機関全体編：営業秘密情報の管理に関する規程等の策定状況 等 個別編：営業秘密情報を管理するための措置の導入状況 等
回答数	機関全体編：79(回収率50.3%) / 個別編：176

3. 本書の位置づけ

(1) 企業向けハンドブックについて

企業等の経営者は、秘密情報を含めた「情報資産」を企業活動の中でどのように有効に活用しつつ、その漏えいリスクにどのように対処していくかを、リーダーシップを持って判断していかなければなりません。企業向けハンドブックは、秘密情報を決定する際の考

え方や、その漏えい防止のために講ずるべき対策例、万が一情報が漏えいした場合の対応方法等を示しており、それによって、経営者をはじめとする企業の方々、自社における秘密情報の管理を適切に実施していく際の参考としていただくことを目的として策定されました。

平成27年1月に改訂した指針には、不正競争防止法における「営業秘密」として法的保護を受けるために必要となる最低限の水準の対策が示されていますが、企業向けハンドブックは、営業秘密としての法的保護を受けられる水準を超えて、秘密情報の漏えいを未然に防止するための対策を講じたい企業の方々にも参考としていただけるよう、情報漏えい対策として有効と考えられる対策をできる限り収集して包括的に紹介しており、企業の方々も漏えい対策を検討・実施する際に、会社の規模、業態、保有する情報の性質などに応じて適切な漏えい対策を選択いただけるように工夫しています。したがって、企業向けハンドブックで紹介する対策の全てを実施しなければ、不正競争防止法の「営業秘密」として法的保護が受けられないというものではありません。

(2) 本書と企業向けハンドブックの関係

企業向けハンドブックは、前述のとおり、企業における秘密情報の保護を想定して作成されていますが、大学が秘密情報の漏えいを防止するための対策を検討する際においても参考とすることができます。特に、大学の事務部門における情報管理を対象とする場合であれば、そのまま適用可能な内容が多くなっています。さらに、企業向けハンドブックの5-2「(2) 共同・受託研究開発」では共同・受託研究開発における他社の秘密情報の侵害を防止するための考え方について説明しており、ここに示された内容は大学においてもそのまま適用できるものです。

本書は、大学が企業向けハンドブックを活用して秘密情報の漏えいを防止するための対策を検討する際、特に考慮すべき事項を示すことを目的としています。

大学で企業向けハンドブックを参考とする際に留意しなければならないことは、前述のとおり、企業向けハンドブックと指針は目的を異にしたものであることと、冒頭に示したように、大学では社会への公表を目的とした研究・教育活動が行われているなど、企業とは異なる点があるということです。また大学の場合、教職員と異なり、大学と雇用関係にない学生等が、秘密情報として保護する必要がある情報（研究に関する情報、研究活動の成果等）に触れる可能性もあります。

本書は企業向けハンドブックで取り扱う対策に加えて、こうした大学特有の事情に配慮した秘密情報の保護のための対策を検討する際の考え方についても説明しています。

第2章 保有する情報の把握・評価、秘密情報の決定

1. 大学における「秘密情報」と秘密情報管理の必要性

企業が有する「情報資産」は、商品の生産、販売、サービスの提供などの様々な企業活動の価値や効率性を高めています。「情報資産」と一口に言っても、顧客情報、発明情報、ビジネスモデル、取引情報、人事・財務情報など多種多様であり、製品やサービスが均質化しつつある近年において、他者との差別化を図り、競争力を高めていくために、「情報資産」の保護・活用は、ますますその重要性を増しています。そのような「情報資産」の中には、秘密として保持すべき情報（秘密情報）が存在します。秘密情報は、一度でも漏えいすれば、たちまち情報の資産としての価値が失われてしまい、その回復は非常に困難なものです。企業の経営に致命的な悪影響を与える場合もあります。

企業と同様に、大学も、自らが創出した研究成果や、入試情報、学内人事・財務情報や、企業等の共同研究に際して相手先企業から提供を受けた研究情報等、様々な「情報資産」を有しています。大学が有する「情報資産」は、何らかの形で社会に対して公表されることを前提としたものも多く、公開済みの研究成果等、秘密として管理する必要のないものがある一方、試験問題や特許出願前（未公開）の研究成果等の秘密情報も様々な存在しています。こうした秘密情報は、一度でも漏えいすれば、その情報の資産としての価値が失われ、回復は非常に困難であり、大学の経営や信用に致命的な悪影響を与える場合もあります。

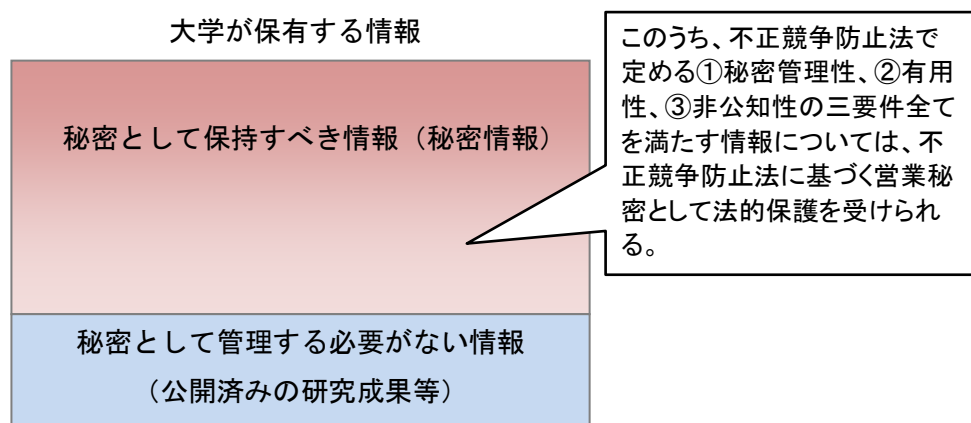


図1 大学が保有する情報の分類

(参考：営業秘密管理指針における営業秘密の定義及び三要件の記載について)

【不正競争防止法における営業秘密の定義について】(指針2頁)

<指針2頁>

○ (不正競争防止法における営業秘密の定義)

不正競争防止法(以下、「法」という。)第2条第6項は、営業秘密を

①秘密として管理されている [秘密管理性]

②生産方法、販売方法その他の事業活動に有用な技術上又は営業上の情報 [有用性] であって、

③公然と知られていないもの [非公知性]

と定義しており、この三要件全てを満たすことが法に基づく保護を受けるために必要となる。

【秘密管理性について】(指針3～15頁)

<指針3～4頁>

(1) 秘密管理性要件の趣旨

秘密管理性要件の趣旨は、企業が秘密として管理しようとする対象(情報の範囲)が従業員等に対して明確化されることによって、従業員等の予見可能性、ひいては、経済活動の安定性を確保することにある。

○ (営業秘密の情報としての特性)

・営業秘密は、そもそも情報自体が無形で、その保有・管理形態も様々であること、また、特許権等のように公示を前提とできないことから、営業秘密たる情報の取得、使用又は開示を行おうとする従業員や取引相手先(以下、「従業員等」という。)にとって、当該情報が法により保護される営業秘密であることを容易に知り得ない状況が想定される。

○ (秘密管理性要件の趣旨)

・秘密管理性要件の趣旨は、このような営業秘密の性質を踏まえ、企業が秘密として管理しようとする対象が明確化されることによって、当該営業秘密に接した者が事後に不測の嫌疑を受けることを防止し、従業員等の予見可能性、ひいては経済活動の安定性を確保することにある。

<指針5～8頁>

(2) 必要な秘密管理措置の程度

秘密管理性要件が満たされるためには、営業秘密保有企業の秘密管理意思が秘密管理措置によって従業員等に対して明確に示され、当該秘密管理意思に対する従業員

等の認識可能性が確保される必要がある。

具体的に必要な秘密管理措置の内容・程度は、企業の規模、業態、従業員の職務、情報の性質その他の事情の如何によって異なるものであり、企業における営業秘密の管理単位における従業員がそれを一般的に、かつ容易に認識できる程度のものである必要がある。

【有用性について】（指針 15 頁）

<指針 15 頁>

有用性の考え方

「有用性」が認められるためには、その情報が客観的にみて、事業活動にとって有用であることが必要である。一方、企業の反社会的な行為などの公序良俗に反する内容の情報は、「有用性」が認められない。

【非公知性について】（指針 16 頁）

<指針 16 頁>

非公知性の考え方

「非公知性」が認められるためには、一般的には知られておらず、又は容易に知ることができないことが必要である。

(1) 「公然と知られていない」状態とは、当該営業秘密が一般的に知られた状態になっていない状態、又は容易に知ることができない状態である。具体的には、当該情報が合理的な努力の範囲内で入手可能な刊行物に記載されていない等、保有者の管理下以外では一般的に入手できない状態である。

2. 保有する情報の把握・評価、秘密情報の決定

ここでは、これまでに秘密情報を区別して管理するための規程等や体制を整備してこなかった大学を念頭に、自学が保有する情報から秘密情報を決定するまでのステップを紹介いたします。各大学が、自学が保有する情報を把握し、その経済的価値や漏えい時の損失の程度といった指標を通じて評価することにより、自らの持つ強みやその源泉を再確認することで、今後の更なる競争力強化等の可能性の検討につなげることができます。

具体的な方法については、本書に記載する企業向けハンドブックにおける対応頁を参照してください。

(1) 大学が保有する情報の全体像の把握（企業向けハンドブック7～9頁）

- 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ます。その際、情報は、紙に記載されていたり、USBメモリ等の機器・媒体に記録された電子データ等のような形で存在するだけではなく、教職員が業務の中で記憶したノウハウなど文章化されず目に見えない形で存在する場合等があります。

- 保有する情報の把握に当たっては、個別担当者の感覚等によりその判断にばらつきが生じないようにするため、プロジェクトや業務の規模、扱う情報の多寡等に応じて、学内で統一的な判断が可能となるような情報の把握方法をとることが望まれます。例えば、以下のような方法が考えられます。また、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こともできます。

（大学運営に係る情報の場合）

- 学長等から指名された責任者等が学内の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方法
- 秘密情報の管理を統括する部署が統一的な基準を示しつつサポートしながら、各部署や個別の担当職員に、その基準に則してそれぞれが有する情報を学長等から指名された責任者等に報告させ、情報を集約することにより把握する方法

（研究開発等の技術に係る情報の場合）

- 秘密情報の管理を統括する部署が統一的な基準を示しつつサポートしながら、各研究室等の教員・研究者等に、その基準に則してそれぞれが有する情報を把握させる方法

等

- 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、「〇〇に関する研究に係る情報」

など、情報の種類を一定程度、一般化・抽象化した形で把握することが必要となります。

- なお、学生が学内において発明を行った場合、雇用契約や譲渡契約に基づき、当該発明に係る権利を学生から譲り受けない限り、大学の情報ではないことに留意する必要があります。

(2) 保有する情報の評価（企業向けハンドブック9～11頁）

- 次に、(1)の作業で把握した情報について、情報が産み出す経済的価値、学外で利用されたり漏えいした場合の損失の大きさ（どの程度社会的信用が低下してしまうのか等）、悪用されるような性格の情報か否か、契約等に基づき学外から預かった情報か否か等、以下の観点を参考に評価を行い、その評価結果に応じて情報を階層化します。

- 大学における評価に関する観点の例を示します。
 - 情報の経済的価値（大学保有特許等、その情報によって生み出される現在の価値）
 - 連携先機関等に与える損失の程度（例えば、情報が漏えいした場合、その情報を使用して事業（研究等）を行う連携先機関に生ずる損失の程度）
 - 情報漏えい時の社会的信用低下による損失の程度（共同研究件数の減少等）
 - 情報漏えい時の契約違反や法令違反に基づく制裁の程度

等

(3) 秘密情報の決定（企業向けハンドブック11～13頁）

- (2)で行った評価の高低を基準に、保護に値するものかどうかを判断します。保護に値する情報であっても、その情報をより効果的に活用するための方法を、情報の性格に照らして検討することが重要です。
- 研究開発等に係る技術情報については、特許権など権利化して他者にライセンスを行ったり標準化を行うことを通じて、技術を広く使用させる活用方法がある一方で、情報を独占することによって技術的優位性を高めるといった活用方法もあります。後者の場合は権利化した上で独占使用する方法や秘密として保持する方法が考えられますが、権利化する場合は研究分野や情報の性質なども考慮し、その情報の価値が最大限高められる活用方法を慎重に選択することが重要です。

- 学生に関する情報等については、権利化、標準化の対象とならない性格のものであり、秘密として保持する方が適切と考えられます。
- 保護を要するものかどうかを判断する際には、想定される管理コスト、訴訟コスト（証拠収集等のための労力、費用、訴訟期間等）等のコスト、漏えいによって被るおそれのある損失、保護により得られる利益（損害賠償請求や侵害差止請求により取り戻すことが容易か否か）の総合考慮という観点から保護する意義がどの程度あるか、法令や他者との契約による特別の管理を求められる情報か否かという視点での判断が必要となる場合もあると考えられます。
- これらの考えに基づき、秘密として保持することを決定した情報が、各大学における秘密情報となります。以下では、真に秘密として保持すべき情報を判断し、各大学の秘密情報を決定する際に参考となる観点を紹介します。
 - ① 運営情報（主に職員が関与する大学の運営等に係る情報）
 - 自大学独自の情報であり、その漏えいにより、自らの社会的信用の低下を招くとともに、大学経営や調達等の業務への支障を来す情報か否か
（大学や部局の経営やマネジメントに関する内部情報、入試情報、学内試験情報、調達関連情報（予定価格等、秘密にする必要があるもの）、財務・経理に関する内部情報、学内の情報ネットワーク構成図などのセキュリティの観点から秘密にすべき内部情報 等）
 - 自大学独自の情報ではない情報や個人情報であり、その漏えいにより、法令違反や他者との契約違反等となり、自らの社会的信用の低下を招いたり、他者との信頼関係を毀損させる情報か否か
（教職員や学生の個人情報、受託やライセンス等の他者との契約等により限定的に開示された営業情報 等）
 - ② 技術情報（主に教員や研究者、学生が関与する研究開発等の技術等に係る情報）
 - 自大学独自の情報であり、その漏えいにより、自大学の出願や研究に支障を来す情報か否か
（自大学独自の研究に基づく発明に係る出願前情報や公開前情報、学会発表や論文発表前における自大学独自の研究内容に関する情報、自大学独自の研究によって生じた研究開発ノウハウや研究成果有体物 等）
 - 自大学独自の情報ではない情報であり、その漏えいにより、法令違反や他者との契約違反等となり、当該他者との信頼関係を毀損させる情報か否か

(共同研究や受託研究の際、連携先・委託元から秘密情報として提供された情報、共同研究に基づく発明に係る出願前情報や公開前情報、学会発表や論文発表前における共同研究内容に関する情報、共同研究によって生じた研究開発ノウハウや研究成果有体物受託やライセンス等の他者との契約等により限定的に開示された技術情報 等)

【企業等との共同研究等を通じた学外の秘密情報について】

- 産学共同研究をはじめとする産学連携等を推進する上で、企業と大学（教職員が契約者になる場合も同じ。）との間で、秘密情報を取り扱う機会が増加します。その際、企業が大学に対して企業の秘密情報を開示する場合もあれば、大学が企業に対して大学の秘密情報を開示する場合があります。また、共同研究等の場合は、大学と企業が協力して一定の秘密情報を新たに生み出す場合もあります。
- このような状況を前提とした場合に、秘密情報の管理を実践する上で重要なのは、予め、大学と企業との間で秘密管理のあり方について共通理解を有しておくことです。大学と企業では、その社会的な役割が異なる以上、双方で秘密管理の程度や範囲、対象について理解が異なるのは当然のことです。したがって、大学と企業との間で共有される秘密情報について、相手側に秘密管理への意識や、そのために費やすことができるコスト等に関する十分な理解を得る必要があります。
- したがって、産学連携等を進める際は、秘密情報として管理すべき情報の範囲のみならず、その具体的な管理の方法について、双方において通常内部で講じている管理方法や、外部組織と共同研究する際に講じている管理方法等を参考にしつつ、大学と企業との間で予め合意しておくことが重要です。また、その際には、どういった分野の研究をするのか、企業から提供を受ける（企業に提供する）のは情報だけか、設備や試料等有体物も含むのか、更には研究員の交流や派遣はあるのかなどの要素を考慮し、必要に応じて、有体物移転契約（MTA）を結ぶなどの対応をするとともに、成果の帰属、またその取扱い（特許出願の有無や取得された特許の維持・管理の分担、発表の有無や発表名義・内容等）についても議論し、理解を得た上で、契約書の形で理解内容を確認しておくことが望まれます。

第3章 秘密情報の分類、情報漏えい対策の選択及びそのルール化

1. 秘密情報の分類、情報漏えい対策の選択及びそのルール化

(1) 秘密情報の分類（企業向けハンドブック14～16頁）

（分類の必要性）

- 第2章において、自大学における「秘密として保持すべき情報」（秘密情報）が決定されることとなりますが、秘密情報は日々の活動（研究等）の中で活用されてこそ価値を発揮するものであることを踏まえると、すべての秘密情報に一律に厳格な管理を行うことは、円滑な活動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ります。例えば、企業等から受け取った秘密情報の漏えいをおそれるあまり、金庫のように常時鍵を掛けて誰も開けてはならない場所に保管して（研究等）に一切使わないのでは、その情報の真価は発揮されず、新たなイノベーションを生み出すことにつながりません。情報の活用と管理のバランスを考慮した管理方法を検討していくことが重要です。
- そのためには、各大学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上で、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です。
- なお、分類の数については、各大学において適正と考えられる分類数は異なるものと考えられますが、あまりに多くの分類数としてしまうと、情報管理が煩雑となり対策が徹底されなくなってしまうなど、対策の有効性・効率性を低減してしまうおそれがあることに留意します。

（分類に当たっての考え方）

- 秘密情報の分類においては、まず、情報の評価の結果を考慮し、評価の高い情報ほど厳格な対策を行うことが考えられます。
 - 一方で、同程度の評価の秘密情報であっても、情報の利用態様に依りて異なる対策を講ずる場合もあります。大学における情報の利用態様として考慮すべき観点の例としては、以下のものが想定されます。
 - 教職員が手軽に閲覧・持出し・利用等をできるようにしておかなければ日々の活動が困難となる情報か否か
 - 情報に対するアクセス権者の範囲が広くならざるを得ない性質のものか否か
 - その情報を活用する教職員の職務は何か
 - 外部ネットワークに接続されたPC等に保管されることが多い情報か否か
 - 日々更新される情報か否か
- 等
- 共同研究相手先企業等から秘密保持義務を負った状態で受領した情報や個人情報保

護法に基づく管理が求められる個人情報など、「法令や他者との契約に基づく特別の管理」を求められる情報の分類や対策には十分な注意が必要だと考えられます。

(秘密情報の分類例)

○ 以下に秘密情報の分類の例を示します。

表 1 秘密情報の分類例

3分類型		4分類型		情報の例
レベル2	機密として保護すべきもの	レベル3	漏えい等の事象が自学の業務等に深刻かつ重大な影響を及ぼすもの	機微情報、入試情報
		レベル2	漏えい等の事象が自学の業務等に重大な影響を及ぼすもの	成績情報、進路情報
レベル1	機密としての保護は要しないが、その漏えい等の事象が自学の業務等に影響を及ぼすおそれがあるもの	レベル1	漏えい等の事象が自学の業務等に軽微な影響を及ぼすもの	教職員出勤簿、 出納記録
レベル0	保護不要	レベル0	保護不要	公開情報

(2) 分類に応じた情報漏えい対策の選択 (企業向けハンドブック 17～20頁)

情報漏えい対策は、目的を考えずに闇雲に実施すると、業務への過度な制限や無駄なコストが発生する可能性があります。そのため、情報漏えいに対し、それぞれの対策がどのような効果を発揮するのかといった目的を意識し、効果的・効率的な対策を選択することが望まれます。そこで、企業向けハンドブックでは、犯罪学の考え方なども参考にしながら、秘密情報の漏えい要因となる事情を考慮し、5つの漏えい対策の目的を設定した上で、それぞれに係る対策を示しています。以下では、企業向けハンドブックに対応する形で、大学における「対策の目的」について説明します。

① 接近の制御

- 秘密情報を閲覧・利用等することができる者の範囲を適切に設定した上で、施錠管理・入退室制限等といった区域制限等を行うことにより、アクセス権を有しない者を対象情報に近づけないようにします。
- 接近の制限に係る対策のポイントは、まず、アクセス権を有する者が、本当にその情報について知るべき者かという観点から適切に限定されることであり、接近の制限に係る対策を講ずる前提として、まずは学内の規程等により、アクセス権設定に係るルールを策定することが必要となります。

② 持出し困難化

- 秘密情報が記載された資料等の回収、学内のノートPCの固定、記録媒体の複製制限、教職員の私物USBメモリ等の携帯メモリの持込み・利用を制限すること等によって、当該秘密情報を無断で複製したり持ち出すことを物理的、技術的に阻止します。

③ 視認性の確保

- 職場のレイアウトの工夫、資料・ファイルの通し番号管理、録画機能付き防犯カメラの設置、入退室の記録、PCのログ確認等により、秘密情報に正当に又は不当に接触する者の行動が記録されたり、他人に目撃されたり、事後的に検知されたりしやすい環境を整えることによって、秘密情報の漏えいを行ったとしても見つかってしまう可能性が高い状態であると認識する状況を作り出します。また、ここでの対策は、教職員等の行為の正当性（身の潔白）を証明する手段としても有効です。
- 現実に監視するというだけでなく、例えば、職場の整理整頓や教職員等に文書管理責任を分担させて情報管理に関する当事者意識を持たせたりすることで、職場を管理の行き届いた状態にすることにより心理的に漏えいしにくい状況を作ることも含まれます。

④ 秘密情報に対する認識向上（不正行為者の言い逃れの排除）

- 秘密情報の取扱い方法等に関するルール策定と周知、秘密情報の記録された媒体へ秘密情報である旨の表示を行うこと等により、教職員の秘密情報に対する認識を向上させます。また、同時に、不正に情報漏えいを行う者が言い逃れできないようにします。

⑤ 信頼関係の維持・向上

- 教職員等に情報漏えいとその結果に関する事例を周知することで、秘密情報の管理に関する意識を向上させます。また、研究環境、職場環境の整備や適正な評価等によって組織への帰属意識を醸成したり、仕事へのモチベーションを向上させることによって、職場のモラルや教職員等との間の信頼関係を維持・向上させます。

(3) 秘密情報の取扱い方法等に関するルール化の考え方（企業向けハンドブック21～22頁）

- 上記で決定した対策を実効的に講じていくためには、その内容を学内のルールとしてとりまとめる必要があります。

- 大学で取り扱う秘密情報、とりわけ、主に教員や研究者あるいは学生が関わる、研究開発等の技術に係る情報については、各研究室・研究科等の単位で、独自に管理している場合も多くあるものと考えられます。しかし、全学的に共通する基準等がない場合、各教職員等による個別判断が求められることとなり、類似の情報に対して全く異なる管理方法が選択される場合があります。このようなとき、本来ならば講じておくべき対策を行わなかったがために、情報が漏えいするリスクが高まり、場合によっては漏えいが発生してしまう可能性もあります。教職員や学生等を情報漏えいリスクから守るためにも、部署・研究室等の単位ごとの個別対策のほかに、大学全体に共通する、一定の統一的なルール策定及びその周知、徹底を行うことが重要となってきます。
- 一方で、情報資産は活用しなければその価値が発揮できません。ルール策定にあたっては、情報の活用と管理のバランスに留意することが必要です。
- ルール化の方法としては、教職員の就業規則に情報管理に関するルールを含める方法と、情報管理規程といった学内の規程を新たに策定ないし改訂する方法などがあります。
- 学内情報管理規程に盛り込む内容としては、以下が想定されます。

- | |
|--|
| <ul style="list-style-type: none"> ①本規程の趣旨・目的 ②用語定義 ③適用範囲（対象となる範囲） ④管理体制（責任者、担当者の割当てと役割） ⑤管理方法（分類、分類に応じた具体的対策） ⑥関係者の責務等（秘密保持や関連法令の遵守等） ⑦罰則等（教職員等が情報漏えいを生じさせた場合の罰則等） |
|--|

- 次表に示す大学では、秘密情報の取扱い方法に関する具体的なルールを策定・公表しています。

表 2 秘密情報の取扱い方法に関するルールを公表している大学の例

新潟大学の研究室における秘密情報の管理に関する規程 http://www.niigata-u.ac.jp/reiki_int/reiki_honbun/aw94408061.html
名古屋大学 産学連携における研究情報管理ポリシー http://www.aip.nagoya-u.ac.jp/researcher/intellectual/images/information_management_policy.pdf
共同研究等の産学官連携における研究成果、秘密情報等の管理に関するガイドライン（神戸大学） http://www.innov.kobe-u.ac.jp/invention/ip_policy/downloads/secret_guidelines.pdf

(4) 大学において合わせて考慮すべき事項

秘密情報の管理に関する対策の検討に際しては、例えば、下記の目的についての対策と重なる部分も多いことから、整合について調整することが考えられます。

① 安全保障貿易管理

大学は、安全保障貿易管理における輸出者等に相当することから、軍事転用可能な技術に関する情報が違法輸出されることのないよう、必要な管理措置を講ずる必要があります。

② プライバシー・機微情報管理

学内で医療情報や遺伝子情報を扱う部局においては、こうしたプライバシーや機微情報を保護するために独自の情報管理に関する規程を策定・運用している場合が多いと考えられます。

③ 研究成果有体物管理

研究成果有体物の取扱いについては、既に各大学においてガイドラインや規程類を策定・運用しているケースが多くあると考えられます。

等

2. 具体的な情報漏えい対策例

企業向けハンドブックの25～94頁には、従業員等、退職者等、取引先、外部者の各ステークホルダーについて、5つの「対策の目的」に応じて有効と考えられる具体的な情報漏えい対策例が提示されており、大学においても企業向けハンドブックを参考に情報漏えい対策を講じることが可能だと考えられます。

例えば、以下のようなケースが考えられます。

- ・大学と雇用関係にある教職員に向けた対策を検討する際、企業向けハンドブックの「従業員等に向けた対策」を参考にする
- ・大学を退職する教職員や他の大学へ移る教職員に向けた対策を検討する際、企業向けハンドブックの「退職者等に向けた対策」を参考にする
- ・委託先や委託元、外注先や外注元、共同研究相手等に向けた対策を検討する際、企業向けハンドブックの「取引先に向けた対策」を参考にする
- ・教職員、学生等、委託先や委託元、外注先や外注元、共同研究相手等以外の外部者に向けた対策を検討する際、企業向けハンドブックの「外部者に向けた対策」を参考にする

また、本書では、大学特有の事項と考えられる秘密情報管理における学生等の扱いについて、第5章において別途説明をしています。学生等が秘密情報に触れる場合に講じるべき対策については、当該学生等の秘密情報への関わり方を考慮しつつ企業向けハンドブックの25～94頁の適宜箇所及び第5章の内容を参考に検討してください。

第4章 秘密情報の管理に係る学内体制のあり方

本書で紹介する取組み全般を、真に実効的なものとするためには、それらの対策が一時的なものとならないようにする必要があります。そのためには、秘密情報の管理の実施状況を定期的にチェックするとともに、状況の変化に応じた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す。本章では、そのような学内体制の整備における基本的な考え方を示しつつ、考えられる学内体制の参考例を提示しています。

(1) 学内体制構築に当たっての基本的な考え方(企業向けハンドブック95～102頁)

- 秘密情報の管理は一旦対策を講ずれば完結するというものではなく、それが継続して実施され、状況の変化に応じて適切に見直しが行われるようにしていかなければなりません。秘密情報の管理に割くことができる費用や人員が限られている中で、網羅的な対策を実施することが困難である場合は、必ずしもその全てを実施しなければならないというものでもありません。守るべき情報の種類等を踏まえて、適切と考えられる対策を選択して実施していくことが重要です。
- また、秘密情報は全ての部門に存在することが考えられ、かつ、その漏えい対策は、知的財産、人事・労務、情報セキュリティ、法務などの多様な観点からの対策を必要とすることから、学内の個々の部門が、それぞれ独自に対策を行い、全体としての調整を欠いたままでは十分な対策を講ずることはできません。情報管理規程等の学内ルールを整備など、本来的に全学的に検討しなければならない対策も存在します。
- 加えて、秘密情報の漏えいが、その情報の価値を失わせるのみならず、社会的信用の低下や他者からの訴訟リスクなど、様々な損失を生じさせるおそれがあることを踏まえると、コンプライアンスの観点からも、経営層が、率先して学内体制の構築に関与していくという意識を持つ必要があります。したがって、経営層が、学内外に向けて、秘密情報の管理に取り組む姿勢(ポリシー)を明確に示し、学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ります。
- どのような学内体制が望ましいのかは、事業の規模や性質によって異なりますが、経営層の積極的な関与の下、以下の例を参考に、体制が単に形式的なものにならないように留意しながら、秘密情報の管理が継続的に実施され、状況の変化に応じた適切な見直しを行うことができる体制とすることがポイントです。大学における体制として、以下の2種類の考え方が想定されます。

① 単一学部からなる大学等の場合

- 下記②のように、別に横断的組織を設置することの効果がいと見込まれるため、情報管理の主管部局を定め、その部局を中心に運用することが考えられます。

② 総合大学等の場合

- 一般に、大学では学部や附属機関毎で事情が異なり、独立性の高い運用をしているケースが多いことから、こうした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：副学長、担当理事等）の指示に従って情報管理を行うことが適切と考えられます。参加すべき部局としては以下が想定されます。

- 総務課（規程策定等担当、法務担当）
- 人事課（人事・労務担当、教育担当）
- 産学連携本部（契約担当、知的財産担当）
- 情報基盤センター（情報システム、ネットワーク運用担当）
- 学内CSIRT³
- 各学部・研究科

- また、秘密情報管理委員会が担う役割としては、以下が想定されます。

- 学内規程の整備・見直し
- 各部門の役割分担の決定
- 情報収集体制の確立
- 情報漏えい事案対応に係るルール（マニュアル等）の策定
- 秘密情報の管理のチェック・見直し
- 周知徹底、教育、意識啓発

- ただし、必ずしも新規の組織を設置しなければならないわけではなく、情報資産の管理を統括する「情報セキュリティ委員会」や、学内のリスクマネジメントを目的とした「リスク管理委員会」、法令等の遵守一般を担当する「コンプライアンス委員会」のような、学内に既に存在している横断的組織に同様の役割を担わせることも考えられます。

(2) 各部局の役割分担の例（企業向けハンドブック102～106頁）

大学における秘密情報の管理に関しては、(1) で定めた秘密情報管理委員会の構成メンバーを中心に、次表の要領で分担することが考えられます。

³ Computer Security Incident Response Team の略。コンピュータやネットワーク上の問題に対処するための組織。Computer Emergency Response Team (CERT) などの呼び方もある。

表 3 各部署の役割分担例

部署名（例）	情報管理に関して学内で担当している役割
総務課	・ 法人文書管理（台帳管理等）
人事課	・ 教職員を対象とする教育の実施 ・ 違反を犯した教職員の処分
産学連携本部	・ 学外機関との秘密保持契約等の雛形整備
情報基盤センター	・ 学内情報システムとネットワークの管理 ・ 学内セキュリティポリシーに基づく運用
学内 CSIRT	・ 学内情報セキュリティインシデントへの対応
その他各部署	・ 自部署で管理する情報の保守

以下の2章は企業向けハンドブックの内容を参照してください。

大学で検討することが望ましい事項は次の通りです。

第5章 他社の秘密情報に係る紛争への備え

- 自大学の情報の独自性を立証できるようにしておくことが重要です（「5-1 自社情報の独自の立証」を参照のこと）。
- 共同研究先企業等の情報をきちんと管理することが大学に求められていることから、他者の秘密情報の意図しない侵害を防止するための対策を行うことが重要です（「5-2 他者の秘密情報の意図しない侵害の防止」を参照のこと（特に「(2) 共同・受託研究開発」を参照のこと））。

第6章 漏えい事案への対応

- 個人に関する情報が漏えいした場合は、報告先や対応が異なることに留意してください。

第5章 秘密情報管理における学生等の扱い

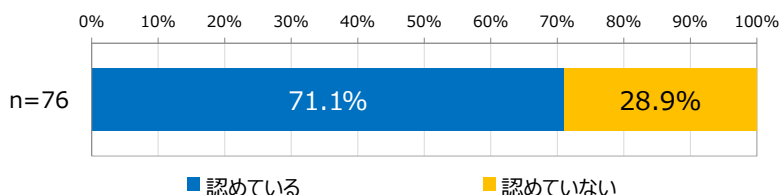
大学の教職員と異なり、大学と雇用関係にない者(教育サービスの受益者である学生、他大学等から派遣された教職員、民間企業等から受け入れた受託研究員、社会人学生など。以下、「学生等」という。)には当該大学の教職員向けの学内規程を適用することはできず、アカデミックハラスメントにも配慮する必要があります。

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ります。大学と雇用関係にない学生等であっても、秘密情報を漏えいした場合には当該学生等はその責任を問われることとなります。特に、営業秘密を漏えいした場合には、不正競争防止法による民事・刑事措置⁴が適用されることが想定され、秘密保持契約を遵守していない場合には債務不履行によって損害賠償を求められることとなります。

また、現在、多くの大学が営業秘密情報を含む活動に学生等が参加することを認めています(下図参照)、本格的な産学共同研究やオープンイノベーションを推進していく上で、これまで以上に学生等を積極的に産学共同研究に参加させることが必要になってくると考えられます。

研究活動を行っている場合の7割程度について、営業秘密情報を含む活動への学生の参加が認められている。

Q. 貴大学においては、営業秘密情報を扱う研究活動に学生等が参加することがありますか。



ヒアリング調査での聴取事項

- 学生を参加させないケースはある。相手先企業から厳しい情報管理条件がつけられた場合は、過去、教員だけが研究対応していた。
- 学生の参加を認めるのは個別の研究代表者の判断に委ねられている。相手企業からは学生の参加に対して懸念を示してくることが少なくない。各部署からの相談では教育にも研究にもプラスとなるとの理由で参加させるのが一般的であるが、相手企業が厳しい場合は、大学と学生の間で取り交わした誓約書の提出を求められる場合もある。それ以上の要請に対しては大学もリスクを負いかねると考えている。
- 学生・大学院生は、職員等とは異なり、基本的に教育を受ける立場にあることから、原則として企業等との共同研究契約及び受託研究契約に基づく研究プロジェクトに参加させないとしている。

「大学における営業秘密管理に関する実態調査」調査結果より

そこで、本章では、学生等が積極的に産学共同研究等に参加することで、共同研究先

⁴民事上の措置としては、差止請求(法第3条)、損害賠償請求(法第4条)、信用回復措置請求(法第14条)等があり、刑事上の措置としては、営業秘密侵害罪(未遂処罰含む)(法第21条第1項各号、第3項、第4項)等があります。具体的には、10年以下の懲役又は2,000万円以下の罰金(併科可)、海外重罰(法第21条第3項、日本国外での不正使用等のケース)が適用される場合については、3,000万円以下の罰金(併科可)が課されます。また、法人処罰については、海外重罰適用のケースで、10億円以下の罰金(法第22条第1項)が課されます。

企業の秘密情報に触れる機会が増えるという想定のもと、学生等を漏えいリスクから守るため、学生等に対してどのような秘密保持の遵守等を求めることが望まれるかといった点について説明します。

本章で説明する対策については、その実施にあたり留意すべき点が多くありますが、情報資産の活用と管理のバランスを考慮しつつ、ステークホルダー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す。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ります。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と考えられます。

1. 研究活動に参加する場合

研究活動の参加に際して、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と考えられます。

～学生がした発明の帰属について～

■学生等が研究活動を行う過程で何らかの発明を行う場合があります。教職員による発明の場合、特許法第35条で定める職務発明に関する規定により、発明は大学に帰属することになりますが、一般的には、大学等と雇用関係にない学生等（大学等の学生、大学院生及びポスドクを含む。）は特許法第35条に定める「従業者等」に該当しないことから、学生等が行った発明は学生等個人に帰属すると考えられます。

■所定の研究活動（例えば、国の委託研究や企業との共同研究等。以下、同じ。）で学生等がした発明について、各大学は自大学のポリシーに従って特許権等の活用の最大化が図られるよう、一元的に管理・活用することも含めて当該発明の取扱いを検討する必要があります。したがって、各大学においては、当該発明の取扱いについて、発明が創出された後に事後的に検討するよりも、事前に（例えば、研究活動に関与する前段階で）取決めをしておくことが望ましいと考えられます。この場合、特にアカデミックハラスメントに留意する必要がありますが、所定の研究活動において学生等がした発明を大学側に承継することに関する同意を、大学が学生等に対して予め求めることは、学生等が研究テーマを自由に選択して、教育の一環として研究が適切に行える環境であること、その研究に係る特定の目的達成のために合理的な範囲での適切な

譲渡契約内容となっていること、学生等に対して発明の取扱いについて十分に説明がされていることが満たされていれば、必ずしもアカデミックハラスメントに該当するわけではないと考えられます。

■雇用関係にある学生等（所定の研究活動に参加し、大学と契約を締結して雇用関係が生じている学生等）が研究活動の中で行った発明は、職務発明として取り扱うことが可能であり、特許法第35条が適用されます。この場合、教職員の職務発明と同様に、雇用関係にある学生等との関係においても、特許法第35条第5項の要件を満たす必要があることに留意が必要です。なお、雇用関係の有無は、発明創出が期待される研究活動に対する給与支払実態により評価されます。研究活動と関係がない金銭付与（例えば、ティーチング・アシスタント等の謝金といった、発明が創出された研究活動とは特段関係がない謝金等）は、少なくとも職務発明制度上の雇用関係の根拠として認められないと解されることに留意する必要があります。

（文部科学省「大学等における職務発明等の取扱いについて」15頁より）

（1）学内研究活動（（2）に該当する研究活動を除く）へ参加する場合

- 特に理工系の学部学生や大学院生などは、卒業研究や論文作成等に際して、何らかの形で学内の研究活動に参加することが多いと考えられます。こうした研究活動に参加する過程で、特許出願前の発明に関する情報や論文・学会発表前の研究成果に関する情報、学内の研究開発上のノウハウとして秘密にされている情報などに触れる可能性があります。
- こうした場合、学生等による研究活動への参加に先立って、教職員が、当該学生等に対して秘密保持に関する誓約書の提出を求めたり、当該学生等と大学等との間で秘密保持契約を交わすことを求めたりすることがありますが、これらのケースでは、共同・受託研究等終了後一定期間の秘密保持を課している場合が多く見られます。こういった場合、学生等が扱う可能性のある情報は、ほぼ大学が保有する秘密情報に限定されることが想定され、学生等が学内で研究活動を行う限りにおいて、当該秘密情報を保持すること自体が、学生等の教育・研究活動上の支障となることはないと考えられます。しかし、例えば、学生等が他の大学に移籍した後も類似の研究活動を行おうとする場合等に、当該研究活動上の支障が生じる可能性等があります。
- 秘密保持に係る誓約書や契約書の雛形については、例えば次の大学がホームページ上で公開しています。
 - 国立大学法人東京医科歯科大学（ <http://www.tmd.ac.jp/tlo/forms/> ）
 - 国立大学法人東京大学（ http://www.ducr.u-tokyo.ac.jp/jp/rules_and_forms/ ）

(2) 学外機関等が関与する共同研究等へ参加する場合

- 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、(1)と異なり、外部機関が保有し、共同研究や受託研究に用いる目的で大学に提供されている秘密情報等に学生等が触れる可能性があります。

- こうした場合、学生等の共同研究等への参加に先立って、(1)のケース同様に、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、共同研究契約における秘密保持条項の遵守が求められること等が考えられます。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ります。

以下に、上記(1)、(2)で示した研究に学生等を参加させる場合に検討すべき事項について説明します。

① 研究活動への学生等の参加の是非の検討

- 前述のように、学生等が秘密情報を扱う場合、学生等に対して秘密保持義務を課すことが考えられますが、この実施にあたっては、教育を受けるために在学している学生等の基本的な立場と、秘密保持義務により学生等が学会発表や就職活動の制限等の不利益を被るおそれがあることに十分な配慮が必要です。秘密保持をはじめとして、学生等に対して過度に広汎な義務を課すような場合は公序良俗違反(民法第90条)として無効となる余地も考えられます。

- こうした状況を踏まえ、学生等の所属する部局の教職員は、こうした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ります。特に、外部機関と共同研究等を行う場合には、産学連携の意義等を十分に説明するとともに、学生等、企業の双方が許容出来るような内容の守秘義務を検討することが重要です。

② 学生等に秘密保持の遵守等を求める方法の検討

上記①の結果をもとに学生等に研究への参加を認めることとした場合、以下に示す(イ)及び(ロ)によって当該学生等に秘密保持の遵守等を求めることが考えられます。

(イ) 学生等を対象とした通則等での指示

- ある学部、学科、研究科等の組織に所属する全ての学生等に対し、当該組織を対

象とした通則等において、研究への参加にあたり秘密保持の遵守等が必要となる旨示しておきます。

- 通則等で指示しただけでは学生等は義務を課せられた自覚に乏しくなるおそれがあるため、指導教員等が研究への参加を希望する学生等に対する当該通則等の遵守（秘密保持の遵守等）に係る指導を徹底するとともに、ルールの周知徹底、教育のためのガイダンスや研修等を行うことで実効性を高めることが有効だと考えられます。

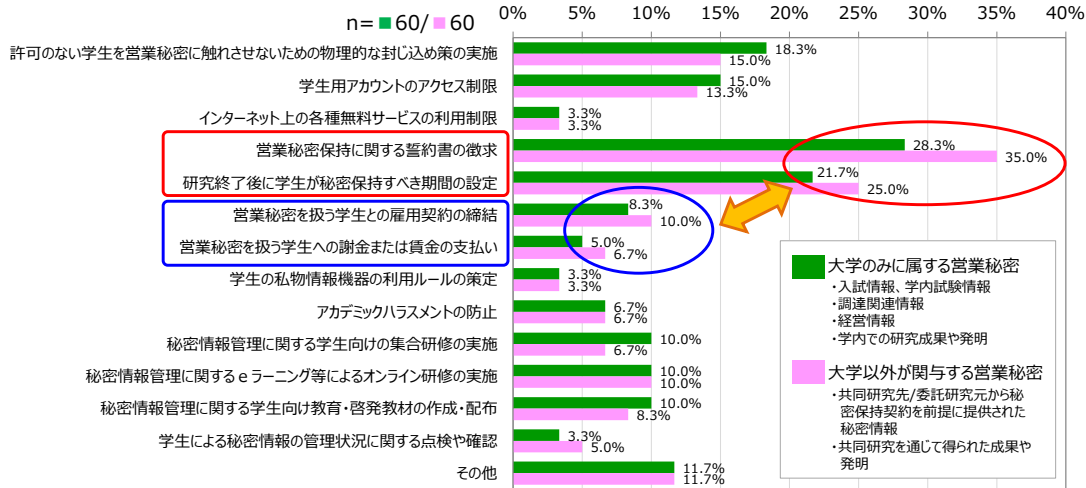
(ロ) 誓約書の提出を求める

- 研究やインターンシップ等に参加を希望する学生等に対し、秘密保持に関する誓約書の提出を求めます。
- 雇用関係にない学生等に対して誓約書の提出を求める際に、強要と受け取られるような形で手続きを求めることは適切とはいえず、あくまで学生等の自由意思に基づいて提出してもらうべきものになります。
- なお、誓約書の代わりに、大学と学生等との間で秘密保持契約（NDA）を締結する場合があります。
- 誓約書の提出を求めるにあたって、研究に参加する学生等を大学が雇用して（リサーチアシスタント（RA）等）賃金を支払い、雇用契約を締結する場合がありますが、その際には、併せて、教職員同様、秘密保持の遵守等を取り決めることが必要となります。
- 学生等が誓約書の提出を拒否した場合、大学は、そうした拒否が学生等にとっての不利益とならないよう、他の研究テーマを与えるなどの対応を通じて、誓約書を提出した学生等との間で教育上の格差が生じないように配慮することが求められます。

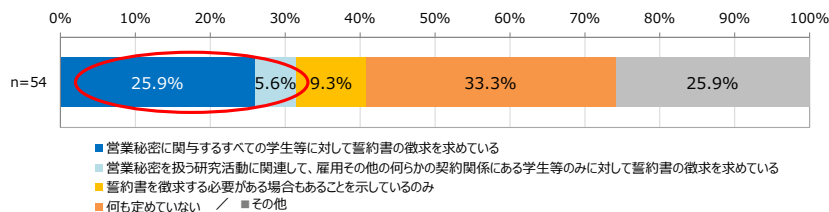
(参考)

「営業秘密保持に関する誓約書の徴求」や「研究終了後に学生が秘密保持すべき期間の設定」をルールとして定めている大学は比較的多いが、「営業秘密を扱う学生との雇用契約の締結」や「営業秘密を扱う学生への謝金または賃金の支払い」をルールとして定めている大学は少ない。

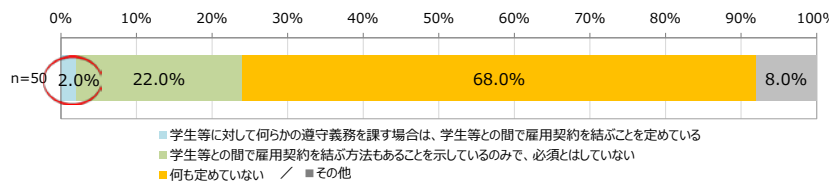
Q. 営業秘密情報を扱う研究活動に参加する学生が秘密情報を取り扱う際のルールにおいて規定されている内容として、あてはまるものすべてを選んでください。



Q. 営業秘密情報を扱う研究活動に参加する学生を対象とした誓約書の扱いについて、どのように定めていますか。



Q. 営業秘密情報を扱う研究活動に参加する学生を対象とした雇用契約の扱いについて、どのように定めていますか。



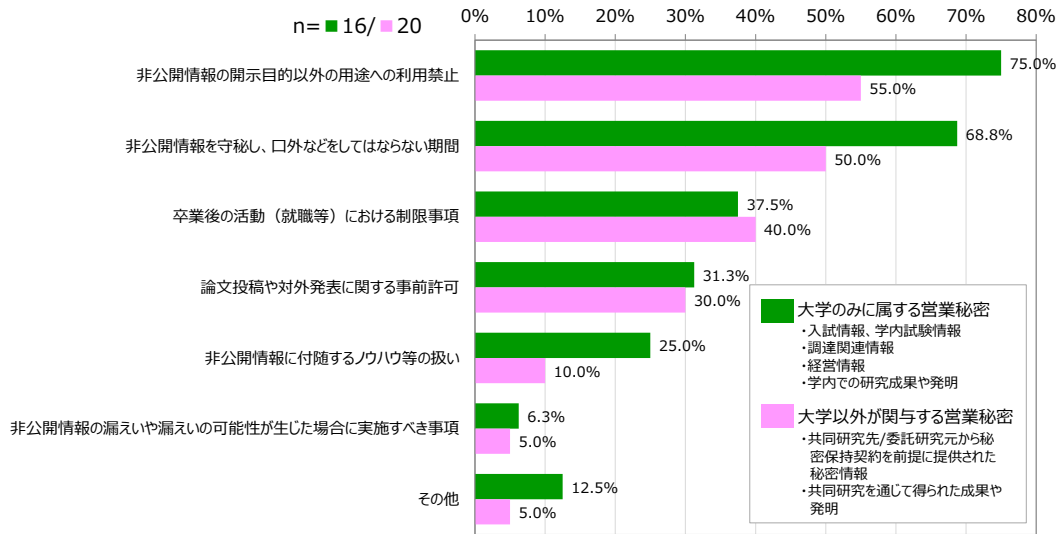
ヒアリング調査での聴取事項

- 通常学生は、大学の職員ではないため、発明があっても大学には届けない。そのため、共同研究に当たっては大学が学生をアルバイトとして雇い、期間中は職員になってもらう。大学の就業規則に基づき、誓約書を書いてもらっている。
- 学生の活動については、雇用契約がない場合は、何もしないとコントロールできなくなってしまう。学生に対しては、強制ではなくお願いベースで趣旨を理解してもらった上で誓約書に署名してもらっている。誓約書は教員を通じて学生に依頼している。
- 学生が共同研究等に関する誓約書を用意し、発明が生じた際に、研究代表者が学生に対して誓約書の意味を説明したうえで、任意の提出を求めている。
- 誓約書の根拠となる規程はなく、学生が自主的に提出していることになる。

「大学における営業秘密管理に関する実態調査」調査結果より

各大学が誓約書に盛り込んでいる内容としては、目的外利用禁止と守秘期間が多い。

Q. 営業秘密情報を扱う研究活動に参加する学生に対して、貴機関が徴求する誓約書に盛り込むことを定めている内容について、あてはまるものすべてを選んでください。



「大学における営業秘密管理に関する実態調査」調査結果より

2. インターンシップへ参加する場合

- 学生等が学外機関でインターンシップに参加し、当該機関内で研究活動に従事する場合等に、企業から秘密情報を開示されたり、学生等が開発した新技術が当該企業の秘密情報となるケースなど、インターンシップ先企業が保有する秘密情報に接する可能性があります。
- こういった場合に、学生等が無用のトラブルに巻き込まれることを防ぐために、大学においても、何が秘密情報に該当するか、どのような点に注意して取り扱うべきかなどをインターンシップ先企業に予め確認するよう学生等に指導しておくことが望まれます。また、学生等が個人としてインターンシップに参加する場合のほか、大学が組織としてインターンシップに関与する場合には、必要に応じ、大学とインターンシップ先企業との間で、学生等が関与するであろう秘密情報の対象や取扱いについて事前に十分協議した上で、企業又は大学から学生等に対してその内容を周知しておくことが望ましいと考えられます。
- 学生等がインターンシップ先企業の秘密情報を侵害してしまった場合には、学生等個人が民事上・刑事上の責任を問われる可能性があることはもちろん、当該学生等の所属大学についても、契約違反や学生等の監督等に係る責任を問われる可能性がある点に注意が必要です。