

本チェックリストは、技術流出対策ガイドス第2版において紹介している事項を抜粋・要約したものです。自社の実施状況の確認等にご活用ください。なお、ガイドスにおいてご説明しているとおり、各事項の実施は企業に対する義務ではありません。

チェック項目		チェック
各章で共通する技術流出対策（第1章）		
1 組織体制の構築・リスクマネジメント		
①	経営層によるリーダーシップとアクション ① 経済安全保障リスクを経営上の重要事項として位置付け、経営者自らが対応を主導しているか？ ② 短期でなく中長期の視点に立ち、過度に萎縮することなく、自社の経済安全保障リスクを適切に把握しているか？	
②	司令塔となる部署の設置 ① 既存部署の活用や機能拡大、専任部署の新設を含め、技術流出対策の司令塔となる組織を設置しているか？	
2 重点的に守るべき技術の特定・評価		
①	重要技術の位置づけを評価 ① 技術の重要性に応じて、技術管理に関する基本的な考え方を構築し、位置づけを整理しているか？ ② 自社の競争力の源泉となるコア技術について、権利化・秘匿化や社内管理を含めた対策を検討しているか？ ③ 安全保障上または経済安全保障上の重要技術に該当するかを評価し、必要に応じて慎重な対応を行っているか？ ④ 自社では未保有だが獲得を目指す技術についても評価を行っているか？	
②	自社の競争力の源泉となるコア技術の特定 ① 技術の重要度、自社の競争力や技術優位性などを考慮して、コア技術を特定・分析しているか？ ② コア技術がどのように存在しているか、形態を確認しているか？	
③	技術の特徴等に応じた適切な知的財産戦略 ① 侵害の発見しやすさや技術格差など、技術の特徴等に応じて、権利化・秘匿化の適切な選択基準を持っているか？ ② 職務発明者や競合他社による特許化への対応を講じているか？ ③ 特許出願時の書類が公表されることを踏まえて、特許明細書等の記載を工夫しているか？ ④ 秘匿化を選択した場合は、秘密管理を徹底しているか？	
④	営業秘密管理の徹底 ① 特許取得やオープン化を行わず秘匿化するコア技術について、秘密管理性が認められるよう管理を徹底しているか？ ② 秘密情報を分類し、立証も意識してセキュリティシステム等を導入しているか？	

チェック項目		チェック
生産拠点の海外進出に伴う技術流出対策（第2章）		
1 計画前・計画段階において取り組むべき事項		
①	日本社内の情報管理体制の整備 ④ 情報管理規程を整備し、社内教育・研修を実施しているか？ ④ 最新情報を規程や研修の内容に反映しているか？	
②	相手国の制度の確認 ④ 技術流出対策の観点から、相手国の制度の確認・リスク分析を行っているか？ ④ 現地情勢や法制度以外のルール・慣行も確認しているか？	
③	相手国の技術的関心の確認 ④ 社内横断的な情報収集・分析体制を整備しているか？ ④ 公的機関等との連携等を通じて、相手国の技術的関心を確認しているか？	
④	相手国の労働法制・慣習・雇用情勢等の確認 ④ 法令遵守の観点から、相手国の労働法制を把握・理解しているか？ ④ 労働法制に限らず、労働慣習等も確認し、社内規程や研修等に反映しているか？ ④ 相手国の雇用情勢も考慮して、移転する技術の範囲を見極めているか？	
⑤	情報管理体制等に関する取引先DDの実施 ④ ヒアリングや現地確認等によって、取引先の情報管理に関するデューデリジェンスを実施しているか？ ④ 財務健全性やコンプライアンス遵守状況に関するデューデリジェンスも実施しているか？ ④ 情報管理が自社の水準に達していない場合、必要な情報管理体制の整備が完了してから契約しているか？	
⑥	ステークホルダーに対する事前説明 ④ 契約内容を確認した上で、海外技術移転の規模等も考慮し、技術流出リスクと対策状況を丁寧に説明しているか？	

チェック項目		チェック
2 契約締結時に取り組むべき事項		
①	提供する技術の内容等の明確化 <ul style="list-style-type: none"> ☞ 契約交渉が開始する前に確実にNDAを締結しているか？ ☞ 技術の重要度に応じた契約審査を実施しているか？ ☞ 技術情報の提供範囲や提供方法を明確にしているか？ ☞ 提供範囲や提供方法を変更する場合は、新たに契約を締結することとしているか？ ☞ 契約書と別に、実務者向けのガイドラインを作成しているか？ 	
②	技術情報の取扱いに係る遵守事項の明確化 <ul style="list-style-type: none"> ☞ 技術情報を取り扱うことができる主体とその方法を限定しているか？ ☞ 取引先DDで確認した情報管理体制の維持を遵守事項として定めているか？ ☞ 遵守事項の履行状況をモニタリングするため、生産拠点への立入りを含む監査条項を定めているか？ 	
③	事情変更が生じた場合の対応の明確化 <ul style="list-style-type: none"> ☞ 技術流出リスクに影響する事情変更が生じた場合を想定した事前承諾事項・通知事項・解除事由を定めているか？ ☞ 社会情勢の変化等に伴い日本からの技術情報の提供が困難になる場合を想定した免責条項を定めているか？ 	
④	契約終了後の手続の明確化 <ul style="list-style-type: none"> ☞ 自社による記録媒体の処分について明確に定めているか？ ☞ 文書等の処分手続が可視化されているか？ ☞ 取引先が契約終了後も守秘義務を負っているか？ ☞ 非公開の紛争解決手続の利用に関する条項を定めているか？ 	
⑤	(合併契約の場合) ガバナンスの確保 <ul style="list-style-type: none"> ☞ 出資比率の過半数を確保・維持しているか？ ☞ 十分な人数の役員を派遣する権利を確保しているか？ ☞ 技術流出のおそれのある行為を拒否権事由や事前承諾事項に定めているか？ ☞ 技術流出対策の観点から、合併解消の条件・解消時の技術情報の取扱いについて定めているか？ 	

チェック項目		チェック
3 海外事業の実施段階において取り組むべき事項		
①	段階的な技術提供 ① 技術情報を段階的に提供し、必要性に応じて情報の開示を制限しているか？ ② 技術流出対策の観点から、適切な契約期間の見極めを行っているか？	
②	情報のブラックボックス化 ① 原材料等の重要な固有名詞や調達元の情報を秘匿しているか？ ② 提供する図面に機密性が高い情報が記載されていないか？	
③	技術情報提供後の情報管理の徹底 ① 技術情報の保存・アクセス等に関する社内ポリシーを策定し、従業員に周知徹底しているか？ ② 重要情報へのアクセス権限の管理・定期的な見直しを行っているか？ ③ 現地に提供した技術情報はリスト等で管理しているか？ ④ 技術ノウハウを分割管理し、全ての情報が一カ所に集約されないようにしているか？ ⑤ 情報セキュリティ体制についての現地監査を実施しているか？	
④	製造設備のメンテナンス管理の徹底 ① 製造設備に関する機微情報の範囲を確認しているか？ ② 日本本社や設備メーカーから技術者を派遣するなどして、信頼できるメンテナンス体制を確立しているか？	
4 撤退・契約終了時に取り組むべき事項		
①	撤退計画に対応した適切な情報管理の徹底 ① 撤退に伴う情報の取り扱いに関する社内ポリシーを策定し、従業員に周知徹底しているか？ ② 重要情報へのアクセス権限の再設定等を行っているか？ ③ 撤退前に技術情報が持ち出されないように監視を強化しているか？ ④ 現地スタッフとの契約で、退職後の秘密保持義務が定められているか等の確認をしているか？	
②	製造設備の適切な管理・処分 ① コア技術が化体している設備を特定し、確実に返却・廃棄しているか？ ② 返却・廃棄する際には、業者を慎重に選定するとともに、立ち会いや現地確認も実施しているか？	
③	撤退後のフォローアップ ① 現地の競合他社の開発状況や特許出願状況など、技術流出につながりうる動向を定期的に調査しているか？ ② 取引先との信頼関係の維持に取り組んでいるか？ ③ 契約や法令に違反する行為を把握した場合には、訴訟等の毅然とした対応を講じているか？	

チェック項目		チェック
5 その他の取組事項		
①	海外の研究開発拠点に対する管理の徹底 ☞ 日本国内と同等の管理体制を整備し、日本本社への報告等の仕組みを構築しているか？	

チェック項目		チェック
人を通じた技術流出への対策（第3章）		
1 技術流出を防ぐために未然に取り組むべき事項		
(1) ルール面での対応		
①	情報管理に関するルールの整備・運用の徹底 <ul style="list-style-type: none"> ☞ 正社員に限らず、役員や派遣従業員等を含め、勤務形態を問わず広く役職員を通じた技術流出を念頭にルールを整備しているか？ ☞ 就業規則に加え、雇用契約等の個別の契約において、技術流出防止に関する定めを設けているか？ ☞ 規程の整備に留まらず、関係部署の連携において経営層が関与する等、全社的に実効的な運用がなされているか？ 	
②	情報管理状況の監査と重要プロジェクトの配置等への反映 <ul style="list-style-type: none"> ☞ 定期的に監査を実施し、経営陣に報告するとともに、社内規程の改定等の情報管理体制の改善に取り組んでいるか？ ☞ コア技術に関与する重要プロジェクト等への配置に当たり、当該役職員の情報管理意識を確認・反映しているか？ 	
(2) 人事面での対応		
③	情報管理に関する定期的・階層的な研修の実施 <ul style="list-style-type: none"> ☞ 役職員に対し、情報管理意識の醸成のため、最新ルールや流出事例を踏まえた定期的な研修を実施しているか？ ☞ 画一的な内容ではなく、職位や所属部署に応じた階層的な研修を実施しているか？ 	
④	法令上必要な事項の採用時確認 <ul style="list-style-type: none"> ☞ 外為法上の非居住者や特定類型への該当性など、法令遵守の観点から必要な事項をあらかじめ確認しているか？ ☞ 特に中途採用の場合は、他社の営業秘密を持ち込んでいないことを確認しているか？ 	
⑤	重要技術を扱う部署への配属に際しての確認 <ul style="list-style-type: none"> ☞ 配属予定の部署・ポジションで扱う重要技術の内容や重要性を踏まえ、漏えいのおそれを事前に評価しているか？ ☞ 適性の確認にあたり、取得する情報を必要かつ合理的な範囲に限定し、目的を説明して対象者の理解を得ているか？ ☞ 評価や配属判断が、労働基準法第3条が定める労働条件の差別的取扱いに該当しないか確認しているか？ ☞ 評価結果を人事評価や懲戒、不利益な配置変更等、目的外に利用しない運用をしているか？ 	
⑥	副業等を通じた情報流出の防止 <ul style="list-style-type: none"> ☞ 副業・兼業からの技術流出を防止するため、就業規則において副業・兼業に関するルールを定め、周知しているか？ ☞ スポットコンサル等の公開情報を確認し、副業・兼業を通じた技術流出事案がないか確認しているか？ 	
⑦	競業避止義務契約の適切な活用 <ul style="list-style-type: none"> ☞ 退職後の技術流出防止のため、就業規則や退職時の誓約書等で競業避止義務を導入しているか？ ☞ その際、企業の守るべき利益に照らし、職位や業務内容に応じた合理的な範囲の制限としているか？ 	

チェック項目		チェック
1 技術流出を防ぐために未然に取り組むべき事項		
(3) システム面での対応		
⑧	アクセスコントロールの徹底 <ul style="list-style-type: none"> ☞ Need-to-Knowの原則に基づき、当該技術情報を知る必要のある役職員にのみアクセス権限を付与しているか？ ☞ 人事異動や転職、退職等に伴い、アクセス権限を速やかに見直し・再設定しているか？ 	
⑨	退職時のアクセス制限 <ul style="list-style-type: none"> ☞ 退職予定者に対し重要な技術情報等へのアクセス権限を必要最低限に制限しているか？ ☞ 退職予定者に対しアクセスログを通常より厳格に取得・分析し、情報流出の予兆を退職前に確認しているか？ ☞ 退職予定日までの貸与物品の返却、退職後の秘密保持義務と違反した場合の対応の説明を徹底しているか？ 	
⑩	デバイスの管理・利用ルールの徹底 <ul style="list-style-type: none"> ☞ 業務用のデバイスは、会社が所有・貸与するものに限定しているか？ ☞ デバイスの紛失・盗難に備え、デバイスへのデータ保存を制限する等対策を講じているか？ ☞ 技術情報の持ち出しを制限するため、USBメモリ等へのコピーを禁止・制限しているか？ 	
⑪	ソフトウェアやSNS等の利用ルールの徹底 <ul style="list-style-type: none"> ☞ ソフトウェアの安全性や取り扱う情報の機微度を踏まえて、ソフトウェアの利用ルールを定めているか？ ☞ SNS等についても、技術流出を防ぐ観点から利用ルールを定めているか？ 	
⑫	技術流出に繋がるおそれのある行為の検知・警告 <ul style="list-style-type: none"> ☞ 大量印刷や大量ダウンロード、外部送信等の通常と異なる行為を検知できる体制やシステムを整備しているか？ ☞ 技術流出に繋がるおそれのある行為を検知していることを周知・警告し、不適切行為の抑止につなげているか？ ☞ 技術情報の重要性等によっては、技術的な設定により、印刷やメール送信を禁止しているか？ 	
(4) オペレーション面での対応		
⑬	工程の細分化・全体工程を知る役職員の限定 <ul style="list-style-type: none"> ☞ 研究開発や製造工程を細分化し、各担当者が知り得る情報を必要最小限に限定しているか？ ☞ 全体工程を把握する役職員を必要な者に限定し、組織として把握・管理しているか？ 	
⑭	海外出張や赴任時の情報管理 <ul style="list-style-type: none"> ☞ 海外赴任者のアクセス権限を適切に再設定しているか？ ☞ 海外に出張・赴任する場合のデバイスの持参や交換に関するルールを定めているか？ ☞ カウンターインテリジェンスに関する研修を実施しているか？ 	
⑮	展示会等を契機とする部外者との接触への対応 <ul style="list-style-type: none"> ☞ 技術者に対する不審なアプローチを防ぐため、出席者の個人連絡先が知られないように対策しているか？ ☞ 技術的な質問に対して回答してもよい範囲を明確にして、出席する技術者に周知しているか？ ☞ 展示会等で公表する資料や展示品を事前に確認しているか？ 	

チェック項目		チェック
2 技術流出した場合に取り組むべき事項		
①	違反に対する毅然とした対応 <ul style="list-style-type: none"> ☞ 技術流出の疑いが生じた場合、迅速に調査・対応することとしているか？ ☞ 技術流出した役職員について、就業規則に基づく懲戒処分や不正競争防止法に基づく責任を追及しているか？ ☞ ステークホルダー等への公表・説明の実施を検討しているか？ 	
②	再発防止策の策定・徹底 <ul style="list-style-type: none"> ☞ 技術流出事案が発生した場合、原因を分析し再発防止策を策定の上、研修や監査等を通じて運用を徹底しているか？ 	
3 技術者の流出に対して取り組むべき事項		
①	イノベーションを生み続ける（技術の陳腐化の加速） <ul style="list-style-type: none"> ☞ 競合他社の慎重や数年先の市場動向等を見据えて、将来必要となる技術の見極めを行っているか？ ☞ 技術開発から実装までを見据えた計画を策定しているか？ 	
②	優秀な技術者の流出防止 <ul style="list-style-type: none"> ☞ コア技術に直結する優秀な技術者について、給与面を含めて、待遇を向上させているか？ ☞ 技術者のモチベーションを維持・向上させるような表彰制度や技術系職位の設置等の施策を講じているか？ ☞ 定年延長や再雇用制度等を導入し、熟練技術者の流出を防止する仕組みを構築しているか？ 	
③	退職者との良好な関係の構築 <ul style="list-style-type: none"> ☞ 技術流出対策の観点から、退職者との良好な関係の構築が重要であることが全社的に認識されているか？ ☞ OBOG会等を通じて、退職者と定期的にコミュニケーションを図っているか？ 	

チェック項目		チェック
共同研究に伴う技術流出への対策（第4章）		
1 計画段階において取り組むべき事項		
(1) リスクマネジメントプロセスの導入		
①	リスクマネジメントプロセスの導入 ① 共同研究を行う際の一連のプロセスを社内ルール化し、業務フローに反映しているか？ ② 社内の担当部署が実施部門の要請を踏まえてDD等を行う体制を構築しているか？	
(2) 自社における研究体制の確認		
②	共同研究に従事する役職員の決定 ① 技術の重要性に応じて共同研究に従事する候補者を選定し、事前に情報管理スキル等を確認しているか？ ② その際、社内における情報管理状況、外国政府との関係性、情報取扱いの非違歴等を確認しているか？	
(3) テーマ選定における取組事項		
③	技術の重要性を踏まえたリスク評価と研究テーマ選定 ① 研究テーマ選定にあたり、当該技術の重要性を評価し、流出時に想定される損失や影響を把握・評価しているか？ ② 流出時のリスク評価や共同研究先のDDの結果等も考慮の上、適切にテーマを選定しているか？	
(4) パートナー選定における取組事項		
④	パートナー候補のDDの徹底 (相手国の観点) ① 国際共同研究に際し、相手国の法制度や商慣習、属性・情勢を事前に確認し、技術流出リスクを分析しているか？ ② 役職員が現地出張する際、相手国における情勢や規制法、他社の情報インシデントの有無等を確認しているか？	
⑤	パートナー候補のDDの徹底 (組織の観点) ① 懸念主体との資本関係や人的関係、各国制裁リストへの掲載や過去の情報インシデントの有無等を把握しているか？ ② その際、技術情報の重要性・機微性や相手方の特性を考慮の上、コストも踏まえ確認項目を調整しているか？ ③ 特に、相手が企業か大学や研究機関かに応じ、確認する項目や重点の置き方を調整しているか？	
⑥	パートナー候補のDDの徹底 (関与する個人の観点) ① 共同研究に参加するメンバーについて、必要に応じて協力を得た上で個人単位のDDを実施しているか？ ② 特に、外国政府等による情報収集活動への協力義務の有無や、情報取扱いに関する非違歴・懲戒歴や前科を確認しているか？ ③ 大学との共同研究の場合、研究セキュリティの観点からの確認事項や、雇用関係のない参加者(学生)の有無を確認しているか？	

チェック項目		チェック
2 契約締結時に取り組むべき事項		
①	事前のNDA締結と段階的な情報開示、NDA締結前の特許出願 ① 非公開情報の提供や事前協議に先立ち、NDAを締結しているか？ ② NDA締結前の情報提供は公開情報に限定し、また、必要に応じて特許を事前出願しているか？	
②	自社の契約書ひな型の活用とリスクに応じた契約条件設定 ① 契約交渉等の個別事情を踏まえ、自社の契約書ひな型を用いて契約締結を行っているか？ ② 技術の重要性や相手方のリスクに応じて、守秘義務や成果帰属等の条項を追加・修正しているか？	
③	共同研究の目的・テーマの範囲の画定 ① 契約締結までに、共同研究の目的やテーマを当事者間で共有し、契約上明確に定めているか？	
④	研究参加メンバーや情報の取扱方法の明確化 ① 共同研究契約や研究計画書において、研究参加メンバーを氏名等で特定しているか？ ② 技術情報の取扱方法や利用範囲を定め、目的外利用や事前承認のない持ち出し等を禁止しているか？	
⑤	提供する技術情報の範囲と、知的財産の帰属等の明確化 ① 共同研究において提供する技術情報の範囲や提供方法を、契約上あらかじめ明確に定めているか？ ② 相手方が単独で特許化・利用することを防ぐため、成果物や知的財産の帰属や利用権を契約で明示しているか？	
⑥	秘密保持義務・競業禁止義務の設定 ① 共同研究契約において、提供した技術情報の不正持ち出しや目的外利用を防ぐため、秘密保持義務や流用の制限、競業禁止義務を契約で定めているか？	
⑦	モニタリング条項の設定と実施による情報管理の確認 ① 相手方の情報管理の確認のため、対面／書面での監査・モニタリング条項を定め、実施しているか？	
⑧	共同研究先の業績悪化・資本変動等に備えた解除事由等の設定 ① 共同研究先の業績悪化や資本構成の変化等について、事前承諾・通知事項・解除事由等として定めているか？ ② 契約解除後のデータやサンプルの返却に関する条項を定め、確実に実行しているか？	
⑨	非公開範囲の設定や、成果公開時の事前承諾手続等の明確化 ① 提供した技術情報について、秘匿化すべき範囲や非公開期間を契約上定め、意図しない公表等を制限しているか？ ② 成果を公表する場合に、内容確認や事前通知・事前承諾の手続きを定め、実際に運用しているか？	
⑩	契約終了後の情報返却・削除義務の明確化と履行確認 ① 契約終了後に提供したデータやサンプル等の返却・削除義務を契約で定め、実際に履行されたか確認しているか？	
⑪	国外訴訟・法制度リスクへの備え ① 契約で準拠法や裁判管轄を日本法や中立的な国際ルールとするよう定め、また、専門家のレビューを受けているか？	

チェック項目		チェック
3 共同研究の実施段階において取り組むべき事項		
①	研究計画等における情報の利用・管理ルールの明確化 ① 契約書に加え、研究計画書や実験規約を作成し、情報や試料の取扱方法、区分管理等の管理ルールを定めているか？ ② 研究参加者に対し、情報管理ルールの遵守や違反時の対応を明示し、理解を得ているか？	
②	相手方への情報管理体制強化要請とモニタリングの実施 ① 相手方に対し、情報管理体制の構築や取扱区分の明確化、研修等を通じた意識向上を求めているか？ ② 契約に基づき、相手方の情報管理状況について定期的又は必要に応じてモニタリングや確認を実施しているか？	
③	情報アクセス制限と物理的セキュリティ強化による漏えい防止 ① 必要に応じ自社が管理権限を持つプラットフォームを用い、閲覧権限等の制限によりアクセスを制御しているか？ ② 重要な技術やサンプルを扱う場合、施設への立入制限や区分管理等の物理的セキュリティ対策を講じているか？	
④	委託先・クラウド利用時の情報管理の徹底 ① 共同研究先による委託を承認するかどうかを判断する場合に、委託先のDDを実施しているか？ ② 委託先における情報管理の状況について、監査等を実施し、不備がある場合には是正を求めているか？ ③ 契約終了時に、委託先を含む関係者から資料やデータの返却・消去が確実に行われたか確認しているか？	
⑤	堅牢なセキュリティ対策の導入や、外部ツールの利用制限の検討 ① 研究データを扱うネットワークやPCにセキュリティ対策を導入し、施設についても入退室管理等を講じているか？ ② 外部の事業者が管理・提供するツールを利用する際は、安全性を検証しリスクに応じた利用制限を設けているか？	
⑥	セキュリティ担当者の配置とサイバー防御態勢の強化 ① 特に機密性の高い研究について、プロジェクト単位で専門のセキュリティ担当者を配置し管理しているか？ ② 定期的な脆弱性診断や訓練等を通じてサイバー防御態勢を継続的に強化しているか？	
⑦	技術流出発生時のインシデント対応計画と対応体制の整備 ① インシデント発生時に速やかな初動対応ができるような対応計画と体制を整備しているか？	
4 研究終了時に取り組むべき事項		
①	終了後のモニタリングと文書等の適切な管理 ① 共同研究終了後も相手方の動向を確認するとともに、仮に紛争になった場合に備えて文書や記録を管理しているか？	
②	技術情報やサンプルの返還・廃棄の徹底 ① 共同研究終了時に、技術情報の返還・廃棄を徹底しているか？廃棄させる場合には、廃棄証明書を求めているか？	

チェック項目		チェック
すり合わせに伴う技術流出への対策（第5章）		
1 取引開始前に取り組むべき事項		
①	取引先のリスク評価を行う ① 技術情報の提供を伴う取引先について、技術流出リスクの観点から、事業内容や経営状況、役員構成や情報インシデントの有無等を事前に評価しているか？	
②	取引開始前の情報提供の範囲の限定 ① 取引開始前の商談や検討段階において、NDAを締結するまでは技術情報を提供しないようにしているか？ ② NDA締結後の商談であっても、提供可能な情報の範囲を限定し、明確にしているか？	
2 契約締結時に取り組むべき事項		
①	秘密保持義務・情報の取扱方法等の規定 ① 取引基本契約等において、目的外利用や第三者提供の禁止、再委託時の制限等を含む秘密保持義務を定めているか？ ② 特に重要な技術情報を提供する場合は、必要に応じて個別にNDAを締結しているか？	
②	資本変動等に備えた解除事由等の設定 ① 共同研究先の業績悪化や資本構成の変化等について、事前承諾・通知事項・解除事由等として定めているか？ ② 契約解除後のデータやサンプルの返却に関する条項を定め、確実に実行しているか？	
3 サプライチェーンの中との連携において取り組むべき事項		
①	サプライチェーンの上流（仕入れ先）に対する情報提供範囲の制限 ① 調達時に、製品開発方針や技術情報が推測されないよう、仕入れ先へ提供する情報を必要最小限に限定しているか？ ② 外国政府の要請等を背景に、技術情報等の開示を求められた場合、安易に応じず、要求の合理性を確認しているか？	
②	サプライチェーンの下流（顧客等）に対する情報提供範囲の制限 ① 仕様調整等の場面において、重要技術が推測されないよう、顧客に提供する技術情報を最小限に限定しているか？ ② 技術情報を提供せざるを得ない場合も、重要技術についてはブラックボックス化等により秘密管理を講じているか？	
4 サプライチェーンの外との連携において取り組むべき事項		
①	サプライチェーン外（製造装置メーカー等）との連携時の情報提供制限 ① 外部関係者と連携する際に、提供する技術情報を必要最小限に限定し、調達先の分散等で情報集中を避けているか？ ② 製造装置のカスタマイズが必要となる場合には、極力自社で行う等により、操業条件の漏えいを防いでいるか？	
②	サプライチェーン外との連携時における情報管理状況の確認 ① 外部事業者との連携時は、情報管理体制を確認するとともに、第三者認証制度の取得を促す等しているか？ ② 技術情報の提供・開示を伴う取引については、提供・開示する事項を限定しているか？	