

Back Number

本論文は

世界経済評論 2022年5/6月号

(2022年5月発行)

掲載の記事です



世界経済評論

定期購読のご案内

年間購読料

1,320円×6冊=7,920円

6,600円

税込

17%

送料無料

OFF

富士山マガジンサービス限定特典

※通巻682号以降

定期購読
期間中

デジタル版バックナンバー読み放題!!



世界経済評論 定期購読



☎0120-223-223

[24時間・年中無休]

お支払い方法

Webでお申込みの場合はクレジットカード・銀行振込・コンビニ払いからお選びいただけます。
お電話でお申込みの場合は銀行振込・コンビニ払いのみとなります。

Fujisan.co.jp
雑誌のオンライン書店

経済安全保障と サイバーセキュリティ



川口 貴久

東京海上ディーアール 主席研究員

かわぐち たかひさ 1985年生まれ。専門は国際政治・安全保障、リスクマネジメント。2008年横浜市立大学卒、10年慶應義塾大学大学院政策・メディア研究科修了。慶應義塾大学グローバルリサーチインSTITUTE客員所員など兼任。近著に『ハックされる民主主義：デジタル社会の選挙干渉リスク』（土屋大洋との共編著、千倉書房、2022）他。

新型コロナウイルス感染症（COVID-19）感染拡大に起因する供給途絶や激化する米中対立を背景として、日本国内で経済安全保障に関する議論が加速化している。2022年通常国会で成立見込みの経済安全保障推進法案は4つの柱から構成され、サイバーセキュリティの観点では特に「基幹インフラの安全性・信頼性の確保」が重要である。これは一定規模以上の基幹インフラ事業者が重要な機器やサービスなどを調達する際、外部からのサイバーリスクがないかを政府が事前に審査するものだ。対象となる事業・事業者・設備は限定される見込みだが、指定事業者以外でも大きなインパクトを持つだろう。また民間企業は、経済安保推進法案の成立を経済安保対応の「終わり」ではなく「始まり」とみるべきだ。例えば、データをめぐる経済安保リスクは今回の法案で重点的に扱わないが、外国政府によるサイバー攻撃や強制的なデータアクセス（ガバメントアクセス）に代表されるようにデータは経済安保の最前線の一つである。今日、企業のリスクマネジメントやサイバーセキュリティに経済安全保障や地政学リスクを考慮することは必須だ。

I 急速に高まる経済安全保障問題

日本政府は2021年から22年にかけて、経済安全保障に関する法整備を加速化させ、民間企業にとってはこの問題に対応することが経営課題となっている。

「経済安全保障」とは、経済的手段によって政治的目標を達成することと定義され、非常に広範な分野・領域が含まれる。米国などでは

「地経学（geoeconomics）」「エコノミック・ステイトクラフト」とも呼ばれる。

経済安全保障は目新しい考え方ではない。日本ではかつて、1970年代にエネルギー、食糧、シーレーンなどを含む「総合安全保障」が提唱された。大平正芳首相が設置し、総合安全保障の検討を行った研究グループも「経済的安全保障」に言及していた。具体的な定義を明示していないものの、「経済的安全保障」を（軍事的な意味での）「狭義の安全保障」と対置させ、

表1 経済安全保障をめぐる政官財の主な動向（2022年2月上旬時点）

2019年	3月	与党	自民党ルール形成戦略議員連盟（会長：甘利明）が提言『国家経済会議（日本版 NEC）創設』を公表
	6月	政府	経済産業省大臣官房に経済安全保障室を設置
2020年	4月	政府	内閣官房国家安全保障局に経済班を設置
	6月	政府	改正外為法の施行
	11月	財界	経済団体連合会（経団連）が提言。「新成長戦略」を公開し、「主體的かつ戦略的な経済安全保障の確保」を提唱
	12月	与党	自民党新国際秩序創造戦略本部が提言「『経済安全保障戦略策定』に向けて」（本部長：岸田文雄，座長：甘利明）を公表
2021年	2月	財界	「国際経済外交総合戦略センター」発足（経団連加盟企業を中心とする新組織）※産経報道
	4月	財界	経済同友会が提言「強靱な経済安全保障の確立に向けて：地経学の時代に日本が取るべき針路とは」を公表
	5月	政府	一部民間企業への経済安保担当役員の設置要請 ※日経報道
		与党	自民党新国際秩序創造戦略本部が提言「中間とりまとめ『経済財政運営と改革の基本方針2021』に向けた提言」を公表（自民党は10月12日、「新国際秩序創造戦略本部」を「経済安全保障対策本部」に改組）
	6月	国会	国家安全保障上の土地取引規制法成立
	10月	政府	経済安全保障担当大臣の設置
		財界	新経済連盟が提言「デジタル経済下のシン・成長戦略」を公表
	11月	政府	経済安全保障推進会議（第1回）の開催
政府		経済安全保障法制に関する有識者会議の設置	
2022年	2月	政府	有識者会議が重点4分野の提言を内閣総理大臣に提出
		財界	経団連が「経済安全保障法制に関する意見：有識者会議提言を踏まえて」を公開
	(予定)		通常国会にて、経済安全保障推進法案が提出・成立の見込み 年内に「国家安全保障戦略」策定の見込み

注：※箇所は、「経済安保の担当役員設置，政府が主要企業に要請へ」日本経済新聞（2021年5月3日）；「〈独自〉経済安保協議の新組織発足へ 経団連企業を中心」産経新聞（2021年7月2日）より作成。

出典：筆者作成。

経済を安全保障の目的および手段として位置付けた¹⁾。

だが、近年では激化する米中対立、新興技術をめぐる競争、地政学的対立を背景としたサイバー攻撃の増加などを背景に、再び「経済安全保障」が注目を集めている。特に2019年以降、与党・自民党、内閣官房や経済産業省などの行政、経団連・同友会・新経連などの財界団体はこの問題に対応してきた（表1）。新型コロナウイルス感染症（COVID-19）感染拡大に起因する医療物資の供給途絶は、政府による経済安

保対応をさらに推し進めた。

とりわけ、岸田文雄政権下の2022年10月、経済安全保障担当大臣が新設され、小林鷹之代議士が任命されて以降、法制度化の動きが加速する。翌11月には、総理を議長とする経済安全保障推進会議が開催され、22年通常国会で経済安全保障推進法案が提出される見込みだ。

II 背景としての米中対立

このように経済安全保障への注目が高まる背

図1 米中の名目 GDP

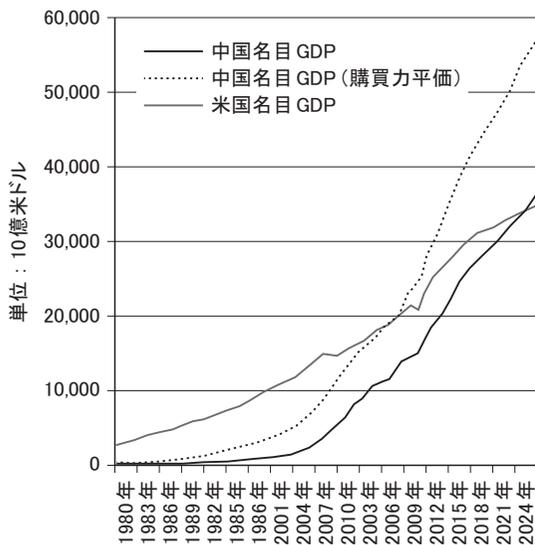
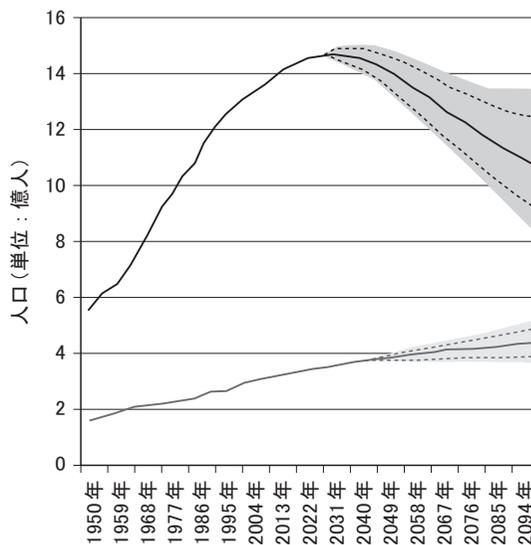


図2 米中の人口動態



出典：(図1) ① 1980-2020年は実値。② 2021-2026年はIMF予測。International Monetary Fund, World Economic Outlook (WEO) Database, World Economic and Financial Surveys (October 2021 Edition)。③ 2027-2035年は2027年以降の名目GDPの平均成長率(%)は米国1.5-2.0%、中国3.5-4.0%と仮定して算出(詳細は割愛)。(図2) United Nations, Probabilistic Population Projections based on the World Population Prospects 2019より作成。太線は実値(2018年以前)および中位推計値(2019年以降)、点線は80%の予測区間、網掛部分は95%の予測区間を表す。

景には、激化する米中対立がある。米中は互いに投資、輸出管理、サイバーセキュリティなどの分野で規制を強化している。

こうした現状は「限定的な米中デカップリング」と呼べる。すなわち、軍事的覇権を左右しうる先端技術の開発、重要物資のサプライチェーン、重要インフラのサイバーセキュリティなど、安全保障に近い分野では既に米中分断が存在し、企業は米中「二者択一」を迫られているということだ。

「限定的な米中デカップリング」は米国前トランプ(Donald J. Trump)政権の対中政策のみに起因するものではなく、米国に対して台頭する中国という中長期的な趨勢・構造、米国側では党派を超えた対中国観・対中競争戦略、中国の長期戦略などに起因する。

1973年の米中国交正常化以来、米国の対中

政策の基本的な考え方は「関与政策(engagement policy)」であった。米国が中国に対して関与を継続することで、中国は市場・経済改革を進め、政治的には民主化し、国際社会で重要な責任を果たすという考え方だ。だが、こうした米国の関与政策は第2期オバマ政権期頃から見直された²⁾。

トランプ政権下の国家安全保障戦略(17年12月)は、「中国とロシアは修正主義国家」とした上で、従来の対中政策の誤りを認める。「何十年もの間、米国の政策は、中国の台頭と戦後の国際秩序への統合を支援することが、中国を自由化するという信念に根ざしていた。しかし、我々の期待とは裏腹に、中国は他者の主権を犠牲にしてその力を拡大した」。バイデン(Joe Biden)政権下の「暫定版の安全保障戦略指針」(21年3月)でも、中国を「経済的、外

交的、軍事的、技術的パワーによって、安定的かつ開放的な国際システムに持続的に挑戦が可能な唯一の競争相手」と位置付ける。

他方、中国も建国 100 周年にあたる 2049 年までに、社会・国家、軍事・安全保障、経済・産業といったあらゆる分野で米国を凌駕し、世界における主導的立場を目指す長期戦略・計画を掲げる。2015 年には「中国製造 2025」（のちに「中国標準 2035」へと発展）を掲げ、「軍民融合」を国家戦略に格上げした。米国は、中国が「中国製造 2025」「軍民融合」の名の下に、国際ルールで禁じられた技術の強制移転を行っていると判断する。具体的には、市場アクセスや許認可と引き換えにした技術移転、中国政府の指示に基づく企業買収、サイバー攻撃による知財窃取等である。

近年では、中国もまた経済安保関連の立法措置を講じる。典型例は、輸出禁止・輸出制限技術リストの改訂（20 年 8 月）、信頼できないエンティティ・リスト制度の制定・施行（20 年 9 月）、反外国制裁法の制定（21 年 6 月）、データセキュリティ法の制定・施行（21 年 9 月）だ³⁾。

そして今後、「米中逆転」の時期が訪れる可能性が高い。2033-34 年には名目 GDP で中国が米国を抜き去り（図 1）、2030 年頃までに西太平洋における米軍の軍事的優位性が揺らぐ。他方、中国の総人口は 2030 年頃から減少に転じ（（図 2）生産年齢人口のピークアウトはさらに早い）、近い将来、米中の「再」逆転が生じるかもしれない——。中国にしてみれば、2030 年前後は、米国と既存の国際秩序に挑戦できる「機会の窓」との見方もある。

Ⅲ 経済安保推進法案とサイバーセキュリティ

米中は「経済」を武器に、地政学的な競争を激化させ、覇権を争っている。こうした現状認識および中期見通しが、今日の経済安保議論につながり、岸田政権は 22 年通常国会で経済安全保障推進法案の成立を目指す。

法案の骨子は、①重要物資や原材料のサプライチェーンの強靱化、②基幹インフラの安全性・信頼性の確保、③官民で重要技術を育成・支援する枠組み（官民技術協力）、④特許出願の非公開化による機微な発明の流出防止の 4 点だ（表 2）。

サイバーセキュリティの観点では特に「基幹インフラ」が重要だ。

この施策の背景には、一度、安全保障リスクがある機器やサービスなどが基幹インフラ内に埋め込まれた場合、事後的にこうしたリスクを除去することは極めて困難という認識がある。

法案の趣旨は国民生活や経済活動に不可欠な基幹インフラに、外部からの不正機能の埋め込みや脆弱性の探索を未然に防ぐこと、つまりサイバーセキュリティ強化である。

「外部」とは、もちろん国内事業者も含まれる。事実、経済安全保障法制に関する有識者会議の提言（22 年 2 月）も、事業者の国籍や資本のみをもってリスク評価・判断することは適切ではない、とする。

だが、念頭にあるのは特定の外国政府・軍・情報機関やその影響下にある企業であることは明らかだ。具体的には中国、ロシア、北朝鮮などを意図していると考えてよい。

そもそも米国のように特定国・特定企業を名

表2 経済安全保障推進法案の骨子：法制上の手当てが必要な4分野

サプライチェーンの強靱化	<ul style="list-style-type: none"> ●特定国への依存度が高い重要物資や原材料（例：半導体や医療関連機器など）の供給途絶リスクを回避するための措置。 ●サプライチェーンの実態を調査した上で特定物資の特性に応じて多様な取り組み（生産基盤の整備、供給源の多様化、備蓄、生産技術の開発・改良等）を講じるもの。
基幹インフラの安全性・信頼性の確保	<ul style="list-style-type: none"> ●国家及び国民の安全に影響を与える事業・事業者が重要な設備（関連する情報システム、維持管理の委託先、クラウドサービスを含む）を調達する際、そのサイバーセキュリティ上の安全性・信頼性を政府が事前審査するもの。 ●想定する具体的事業分野はエネルギー、水道、情報通信、金融、運輸、郵便。
官民技術協力	<ul style="list-style-type: none"> ●宇宙・海洋・量子・AI・バイオ等の分野における先端的な重要技術を開発するため官民の協力体制を構築するもの。 ●具体的には、経済安保重要技術育成プログラム等の資金支援、官民伴走の協議会設置、専門的見地で助言するシンクタンクの新設等。
特許出願の非公開化	<ul style="list-style-type: none"> ●国家安全保障上極めて機微な発明の特許出願を非公開とするもの。あわせて、機微な発明の流出を防ぐための措置（違反時には罰則あり）、非公開化の審査対象となる発明の日本国への第一出願義務を定めるもの。

出典：経済安全保障法制に関する有識者会議「経済安全保障法制に関する提言」（2022年2月1日）を基に筆者作成。

指して、政府調達・重要インフラ調達から排除を試みる国は少数派だ。例えば、豪州政府は18年8月、第5世代移動通信システム（5G）調達について、「オーストラリアの法律に違反するような外国政府からの指示に従う可能性のあるベンダーの関与」はリスクであると発表した。

こうした安全保障上の懸念のあるベンダーは平時における機密情報窃取のみならず、有事ではインフラの機能妨害・破壊活動をもたらさう。ウクライナとロシアの軍事衝突の懸念が高まる22年2月14日、米国土安全保障省サイバーセキュリティ・インフラセキュリティ庁（CISA）は、ロシアによる電力や通信等の重要インフラに対するサイバー攻撃は「戦力投射の重要要素」として警鐘を鳴らした。潜在的標的はウクライナのみならず、米国をはじめとする第三国も含まれる、という。同様に台湾海峡有事のリスクが高まった場合、日本の重要インフラは破壊的サイバー攻撃の潜在的な標的だ。

民間企業にとって特に重要な関心は、自社がこうした事前審査の対象になるか否かだろう。

現時点で想定されている基幹事業は大分類では、エネルギー、水道、情報通信、金融、運輸、郵便の6分野（メディアではこれを細分化し、14業種と報じている）である。さらに、事業者の指定にあたっては、企業規模や地域における市場シェア等も考慮されるため、極めて限定される。

なお、法案などで指定される業種と、サイバーセキュリティ基本法にいう「重要社会基幹事業者」（いわゆる「重要インフラ事業者」）との関係は自明ではないし、一部の与党幹部からはより幅広い業種を指定すべきとの意見もある。

いずれにせよ政府による事前審査の対象は限定される見込みだが、指定事業者以外でも大きなインパクトを持つだろう。

仮に自業界や自社が基幹インフラに指定されなくても、上場企業であれば、法案の趣旨や情報インフラの「安全性・信頼性の確保」という観点から、事前審査で期待される水準と同程度に自社の重要設備、サービス、業務委託先の精査を行うべきだ。

法案は、法律上の最低限の要求事項を示しただけに過ぎず、「非」基幹インフラ事業者は自社の経営判断としてどこまでやるかを求められる。

IV サイバー分野の残された課題： データをめぐる経済安全保障

経済安保推進法案の背景や射程をふまえると、法案の成立は、経済安保対応の「終わり」ではなく「始まり」とみるべきだ。秋の臨時国会以降では人権対応状況の開示やセキュリティクリアランスも議論されるだろう。また、年内に新たな「国家安全保障戦略」が策定され、経済安保推進法案に限定されない「経済安全保障」が盛り込まれる見通しだ。

そもそも与党・自民党の経済安保提言（21年5月）では、サイバーセキュリティは様々な分野を横断する大きな柱の一つだった。しかし、経済産業省所管事項が中心ともいえる経済安保推進法案ではサイバーセキュリティは相対的に小さな扱いとなった。

経済安保推進法案は重要な一歩だが、本来、経済安全保障とサイバーセキュリティでカバーすべき論点・施策が全て盛り込まれているとは言い難い。例えば、今回の法案であまり触られていないサイバーセキュリティ関連の課題は、「21世紀の石油」たるデータをめぐる問題だ。

今日、ビジネスに関連する様々なデータを収集し、利活用することがどの産業でも重視されている。しかし、こうした大量のデータは安全保障上のリスクにもさらされている。その一つが、政府による強制力をもった民間企業保有データへのアクセス、いわゆる「ガバメントア

クセス」である。

ガバメントアクセスは刑事捜査などの一環としてどの国でも従来から行われてきた。だが、近年、懸念されているのは、諜報目的や産業振興目的でのガバメントアクセスである。

これを可能にするのは、外国企業に対して、自国内にデータを保存するように要求し、第三国移転を禁止・制限する法制度、「データローカライゼーション規制」である。その典型は、個人データを対象とする欧州「一般データ保護規則（GDPR）」、産業データを対象とする中国「データセキュリティ法」である。外国企業のデータを物理的に自国領土内におくことで、法執行権限を及ぼすことができる。

だが、日本国内にデータを保管していれば安心というわけではない。外国の委託先企業などを通じた「越境アクセス」のリスクがあるからだ。

2021年3月、日本の大手コミュニケーションアプリの中国関連会社が、日本国内に保管された個人データにアクセスしていたことが判明した。法令違反があったわけではないが、経済安全保障上の観点から懸念が生じた。

実際、中国は世界各国の国民データの収集に注力している⁴⁾。中国の国家情報法は中国企業に対して「国家情報工作」への協力を求める。そして、正式な令状や行政からの依頼があるならともかく、実際にどれほど「外国政府」からのアクセスがあるかは分からない。こうした状況から、中国からの「越境アクセス」が経済安保上の懸念としてみなされたといえる。

システムの開発や運用を海外企業に委託する日本企業は少なくないし、海外のクラウドサービスを使っていない企業は皆無だろう。どの企業でも同じような懸念は生じる。

そのため、経済安保推進法案の「基幹インフラの安全性・信頼性の確保」でも、運用委託先会社やクラウドサービスの事前審査が盛り込まれたのだろう。

企業はガバメントアクセスをはじめとする安全保障リスクを考慮して、データの管理を行う必要がある。データの保存先や運用委託先としての「国・地域」という観点では、民主主義の成熟度は重要な指標の一つだ。議会は情報機関に対する監視・監督権限を持つのか、司法は情報機関の活動に権限を与える（与えない）ことができるのか、権力から独立したメディアは行政をチェックできるのかは、不当なガバメントアクセスのリスク量を押し量ることができる。

もちろん、どの国でも不当なガバメントアクセスは生じうる。かつてエドワード・スノーデン（Edward Snowden）事件で明らかになったように、米国でも違法ないし不適切なアクセスは存在しうるが、米国ではこれを公に批判することが許される。

ある国が実際にサイバー攻撃に従事しているかどうか重要な判断要素だ。中国政府は否定しているが、中国以上にサイバー空間上で企業の機密情報と個人データを継続的に狙う国はない。

データの保管場所や委託先所在国として、どのような国・地域が許容されるのか。日本政府としての想定を推察することもできる。

林芳正外務大臣は専門誌『外交』のインタビューの中で、経済安保分野での国際ルール形成、サプライチェーン、そして「データのフリーフロー」での各国とのハーモナイゼーション（協調・連携）を提唱する。具体的には、「同盟国アメリカ、同志国（like-minded countries）のヨーロッパ諸国やクアッド（日米豪印）」な

どを例示する⁵⁾。

「データのフリーフロー」とは、正確に言えば「信頼性のある自由なデータ流通（Data Free Flow with Trust: DFFT）」のことで、安倍晋三総理（当時）が2019年1月、ダボス会議で提唱した。データの自由な流通をめぐる対立は、自由主義と権威主義という対立軸のみならず、米国と欧州の間にも存在する。データの「自由な流通」と「安全」を両立させ、こうした米欧対立を解決する一つの考え方がDFFTである。林外相のコメントをふまえると、国レベルでは米国、西欧、豪州、インドは「with Trust」があると考えても良いのだろう。

しかし、データの保存「国」や委託先企業の所在「国」のみに依存した判断も危うい。委託先企業の資本関係や株主、経営者、創業の経緯、重要なビジネスパートナーに関する実態を詳細に調査するデューデリジェンスは必須だ。一部の重要インフラ事業者では、既にクラウドサービスを利用する際にそうしたデューデリジェンスがルール化されている。

V 経済安保・地政学リスクを考慮したサイバーセキュリティ態勢

経済安全保障や米中対立といった地政学リスクは企業経営に直結する課題だ。企業は経済安全保障を考慮したガバナンス、リスクマネジメント態勢を構築する必要がある。組織の意思決定、情報収集・分析、リスク評価、対外コミュニケーションで安全保障の観点を確保すべきだ⁶⁾。

サイバーセキュリティ分野についても同様である。

経済安全保障を考慮したサイバーセキュリ

ティとは、脅威として単なる個人のハッカーや犯罪集団だけではなく、外国の軍・情報機関を想定するということだ。攻撃手法はサイバー攻撃に加えて、自らの管理・影響下にある企業製品・サービスを通じた情報窃取・破壊活動、民間企業関係者のリクルーティング（産業スパイなどへの勧誘活動）など多岐にわたる。したがって、調達機器や委託先の精査のみならず、前提となる基本的なサイバーセキュリティ態勢やセキュリティ投資、データマネジメント、内部犯や人的セキュリティ対策も必須だ。

また法令順守は民間企業にとって最低限のラインであり、法令だけを遵守していればよいという話ではない。経済安保推進法案の基幹インフラで例えるならば、政府の事前審査の対象となるか否かは重要だが、全てではない。仮に事前審査の対象外の企業や設備であっても、自社の事業やリスクをふまえて法案の趣旨と同程度の水準を目指すべきだろう。少なくとも内部での議論・検討は必須だ。むしろ法令の要求事項ではないが故、企業としての自主的なリスク判断が求められる難しさがある。

経済安保推進法案の成立は経済安保対応の「終わり」ではない。民間企業はますます加速

するであろう経済安全保障政策・動向をふまえて、リスク管理やサイバーセキュリティ態勢を高度化させる必要がある。

(2月15日脱稿)

【注】

- 1) 政策研究会・総合安全保障研究グループ（議長：猪木正道）「総合安全保障研究グループ報告書」（1980年7月）。データベース「世界と日本」（代表：田中明彦）より。https://worldjpn.grips.ac.jp/documents/texts/JPSC/19800702_01J.html
- 2) 東京大学・佐橋亮によれば、米中国交正常化以降の米国の対中政策の基調は支援と関与政策であった。その背景には米中間の国力差に加えて、米国が中国に関与を続けることで、中国は①経済・市場改革を進め、②政治改革を行い、③既存の国際秩序を受け入れて国際社会で貢献を果たす、という将来に対する3つの期待があった。しかし、米国の対中政策の見直しは、米中間の国力差が縮小し、3つの期待が裏切られたと認識したことに起因する。佐橋亮『米中対立：アメリカの戦略転換と分断される世界』（中央公論新社、2021年）、162-163頁。
- 3) 津上俊哉「中国の『経済安保戦略』で確実に押さえておくべき3つのポイント」nippon.com（2022年2月2日）より抜粋。https://www.nippon.com/ja/in-depth/a07902/
- 4) 川口貴久「中国が狙う世界の国民データと諜報活動」WEDGE Infinity（2022年2月5日）https://wedge.ismedia.jp/articles/-/25654
- 5) 林芳正、田中明彦「経済安全保障に不可欠な同志国とのハーモナイゼーション」『外交』Vol.71（2022年1・2月）、6-14頁。
- 6) 詳細は、川口貴久・柴田慎士「経済安全保障を考慮したガバナンス・リスクマネジメント態勢」『リスクマネジメント最前線』2021-6（2021年8月23日）。https://www.tokiorisk.co.jp/publication/report/riskmanagement/pdf/pdf-riskmanagement-355.pdf



YouTube

動画配信・世界Econo.Bizセレクト

国際貿易投資研究所ではYouTubeによる動画配信を行っています。
ホームページよりアクセス可能です。(https://iti.or.jp/)

【主な動画配信】ITI（国際貿易投資研究所）連続セミナー「チャイナ+1としてのメコン」第2回「メコン地域における一帯一路の現状と展望：CLMを中心に」藤村 学（2022.3.16）／ITI（国際貿易投資研究所）連続セミナー「チャイナ+1としてのメコン」第1回「タイ、新興投資国として高まる存在感」牛山隆一（2022.3.16）／世界経済評論 2022年3・4月号 著者を囲む読者座談会（90分）—世界Econo.Bizセレクト No.24—（2022.3.2）／「イスラーム金融と国際基準：望まれるコンベンショナル金融との連携強化」世界経済評論インパクト No.2403（22.01.24付）金子寿太郎 世界Econo.Bizセレクト No.23（2022.2.25）／世界経済評論 2022年1・2月号 著者を囲む読者座談会（90分）—世界Econo.Bizセレクト No.22—（2022.1.4）

一般財団法人 国際貿易投資研究所 (ITI) TEL：03(5148)2601 / FAX：03(5148)2677
〒104-0045 東京都中央区築地 1-4-5 第37興和ビル3階 E-Mail：jimukyoku@iti.or.jp/ URL：https://iti.or.jp/