

外国企業との連携に係る関連ガイドライン等について（参考）

令和3年6月25日

内閣サイバーセキュリティセンター（NISC）
基本戦略第1グループ

産学官連携による共同研究強化のためのガイドライン

【追補版】

産学官連携を通じた価値創造に向けて

令和2年6月30日

文部科学省

経済産業省

4 知的財産権の積極的活用を前提とした契約

現状と課題

- 特許の出願形態について、日本では単独出願が共同出願より少なく¹、大学の特許がほとんど単独出願である米国とは大きく状況が異なる。
- 共同出願の場合、その活用は共有先の企業にほぼ限られるため、例えば当該企業が防衛的に当該特許を保有していたり、社内の方針によって活用の道が閉ざされたりといったケースにおいては、結果として大学の「知」の一部が新たな価値の創出に貢献できなくなる可能性もある。このような状況を踏まえ、企業との共同出願の特許について、当該企業へ有償譲渡を行う取組もみられる²。
- 研究成果の製品・サービス化や社会実装を行うフェーズで知的財産権を活用する場面においては、その保有関係は、よりシンプルであること、すなわち、保有主体が分散されていない状態であることが望ましい。

（安全保障上の要請）

- また、外国企業との共同研究等の連携活動については、令和元年6月に、①連携の基本的な考え方、②安全保障貿易管理等の遵守すべき法令、③リスクマネジメントの方策、④実務的な留意事項及び手順、⑤国内外の大学・公的研究機関の具体的な取組事例がガイドラインとしてとりまとめられた³。
- 近年の機微技術の窃取等による安全保障上の懸念の広がりが⁴を踏まえると、大学等においても安全保障貿易輸出管理の厳格な運用が求められるところである。外国企業との連携に当たっては、常に知的財産権やその他の非公開性の情報の提供が前提となる契約の形態次第で、大学等における輸出管理体制への負荷とリスクを増大させる結果となりがねないことを考慮すべきである。

¹ 文部科学省「平成30年度大学等における産学連携等実施状況について」

² 「大学における産学連携活動マネジメントの手引き」〈平成28年3月 経済産業省 産業界連携推進 大学連携推進室〉

³ 「大学・国立研究開発法人の外国企業との連携に係るガイドライン—選正なアプローチに基づく連携の促進—（中間とりまとめ）」〈令和元年6月 内閣府政策経路部（科学技術・イノベーション担当）〉

⁴ 「産学連携推進会議 通商・貿易分科会 安全保障貿易管理小委員会 中間報告」〈令和元年10月8日 経済産業省〉

大学・国立研究開発法人の 外国企業との連携に係るガイドライン

－適正なアプローチに基づく連携の促進－

（中間とりまとめ）

令和元年10月
内閣府 政策統括官
（科学技術・イノベーション担当）



ガイドラインの概要

I. 基本的な考え方

- ▶ グローバルな競争を勝ち抜くためには、**国内外を問わず**一流の企業・研究機関との連携強化が不可欠
- ▶ 一方、「意図せざる技術流出」を防ぐため、関係**法令遵守**、**リスクマネジメント**は高いレベルが必要
- ▶ 各機関の**活動目的に則した**外国企業との連携方針や、連携を開拓、維持、発展させる**組織的な仕組みづくり**が必要（情報発信強化、連携相手の探索機能強化、専門人材）
- ▶ **win-win**の関係を目指した連携の構築

①適正なアプローチ ②外国企業との連携促進 ③連携機能強化

II. 法令・規則等

- ▶ 外国企業との連携において**遵守すべき法令・規則等**
 - ・ 安全保障貿易管理
 - ・ 不正競争防止法（営業秘密の保護）
 - ・ その他の法令・規則

III. リスクマネジメント

- ▶ 法令遵守に加えた**リスクマネジメント体制の構築**
 - ・ 産学官連携活動の推進に伴うリスクマネジメント
 - ・ 機微技術管理の国際動向

IV. 実務的な留意事項

- ▶ **戦略・体制整備とプロセスの管理**
 - ・ 連携戦略・体制の整備
 - ・ 連携プロセスの管理
 - ・ モニタリング・フォローアップ

V. 外国企業との連携の具体的な取組事例

- ▶ **好事例の横展開**を通じた積極的な取組の促進
 - ・ 外国企業との積極的に進めている国内の大学・国研等の取組事例
 - ・ 海外の大学・研究機関の取組事例

基本的な考え方

適正なアプローチに基づく連携の促進

- ・ 国内外を問わず一流の企業・研究開発機関との連携強化が不可欠
- ・ 海外企業との連携による資金獲得を通じた研究力向上

- ・ 「意図せざる技術流出」を防ぐ関係法令遵守
- ・ リスクマネジメントの体制整備

適正なアプローチに基づく 外国企業との連携促進

- ・ 各機関の活動目的に則した外国企業との連携戦略の策定
- ・ 連携プロジェクトを発展させる組織的な仕組みづくり
- ・ 外国企業とのwin-winの関係を旨とした連携の構築

以下のような効果も期待

- ・ 大学と外国企業との連携から、日本企業の優れた技術の展開など、産業振興への貢献
- ・ 日本の技術の展開など産業を通じた世界への価値提供

法令・規則等

- 1 安全保障貿易管理
- 2 不正競争防止法（営業秘密の保護）
- 3 その他の法令・規則

（日本版バイ・ドール規定における知的財産の扱い／委託費・補助金のルール／他国の特許法令等）

【要点】

- ・ 安全保障貿易管理は、産学官連携で実施される技術の提供も管理対象となる。各機関の規模に則した管理体制の構築、経営層や研究者の理解と協力が不可欠。
- ・ 営業秘密の管理は人材流動性、悪意のある接触、法令の違い、持ち出し発覚後拡散防止が困難等に特に留意。
- ・ 産業技術力強化法の日本版バイ・ドール規定で、政府資金の研究開発から派生した知的財産権を第三者に技術移転する場合は、国等の承認が必要。国の委託費や補助金に関連する研究においては、交付要綱等においてルールを規定。

サイバーセキュリティ関係法令 Q&A
 ハンドブック
 Ver1.0

令和2年3月2日

内閣官房内閣サイバーセキュリティセンター (NISC)

Q48 サイバーセキュリティと輸出管理

サイバーセキュリティに関する物の輸出や技術提供を行う場合において、輸出管理に関する法令上、どのような点に留意すべきか。

タグ：外為法、輸出貿易管理令、外国為替令、貨物等省令、貿易外省令、役務通達、輸出管理、ワッセナー・アレンジメント、侵入プログラム関連品目

1. 概要

輸出管理制度においては、規制リストに掲載されている貨物の輸出及び技術の提供を行う際には、原則として経済産業大臣の許可が必要となる。規制対象となる行為の範囲は広く、電子メールでデータを送付することも対象行為となり得る。

サイバーセキュリティに関しては、サイバー攻撃に転用されるおそれがあるものについて、国際的な枠組み（輸出管理レジーム）の一つであるワッセナー・アレンジメントで検討され、侵入プログラム関連品目等が規制対象とされている。

侵入プログラム関連品目の中には、それに関わる脆弱性情報や、マルウェアに関する情報が含まれるが、セキュリティの脆弱性の開示に係るもの又はサイバー攻撃の対応に係るものは規制対象から除かれることが多く、サイバーセキュリティの実務への影響が低くなるよう配慮されている。

2. 解説

(1) 輸出管理制度

安全保障上リスクのある貨物や技術が、我が国及び国際的な平和及び安全の維持を脅かす国家やテロリスト等に渡り、大量破壊兵器等や通常兵器の開発等に転用されることを未然に防ぐため、国際的な枠組み（輸出管理レジーム）により輸出管理が推進されている。

我が国においては、外国為替及び外国貿易法（以下「外為法」という。）によって、輸出管理（貨物の輸出及び技術の提供の管理）を行っており、具体的には、規制対象となる貨物の輸出（外為法第48条第1項及び輸出貿易管理令）や技術の提供（外為法第25条第1項、第3項及び外国為替令）について経済産業大臣の事前の許可が必要である。

ア 規制対象について

外為法に基づく規制対象については、政省令で定める品目（武器、機微な汎用品など）に該当する貨物の輸出又は技術の提供を規制する「リスト規制」と、「リスト規制」に該当しない貨物又は技術であっても、その用途や需要者に兵器の開発等に関する懸念がある場合などに貨物の輸出又は技術の提供を規制する「キャッチオール規制」がある。

輸出令第8項		貨物等省令第7条		解釈		(参考)関係するECCN番号
項番	項目	項番	項目	用語	用語の意味	
輸出令第8項	電子計算機若しくはその附属装置又はこれらの部分品(4の項の中欄に掲げるものを除く。)であつて、経済産業省令で定める仕様のもの	貨物等省令第7条第五号	電子計算機若しくはその附属装置又はこれらの部分品であつて、侵入プログラムの作成、指揮統制又は配信を行うように特に設計又は改造されたもの	侵入プログラム	<p>電子計算機又は電気通信回線に接続する機能を有する機器の監視ツールによる検出を回避し、又は防御手段を無効化するように設計又は改造されたプログラムであつて、次のいずれかの操作を実行するものをいう。</p> <p>イ 電子計算機又は電気通信回線に接続する機能を有する機器からデータ又は情報の抽出を行うこと、若しくはシステムや利用者のデータを変更すること</p> <p>ロ 外部からの命令の実行を可能とするために、プログラム又はプロセスの標準的な実行パスを改造すること</p> <p>注1：電気通信回線に接続する機能を有する機器には、モバイル機器、スマートメータを含む。</p> <p>注2：監視ツールとは、装置のシステム動作又はプロセスを監視するプログラム又は装置をいう。これには、アンチウイルス(AV)製品、エンドポイントセキュリティ製品、パーソナルセキュリティ製品(PSP)、侵入検知システム(IDS)、侵入防止システム(IPS)又はファイヤーウォールを含む。</p> <p>注3：防御手段とは、データ実行防止(DEP)、アドレス空間配置のランダム化(ASLR)、サンドボックス等のコード実行の安全性を保障するために設計された技術をいう。</p>	
				部分品	他の用途に用いることができるものを除く。	
				貨物等省令第7条に掲げる貨物	次のいずれかに該当するものを除く。	イ 医療用に設計された装置 ロ 医療用に設計された装置に組み込まれたもの

外為令第8項		貨物等省令第20条		解説		プログラム	プログラムを 除く技術	
項番	項目	項番	項目	用語	用語の意味			
外為令 第8項 (2)	電子計算機若しくはその附属装置又はこれらの部分品の設計、製造又は使用に係る技術であつて、経済産業省令で定めるもの((1)及び4の項の中欄に掲げるものを除く。)	貨物等省令 第20条 2項 第六号	侵入プログラムの作成、指揮統制又は配信を行うように設計若しくは改造されたプログラム(プログラムの更新又は改良を行うために特に設計したものであって、これを受け取るシステムの所有者又は管理者の許可を得た場合にのみ動作するものうち、更新又は改良されるプログラムを本号に該当するプログラム又は侵入プログラムに変更しないように設計したものを除く。)又はそのプログラムの設計、製造若しくは使用に必要な技術(プログラムを除く。)	侵入プログラム	<p>電子計算機又は電気通信回線に接続する機能を有する機器の監視ツールによる検出を回避し、又は防御手段を無効化するように設計又は改造されたプログラムであつて、次のいずれかの操作を実行するものをいう。</p> <p>イ 電子計算機又は電気通信回線に接続する機能を有する機器からデータ又は情報の抽出を行うこと、若しくはシステムや利用者のデータを変更すること</p> <p>ロ 外部からの命令の実行を可能とするために、プログラム又はプロセスの標準的な実行パスを改造すること</p> <p>注1: 電気通信回線に接続する機能を有する機器には、モバイル機器、スマートメータを含む。</p> <p>注2: 監視ツールとは、装置のシステム動作又はプロセスを監視するプログラム又は装置をいう。これには、アンチウイルス(AV)製品、エンドポイントセキュリティ製品、パーソナルセキュリティ製品(PS P)、侵入検知システム(IDS)、侵入防止システム(IPS)又はファイヤーウォールを含む。</p> <p>注3: 防御手段とは、データ実行防止(DEP)、アドレス空間配置のランダム化(ASLR)、サンドボックス等のコード実行の安全性を保證するために設計された技術をいう。</p>	○	○	
			貨物等省令第20条2項第七号	侵入プログラムの設計に必要な技術(プログラムを除く。)	貨物等省令第20条第2項第六号中のプログラム及び技術並びに同項第七号中の技術	<p>ハイパーバイザー、デバッガー、ソフトウェアリバースエンジニアリング(SRE)ツール、デジタル著作権管理(DRM)システムのプログラム、資産の追跡又は回復のために製造者、管理者又は利用者によってインストールされるように設計されたプログラムを除く。</p>	—	○
			貨物等省令第20条に掲げる技術		貨物等省令第20条に掲げる技術	医療用に設計された装置に組み込まれたプログラムを除く。		

輸出令第9項		貨物等省令第8条		解釈		(参考)関係するECCN番号	
項番	項目	項番	項目	用語	用語の意味		
輸出令第9項(5の5)	インターネットを利用する方法による通信の内容を監視するための装置又はその部分品	貨物等省令第8条第五号の五	インターネットを利用する方法による通信の内容を監視するための装置又はその部分品であって、次のイ及びロに該当するもの(マーケティング活動、ネットワークのサービス品質管理又は利用者の体感品質管理のために設計された装置を除く。)	貨物等省令第8条第五号の五中のキャリアクラス	国家級の大容量通信回線網を含む。		
			イ キャリアクラスのIPネットワーク上で次の(一)から(三)までの全ての機能を実現するもの	貨物等省令第8条第五号の五中のアプリケーション層	OSI参照モデル(ISO/IEC7498)のレイヤー7を含む。		
				貨物等省令第8条第五号の五中のメタデータ及びアプリケーション	音声、映像、伝達内容、付加情報を含む。		
				ハードセレクター	個人に関連する単独又は一連の情報をいう。		
			* 対応する貨物等省令は、第8条第1項第一号及び第五号の五	ロ 次の(一)及び(二)を実行するために設計したもの	(一) ハードセレクターに基づく検索		姓名、電子メールアドレス、住所、電話番号、所属団体等の情報を含む。
				(二) 特定の個人又は集団の関係の解析			

安全保障貿易管理

輸出令及び貨物等省令のマトリクス（貨物マトリクス）

暗号装置又はその部分品

輸出令第9項		貨物等省令第8条		解釈		(参考)関係するECCN番号
項番	項目	項番	項目	用語	用語の意味	
輸出令第9項(7)	暗号装置又はその部分品	貨物等省令第8条第9号	暗号装置又は暗号機能を実現するための部分品であって、次のイからホまでのいずれかに該当するもの(第3条第十九号ハ(二)2.本号へ、第十一号までの規定中の装置若しくはシステム又はその部分品を除く。)	貨物等省令第8条第9号から第十一号までの規定中の装置若しくはシステム又はその部分品	他の貨物の部分品である場合においても、貨物等省令第8条第九号から第十一号までのいずれかに基づいて判定するものとする。	5A002a
			イ 対称アルゴリズムを用いたものであって対称鍵の長さが五ビットを超えるもの又は非対称アルゴリズム(アルゴリズムの安全性が次の(一)から(六)までのいずれかに該当する困難性に基づくものに限る。以下この号において同じ。)を用いたものであって、データの機密性確保のための暗号機能を有するように設計し、又は改変したものの(当該暗号機能を使用することができるもの(当該暗号機能が有効化されているものを含む。))又は安全な仕組みの暗号機能有効化手段以外の手段で暗号機能を有効化できるものに限る。)のうち、次の(七)から(十)までのいずれかに該当するもの(十一)から(二十)までに該当するものを除く。		貨物等省令第21条第1項第九号及び同項第九号の二に該当するプログラムのみによる第8条第九号から第十一号までのいずれかに該当する貨物の有する機能と同等の機能を実現するものを除く。	
			(一) 五〜二ビットを超える整数の素因数分解	暗号機能有効化の手段	製造者により提供される仕組み(装置若しくはプログラムと一対一で対応するもの又は一人の顧客が有する複数の同種の装置若しくはプログラムのために顧客と一対一で対応するものを含む。))によって、使用者が暗号機能を特別に有効化し、又は使用可能にするあらゆる手段であって、貨物又は技術によって実現されるものをいう(例えば、シリアルナンバーを基にしたライセンスキー又はデジタル署名の証明書等の認証をするものをい	
			(二) 有限体上の乗法群における五〜二ビットを超える離散対数の計算			
			(三) (二)に規定するもの以外の群における一〜二ビットを超える離散対数の計算			
			(四) 格子に関連する最短ベクトル又は最近接ベクトル問題			
			(五) 超特異楕円曲線の同種写像の探索			
			(六) ランダムな符号の復号			
			(七) 情報システムのセキュリティ管理機能を主たる機能として有するもの	対称アルゴリズム	暗号化と復号の両方に同一の鍵を使用する暗号アルゴリズムをいう。	
			(八) デジタル通信装置、有線若しくは無線回線網による電気通信回線を構築、管理若しくは運用するための装置又はこれらの部分品(七)に該当するものを除く。	対称鍵の長さが五ビットを超えるもの	奇偶検査のための付加されるパリティビットは含まない。	
			(九) 電子計算機若しくは情報の記録及び保存若しくは処理を主たる機能として有するもの又はこれらの部分品(七)又は(八)に該当するものを除く。	非対称アルゴリズム	暗号化と復号に数学的に関連性を有する別々の鍵を使用する暗号アルゴリズムをいう。	
			(十) 次の1及び2に該当するもの(七)から(九)までに該当するものを除く。	512ビットを超える整数の素因数分解	RSA方式を含む。	
			1 当該貨物の有する暗号機能が当該貨物の主たる機能以外の機能を支援するために用いられているもの	有限体上の乗法群における512ビットを超える離散対数の計算	有限体上のDiffie-Hellman方式を含む。	
			2 当該貨物の有する暗号機能が当該貨物に組み込まれたもの(この号から第十二号までのいずれかに該当するものに限る。))又は第21条第1項第七号、第九号の二、第八号の二、第八号の三、第九号、第九号の二若しくは第十七号のいずれかに該当するプログラム(公開されているものを除く。))によって実現されているもの	第八号第九号イ(三)中の(二)に規定するもの以外の群における112ビットを超える離散対数の計算	楕円曲線上のDiffie-Hellman方式を含む。	
			(十一) 暗号機能を有するスマートカード若しくはそのリーダーであって、次のいずれかに該当するもの又はこれらの部分品	楕円に関連する最短ベクトル又は最近接ベクトル問題	ポスト量子、量子安全、耐量子といる。	
			1 スマートカードであって、次のいずれかに該当するもの		NewHope、Frodo、NTRUEncrypt、Kyber、Titanium方式を含む。	
			一 次のいずれかに該当するものに限定されて使用するものであって、他の用途のためにプログラムの書き換えを行うことができないもの		ポスト量子、量子安全、耐量子といる。	
			イ (七)から(十)までのいずれにも該当しないもの		McEliece、Niederreiter方式を含む。	

輸出令第9項		貨物等省令第8条		解釈		(参考)関係するECCN番号
項番	項目	項番	項目	用語	用語の意味	
(続き)輸出令第9項(7)	(続き)暗号装置又はその部分品	(続き)貨物等省令第8条第9号	対称アルゴリズムを用いたものであって対称鍵の長さが五ビットを超えるもの又は非対称アルゴリズムを用いたものであって、データの機密性確保のための暗号機能を有するように設計したものの以外のもの	データの機密性確保のための暗号機能	デジタル方式の暗号処理(情報の内容の秘匿又は情報の不正な改ざん若しくは不正な利用の防止を目的として情報の変換(秘匿パラメータを用いた情報の変換に限る。))を行う処理をいう。固定式(符号化又はデータ圧縮のアルゴリズムが外部からのパラメータを受け入れず、かつ、使用者によって変更できないもの)の符号化及びデータ圧縮を除く。))を行うものうち、次のイからホまでのいずれか以外の暗号機能を含む。	
			ハ (十二)から(十六)までに該当するもの		二 個人情報(生存する個人に関する情報であって、当該情報に含まれる氏名、生年月日その他の記述等により特定個人を識別することができるもの(他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるもの(認証及び金銭債権に係るものその他これらに類するものを含む。))を含む。))をいう。(十一)において同じ。))又は団体情報(法人その他の団体の情報であって、認証及び金銭債権に係るものその他これらに類するものを含む。))をいう。(十一)において同じ。))に係る情報が記録され、又は記録されるように設計したものであって、次のイからハまでの全てに該当するもの	
			イ 暗号機能を専ら当該スマートカードに記録された個人情報又は団体情報の保護のためにのみ使用するもの		イ 認証(使用者、プロセス又は機器の妥当性を確認すること(例えば、情報システムのリソースへのアクセスを許可するために妥当性を確認すること)をいう(メッセージその他情報の発信元又は内容の妥当性を確認すること及びパスワード、個人識別番号、データ又は類似のデータの保護に直接関連しないファイリング若しくはテキストの暗号化機能以外の全てのアクセス制御機能を含む。))	
			ロ 専ら公共施設若しくは商業施設において使用し、又は当該スマートカードに記録された個人情報又は団体情報に係る情報の認証のために使用するもの		ロ デジタル署名 ニ 否認防止 ホ デジタル著作権管理(複製することを禁止されたプログラムの実行を含む。))	
			ハ 当該スマートカードを使用する者が当該スマートカードの有する暗号機能を変更することができないもの		ハ 娯楽施設若しくは装置の有する機能であるもの、商業放送又は医療用の記録管理のために行われる暗号化又は復号	
			2 リーダライタであって、専ら1に該当するスマートカードに記録された個人情報若しくは団体情報に係る情報を読み取り、又は当該スマートカードに個人情報若しくは団体情報に係る情報を記録するように設計し、又は改変したものの(電気通信回線を通じて読み取り、又は記録するものを含む。))		二 トイからハまでのいずれかに該当する機能を支援するための鍵管理機能	
			(十二) 暗号装置であって、銀行業務若しくは決済(料金の徴収及び精算又は割賦販売(昭和36年法律第159号)第2条第3項に規定する包括的購入あつせん)に係る業務を含む。))に使用するように設計したものの又はその部分品	暗号機能有効化の手段を用いないで使用者による暗号機能の使用が可能であるものをいう。		
			(十三) 民生用の携帯用電話機端末(携帯回線網用の電話その他の無線回線網用の電話をいう。(十五)において同じ。))若しくは移動用電話機端末(専ら自動車その他の移動体において使用するように設計したものをいう。(十五)において同じ。))であって、次の1及び2に該当するもの又はこれらの部分品	情報システムセキュリティ管理機能	情報又は通信のアクセシビリティ、機密性及び完全性を保証するための全ての手段及び機能(誤作動を防ぐための手段及び機能を除く。))をいう。暗号処理(情報の内容の秘匿又は情報の不正な改ざん若しくは不正な利用の防止を目的として情報の変換(秘匿パラメータを用いた情報の変換に限る。))を行う処理をいう。固定式(符号化又はデータ圧縮のアルゴリズムが外部からのパラメータを受け入れず、かつ、使用者によって変更できないもの)の符号化及びデータ圧縮を除く。))。暗号機能有効化の手段、暗号解析(秘密の数値又は明文を含む機密データを抽出するために暗号システム又はその入出力を解析するものをいう。ISO 7498-2-1988(E)、paragraph 3.1.8を含む。))、情報の漏れ防止、コンピュータの安全性を確保するための手段及び機能を含む。	
			1 他の電話機端末その他の装置(無線アクセスネットワーク装置を除く。))に符号化されたデータを直接送信することができないもの			
			2 無線ネットワーク制御装置、基地局制御装置その他の無線アクセスネットワーク装置を經由して暗号化されたデータを伝送することができないもの			
			(十四) コードレス電話機端末間で暗号化機能を用いないコードレス電話装置であって、コードレス電話機端末と家庭内基地局の間無線中継器がない場合の一無線区間で電波到達距離長が距離が400メートル未満のもの又はその部分品			

安全保障貿易管理 輸出令及び貨物等省令のマトリクス (貨物マトリクス)

暗号装置又はその部分品

輸出令第9項	輸出令第9項	貨物等省令第8条	用語	用語の意味	(参考)関係するECCN番号
(続き) 輸出令第9項(7)	(続き) 暗号装置又はその部分品	(続き) 貨物等省令第8条第九号	(十五) 民生用の携帯用電話機端末若しくは移動用電話機端末又は同等の無線機端末であつて、公開された又は商業用の暗号標準(無断の複製を防止するためのものであつて、公開されていないものを)を用いたもののうち、暗号機能が使用者によって変更できず、使用に際して供給者が販売店の技術支援が不要であるように設計したもので、かつ、特定の民生産業用途に用いるために設計を変更したものの(暗号機能を変更していないものに限る。)又はこれらの部分品	スマートカード スマートカードの形状は問わない。 製造者がカタログ等において、電波の到達距離が400メートル未満のもの パーソナルエリアネットワーク 任意の独立したデジタル情報送受信装置が、互いに直接通信することができ、かつ、個人又はパーソナルエリアネットワークが物理的に近接する範囲(一部屋、自動車及びそれらの周辺など)の通信に制限されたデータ通信システムをいう。また、ローカルエリアネットワークは、パーソナルエリアネットワークの範囲を地理的に超えるものをいう。	(参考)関係するECCN番号
		(十六) 無線パーソナルエリアネットワークに用いられる装置であつて、公開された若しくは商業用の暗号標準のみを用いたもの又はその部分品	暗号機能を使用して通信を行うことができる範囲が30メートルを超えない範囲に限定されているもの	製造者がカタログ等において、暗号機能に係る通信距離が30メートルを超えないものとしているものをいう。	
		(十七) 民生用に設計した移動体通信用の無線アクセスネットワーク装置であつて、暗号機能が使用者によって変更できず、使用に際して供給者又は販売店の技術支援が不要であるように設計したもののうち、無線周波数の出力が、1ワット(20デシベルエムエム)以下であつて、同時に接続できるデバイスが16以下のもの又はその部分品	暗号機能を使用して通信を行うことができる範囲が4.0メートルを超えない範囲に限定されているもの	製造者がカタログ等において、暗号機能に係る通信距離が4.0メートルを超えないものとしているものをいう。	
		(十八) ルーター、スイッチ、ゲートウェイ若しくはリレーであつて、情報システムのセキュリティ管理機能が装置の操作、管理若しくは保守に関するものに限定されており、かつ、公開された若しくは商業用の暗号標準のみを用いたもの又はこれらの部分品	貨物等省令第8条第九号イ(十八)、(十九)エ、(二十)中の操作、管理又は保守	次のイからハまでのいずれか一つ以上に該当する作業を行い、二若しくはホのいずれかに該当する作業又はこれらに関連する該管理機能は含まない。 イ 次のいずれかの確立又は管理 (一) 使用者又は管理者のアカウント又は権限 (二) ある貨物又はあるプログラムの設定 (三) (一)又は(二)を支援するための認証データ ロ ある貨物若しくはあるプログラムの稼働状態又は性能の監視又は管理 ハイ又はロを支援するためのログ又は検査データの管理 ニ イ(一)又は(二)を支援するための認証データの確立又は管理に直接関係しない暗号機能の提供又は機能向上 ホ ある貨物又はあるプログラムのオフラインプレージングやデータブレーンにおいて暗号機能を実現せるもの	
		(十九) 汎用目的の計算機能を有する装置若しくはサーバーであつて、情報システムのセキュリティ管理機能が次の1及び2に該当するもの又はこれらの部分品 1 公開された又は商業用の暗号標準のみを用いたもの 2 次のいずれかに該当するもの 一 ヘに該当する中央演算処理装置において実現されているもの 二 オペレーティングシステム(第21条第1項第七号、第七号の二、第八号の二、第九号、第九号の二又は第十七号のいずれかに該当するものを除く。)において実現されているもの 三 装置の操作、管理又は保守に限定されているもの	汎用目的の計算機能を有する装置若しくはサーバー	特定の機能を有するように専用設計された計算機能を有する装置又はサーバーを除く。	
		(二十) ネットワークに接続する民生産業用途のために設計したものであつて、次の1及び2に該当するもの又はこれらの部分品 1 次のいずれかに該当するもの 一 ネットワークに接続可能な端末であつて、次のいずれかに該当するもの イ 情報システムのセキュリティ管理機能が、任意でないデータの秘匿又は操作、管理若しくは保守に限定されているもの ロ ネットワークに接続する特定の民生産業用途に限定されているもの 二 ネットワーク装置であつて、次のイ及びロに該当するもの イ 一に該当する端末と通信するために設計し、ロに該当する端末のネットワークに接続する民生産業用途の支援に限定されているもの、又は当該ネットワーク装置若しくは本号イ(二十)に該当する他の貨物の操作、管理若しくは保守に限定されているもの 2 情報システムのセキュリティ管理機能が、公開された又は商業用の暗号標準のみを用いたものであつて、当該貨物の有する暗号機能当該貨物を使用する者によって変更できないもの	ネットワークに接続する民生産業用途	情報システムのセキュリティ管理、デジタル通信、汎用的なネットワーク又は汎用的な計算をするに於ける以外の用途であつて、ネットワークに接続する消費者用途又は民生産業用途をいう。	
			任意でないデータ	システムの安定性、性能又は物理的測定に直接的に関連するセンサーのデータ又は計測したデータ(温度、圧力、流速、質量、体積、電圧、物理的位置など)であつて、当該貨物を使用するものによって変更できないものをいう。	

輸出令第9項	輸出令第9項	貨物等省令第8条	用語	用語の意味	(参考)関係するECCN番号	
(続き) 輸出令第9項(7)	(続き) 暗号装置又はその部分品	(続き) 貨物等省令第8条第九号	ロ 暗号機能有効化の手段を用いることによつてのみ、ある貨物又はあるプログラムの暗号機能有効化するものであつて、次のいずれかに該当するもの (一) ある貨物(本号から第十二号までに該当しないものに限る。)を本号に該当するもの(本号に該当しないものに限る。)に交換し、又はあるプログラム(第二十一条第一項第七号、第七号の二、第八号の二、第九号、第九号の二又は第十七号に該当しないものに限る。)を第二十一条第一項第九号(第八号第九号又はハからホまでに係るものに限る。)に該当するものに変換するように設計し、若しくは改造したもの (二) 本号から第十二号までのいずれかに該当するもの又は第二十一条第一項第七号、第七号の二、第八号の二、第九号の二又は第十七号に該当するもの(本号に該当する貨物の有する機能と同等の機能を追加することができるように設計し、若しくは改造したもの) ハ 量子暗号を用いるように設計し、又は改造したもの 二 次のいずれかに該当するワルトワイドバンド変調技術のためのチャンネル符号、スクランブル符号又はネットワーク認識符号の生成に暗号処理技術を用いるように設計し、又は改造したもの	暗号機能有効化の手段を用いることによつてのみ、ある貨物又はあるプログラムの暗号機能有効化するもの 次のいずれかに該当するもの(第九号イに該当しないものに限る。)に交換し、又はあるプログラム(第二十一条第一項第七号、第七号の二、第八号の二、第九号の二又は第十七号に該当しないものに限る。)を第二十一条第一項第九号(第八号第九号又はハからホまでに係るものに限る。)に該当するものに変換するように設計し、若しくは改造したもののロ 暗号機能有効化の手段を用いることによつてのみ、貨物等省令第8条第九号から第十二号までに該当する貨物又は第二十一条第一項第七号、第七号の二、第八号の二、第九号の二に該当するプログラムに第九号イに該当する貨物の有する機能と同等の機能を追加することができるように設計し、又は改造したもの	(参考)関係するECCN番号	
		(一) 帯域幅が500メガヘルツを超えるもの (二) 瞬時帯域幅を中心周波数で除した値が20パーセント以上のもの ホ スペクトル拡散のための拡散符号の生成(周波数ホッピングのためのホッピング符号の生成を含む。)に暗号処理技術を用いるように設計し、又は改造したもの(二)に該当するものを除く。 ヘ 次の(一)又は(二)のいずれかに該当するもの(該当することが貨物の製造者、販売者又は輸出者によって書面により確認できるものに限る。) (一) 次の1から3までの全てに該当するもの 1 購入に際して何らの制限を受けず、店頭において又は郵便、民間事業者による信書の送達に関する法律(平成14年法律第99号)第2条第6項に規定する一般信書便事業者若しくは同条第9項に規定する郵便物取扱事業者による民間第2項に規定する信書便若しくは公衆電気通信回線に接続した入力装置(電話を含む。)による注文又は、販売店の在庫から販売されるもの 2 当該貨物の有する暗号機能を当該貨物を使用する者によって変更できないもの 3 当該貨物の有する暗号機能の採用に際して当該貨物の供給者又は販売店による技術支援の必要がないもの (二) (一)に該当する貨物のために設計された部分品であつて、次の1から3までの全てに該当するもの 1 情報システムのセキュリティ管理機能が当該部分品の主たる機能ではないもの 2 (一)に該当する貨物の有する暗号機能を変更できず、かつ、当該貨物に新しい暗号機能を追加できないもの 3 当該部分品の機能が固定されており、特定の機能のみで設計し、又は改造していないもの	量子暗号 物理システムの量子力学的特性(量子力学、量子場理論又は量子電力学等)によって明確な量子力学的物理特性を含む。)を測定することにより、暗号の共有性を確立させるための一連の技術を用いる。量子鍵配布(QKD)ともいう。			
		(二) (一)に該当する貨物のために設計された部分品であつて、次の1から3までの全てに該当するもの 1 情報システムのセキュリティ管理機能が当該部分品の主たる機能ではないもの 2 (一)に該当する貨物の有する暗号機能を追加できないもの 3 当該部分品の機能が固定されており、特定の機能のみで設計し、又は改造していないもの	暗号装置又はその部分品 暗号装置又はその部分品のうち、情報システムのセキュリティ管理機能を無効化し、機能を低下させ又は迂回させるものであつて、次のいずれかに該当するもの イ 暗号解析を行うように設計し、又は改造したものの(リパースエンジニアリングの方法により暗号解析機能を実行するように設計し、又は改造したものを含む。) ロ 電子計算機の端末又は通信端末から生データ抽出するもの(イ又は第七号第五号に該当するものを除く。)であつて、その機能実現のために電子計算機の端末又は通信端末の設計又は製造を迂回することができるように設計したものの(電子計算機の端末又は通信端末の設計又は製造のために特に設計したシステム又は装置、若しくは次の(一)から(四)に掲げるものを除く。) (一) デバイスカーバ/サーバーバイパー (二) 論理データ抽出に限定されたもの (三) チップオフやJTAGを使用してデータ抽出するもの (四) ジェイルブレイク又はルート化用に特別に設計されたもの	暗号解析機能 平文、パスワード又は暗号鍵を含む、秘密の実数又は複素データを抽出するために暗号の仕組みを解読するよう設計された機能を用いる。		
			貨物等省令第8条第十一号	暗号装置又はその部分品 暗号装置又はその部分品のうち、情報システムのセキュリティ管理機能を無効化し、機能を低下させ又は迂回させるものであつて、次のいずれかに該当するもの イ 暗号解析を行うように設計し、又は改造したものの(リパースエンジニアリングの方法により暗号解析機能を実行するように設計し、又は改造したものを含む。) ロ 電子計算機の端末又は通信端末から生データ抽出するもの(イ又は第七号第五号に該当するものを除く。)であつて、その機能実現のために電子計算機の端末又は通信端末の設計又は製造を迂回することができるように設計したものの(電子計算機の端末又は通信端末の設計又は製造のために特に設計したシステム又は装置、若しくは次の(一)から(四)に掲げるものを除く。) (一) デバイスカーバ/サーバーバイパー (二) 論理データ抽出に限定されたもの (三) チップオフやJTAGを使用してデータ抽出するもの (四) ジェイルブレイク又はルート化用に特別に設計されたもの	貨物等省令第8条第十一号 電子計算機の端末又は通信端末のオペレーティングシステム又はファイルシステムによる変換を伴わずに当該装置の記憶媒体(例えば、RAM、フラッシュメモリ又はハードディスク)からバイナリデータを取り出すことを行う。	

輸出令第9項		貨物等省令第8条		解釈		(参考)関係するECCN番号
項番	項目	項番	項目	用語	用語の意味	
輸出令第9項(8)	情報を伝達する信号の漏えいを防止するように設計した装置又はその部分品	貨物等省令第8条第十号	暗号装置又は暗号機能を実現するための部分品以外の情報システムのセキュリティ管理機能を実現する装置又は部分品であって、次のいずれかに該当するもの			
			ロ 情報を伝達する信号の漏えいを防止するように設計し、若しくは改造した装置(電磁波の放射による人体への危害若しくは他の装置の誤動作の誘発を防止することを目的として信号の漏えいを防止するように設計し、若しくは改造したもの又は電磁波妨害防止標準に基づいて信号の漏えいを防止するように設計し、若しくは改造したものを除く。)又はその部分品(情報を伝達する信号の漏えいを防止する機能を実現するために設計し、又は改造した部分品に限る。)	情報を伝達する信号の漏えいを防止するように設計し、又は改造した装置	情報又は通信の秘密を保持することを目的として漏えいを防止するように設計し、又は改造したものに限る。	5A002.a.4
輸出令第9項(10)	盗聴の検知機能を有する通信ケーブルシステム又はその部分品	貨物等省令第8条第十号	暗号装置又は暗号機能を実現するための部分品以外の情報システムのセキュリティ管理機能を実現する装置又は部分品であって、次のいずれかに該当するもの			
			イ 盗聴の検知機能を有する通信ケーブルシステム又はその部分品(盗聴の検知機能を実現するために設計し、又は改造した部分品に限る。)	盗聴の検知機能を有する通信ケーブルシステム	物理層(OSI参照モデル(ISO/IEC 7498)のレイヤー1を含む。)で盗聴の検知機能を実現するものに限る。	5A002.a.8

産業技術力強化法

（国が委託した研究及び開発の成果等に係る特許権等の取扱い）

第十七条 国は、技術に関する研究開発活動を活性化し、及びその成果を事業活動において効率的に活用することを促進するため、国が委託した技術に関する研究及び開発又は国が請け負わせたソフトウェアの開発の成果（以下この条において「特定研究開発等成果」という。）に係る特許権その他の政令で定める権利（以下この条において「特許権等」という。）について、次の各号のいずれにも該当する場合には、その特許権等を受託者又は請負者（以下この条において「受託者等」という。）から譲り受けなければならないことができる。

- 一 特定研究開発等成果が得られた場合には、遅滞なく、国にその旨を報告することを受託者等が約すること。
- 二 国が公共の利益のために特に必要があるとしてその理由を明らかにして求める場合には、無償で当該特許権等を利用する権利を国に許諾することを受託者等が約すること。
- 三 当該特許権等を相当期間活用していないと認められ、かつ、当該特許権等を相当期間活用していないことについて正当な理由が認められない場合において、国が当該特許権等の活用を促進するために特に必要があるとしてその理由を明らかにして求めるときは、当該特許権等を利用する権利を第三者に許諾することを受託者等が約すること。
- 四 当該特許権等の移転又は当該特許権等を利用する権利であって政令で定めるものの設定若しくは移転の承諾をしようとするときは、合併又は分割により移転する場合及び当該特許権等の活用に支障を及ぼすおそれがない場合として政令で定める場合を除き、あらかじめ国の承認を受けることを受託者等が約すること。

産業技術力強化法施行令

（国が譲り受けなければならない権利等）

第二条 法第十七条第一項の政令で定める権利は、特許権、特許を受ける権利、実用新案権、実用新案登録を受ける権利、意匠権、意匠登録を受ける権利、著作権、回路配置利用権、回路配置利用権の設定の登録を受ける権利及び育成者権とする。

- 2 法第十七条第一項第四号の政令で定める権利は、特許権、実用新案権若しくは意匠権についての専用実施権又は回路配置利用権若しくは育成者権についての専用利用権（次項において「専用実施権等」という。）とする。
- 3 法第十七条第一項第四号の政令で定める場合は、次に掲げる場合とする。
 - 一 受託者等（法第十七条第一項に規定する受託者等をいう。）であって株式会社であるものが、その子会社（会社法（平成十七年法律第八十六号）第二条第三号に規定する子会社をいう。）又は親会社（同条第四号に規定する親会社をいう。）に特許権等の移転又は専用実施権等の設定若しくは移転の承諾（以下この項において「移転等」という。）をする場合
 - 二 大学等における技術に関する研究成果の民間事業者への移転の促進に関する法律（平成十年法律第五十二号）第四条第一項の承認を受けた者（同法第五条第一項の変更の承認を受けた者を含む。）又は同法第十一条第一項の認定を受けた者に移転等をする場合
 - 三 技術研究組合が組合員に移転等をする場合

委託研究開発における知的財産マネジメントに関する運用ガイドラインを策定しました

本件の概要

経済産業省は、平成27年5月に国の委託研究開発プロジェクトの担当者が知的財産マネジメントを実施するに当たり考慮すべきと考えられる事項を運用ガイドラインとして取りまとめました。

また、令和2年1月に国の委託研究開発プロジェクトへの国外企業等の参加等に際して留意すべき点、及び令和3年4月に国の委託研究開発プロジェクトから派生した知的財産権をライセンスする際に留意すべき点を運用ガイドラインに追加する改訂を行いました。

本ガイドラインに基づいて、研究開発プロジェクトごとに適切な知的財産マネジメントを実施することで国富の最大化を目指します。

2. 本ガイドラインの概要

(1)適用対象

本ガイドラインは、経済産業省の予算により、経済産業省又は経済産業省所管の独立行政法人が委託する技術に関する研究開発を適用対象としています。

(3)改訂（令和2年1月）のポイント

「国の研究開発プロジェクトにおける国際連携強化に関する基本的な考え方」（令和元年11月6日）を踏まえ、主に以下の内容について改訂を行いました。

- 研究成果に係る知的財産権について国外企業等と国との共有（持分の50%以上は国に帰属）を原則とすること（令和3年5月に国外企業等と国との共有とする規定を例外的に適用しない場合の考え方を追記）（運用ガイドライン2-2-2(2)）。
- 親会社又は子会社（これらの会社が国外企業等である場合に限る。）への移転等の場合には、委託者に連絡の上、事前に調整を行うこと（運用ガイドライン2-2-2(7)）。
- 安全保障貿易管理の観点を踏まえ、技術情報等の流出を防止すること（運用ガイドライン2-2-4(1)）。

委託研究開発における知的財産マネジメント
に関する運用ガイドライン

平成27年5月
(最終改訂令和3年5月)
経済産業省

(関連部分抜粋) p9-10

(2) 研究開発の成果に係る知的財産権の帰属

研究開発の成果の事業化は、成果の内容や価値を理解している者が行うことが望ましく、当該成果を得たプロジェクト参加者自身が第一候補となる。

このため、事業化（自ら事業活動を行う場合のほか、研究開発成果を第三者に移転することにより事業化を目指す場合も含む。）することに意欲的なプロジェクト参加者に対しては、成果を最大限事業化に結び付ける視点を踏まえた上で、基本的に日本版バイドール規定を適用し、研究開発の成果に係る知的財産権（以下「フォアグラウンド I P」という。）を保有させることが妥当である。

ただし、当該プロジェクト参加者が国外企業等（日本以外の国の企業、大学若しくは研究機関又は外国籍の研究者をいう。以下同じ。）である場合については、国費を投じて実施した研究開発の成果の事業化を国内企業等が行えない等のおそれを回避する観点から、フォアグラウンド I Pについて国外企業等と国との共有とすることを原則とする。また、この場合、国外企業等と国の持分の合計のうち50%以上の持分は国に帰属させるものとする。^{4・5}

⁴ 「国の研究開発プロジェクトにおける国際連携強化に関する基本的な考え方」（令和元年11月6日経済産業省産業技術環境局総務課・研究開発課）P7-8参照

https://www.meti.go.jp/policy/innovation_policy/basic_policy.pdf

⁵ 「50%以上」の国の持分は、知的財産権全体に対する国の持分の割合ではなく、国外企業等の持分と国の持分の合計に対する国の持分の割合である。例えば、国とプロジェクト参加者のA社（国内企業）、B社（国外企業）の3者で知的財産権を共有することとなった場合、「A社50%、B社25%、国25%」としたり、「A社33%、B社33%、国34%」とすることで、B社の持分と国の持分の合計に対して、国の持分が50%以上になることを意味する。

日本版バイドール制度関連 戦略的創造研究推進事業（CREST等）募集要項

2021年度

戦略的創造研究推進事業
(CREST・さきがけ・ACT-X)
(第1期)

募集要項

募集期間：

2021年3月23日（火）～ 5月18日（火）午前12時（正午）：CREST

2021年3月23日（火）～ 5月11日（火）午前12時（正午）：さきがけ・ACT-X



国立研究開発法人科学技術振興機構 (JST)
戦略研究推進部

2021年3月

(関連部分抜粋) p38

5.2.2 研究契約

- 研究課題の採択後、原則として JST は研究代表者及び主たる共同研究者、個人研究者の所属する研究機関との間で委託研究契約※を締結します。
- 研究機関との委託研究契約が締結できない場合、公的研究費の管理・監査に必要な体制等が整備できない場合、また、財務状況が著しく不安定である場合には、当該研究機関では研究が実施できないことがあります。詳しくは、「5.2.8 研究機関の責務等」をご参照ください。
- 研究により生じた特許等の知的財産権は、委託研究契約に基づき、産業技術力強化法第 17 条(日本版バイ・ドール条項)に掲げられた事項を研究機関が遵守すること等を条件として、原則として研究機関に帰属します。ただし、海外の研究機関に対しては適用されません。

※ 最新の委託研究契約書の雛型については、以下のウェブサイトをご参照ください (2021 年 4 月 1 日公開予定)。

<https://www.jst.go.jp/contract/download/2021/2021kisokens201keiya.pdf>

(関連部分抜粋) p50

第 5 章 CREST・さきがけ・ACT-X 共通事項

(2) 研究実施機関が海外機関の場合

- 研究機関は、原則として JST が提示する内容で研究契約を締結しなければなりません (研究内容の特性等を勘案し、合理的な理由であると認められる事項については、契約条文を調整できる場合もあります)。また、研究契約書※、研究計画書に従って研究を適正に実施する義務があります。研究契約が締結できない場合、もしくは当該研究機関での研究が適切に実施されないと判断される場合には、当該研究機関における研究実施は認められません。

※ 海外機関用の研究契約書雛型等については、以下の URL より応募される研究領域のページにアクセスいただき、「応募方法」の項目内の「参考資料」をご参照ください。

<https://www.jst.go.jp/kisoken/boshuu/teian/top/rvoiki.html>

- 研究機関は、研究契約及び JST が別に指針等を指定する場合は当該指針等に基づき、研究機関の責任において適切に研究費の支出・管理を行うとともに、研究費の支出内容を表す経費明細(国内機関の場合の収支簿に相当)を英文で作成して提出する義務があります。また、研究機関は、契約期間中であっても JST の求めに応じて執行状況等に係る各種調査に対応する必要があります。
- 研究の実施に伴い発生する知的財産権は、JST へ無償譲渡するか、JST と均等共有となります。均等共有とする場合、知的財産権の保護申請、維持等に必要費用等も JST と均等に負担する義務があります (海外機関に対しては、産業技術力強化法第 17 条(日本版バイ・ドール条項)は適用されません)。これに伴い、知的財産権となり得る発明等がなされた場合は、速やかに (10 営業日以内) に JST へ報告する必要があります。

※経済産業省が公表している「外国ユーザーリスト^{*4}」に掲載されている機関など、安全保障貿易管理や国家安全保障の観点から、JST が研究契約を締結すべきでないと思われる場合があります。

※ACT-X では海外機関で ACT-X 研究を実施することはできません。

^{*4} 経済産業省は、貨物や技術が大量破壊兵器等の開発等に用いられるおそれがある場合を示すため「外国ユーザーリスト」を公表しています。

<https://www.meti.go.jp/policy/anpo/law05.html#user-list>