日機連２０２１

2021 年度ポストコロナの
製造業グローバル・バリューチェーン変革
に関する調査研究
報告書

Ⅱ．セキュリティ　編

2022 年 3 月

一般社団法人　日本機械工業連合会

事業基盤研究委員会

製造業グローバル・バリューチェーン変革に関する調査研究（部会）

この報告書は、競輪の補助金により作成しました。

https://jka-cycle.jp/

通商・セキュリティテーマ検討会　委員名簿

2022年3月

一般社団法人日本機械工業連合会

（敬称略）

事業基盤研究委員会 委員長	（株）ＩＨＩ　顧問	石　戸　利　典
同 副委員長	三菱電機（株）シニアアドバイザー	諸　岡　暢　志
テーマリーダー （通商）	みずほリサーチ&テクノロジーズ（株）　調査部主席研究員	菅　原　淳　一
テーマリーダー （セキュリティ）	日本輸出管理研究所　代表	高　野　順　一
委員	川崎重工業（株）　マーケテイング本部　渉外・調査部長	福　岡　康　文
委員	（株）島津製作所　経営戦略室　副室長	佐　野　正　一
委員	ダイキン工業（株）　法務コンプライアンス知財センター 企業倫理リスクマネージメントグループ　貿易管理担当課長	瀬戸口　隆　之
委員	（株）ダイヘン　執行役員　企画本部長	森　岡　正　名
委員	（株）東芝　経営企画部 企画・IR室 官公庁渉外担当	子　安　信　彦
委員	東芝デバイス&ストレージ（株）　貿易管理部 輸出管理企画担当	逵　　光　輝
委員	（株）日立製作所　グローバル渉外統括本部 産業政策本部 国際渉外部　部長代理	山　崎　容　子
委員	三菱重工業（株）　グループ戦略推進室 戦略企画部 グローバル経営推進部　主幹部員	山　角　洋　之
コンサル	（株）東レ経営研究所　繊維市場調査部長兼企画管理部主幹	高　月　順一郎
事務局（日機連）	副会長　専務理事	中　富　道　隆
事務局（日機連）	事務局長兼総務部　部長	角　町　昌　之
事務局（日機連）	RRI兼DX技術部　部長	益　子　龍太郎
事務局（日機連）	業務部兼DX技術部　上席調査役	青　木　楠　雄

目　次

第１章　国際ビジネス環境における安全保障状況の重要な変化

１　はじめに

究極の国家間の利害紛争の「解決」の手段として、武力行使（＝軍事行動）は、以前は現在よりはるかに容易に行われていたと言える。第２次世界大戦以降、軍事力による現状変更を認めない国際ルールが一応成立した結果、経済発展は平和の象徴であり、安全保障（＝軍事）と経済発展はある意味対極の概念として定着してきた。本質的に考えれば、安全保障は国家の存在意義の最も根源的な部分であり、経済を含めどんなこととも根本では繋がるものであり、安全保障と経済を分離することはできないのだが、特に日本では完全な別物という風潮が主流であった。

1999 年に中国人民解放軍国防大学の教授である喬良と王湘の共著である「超限戦」が上梓された。この著書では、平時と戦争時の区別をせず「武力と非武力、軍事と非軍事、殺傷と非殺傷を含む全ての手段を用いて、自分の利益を敵に強制的に受け入れさせる。」と言うコンセプトが明確に打ち出されている。同著によれば、ソ連崩壊後１強となった米国がその圧倒的な軍事力により湾岸戦争で完全な勝利を収めた事実に衝撃を受け、純軍事力だけでは、今後何年経っても中国は米国に勝利することはできないと判断したと書かれている。最近巷でよく聞かれるようになった「経済」の武器化・経済安全保障などのコンセプトを先取りしたものと言える。

国際ビジネスを行う企業の立場から見ると、前述のように今までは非軍事の経済活動（国際ビジネス）は基本的に「善」であり「誰も文句を言わない」自由なものであったが、突然各国の「安全保障上の制約」を受けるリスクが多大に増加したということである。経営者にとっては頭の痛いことだが、より国際ビジネスが難しいものとなり、今までは気にする必要がなかった安全保障目線での調査や分析が必須となってしまった。

２　変化の本質とは？

中国は以前から、長期的に「超限戦」的な政策を続けてきたわけだが、なぜ最近になって問題として表面化してきたのかという点を考えたい。結論としては、米国が中国の経済的な発展を米国にとっての脅威と見たからであることは間違いない。さらに、米国が最も脅威と感じているところはどこかと考えた場合、これは本質的には技術発展・技術開発力が焦点であると捉えることができる。

ほんの少し前まで、新しい技術を作り出す、又は既存の技術の延長であっても革新的なレベルまで引き上げるようなきっかけを作り、実質的に主導するのは「軍事」であった。軍事技術開発には、商業的なセンスでの採算は考える必要がなく、多額の投資が可能である。その結果生まれたものが集積回路（＝半導体技術）であり、インターネットである。その意味では、最大の軍事力と、それゆえの最大の軍事予算を持つ米国が圧倒的に有利であったことは間違いないと言える。

しかしながら、技術の進歩・多様化・変化の速さは、軍事技術先行のモデルを打ち砕いた。例えば、スマートフォンなどの頻繁なモデルチェンジや試行錯誤的に新商品を出して売れなければまた新しい商品を出すと言うような事業戦略は、軍事技術の開発とは時間軸が全く違う。種類にもよるが、一旦定まった軍事装備の変更はそれなりの手間とコストがかかり、数ヶ月単位で行うような商品戦略とは全く違う。

また別な観点から、半導体に注目すると、その設計技術や製造技術を高めるには、一定の市場規模が継続的に必要となり、それは軍事用途だけでは到底カバーできるものではない。

軍民融合政策は技術発展を進める最適のやり方であったと言うことができる。軍民融合は、輸出管理業務に携わる者にとっては軍事用途と民生用途の区別が極めて難解となり正直好ましいものではない。軍事ではなく民間用途がより高度な技術開発を結果的に主導するという意味合いで、軍事技術開発の方向性としても大きな意味があったということである。

具体的には、ドローンによる集団攻撃や、高度な自律化などによる高性能の巡航ミサイルは、軍事力のバランス変更に大きな影響を与えている。例えば、原子力空母を中心とする米国の打撃群は米国軍事力の象徴であり、同盟国にとっての守護神だが、多数のドローンなどで攻撃を受けた瞬間、守護神から疫病神に変化する。（被害を被った原子力空母を受け入れて修理する国はあるだろうか？）高性能な半導体やAIによる自律技術と伝統的な軍事力の対比として象徴的な例ではないだろうか。

近年の半導体・通信・AIの進歩はほとんど「産業革命」であり、この新技術を早く使いこなしたところが経済面での利益享受は当然として、軍事技術に導入できた国が覇権国となるというのは、第1次産業革命を制した英国が最初の覇権国となったというアナロジーから納得性があると言えるのではないか。

半導体・通信・AI技術が、「新しい戦争」での覇権ツールである理由を整理すると

① 新しい軍事技術・民間ビジネス発展の根源であること。
② 軍事戦略の前提となる、情報収集能力を圧倒的に強化すること。
③ 特に強権的な政治体制をもつ国にとって、効率的な国内統治のツールであり、体制安定化に貢献すること。
④ 外国への世論誘導・工作のツールであり、選挙を定期的に行う民主主義国家に影響力を与えるには極めて効果的なこと。

と言えると思う。

中国は、これらの新技術を最も理解している「国家」であると考えている。

3　注目すべきポイント

分析すべきことは多数あるわけだが、企業としてまず何をするべきかという観点から取り組むべき問題点を整理すると下記のようになる。

① 通商関連の法規制（制裁・輸出管理等）の拡大と複雑化：（Economic State Craft の拡大）へのリスクマネジメント
② サプライチェーンの変化に対応した事業戦略
③ 技術移転（流出・盗難防止）の管理

安全保障は国家の責任であることは間違いない。しかし、現在の日本の仕組みは安全保障での状況対応に敏速に対応できる状況には遠いと考えるべきである。何もせずに国の対応を待ってそれに協力するということだけではなく、企業としての自己防衛と日本自体の安全保障のために何をすべきかビジネスの現場でも考える必要がある。

本レポートは、このような状況下、国際ビジネスに携わる日本の企業がどのような行動をとるべきかを考察するものである。②のサプライチェーンの見直しは、企業の事業継続に直接的な影響をあるが、このレポートでは触れない。①の法規制強化の方向とその対策を主体に考察し、③の技術移転については、法令強化と重なる部分について触れる。

第２章　法規制の複雑化についての整理（これまでの米国施策と今後の予想）

海外の中で米国の法制度の影響がビジネスに対してしての影響が最も大きいという現実があり、ここでは、制裁政策、次に輸出管理、最後に厳密には法令ではないが、米国が米国企業に求めている自主管理の 3 点について、最近の状況を整理する。

１　制裁

まず制裁について、注目すべき動きを紹介するが、先に結論として重要ポイントまとめると下記となる。

①　米国はこれからも金融制裁を多用する。
②　人権を名目にすることが増え、人権重視がより強調されていく。
③　人権を理由に、監視技術関連（AI・通信を含む）への管理を強化する。

１―１　グローバルマグニッキー法と EO13818

米国の制裁は複雑である。多くの制裁法があり、大統領は法律と同じような効力を持つ大統領令（Executive Order）を発行する権限が与えられている。米国にはすでに多くの制裁法があるが、注目すべきはグローバルマグニッキー法とそれを改正した大統領令 13818 である。グローバルマグニッキー法は、2012 年にできた法律で、人権侵害と腐敗に対する制裁法としては有名なものである。そしてトランプ政権の初期に（2017/12）に「使い易く」改良する大統領令 13818 を発行している。改正のポイントをまず下記表１に示す。これを使った制裁とこの法律を根拠にして新たに成立した制裁法がかなり活用されている。

表１　グローバルマグニッキー法と E013818 による変更のポイント

	Global Magnitsky 法(2012)	EO13818(2017/12)
人権侵害	国際的に認められた人権と自由を獲得、行使、擁護、または促進することを求める個人に対する超法規的殺害、拷問、またはその他の人権侵害	深刻な人権侵害
腐敗	重大な汚職行為(複数･長期間)	汚職

つまり、もとの設計では人権侵害それ自体ではなくて、人権侵害防止を進める個人を、不法に逮捕し処刑等した政府機関・役人が対象ということで、かなり限定的であった。これを、深刻という形容詞は一応あるが、通常の人権侵害に拡大された。腐敗につい

ても、重大な汚職行為という表現に、複数の長期間にわたるというニュアンスがあったが、単なる汚職となったということで、米国政府にとっては相当使い易くなった。
EO13818 での制裁のクライテリアをもう少し詳しく見る意味で、E013818 の対応部分を表 2 に示す。

表 2

<table>
<tr><td></td><td colspan="2">EO13818 による制裁対象クライテリア</td></tr>
<tr><td rowspan="3">基本的なクライテリア</td><td colspan="2">人権侵害行為に責任がある、加担している、あるいは直接的または間接的に関与している者</td></tr>
<tr><td rowspan="2">汚職：現役もしくは元政府関係者、またはその関係者のために行動する者で、以下の行為に責任を負い、加担し、または直接もしくは間接的に関与した者。</td><td>国家資産の不正流用、個人的利益のための私的資産の収用、政府契約や天然資源の採取に関する汚職、賄賂を含む汚職、</td></tr>
<tr><td>汚職の収益の移転または移転の助長</td></tr>
<tr><td rowspan="2">補足的なクライテリア</td><td colspan="2">上記対象が組織（政府機関を含む）の場合、その組織の長</td></tr>
<tr><td colspan="2">関与しようとした者（未遂も対象）</td></tr>
<tr><td rowspan="2">2次制裁的効果</td><td colspan="2">制裁された者に重大な支援（資金・物資・技術的な支援や商品・サービスの提供）をおこなった者</td></tr>
<tr><td colspan="2">制裁された者が所有・支配する組織等</td></tr>
</table>

基本的なクライテリアとしては人権侵害と汚職だが、注目すべき点としては

① 人権侵害には政府関係者の縛りがなくなっている（民間人も対象）。
② 汚職については、汚職による収益の移転を明示的に示している。
③ 基本的なクライテリアで責任があるとした組織の長・責任者を対象とすることや、未遂であっても対象とする包括的に補足する条項がある。
④ 例によって、2 次制裁的な効果を狙う条項が組み込まれている。

等があり、範囲が広がっているのが良くわかる。

日本企業にとって注意すべき点は、2 次制裁効果のある他の米国制裁の場合と同様で、取引先等が対象に指定された場合となる。

このケースは、イラン制裁で2次制裁が強化されたころから、かなりの企業はすでに経験済みですでに熟知されているリスクであるが、改めて列挙すると、

① 日本の銀行はまず決済等の送金業務に応じないので、取引継続は即座に困難。

② その取引先と行う取引が「重大な支援」に当たると見做された場合は、自らも金融制裁の対象となるリスクが生じる。

の2点となる。

１―２　大統領令トランプの 13959 とバイデンの 14032

リスクの観点からは日本の企業には直接的な影響としては少ないのだが、米国の制裁の方向性を見るのに有効だと考えられるので、トランプとバイデンの２つの大統領令（ＥＯ）について説明する。

トランプ政権において、中国の技術開発が米国の資金で行われているという分析のもと、財務長官が指定する中国の軍事関連企業 Communist Chinese Military Company への投資を禁止する大統領令 13959 が発行された。株式は当然として、関連する金融商品等も対象である。あらゆる金融取引を禁止する本格的な金融制裁よりは軽いものだが、一連の中国対策の一環として取られた政策である。

バイデン大統領は、以前は大統領令という制度自体を議会の軽視になると批判していたが、大統領になった後、歴代大統領の最多ともいえるペースで大統領令を発行してきた。内政面でトランプを否定する形のものも多かったが大統領令 14032 は 13959 を改善・強化したという位置づけである。

軍事関連企業＝CCMC の定義は確かにあいまいであり、これを整理したというのが修正のポイントで、

「防衛・調達部門と監視部門で活動した個人または企業」

としたことである。（CCMC という言葉は今も残っている。）13959 は、それ以外にもわかりづらいところが多く評判が悪かったのだが（トランプも一度補正する大統領令 13974 を出している）、監視部門を明示的に標的とした点に留意すべきだと考えている。

１―３　イノベーション競争法で議会が大統領に対して、もっと対中国に活用すべきとした法令

2021 年 12 月の時点では成立していないが、2021 年 6 月に上院で可決されたイノベーション・競争法の中の中国対応法において、議会が大統領に対して下記表 3 にあげる法律で制裁を加えることができる旨を指摘して、もっと積極的にこの法律を使うべきであるという記述がみられる。

表 3

(A) グローバル・マグニッキー法
(B) 国防権限法 2015 Section 1637 (サイバー空間における経済・産業スパイへの対処に関するもの).
(C) フェンタニル制裁法
(D) 香港自治法 (中華人民共和国の香港に関する特定の義務の侵害に関する制裁措置).
(E) 香港人権・民主化法第 7 条(香港における基本的な自由と自治を損ねることに関する制裁の賦課)
(F) ウィグル人権法第 6 条(新疆ウィグル自治区での少数民族の人権侵害に関する制裁措置)。
(G) 輸出管理改革法
(H) 国防権限法 2020 第 1260I 条(Huawei Technologies Co. Ltd.を Entity List から削除することを制限)
(I) 国防権限法 2019 第 889 条(a)(1)(B)(特定の中国企業が製造した電気通信機器またはサービスを使用する事業体との連邦政府契約の禁止)。
(J) 2016 年北朝鮮制裁および政策強化法(22 U.S.C. 9201 et seq.)
(K) 2019 年オットー・ワームビア北朝鮮核制裁及び施行法

さらに、2021 年 12 月には、ウィグル強制労働防止法も成立した。

人権を名目にした本格的な金融制裁（完全な資産ブロック）が含まれている制裁は、A・D・E・F（とウィグル強制労働防止法）であり、金融制裁とはニュアンスが違うものが G・H・I で、それ以外は金融制裁に分類可能だがフルセットではない制裁というものである。いずれにせよ、上院は大統領にもっと中国に制裁を使えと主張している事実自体についても留意すべきである。

２　輸出管理

輸出管理は、技術の流出を防ぐための古典的・典型的な手段である。米中対立が技術戦争であること、さらに、米国の輸出管理法令が再輸出規制・みなし再輸出規制を通じて外国企業も法的に管理対象としているため、過去処罰の対象となった外国企業の例も多数存在し、企業として神経を使わざるを得ない部分である。

２－１　エマージングテクノロジーのリスト化

米中対立が技術戦争であることから、中国へのエマージングテクノロジーを規制する必要があり、その一番手が輸出管理の強化という考え方で、ＥＣＲＡ（Export Control Reform Act）が成立した。2018 年、商務省にはエマージングテクノロジーの迅速なリスト化が期待されていたが、結果としては 2021 年末の段階で当初期待されたようなリストは出てきていない。

このエマージングテクノロジーのリストについては、米国への対内投資管理の規制強化（FIRRMA による）での活用も期待されていたため、特に米国議会では不満が大きい。商務省の部署である BIS の次官補への公聴会などが開かれているが、まだその不満は解消されていない。

２－２　中国向け許可例外の強化

米国を含む国際的な輸出管理には、品目に注目したリスト規制と、その用途に注目したエンドユース規制（キャッチオール規制）の2つのコンセプトがある。米国の輸出管理のリスト規制は、国を細かく分類（ランク付け）して、それぞれの国への規制品目を緻密に管理する仕組みがとられている。これはかなり複雑な仕組みで、詳述はさけるが、一言で言うと

① 国毎に規制される品目を変えている。（国毎に規制リストがある状態になっている。）

② 一定の状況に対して許可が不要となる許可例外（＝LE）の制度があるが、その適用条件も国毎に設定されている。

という手法である。例えば、イランを例にすると、もっとも厳しい輸出管理の対象国であり、その結果、どの国よりも規制される品目が多く、使用可能な許可例外も極めて少なくなっているということである。

この許可例外の制度を 2020 年 4 月に大きく見直し、中国に対して使える許可例外を一部廃止（CIV）、または、対象となる品目などを絞るなどの厳格化をして（APR)、結果として中国向けへの強化を行った。

実は国毎と言っても、いくつかの国をまとめて米国の基準としてカントリーグループというものをつくっており、中国が属するカントリーグループ D に対してその強化をおこなったので、中国以外のカントリーグループ D の所属国がある意味とばっちりを受けたと言える。

２－３　ミリタリーエンドユース（MEU）規制の強化とミリタリーインテリジェンスエンドユース（MIEU）規制の新設

米国の場合、以前より MEU 規制（正確には Military End Use or User Control）の規制があった。簡単に説明すると

- 一定の対象国に対し
- それらの対象国ではリスト規制では許可不要の品目の一部に対して（国際的に規制されていない品目が主体）
  - A　軍隊等が使用する通常兵器を開発・製造する用途に用いられる場合
  - B　軍隊等がエンドユーザーの場合（用途は問わない）

に許可申請の義務を与える規制である。

強化のポイントは下記である。

① 対象国は、中国・ロシア・ベネズエラであったのだが、実は中国のみ上記のBについては免除となっていたが、中国にもBのエンドユーザーの規制を加えた。

② 対象となる一定の品目を大幅に拡大した。（特に半導体・通信関係のかなりの品目を追加した。）

また、「ミリタリーエンドユーザーリスト」を新規に作り、輸出者に周知した。このリストに掲載されていなくても「軍隊等」と見做されればこの規制は適用されるので、「参考」のリストということになるが、軍隊等の定義のなかには軍隊を支援する企業も含まれるので、知らなかったと言わせない状況を整えたということだろう。

また、MEU規制の対象国には、2021年6月にミャンマー、12月にカンボジアが追加された。

MIEU規制は、MEU規制によく似ているが、対象品目がさらに広がり、全品目（EAR99まで）が対象となっている。また、対象国もミリタリーエンドユースの国にイラン、キューバ、北朝鮮、シリアが加わっている。対象となるユーザーの定義は、軍関係の中でも、軍に直結した情報機関となっている。わかりづらいのだが、軍ではなく、政府に直結した情報機関はMIEUではなく、MEUで規制される。（下記、表4参照）

表4　MEUとMIEUの違い

	MEU	MIEU
対象国	中国･ロシア･ベネズエラ･ミャンマー･カンボジア	MEUの対象国 ＋ イラン･北朝鮮･シリア･キューバ
対象ユーザー	● 軍(陸軍、海軍、海兵隊、空軍、沿岸警備隊) ● 国家警備隊 ● 国家警察 ● 政府の情報機関または偵察機関 ● またはこれらを支援する人･事業体	● 情報組織または偵察組織で、下記に属する ■ 軍(陸軍、海軍、海兵隊、空軍、沿岸警備隊) ■ 国家警備隊

２－４　エンティティリスト（Entity List）の活用

輸出許可が必要となる個人・事業体をリストにして、これに掲載されたら輸出許可の義務が生じるのが米国輸出管理規制でのEntity List規制である。用途による規制は概念としては重要であり、輸出者は最終用途を判断するのにそれなりに労力をかけるのだが、「真の用途はその需要者しかわからない。」というのも事実である。法律的には、どこの国でも輸出が行われる時点以前の知識での判断と良いとされるが、知らなかったことを証明する難しさは常につきまとい、輸出管理部門を常に悩ませている。そして用途を決定する際には、需要者からの情報は当然関係するし、需要者が信用できるか？という判断が最終決定の大きな要素になってくる。従い、許可申請が必要な客先をリスト化する規制は、輸出者にとって判断がやりやすい規制である。（日本にも、大量破壊兵器キャッチオールでの外国ユーザーリストが同じような効果を持っている。）

このようなエンドユーザーをリスト化する規制は、わかりやすいという点で規制としては非常に効果的であるが、通常はリストに掲載した企業が所属している国が外交面を含むいろいろな対応策をとってくるので、米国以外の普通の国はその国独自の基準ではあまりやりたくないという事情が存在することも事実である。

この2年間で、米国はエンティティリストに掲載できる根拠（掲載理由）をどんどん増やしており、その中に「人権侵害」も明示的に追加された。根拠を増やしただけではなく、従来からある掲載理由も駆使して掲載する組織を増加させている。

EU では人権侵害に係るキャッチオール規制として、監視に関連する品目が人権侵害的な監視用途に使われた場合であると政府が輸出者に通知した場合に許可が必要となり、輸出者がその事実を知ったときは政府に相談する義務が発生するという人権侵害キャッチオールが開始された。米国では、用途規制として例えば人権侵害用途と知った場合に輸出許可申請義務をあたえるような規制はないが、エンティティリストの掲載理由に人権を加えたことにより、効果的なキャッチオール規制を実現しているとみることもできる。

２－５　直接製品ルールの大改革

米国の輸出管理規制が日本の輸出者を悩ますのは、外国で製造した製品をその外国から輸出する場合であっても、米国の輸出管理規制に抵触してしまう場合があるからである。

米国から米国の品目をある外国へ輸出して、その外国からその品目を再度輸出する場合に、「再輸出」という概念で規制の対象とするのが、米国の輸出管理規制の考え方である。さらにこれに加えて、一定の米国の技術を作って製造した外国の製品は米国の輸出管理の対象であるというルールが存在している。最初から外国にあるので、再輸出という言葉はわかりづらいが、これをその外国から輸出する際にも米国の輸出管理の対象となり、場合によっては米国に対して許可申請の義務が生じるということ。これを直接製品ルールというが、実際問題として、これが適用されるケースは今まではかなり限定的であった。

米国は中国のハイテク半導体に対して影響を与えるため、台湾の TSMC 社が Huawei に対して行う Foundry ビジネス（＝複雑な半導体委託製造）を止めることを目標に、この直接製品ルールを大幅に変更した。Huawei とその関係会社はすでに Entity List に掲載されていたが、旧ルールでは

① 台湾からの輸出を止めたい半導体は米国産の技術が関連していたとしても、直接製品ルール対象となる技術ではないため、直接製品として米国法の対象とすることができず、Entity List に掲載されていても意味がなかった。

② Entity List は輸入者が対象なのだが、グローバル規模で行う Foundry ビジネスでは TSMC が輸出者で Huawei が輸入者というような単純な輸出ではなくもっと複雑なサプライチェーンで構成されていた。

ということから、TSMC から Huawei への輸出を止めることは不可能であった。そのため、直接製品のスタートとなる特定の米国品目の範囲を広げ、半導体関連ではほぼかならず関係してしまうような極めて汎用的な、それゆえ国際的には規制していないような技術まで広げ、半導体関係であればほぼなんでも米国の輸出管理対象にしてしまった。さらに単なる購入者を対象としていた Entity List のルールをサプライチェーンのどこかで関係すれば対象となるように、極めて広範囲とした。

ただ、これだとあまりに影響が大きいため、同時に、Entity List に掲載された Huawei とその関係会社に脚注１（footnote1）をつけ、この脚注１のユーザーのみに改正直接製品ルールが適用されるという形にした。しかしながら、それでもこれは大改革である。Huawei を規制するために、輸出管理規制のかなり根本的な部分まで遡って対応したということであり、日本の感覚ではまずありえないような改正であった。

ここまでの改正をするという事実に、米国の非常な決意が感じられる。ある意味おそろしいほどである。

２－６　今後の動向

２－１で触れた、米国議会の BIS への公聴会で、BIS は次の態度を表明した。（議会は納得していないが）。

① エマージングテクノロジーのリスト化は米国単独ではなく、レジーム（ワッセナーアレンジメント等）を主体に行う。（多国間の規制として行う。）

② リスト規制を行うには、その技術が安定していることと産業界と規制対象となる部分が明確に合意できることが必要であり、このプロセスを無視して拙速な規制は避ける。

③ 中国の技術流出への施策としては、MEU/MIEU/Entity List を活用して対応してきた。効果はでているので、これを継続する。

2021 年の 12 月にバイデン大統領が呼びかけた「民主主義国サミット」において、監視技術の輸出管理を複数国で進めるイニシアティブが発足している。オーストラリア、デンマーク、ノルウェー、米国が発起人であり、すぐにカナダ、フランス、オランダ、英国が参加表明をしている。

EU では監視品目の人権キャッチオールが開始されているし、英国では通常兵器キャッチオールの対象国に中国を追加しさらにキャッチオールの発動要件に、単に通常兵器の開発・製造ではなく、「人権侵害」を加えるように輸出管理法令を改正する方針を発表している。

まだ、確定していない部分が多いが、現在の参加表明国の規制や公聴会での BIS の主張を考えると、この多国間の人権侵害に係る輸出管理はキャッチオール規制型になる可能性が高いと考えられる。さらに、米国では政治腐敗に対しても輸出管理をという主張を開始している。

日本の状況を見ると、2021 年の産構審小委員会の中間報告では先端技術のリスト規制をイメージした多国間の仕組みを日本が主導で進めるべきとの方針があった。それとはやや違う方向性である。日本が主張しているのは多国間（少数有志国間）の先端技術リスト規制ベースの仕組みである。その規制しようとする先端技術を有する国が参加する必要があるので、メンバーも人権輸出管理メンバー国とは多少変わってくる。（例えば、米国・日本・英国・ドイツ・オランダ？＋韓国？）

しかし、リスト規制ベースの多国間取り組みとしても、その目的の明示（なんのための取り組みか？）が必要となる。その時はやはり人権保護を無視するわけにはいかず結局この民主主義サミットでのイニシアティブを無視することはできないだろう。

現在の外為法の体系だと、人権侵害理由での規制は日本ではやりづらい側面があるとの記述も産構審小委員会の中間報告にみられるが、日本としても何とか対応せざるを得ないだろうし、対応すべきことだと考える。

３　米国が米国企業に求める自主管理

文化の問題と言えばそれまでだが、日本の場合法律の遵守は当然として、さらにそれを広げた部分を自主的に管理するという傾向がある。米国の場合は、法律でやるべきこととやってはならないことが単純に決まっていて、分かりやすい面もあった。最近、米国でも日本の仕組みを参考にしたか、企業に社内で体制を整えて法的義務ではない自主管理を要求する傾向が増えてきていると感じられる。

３－１　ビジネスアドバイザリー

新疆ビジネスサプライチェーンアドバイザリーと称して、2020 年 7 月に 4 省庁（国務省・財務省・商務省・国土安全保障省）の合同の文書が出た。まだ、成立していないウィグル強制労働防止法の事前注意喚起の目的かと思われたが、新疆でのビジネスを行う企業に対して、リスクを認識の上、詳細調査(Due diligence)を行いそのリスクを分析した上でビジネを行うことを呼びかける内容であった。

さらに、2021 年 7 月には同じ新疆ビジネスサプライチェーンアドバイザリーとして、2020 年の 4 省庁に加えて、労働省と USTR が加わって 6 省庁合同に発展したものが出された。内容は、昨年のものと基本的なスタンスは変わらないものの、より厳しい内容で、新たに児童労働の防止の視点や監視用装置などが追加されている。

また、同じく 2021 年 7 月には香港ビジネスアドバイザリーも出た。こちらは、香港の自治の侵害を人権侵害として焦点を当てていると言う差はあるものの、基本的なスタンスは新疆ビジネスアドバイザリーと変わらない。どちらも法的効力はないと明記されているが、本格的な規制の前の事前警告のニュアンスが入っているとも考えられる、

３－２　財務省 OFAC の制裁自主管理プログラム（SCP）

2019 年に金融制裁を担当している OFAC でも、企業が制裁リスクに対応し、許可申請等を間違いなく行うために、Sanction Compliance Programs のガイドラインを提示しており、それなりの体制を整えて違反を自主申告した場合に処罰が緩和される可能性を示唆している。

３－３　国務省「国連指導原則を導入するためのガイドライン」

また、国務省は単独で「ビジネスと人権に関する国連指導原則を導入するためのガイドライン」を 2020 年に発行している。これは、「意図的及び非意図的な監視機能を持つ製品やサービス（＝本項では以下「監視品目」とする）」を製造する米国の製造者を対象として、特に「外国政府をエンドユーザとする場合」を想定しているが、人権に関する Due Diligence の基準を示したと解釈している。このガイドライン自体にも、当然法的義務は発生しないが、人権関連の制裁が強化されることを暗示していると言える。

４　全体のまとめ

本章の１の制裁の動向として記載したことと重複するが、制裁を含んで規制全体としての傾向を大きくまとめる。

① 米国は人権を名目とした規制を強化し、それは制裁だけではなく輸出管理などの規制も含まれる。
② 人権を名目に特に、半導体・通信・AI の技術の中枢である先端監視技術分野が主戦場となる。
③ 単純に品目を指定することが難しいため、用途的な規制が主体になるが、その場合企業側の協力も重要となるため、自主管理のガイドラインを推奨している。
④ 影響力を高めるために、多国間の仕組みを使う。（例えば、人権の輸出管理では、多国間版の実質的な「人権侵害 Entity List」のようなものを作るなどが考えられる。）

第３章　日本企業が検討すべき対策

１　考え方

事業を行う上で、調達・市場・製造拠点などの検討に直接影響するのはサプライチェーン政策の見極めと対応であるが、本稿では制裁・輸出管理の問題に絞って考察を行う。また、考慮すべきポイントとして次の点を強調したい。

１−１　想定するシナリオ

人権侵害に対する米国・欧州からの糾弾は今後ますます激しくなると予想する。その根拠は以下の通りである。

- 国際社会からの要求に対して、対応が難しい場合、「内政不干渉の原則」を持ち出すことは常套手段であるが、国連に加盟する以上人権侵害について内政不干渉は基本的には主張できない。
- 中国は自らの統治体制をあたらしい共産主義として民主主義より優れたものとして位置付けている。これに対抗するためには、米国としては大量虐殺禁止条約の立証要件を活用することは自然な流れである。
- 人権侵害防止は WTO ルールを超越できる可能性があり、例えば中国に対して多国間取り組みで先端技術（先端半導体製造技術など）を制限するようなシチュエーションで人権侵害防止を名目とすることを想定しているのではと考えられる。
- また、半導体技術を使用した結果の監視関連の機器や技術についてはすでに米国や EU が明確にターゲットにしている。これは、強権主義国家がその政権維持のための抑圧手段として使えるということから、まさに人権侵害のツールであるだけでなく、前章でも述べたように「新しい戦争」における覇権技術であるからであると考えられる。人権侵害の度合い？としては、監視自体は直接的には虐殺・拷問・強制労働・児童労働に比べれば、まだ軽そうな印象をもつことは禁じ得ないが、この部分が焦点となると予想している。十分な注意が必要である。
- 中国はある分野では、すでに世界でも先端の技術開発力を有しているが、米国は技術の窃盗を利用してきたと主張してきている。その結果技術漏洩については、米国は同盟国にさらに強く対策を要求してくると考えられる。

１−２　対象とすべきリスク

人権侵害防止にかかる制裁等が増える中、当然の帰結として意図せず人権侵害企業と取引をしてしまう可能性は高まり、その結果、

A)　米国の制裁対象と自らがなってしまうリスク

B)　人権団体等から指摘を受けて、風評被害等に晒されるリスク

の2つのリスクが高まり、これらのリスクに対応する対策を構築する必要がある。

また、現在特にスポットが当たっている

C) 情報漏洩のリスク

についても、認識しなくてはならない。技術漏洩はそれ自体が自社にとってのダメージであるだけではなく、輸出管理の視点で違法とされてしまう可能性もある。米国がとにかくどうにかしたい分野でもあり、些細なミスでも一罰百戒の材料とされてしまう可能性がこしばらく高まるだろう。

２　推奨する対策

企業活動において全く当たり前のことだが、適切な情報を集め、適切な知見をもつスタッフが分析し、経営陣で適切な権限をもつものが判断を行い、さらにその判断が確実に実施される体制が必要である。その「適切な」の部分が、おそらく多くの企業にとって従来の「日本の常識」から急速に乖離しつつあるのが現状なのだろう。その根本理由は「国際的な安全保障状況の変化」であり、その中で目の前に現れつつあるリスクが、前項に挙げたものである。当然、安全保障状況の変化がビジネス環境への影響が比べ物にならないくらい大きくなったことに対応するための組織改革が必要になるわけだが、現時点での「正解」は誰もわからないだろう。

以下の対策は、「目前のリスク」への対応であるが、新しい体制を模索するための第１歩でもあると捉えて頂きたい。

２－１　情報収集・分析機能

今後すべての事業戦略（市場戦略・調達戦略・投資戦略等すべて）の策定にあたり、各国、特に米国の制裁法令等のリスクを十分に考慮する必要があり、事業戦略策定時にその要素を織り込める体制が必須となる。一定の知識を有するチーム・スタッフが事業戦略策定のどこかのプロセスで参加できているようにしなくてはならない。その場合、そのようなチームの育成からしなくてはならない場合が普通だろう。会社の組織構造または企業文化などで異なるが、法務部門・輸出管理部門の強化または実戦部隊の事業部門への啓蒙・教育がテーマとなる。関連する米国制裁法等の知識が最初のテーマとなるが、それ自体はそれほど難しいということではない。難しい部分は、制裁や関連する政策が国際情勢に応じて変化が激しいため、その変化をフォローし既存の事業戦略との乖離を分析しつづけることや、それらの政策の背景となる国際情勢・地政学的な情報に慣れ親しむことであると考える。

２－２　ダメージコントロールのシナリオ

人権侵害企業と知らずに取引をしてしまう可能性などは常に存在するため、その時のダメージコントロールの体制を整える必要がある。ダメージコントロールの相手先としては、１－２の通り、

A） 米国の国務省や OFAC

B） 人権団体

と言うことになる。どちらが相手にせよ、良識のある企業としてとるべき対策はとっており、悪意はなかったことを証拠として示すなどして、説明責任を果たす行動が取れるかどうかが基本となる。その結果、相手が米国の政府であれば、にとにかくペナルティを下げ、うまく行けば示談で済む可能性が増加し、相手が、人権団体であれば、一般大衆に「口先だけではなく、本当に調査等行った上でビジネスを行っている」と言う印象をできる限り多く持ってもらうことが可能になる。

この場合の推奨する対策としては、人権侵害排除に重点をおいた「統合取引管理体制」（Integrated Trade Management Program）の導入となる。次章でその概要を解説する。

２－３　情報漏洩対策

法令対応の観点から考えると、今回の見做し輸出の改正への対応ということになるが、すでに一定の輸出管理体制を整えている企業は、今回の改正の対応自体はそれほど難しくない。自社が所有する技術と外為法に照らしてそれが、リスト規制該当かどうかを判断できる下地が基本的にあるはずだからだ。そうではない中小企業はかなり大変だろうが、盗まれるような技術をもつ中小企業は絶対数はそれほど多くないだろうとみて、やや遅れてもリスクが少ないと政府としては考えているのではと想像する。

しかしながら、安全保障の観点から見た場合、本質的な問題は「スパイ対策」である。

さすがに、この部分の法整備は進むと考えており、公式の社内の体制やルール構築はその法整備を待つのが妥当だろう。しかしながら、どんな法律ができようと、次の２つのプロセスが必要になる。

① 採用時にどの程度疑わしいかを会社として判断する。

② その判断結果にもとづき、採用の決定自体や、どのような仕事をさせるか（自社にとって本当に重要な技術と輸出管理での規制対象技術に近づけない等）の判断を、その時点での労働法規等・労働契約等に矛盾しない形で行う。

今回の見做し輸出規制の改正では、輸出管理上の事由での措置が従業員に不利益を与えることもあり得るという FAQ も見られる。しかしながら、すでにできている労働協約・個人との労働契約の関係など実際の状況は非常に多様である。スパイ対策と労働基準法のギャップは大きく、ほとんどの企業では、人事部門は輸出管理や制裁対応になじみがない場合が多いので、人事部門との情報の共有は当然のこと、人事部門を経済安全保障における情報漏洩施策の企画策定に早い段階で参加させることを考えるべきである。

第４章　統合取引管理体制(Integrated Trade Management Program)

１　考え方

第３章での対策としての対応組織の具体的な例示を試みたものである。社内の実態情報を確実に吸い上げることと、いざとなったときの統制、リスクが生じた場合のダメージコントロールの対策である。最初の時点で体制構築に携わる人材の育成が大きな課題となることは間違いないし、この体制ではカバーできない場合も各社の事情で多数あり得ると考えられるので、引き続き委員会で討論を継続して、より具体的な各社の参考になりうるモデルを示していきたい。

２　必要な要素

２－１　専門人材

どのようなコンプライアンス管理体制でも同じだが、米国法務や輸出管理に係る法律知識が一定以上あり、かつ貿易実務などビジネスの現場でどのようなことが起こっているかを知っている人材を揃える必要がある。通常はなかなかそのような人材はいないため、養成から始める必要がある。現在、輸出管理に携わっている人材に一定の教育期間を与え強化する、または法務部門・事業部門からの人材を強化するという対策が必要となる。これらの人材は体制つくりと体制完成後の審査、そして、いざというときのダメージコントロールで重要な役割を果たすことが期待される。また、統合取引管理体制だけの観点ではなく、これらの人材は本稿で議論している新しいリスクへの対応全般にとって重要な役割を果たすことができる。例えば第３章２－１の事業戦略作成時のアドバイザリーチームとしても活用できる。

２－２　経営陣からのコミットメント

「法律を遵守する。」「人権侵害を（自ら）しない、人権侵害を行っている企業との取引停止を含め、人権侵害の促進に繋がる取引を行わない。」などの基本ステートメントがまず必要である。Global Compact や OECD 基準が過去何度か話題となったので、普通はすでにこの手のステートメントは公表されているはずだが、その実行のために「このようなやり方で進める」というところまで踏み込むことが必要である。現時点では、「ビジネスと人権に関する国連指導原則」が妥当と考えている。これは、米国の国務省が推奨していることもあるが、国連加盟国はこれを進める行動計画を作成する義務があり、日本でも 2020 年 10 月に「ビジネスと人権に関する行動計画」が、関係府省庁連絡会議から発表されている。

２－３　対象とする取引範囲

前述の「ビジネスと人権に関する行動計画」では、この統合取引管理体制でのポイントよりさらに広く、特に会社自身の行動について非常に広範囲をカバーしている。それらにはガバナンスとしては事前管理・事前審査がそぐわないものもある。（例えば事前管理より監査を主体とする形にした方が効率的かつ有効な場合がある。）いずれにせよ、まずこの管理体制でどの部分をカバーするかを明示する必要がある。

取引という観点から言えば、販売と調達でカバーできると考えるが、企業によっては研究開発（特に共同研究）も対象取引に加えた方が良い場合がある。また、自身が取引ではなく内部で強制労働などの人権侵害を行なわないなどの視点も無視するわけには行かない。日本の会社は良いとしても、自社が支配する海外拠点への指導なども考慮する必要がある。また、情報漏洩にスパイ対策が求められることを考えると、人事部門等の協力も必要となる。

２－４　組織

前述の取引の範囲を決定するとき同時に考えることであるが、輸出管理より広い範囲をカバーするため、取引の種類（販売・調達・投資・情報漏洩対策・自社の人権遵守の証明など）に合わせて管理組織を設計する必要がある。社内の業務として管轄・管理している組織をうまく組み込む必要がある。

２−５　規程

２−２のコミットメントに従い、組織やポジションを定め、その責任を明確にする必要がある。明確にしようとすると必然的に規程を作成した方が良いと言うことになる。
やり方としては、

① 取引のリスクの大小を判断する基準を決める・
② その基準に沿ってまず、第１次の判断を行い、リスクがあるが継続したい取引には「詳細調査」を行う。
③ 「詳細調査」の結果、ビジネスの当事者以外の責任者が取引の是非を決定する。会社規程での事業本部長とか営業担当取締役が社長を除くビジネス遂行の責任者となるが、一定の場合に「総合取引管理規程」の責任者に差し止めができる権限を与える。
④ 輸出管理規程はどの会社でもすでにあるだろうから、輸出管理規程の上位規程として、輸出管理規程の対象取引は輸出管理規程に依拠する形などが考えられる。（その場合は、輸出管理の取引審査時に人権侵害の視点を追加する必要がある。）

２−６　取引時の調査（取引審査）の具体的方法

規程ではなくその運用細則となる場合もあるが、詳細調査のやり方とその内容を管理部門（最低でも別人格）が確認する。（管理部門の場合は承認する。）を明記する。ここでも、リスクによってやり方は複数あっても良い。

ただし、米国国務省やOFACがガイドラインを出していることから、ガイドラインを参考にして規程や詳細調査の手法を定めている形にしておくのが一つの方法と考える。（問題が起きたときの交渉時に優位に働く可能性がある。）管理部署がそれらのガイダンスの存在を知っており、規程・細則とどのような関係があるかを言えるような状況にしておくべきである。

２−７　取引審査のシステム（ワークフロー）

輸出管理については、成約管理や船積み管理のシステムと統合したシステムを持っているところはほとんどだろうが、輸出管理でカバーできていない取引でも一定の電子システムがないと非効率な状況を生み出す。

２−８　教育や周知体制

規程に盛り込むことは当然だが、行ったことが証明できるようにしておく必要がある。（E-Learningの個人の受講ログや理解度テストの記録などで十分。）

２−９　監査

定期的な監査も、規程に盛り込むことは当然だが、本当に実施して監査記録を残すことは必要。輸出管理の監査と兼ねておき、輸出管理でカバーできない取引は別途適当な期間（毎年でなくても良い）監査を行う形式が妥当と考える。また、対象によっては規程の運用状況の監査だけではなく、詳細調査(Due Diligence)の性格が強いものとなる場合もあるため、何通りかの監査スタイルを設定してく必要がある。

３　具体例（モデルケース）

前項で一般論としてコンセプトを説明した。各社のおかれている事業環境や組織・体制、またそれらの土台になっている企業文化はそれこそ千差万別であり具体例がまるであてはまらない場合がほとんどだろうが、一般論として語るよりも具体例を自社の状況に合わせて評価した方が、理解が深まる場合も多いと考えられるので、一定部分について、具体例を挙げてみたい。

規程等を作成したときの条文で普遍的なものをまず具体例としてあげ、その内容を解説する形で説明する。

３―1　基本方針または目的等

【具体例】

（基本方針）

当社は世界人権宣言（UDHR）及び市民的及び政治的権利に関する国際規約（ICCPR）を尊重し、OECD 多国籍企業行動指針および国連「ビジネスと人権に関する指導原則」に則り、人権を尊重することを基本方針とし、企業活動の原則を下記のように定める。

- 自ら人権侵害となる行為は行わない。万一、人権侵害となる事態が起きた場合にはそれに対処する。
- 自らは直接責任を負わないが、取引関係によるまたは自社の製品もしくはサービスにより人権侵害が発生するおそれがある場合は、その回避又は軽減に努める。

【解説】

前述のように、ダメージコントロール上での留意点は

- 米国の人権関連制裁に対象とならないこと。万一の場合、示談成立・処罰軽減への道を残すこと。
- 人権団体からのクレーム対象とならないこと、万一の場合、風評リスクを極小化すること

である。

規程上の目的は、大きな意味での人権尊重となる。仮に、日本の法律では認められている取引をとりやめるという場合、明確な人権尊重の会社方針（しかも国連のガイドラインにそった）からの判断でとりやめるということができるようにすることである。米国との関係でビジネス上（つまり広い意味で収益的にマイナスなので）判断しているということでは、実際に人権団体からクレーム等を受け対応を迫られた場合に逆効果となる場合も考えられる。

具体的な例を挙げれば、米国の制裁回避のために米国の制裁リストをチェックするということではなく、人権侵害企業とは取引をしない方針を明示して、米国の制裁リストは、人権侵害があった可能性の情報としてチェックしており、その結果人権侵害の疑いが生じ、米国の制裁回避ではなく、人権侵害の可能性を否定できないので取引を停止するということである。

また人権侵害の定義だが、一般的な人権ということで問題はないのだが、米国国務省の「ガイドライン」では、人権の定義として下記の国際宣言等を推奨している。従いこれに触れる形で目的または基本方針を記述している。

- 世界人権宣言（UDHR）
- 市民的及び政治的権利に関する国際規約（ICCPR）
- OECD 多国籍企業行動指針
- 国連「ビジネスと人権に関する指導原則」

国連「ビジネスと人権に関する指導原則」II. 人権を尊重する企業の責任 A.基本原則13には下記の記述があり、これを企業側のからの言葉となるように作成した。

13. 人権を尊重する責任は企業に以下の事項を要求する。

- *企業活動による人権への悪影響の惹起またはその助長を回避し，惹起した際には対処すること。*
- *企業活動と直接関連する，または取引関係による製品もしくはサービスに直接関連する人権への悪影響については，企業がその惹起に寄与していなくても，回避又は軽減に努めること。*

３－２　組織等

【具体例】

（取引統括管理最高責任者）

1 基本方針に基づき、人権を尊重する企業活動を確実に行うために、代表取締役又はそれに相当するものを取引統括管理最高責任者とする。

2 取引統括管理最高責任者は以下の業務を行う。

（1）本規程の制定改廃

（2）統括管理部門の設置

（3）取引審査の最終判定

（統括管理部門の業務）

統括管理部門は下記の業務を行う。

1 懸念取引先リスト･懸念国リスト･懸念品目リストの作成と改正

2 取引審査票起票ルールの作成と改正

3 取引審査票の承認または否認

【解説】

単純化した方がイメージをつかみやすいとの判断から、一元管理モデルとしてあるが、実際の場合は、取引の種類毎に個別に規程を作った方がスムーズに進む場合が多いのではと考える。この場合の取引の種類とは主に下記のようなものとなるだろう。

① 販売（＝輸出管理）

② 調達

③ 投資

④ 海外拠点管理

３－３　取引審査等

【具体例】

（懸念取引先リスト）

1 取引先の分類：

統括管理部門は、別表（参考3が例示）に示す情報ソース等を確認し、最高責任者の承認のもと取引先を下記のように分類する。

A　懸念取引先：統括管理部門が人権侵害を確認した先またはその懸念が極めて高いと判断した取引先で、原則として取引を認めない先。（その時点で過去の取引実績がない事業体を含む。）

B　準懸念取引先：統括管理部門が人権侵害を行っているまたは何らかの関与している可能性があると判断したが、取引する品目等によっては取引を認める可能性がある取引先

C　一般取引先：上記 A・B に該当しない取引先

分類 A・分類 B の取引先を合わせて懸念取引先とする。

2 事業部門は新しい取引先と取引を開始するため、取引先登録を行う際に取引審査票を提出し、統括管理部門の承認を得なくてはならない。

3 統括管理部門は定期的に、懸念取引先と一般取引先の状況を調査し、懸念取引先の分類や一般取引先を懸念取引先リストに掲載しなくてはならない場合は、その旨を全社に周知しなければならない。

4 事業部門は、懸念取引先と取引を行う場合、又は、当該取引に懸念取引先が関与する情報を得ている場合は、取引審査票を統括管理部門に提出し、同部門の審査を経て、最高責任者の承認を得なくてはならない。

（懸念品目リスト）

1 統括管理部門は、取引を行う品目について人権侵害懸念が高いと考えらえる品目を懸念品目リストに掲載する。

2 懸念品目は取引の種類（販売または調達）毎に設定する。

3 懸念品目は対象国ごとに設定することができる。

4 事業部門は、取り扱う品目が懸念品目リストに掲載されている場合は、取引先が一般取引先であっても取引審査票を統括管理部門に提出し、取引推進の承認を得なくてはならない。

（懸念国リスト）

1 統括管理部門は取引の対象となる国を評価し、人権侵害が報告されている国、人権侵害がおこなわれている可能性が高いと考えられる国を懸念国リストに掲載する。

2 事業部門は取引の対象国が懸念国リストに掲載されている国の場合は、取引先・品目にかかわらず取引審査票を統括管理部門に提出し、取引推進の承認を得なくてはならない。

（取引審査票）

1　取引先が一般取引先であり、懸念取引先の関与も確認されておらず、品目・対象国がそれぞれの懸念リストに掲載されていない場合でも、当該取引が人権侵害に関与しているという情報を得た場合は、事業部門は統括管理部門に相談しなくてはならない。統括管理部門が取引審査票の提出が必要と判断した場合は、統括管理部門に取引審査票を提出する。

2　取引先が一般取引先であり、懸念取引先の関与も確認されておらず、品目・対象国がそれぞれの懸念リストに掲載されておらず、人権侵害に関与しているという情報がない場合は、営業部署は取引審査票を提出する必要はない。ただし、当該取引に関し成約責任をもつものは、リストに掲載されていないこと等を確認した日時を記録し保存しなくてはならない。

【解説】

この項は、米国国務省のガイドラインを参考にしている。

同ガイドラインでは、一律ではなくリスクベースの人権 Due Diligence を推奨しているが、そのリスク評価として、国務省・財務省・商務省がそれぞれの制裁リスト等の確認をまずあげており、さらに扱う商品・サービス（＝品目）とその用途の評価を行うこととしている。（前述のように、監視品目の管理を強く志向している。さらに、監視品目を国家が人権侵害目的につながる用途に使わせないことを最大の目的としている。）

また、強制労働の観点では新疆ウィグル地区での生産品目を管理しなくてはならない。さらに、リスクベースのアプローチとして、そのような行為をしそうな国家かどうかを判断せよとしている。

当然、中国を意識しているわけだが、中国のみならず、中国が支援する強権主義の国（中国が監視システムの構築に協力している）も含まれている。

（懸念取引先リスト）

取引先管理が米国の制裁管理の主要部分となる。従い、米国の制裁リストの意味合いを理解したうえで、その掲載状況をできる限り迅速に把握し、自社の取引先との関係について確認をする体制が必要となる。勿論、米国のリストに掲載されているのは必ずしも人権理由だけではないため、明確に人権理由でないものは準懸念先として掲載することを一応想定している。また、参考３に情報取得用のソースを示すが、これは米国国務省ガイドラインが推奨しているリソースである。

（懸念品目リスト）

リスクベースのアプローチとして、どのような製品・サービスが（場合によってどのような国で）リスクが高いかという視点を入れた方が、より緻密な管理ができるという判断である。販売の場合と調達（外注を含む）場合で、懸念品目が異なることも想定してい

る。これは各社の事業内容によるところが多いと考えられる。米国・欧州の懸念の焦点であることから監視品目に特に注意を払う必要があるが、実際問題としては監視品目自体の定義はかなりむずかしい。実際問題としては用途と合わせて判断していく必要があるだろう。

（懸念国リスト）

リスクベースのアプローチで、国として人権侵害可能性が高いか否かを管理する体制は導入する必要がある。懸念品目リストを懸念国別に設定した場合は、例示のケースより、もう少し複雑なルールになりうる。これは精緻な管理をするという意味合いもあるが、懸念のない国を明確にするために懸念国を決めるという考え方でもある。懸念国を懸念度でランクを付け運用を変えるやり方もありうる。

（取引審査票）

管理を行ったという証跡である。大きくリスクを取引先・品目・対象国で判断して、リスクの高い部分を洗い出すということになる。

取引審査に対して、統括管理部門が判定をする。機微な場合は最高責任者が最終判定を行うことになる。

最終判定の結果は

① 取引不可
② 保留（更に緻密な Due Diligence を行うことを指示。）
③ 条件付きの承認
④ 承認

となると想定している。

取引審査自体で、すでに Due Diligence を行っていると言えるがが、建前としては Due Diligence の最初の段階であり、第 2 段階の Due Diligence を行ったうえで判断というのが②の意味合いである。第 2 段階の Due Diligence としては営業部署以外の専門チーム（場合によっては監査チーム）または外部第 3 者によるインタビューや実地調査ということになるが、ほとんどの場合は困難だろうから、②を行うのは例えば人権侵害の噂がたったが、取引を継続したい状況で、噂自体が怪しいのでそれが間違いであると示すことが必要な場合等に限定されると考えている。

③の条件付きの承認は大きく分ければ 2 つのケースが考えられる。

一つは、既存の取引先が制裁の対象となった場合で、基本的に取引を停止したいが契約上・商道徳上即時に取引停止が難しい場合である。その場合に、既存の契約が終了するまでとかの条件で継続を認めるというようなことになるだろう。

もう一つは小さいながら懸念が残る場合、例えば懸念情報があることにはあるのだが、その情報自体の信憑性がそれほど高くないような場合である。

いずれにしても常に完全な情報が入手できることはまずないので自信をもって正確だと断言できない場合は常に存在する。そのときに保全措置を前提として、取引推進に条件を付ける形になる。

保全措置の典型的なものは、自社の人権方針を明示したうえで、取引先と下記について合意をする。（契約内容に盛り込むまたは、誓約書等を入手する。）

① （取引先が）自ら人権侵害行為はしていない・今後もしない。
② 販売先または委託先に人権侵害がないことを確認して取引する。
③ その取引先自身またはその販売先や委託先に対して、人権侵害団体やシンクタンクまたは外国政府から人権侵害の疑いを指摘されるような事態が起きた場合、当社に実情を説明し、間違いであることを証明するか、あるいは委託先にそのような事実があった場合は解決する。
④ 一定期間の猶予の後、当社として人権侵害が解決できたと判断できない場合、契約をキャンセルする。

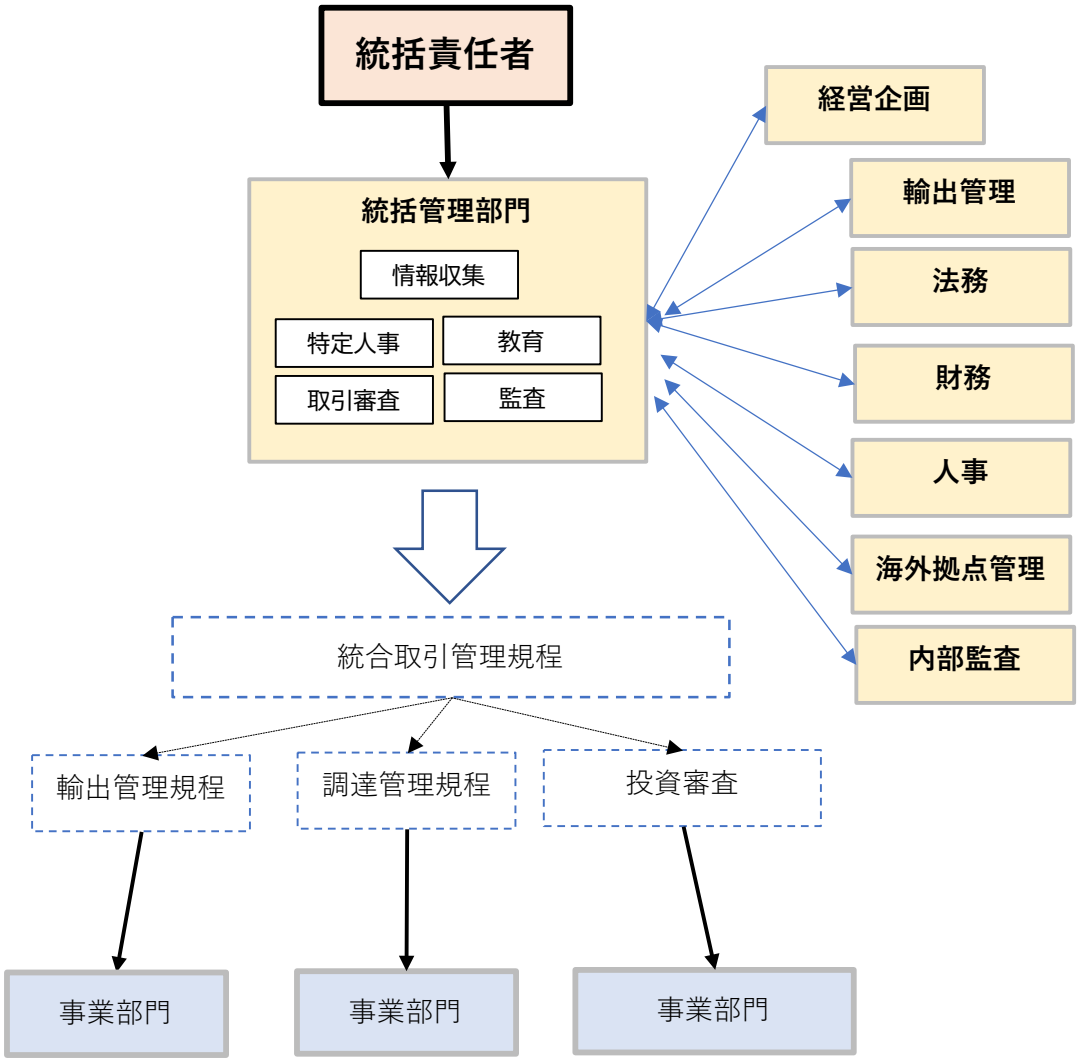
市場での力関係ということになるが、仮に自社の製品に優位性があり、メンテナンス等のサービスが必須のような場合は、単純なキャンセルではなくてメンテナンスサービスの停止など、状況に応じて相手先に影響力のあるやり方を選択するオプションもありうる。

今後の国内の法整備にもよるが、法律上の白黒ではなくて、自主判断となるため、統括管理部門には、その判断が尊重されるように一定の権限を与える必要がある。

以下、参考として
参考１　今回の例示の仮想的な組織イメージ図
参考２　今回の例示のフローのイメージ図
参考３　統括管理部門が参考にすべき情報ソースの参考例として、米国国務省の「Guidance on Implementing the UN Transaction Linked to Foreign Government End-Users for Products or Services with Surveillance Capabilities」の Appendix 1 HUMAN RIGHTS TOOLS, REPORTS & GUIDANCE の和訳版（私訳）を添付する。

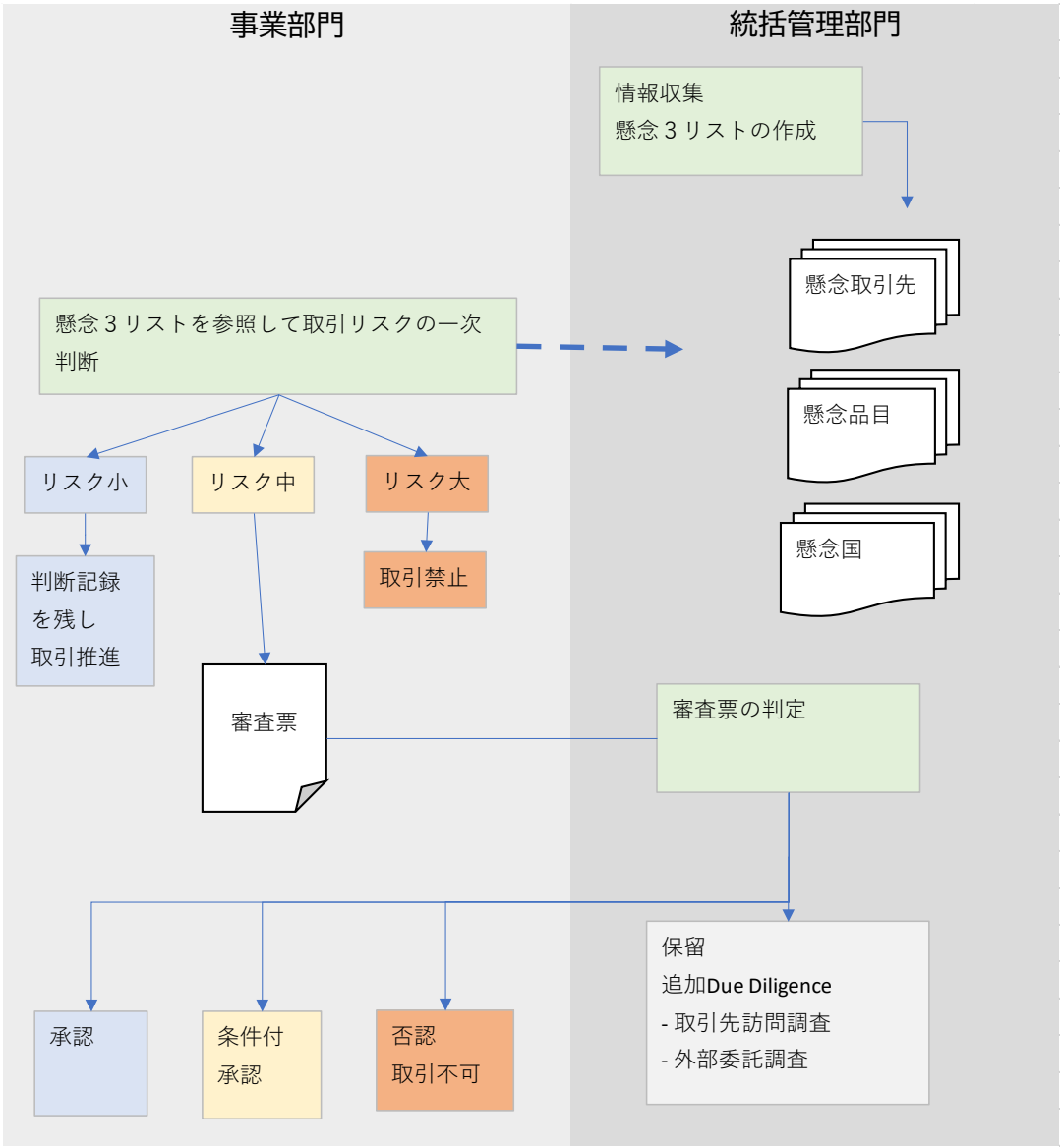
以上

参考１　組織イメージ図



- 統括責任者は管理部門を統括する役員であることが望ましい。
- 統括管理部門と各管理組織間はスタッフの兼務を想定。
- 統括管理部門内の BOX は行うべき業務だが、将来的にはチームとするイメージ

参考２：業務フローイメージ図



1. 統括管理部門は懸念３リスト（懸念取引先・懸念品目・懸念国）を作成、リスク一次判断のルールを設定する。
2. 事業部門は、取引を行う前に、リスク一次判断のルールに基づき、リスクの大小を判断。
   (a) リスク大　取引禁止
   (b) リスク中　取引審査票を起票して統合管理部門の判定を求める
   (c) リスク小　リスク小と判断した根拠・記録を残し、取引推進。（監査時にその記録はチェックされる）
3. 統括審査部門は取引審査票を審査し
   (a) 追加 Due Diligence の必要がある場合は、この手配を行う。
   (b) 事業部門に対して、取引不可・条件付き承認・承認を戻す。

参考 3　HUMAN RIGHTS TOOLS, REPORTS & GUIDANCE 訳

情報ソース又はツール	説明	更新頻度
米国政府の情報又はツール		
U.S. Department of State Country Reports on Human Rights Practices https://www.state.gov/reports-bureau-of-democracy-human-rights-and-labor/country-reports-on-human-rights-practices/	世界人権宣言やその他の国際文書で定められている、国際的に認められた個人、市民、政治、労働者の権利を網羅。報告書には、外国の政府機関に関する具体的な情報を含む。	毎年
U.S. Department of State Investment Climate Report https://www.state.gov/investment-climate-statements/	世界の 170 以上の経済圏のビジネス環境に関する情報を提供する。米国企業にとって市場となりうる様々な経済を分析。トピックは、投資への開放性、法的規制システム、紛争解決、知的財産権、透明性、パフォーマンス要件、国有企業、責任ある企業行動、汚職など。	毎年
米国政府外のツール・レポート・イニシアティブ・ガイダンス		
Access Now https://www.accessnow.org/	新しい技術がもたらす脅威を追跡し、緩和するための市民社会の取り組みを支援している。レポートはコンテンツタイプ別、地域別に分類されている。	随時頻繁に
Africa - State of Internet Freedom in Africa Report https://www.accessnow.org/	過去 20 年間の政府のインターネットコントロールの傾向をマップ化したもの。	毎年
Africa - Digital Rights in Africa Report https://paradigmhq.org/report/digital-rights-in-africa-report-2018/	監視技術に関連するアフリカのデジタル権についての報告。	毎年
Amnesty International https://www.amnestyusa.org/tools-and-reports/reports/	報告書は、監視を含む様々な問題に関する人権侵害のパターンを記録したものです。報告書は課題別、国別に作成されています。	随時頻繁に
The Citizen Lab https://citizenlab.ca/	ウェブサイトでは、市民社会に対するデジタル・スパイ活動の調査、インターネット・フィルタリングやその他のオンライン上の表現の自由に影響を与える技術や慣行の文書化、一般的なアプリケーションのプライバシー、セキュリティ、情報管理の分析、個人データや監視活動に関する企業と政府機関の関係に関連する透明性と説明責任のメカニズムの調査などを行っている。 個人情報やその他の監視活動に関する企業と政府機関との関係に関連する透明性と説明責任のメカニズムを検証する。	随時頻繁に
Civicus https://monitor.civicus.org/	インタラクティブな世界地図を作成し、シビックスペースの動向に関する最新情報を提供している。 また、より詳細なレポートも掲載されている。	随時頻繁に
Committee to Protect Journalists https://cpj.org/	報道機関への攻撃や報道の自由を妨げるものについての国別報告書	毎年
CYRILLA https://cyrilla.org/	デジタル著作権に関する法的情報の共有、比較、視覚化を容易にするオンラインデータベース	毎月
Freedom in the World Report https://freedomhouse.org/report/freedom-world	世界各国の政治的権利と市民的自由の状況を評価。 195 の国と 14 の地域について、数値による評価と説明文が掲載。	毎年
Freedom on the Net Report https://freedomhouse.org/report/freedom-net	ネットの自由度を国別にランク付けして評価し、最新の動向をグローバルに概観し、詳細な国別レポートを掲載。この報告書には、色分けされた地図が含まれており、自由、一部自由、自由ではないとランク付けされている。	毎年

Global Network Initative (GNI) and Country Legal Framework Resource https://clfr.globalnetworkinitiative.org/	表現の自由とプライバシーに関する GNI 原則は、関連する実施ガイドラインとともに、インターネットおよび通信技術産業とその利害関係者に、世界的な人権の享受を保護し促進するための指針を提供している。 各国の法的枠組みに関する資料では、世界の表現の自由とプライバシーに影響を与える法的環境を調査している。	定期更新はウェブサイトで通知
Global Surveillance Index https://carnegieendowment.org/2019/09/17/global-expansion-of-ai-surveillance-pub-79847	176 カ国の AI 監視利用に関する実証データをまとめている	2019/9 月発行
Human Rights Watch Country Reports https://www.hrw.org/countries	世界各地の人権侵害に関する報告と調査。	毎年
Latin America – CELE https://observatoriolegislativocele.com/en/	ラテンアメリカにおける表現の自由と情報へのアクセスに焦点を当てた法律の分析	随時頻繁に
Ranking Digital Rights Corporate Indicators https://rankingdigitalrights.org/	デジタルプラットフォーム、サービス、デバイスの提供者に対して、人権、特にプライバシーと表現の自由に関する公的な報告に関するガイダンスを提供。	毎年
World Justice Project Rule of Law Index https://worldjusticeproject.org/our-work/research-and-data/wjp-rule-law-index-2019	世界 126 の国と地域において、一般市民が法の支配をどのように経験し、認識しているかを測定している。	毎年
国際条約、原則、ガイダンス（厳選されたもの）		
International Covenant on Civil and Political Rights (ICCPR) https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx	ICCPR は、1966 年に国連で採択された国際人権条約である。米国政府は 1992 年にこの条約を批准し、プライバシーに対する恣意的または違法な干渉から自由である権利や、表現の自由の権利など、この条約で規定されている人権を保護・保全する義務を負っている。	
OECD Guidelines for Multinational Enterprises http://mneguidelines.oecd.org/guidelines/	OECD 多国籍企業ガイドラインは、各国政府が加盟国で活動する多国籍企業に宛てた勧告である。拘束力のない原則と基準を提供している。 ガイドラインは、適用される法律および国際的に認知された基準に沿った、グローバルな文脈における責任ある企業行動のための拘束力のない原則および基準を提供するものである。本ガイドラインは、各国政府が推進を約束した、多国間で合意された唯一の責任ある企業行動の包括的な規範である。OECD ガイドラインは、国連の「ビジネスと人権に関する指導原則」を参考にし、これに沿ったものとなっている。米国政府のナショナルコンタクトポイントは、OECD ガイドラインに関連する問題が発生した場合、紛争解決および調停メカニズムを提供する。	
OECD Due Diligence Guidance on Responsible Business Conduct http://mneguidelines.oecd.org/guidelines/	OECD ガイドラインに基づき、2018 年 5 月、OECD は責任ある企業行動のための新しいデューデリジェンスガイダンス（以下、「ガイダンス」）を発表した。ガイダンスは、OECD ガイドラインに基づく企業のデューデリジェンス責任について詳しく説明している。これは経済のすべてのセクターで、規模や地理的な位置にかかわらず、すべての企業が使用することを目的としている。 バリューチェーンの位置に関係なく、すべての経済セクター、すべての企業が使用することを目的としている。その主な目的は、企業がデューディリジェンスの責任を理解し、実行するのを助けることである。本ガイダンスでは、リスクと影響について明示的に言及し、企業がこれらのリスクと影響を特定して対処する必要性を強調し、その方法について推奨している。	

UN Guiding Principles on Business and Human Rights https://www.oecd.org/investment/due-diligence-guidance-for-responsible-business-conduct.htm	2011 年に国連人権理事会のコンセンサスを得て承認された指導原則は、国と企業が、企業による人権への影響を防止、対処、救済するためのグローバルなガイドラインである。	
UN Universal Periodic Review https://www.ohchr.org/en/hrbodies/upr/pages/uprmain.aspx	普遍的定期審査（UPR）は、すべての国連加盟国の人権記録を審査するものである。UPR は、国連人権理事会の支援のもと、国が主体となって行うプロセスです。 UPR は、国連人権理事会の下で行われる国家主導のプロセスであり、各国が自国の人権状況を改善し、人権上の義務を果たすためにどのような行動をとったかを宣言する機会となっている。	

第５章　まとめ
安全保障状況変化がもたらす新たなビジネスリスクとその対応について

Ⅰ　国際ビジネス環境における安全保障状況の重要な変化

１　はじめに

安全保障は国家の存在意義の最も根源的な部分であり、安全保障と経済を分離することはできないのだが、特に日本では完全な別物という風潮が主流であった。

近年、各国の「安全保障上の制約」を受けるリスクが多大に増加し、今までは気にする必要がなかった安全保障目線での調査や分析が必須となった。

２　変化の本質とは？

経済安全保障の問題が最近になって表面化してきたのは、米国が中国の経済的な発展とそれを支える技術発展・技術開発力を最も脅威と感じているからである。

中国は軍民融合政策を巧妙に使い、「産業革命」ともいえる新技術（半導体・通信・AI）を国家として発展・利用する体制を作り上げたが、これらがまさしく覇権技術である。その理由を整理すると下記のようになる。

① 新しい軍事技術・民間ビジネス発展の根源であること。
② 軍事戦略の前提となる、情報収集能力を圧倒的に強化すること。
③ 特に強権的な政治体制をもつ国にとって、効率的な国内統治のツールであり、体制安定化に貢献すること。
④ 外国への世論誘導・工作のツールであり、選挙を定期的に行う民主主義国家に影響力を与えるには極めて効果的なこと。

３　注目すべきポイント

企業としてまずするべきことの観点から、取り組むべき問題点は下記の通り整理できる。

① 通商関連の法規制（制裁・輸出管理等）の拡大と複雑化:（Economic State Craftの拡大）へのリスクマネジメント
② サプライチェーンの変化に対応した事業戦略
③ 技術移転（流出・盗難防止）の管理

国の対応を待ってそれに協力するということだけではなく、企業としての自己防衛と日本自体の安全保障のために何をすべきか、ビジネスの現場でも考える必要がある。

Ⅱ　法規制の複雑化についての整理（これまでの米国施策と今後の予想）

ビジネスに対しては、米国の法制度の影響が最も大きいという現実がある。ここでは、制裁政策、輸出管理、自主管理の 3 点について、最近の状況を整理する。

１．制裁

制裁について、注目すべき動きの重要ポイントまとめると、下記の通り整理できる。

①米国はこれからも金融制裁を多用する。

②人権を名目にすることが増え、人権重視がより強調されていく。

③人権を理由に、監視技術関連（AI・通信を含む）への管理を強化する。

米国にはすでに多くの制裁法があるが、法令関連で注目すべきは、グローバルマグニッキー法を大統領令 13818 で改正したことにより、人権侵害理由での制裁が非常に容易になり、それを根拠にした法律の制定や、実際の制裁行使が行われていることである。それに加えて 2021 年 12 月の時点では成立していないが、2021 年 6 月に上院で可決されたイノベーション・競争法の中の中国対応法で上院は大統領にもっと中国に制裁を使えと主張していることを留意すべきである。

２　輸出管理

米中対立が技術戦争であること、さらに、米国の輸出管理法令が再輸出規制・みなし再輸出規制を通じて外国企業も法的に管理対象としているため、企業として神経を使わざるを得ない部分である。輸出管理において米国が進めてきた動きとしては、以下のものがある。

・エマージングテクノロジーのリスト化
・リスト規制における中国向け許可例外の強化
・ミリタリーエンドユース（MEU）規制の強化とミリタリーインテリジェンスエンドユース（MIEU）規制の新設
・エンティティリスト（Entity List）の活用
・直接製品ルールの大改革

今後の方向としては、輸出管理の管轄省庁である商務省 BIS の下記発言に注目すべきである。（議会がエマージングテクノロジーのリスト化が十分でないとう判断で開いた公聴会での発言）

① エマージングテクノロジーのリスト化は米国単独ではなく、レジーム（ワッセナーアレンジメント等）を主体に行う。（多国間の規制として行う。）

② リスト規制を行うには、その技術が安定していることと産業界と規制対象となる部分が明確に合意できることが必要であり、このプロセスを無視して拙速な規制は避ける。

③ 中国の技術流出への施策としては、MEU/MIEU/Entity List を活用して対応してきた。効果はでているので、これを継続する。

これは、多国間での協調を主力にすることと、中国への対応をリスト規制ではなく、用途・需要者への規制を主力で行うことを示している。更に、バイデン大統領が民主主義サミットにおいて、人権侵害に着目した輸出管理のイニシアティブを発表したことを考えると、米国の方向性は日本の産構審の中間報告で示された一部の高度な技術を持つ有志国による新しいレジーム（リスト規制ベースが予想される）との構想とは一部合致しない面もあり、日本としては微妙な対応が必要となろう。

3　米国が米国企業に求める自主管理

米国政府が企業に体制を整えて法的義務ではない自主管理を要求する傾向が増えてきている。その事例を以下に示す。

・ビジネスアドバイザリー（新疆ビジネスサプライチェーンアドバイザリー、香港ビジネスアドバイザリー）（追記：2022 年 1 月末にはミャンマービジネスアドバイザリーも発表された。）
・財務省 OFAC の制裁自主管理プログラム（SCP）
・国務省「ビジネスと人権に関する国連指導原則を導入するためのガイドライン」

4　全体のまとめ

制裁を含めて規制全体としての傾向を大きくまとめると以下の通りとなる。

① 米国は人権を名目とした規制を強化し、それは制裁だけではなく輸出管理などの規制も含まれる。
② 人権を名目に特に、半導体・通信・AI の技術の中枢である先端監視技術分野が主戦場となる。
③ 単純に品目を指定することが難しいため、用途的な規制が主体になるが、その場合企業側の協力も重要となるため、自主管理のガイドラインを推奨している。
④ 影響力を高めるために、多国間の仕組みを使う。（例えば、人権の輸出管理では、多国籍版の実質的な「人権侵害 Entity List」のようなものを作るなどが考えられる。）

Ⅲ　日本企業が検討すべき対策

1　対象とすべきリスク

人権侵害に対する米国・欧州からの糾弾は、今後ますます激しくなると予想される。人権侵害防止にかかる制裁等が増える中、意図せず人権侵害企業と取引をしてしまう可能性は高まり、その結果、A)米国の制裁対象と自らがなってしまうリスク、B)人権団体等から指摘を受けて、風評被害等に晒されるリスク　の２つのリスクが高まり、これらのリ

スクに対応する対策を構築する必要がある。また、現在特にスポットが当たっている、C)情報漏洩のリスク　についても認識しなければならない。

２　対策

国際的な安全保障の変化がビジネス環境への影響が比べ物にならないくらい大きくなったことに対応するための組織改革が必要なことは明白だが、各企業にとっての「正解」を示すことは困難だが、それを模索するためのポイントを示す。

- 情報収集・分析機能の強化
  上記を担当するスタッフに対して、米国の制裁政策関連知識を必須に政策の背景となる国際情勢・地政学的な知見を付与すること。あるいは最初から育成すること。
- ダメージコントロールのシナリオの準備
  １のA)B)に示すリスクが発生をできる限り避ける体制を作っておくことが、不運にも発生してしまった場合の最良のダメージコントロールにつながる。人権侵害排除に重点をおいた「統合取引管理体制」（Integrated Trade Management Program）の導入を推奨する。次章でその概要を解説する。
- 情報漏洩対策
  昨今の安全保障状況の変化が「スパイ対策」を要求しているということであり、自社の重要な技術を防衛するために更に厳密な情報漏洩対策が必要になっている。労働関連法令との整合性に留意する必要もあるため、人事部門を早い段階から関与させるべきである。

Ⅳ　統合取引管理体制（Integrated Trade Management Program）

ダメージコントロールの対策としては、管理体制をあらかじめ作っておくことである。その為の要素を説明した上で、具体例（モデルケース）を示すが、そこは本編を参照願いたい。

- 専門人材
  体制を構築するにも、管理・維持するためにも米国制裁や国際情勢・地政学的な知見を有するスタッフが必要である。また、これらのスタッフは事業戦略策定時等にも活用できる。このスタッフの育成がいずれにせよ重大な要素である。
- 経営陣からのコミットメント
  経営陣からのコミットメントは当然の要素であるが、「ビジネスと人権に関する国連指導原則」を参照することを推奨する。
- 対象とする取引範囲の設定
  販売・調達・共同研究・海外拠点管理等が考えられるが、各企業の状況に合わせて取り決める必要がある。

- 組織

  取引の種類（販売・調達・投資・情報漏洩対策・自社の人権遵守の証明など）に合わせて管理組織を設計する必要がある。既存の社内の管理組織をうまく組み込む必要がある。

- 規程

  基本的な管理の流れを定めるため規程を作る必要があるが、下記のような形を提案する。

  ① 取引のリスクの大小を判断する基準を決める。

  ②その基準に沿ってまず、第１次の判断を行い、リスクがあるが継続したい取引には「詳細調査」を行う。

  ③「詳細調査」の結果、ビジネスの当事者以外の責任者が取引の是非を決定する。

  輸出管理規程はどの会社でもすでにあるだろうから、輸出管理規程の上位規程として、輸出管理規程の対象取引は輸出管理規程に依拠する形などが考えられる。（その場合は、輸出管理の取引審査時に人権侵害の視点を追加する必要がある。）

- 取引時の調査（取引審査）の具体的方法

  米国国務省や OFAC がガイドラインを出していることから、それらを参考にして詳細調査の具体的な方法を定めることを推奨する。

- 取引審査のシステム（ワークフロー）

  輸出管理等ですでに使用しているシステムの拡大等を検討すべきである。

- 教育や周知体制

  実施の証明ができるように記録することがポイントとなる。

- 監査

  体制の監査が必要だが、日々の取引審査より監査の方がより有効な場合もあるため、いくつかのタイプの監査を考えておく必要がある。

＜参考＞

2021 年度検討会開催一覧

開催日	会合名	講演名と講演者
7/19（月）	通商・セキュリティテーマ第 1 回検討会	「産業構造審議会　通商・貿易分科会　安全保障貿易管理小委員会　中間報告」 経済産業省　貿易経済協力局　貿易管理部長　風木 淳　氏
		「バイデン政権下の米中対立とデカップリングの進展」 みずほリサーチ＆テクノロジーズ株式会社　調査部　主席研究員　菅原 淳一　氏
		「複雑化する輸出管理と日本企業の課題」 日本輸出管理研究所　代表　高野 順一　氏
10/19（火）	通商・セキュリティテーマ第 2 回検討会	「米中対立下のサプライチェーン再構築と機械産業への影響」 専修大学　商学部　教授　池部 亮　氏
11/2（火）	通商・セキュリティテーマ第 3 回検討会	「イノベーション競争法案から見る「米国の本気」」 日本輸出管理研究所　代表　高野 順一　氏
1/17（月）	通商・セキュリティテーマ第 4 回検討会	「報告書の議論」 みずほリサーチ＆テクノロジーズ株式会社　調査部　主席研究員　菅原 淳一　氏
		「報告書の議論」 日本輸出管理研究所　代表　高野 順一　氏

非売品
禁無断転載

2021 年度ポストコロナの
製造業グローバル・バリューチェーン変革
に関する調査研究報告書
Ⅱ．セキュリティ　編

発　行　　2022 年 3 月
発行者　　一般社団法人　日本機械工業連合会
〒105-0011
東京都港区芝公園三丁目 5 番 8 号
電　話　０３－３４３４－５３８３