

中国の最近の輸出規制とその関連動向（第2版）

－2022年秋以降の動向を中心として

2023.1.31／同 2.27 第2版

CISTEC 事務局

2022年秋以降に、中国の輸出規制とその関連で動きがあったので、概要を紹介する。

第2版の追加分は、赤字で表記。

【全体の構成】

1. 「中国輸出禁止・輸出制限技術リスト」改正に関してパブコメ草案を公開（2022.12.30）
2. 輸出管理法に基づく両用品リストの定例改正（2022.12.30）
3. データ安全法体系による「重要データ」の越境移転規制と輸出管理法の規制との関係
4. 学術論文データベース企業「知網」に対する独禁法及び国家安全法等による調査
5. 政府調達における国産品優先／外国製品排除の動向
6. 「信頼できないエンティティ・リスト」に米国2社を初掲載
7. 「反スパイ法」修訂草案二審稿が公表

【参考1】《重要データ識別規則（意見募集稿）》における「重要データ」等について
（抄訳）

【参考2】《情報安全技术 ネットワークデータ処理安全要求》（2022年11月1日実施）
（抄訳）

1. 「中国輸出禁止・輸出制限技術リスト」改正に関してパブコメ草案を公開（2022.12.30）

- 「中国輸出禁止・輸出制限技術リスト」は、対外貿易法下の技術輸出入管理条例に基づいて、WTO加入当時から定められていた。これが、2020年8月末に、当時の米中緊張の流れの中で、一部の調整（追加、修正、削除）が行われ、ハイテク技術（新興技術的なもの）が大幅に追加されたという経緯がある。

当時の追加については、以下の資料のP6～を参照されたい。

- ◎中国における「信頼できないエンティティ・リスト」、「輸出禁止・輸出制限技術リスト」の施行について（2020年9月23日）

<https://www.cistec.or.jp/service/uschina/30-20200923.pdf>

- その後大きな動きはなかったが、昨2022年12月30日に商務部より、同リスト改正に関してパブコメ草案が公開された。

<http://fms.mofcom.gov.cn/article/tongjiziliao/202212/20221203376696.shtml>

上述の2020年8月の一連の調整（追加、修正、削除）は、技術品目が追加されたものの、リスト「改正」ではなく、既存リスト（2008年施行）は廃止されず、そのまま存続した上で、調整が加えられたものだった。

他方、今回は正式に「改正」となり、2020年8月の調整を含めた2008年版は廃止されて、新たに2023年版としてまとめられた形となっている。

○改正概要は添付の通り、2020年調整内容を織り込んだ上で、「削除条目32件、修正条目36件、追加条目7件」とされている。

その概要については、中国の環球法律事務所が解説を出しており、わかりやすく分類している。

◎《中国禁止出口限制出口技术目录》修订并公开征求意见（2023.1.19）

<http://www.glo.com.cn/Content/2023/01-20/1001344473.html>

同解説では、次のように指摘されている。

- ・削除された技術品目のほとんどは、農業、食品、繊維、化学、機器製造などの伝統的な産業に属しており、ハイテク産業関連の削除はほとんどない。
- ・2020年のリスト改訂で追加された技術品目は、「建設機械の応用技術」を除き、保持されている。
- ・既存品目は、技術例、説明の追加、パラメータの増加などを通じて、各技術品目の制御ポイントを詳細に調整するために変更されている。
- ・今回の追加では、生物研究、希土類、太陽光発電、スマートカーなどの技術品目が追加され、政策立案者が国家安全保障と公共の利益を保護するという考えが示された。

○追加・改正された主な技術条目は、次のようになっている。希土（レアアース）部分、パソコン部分は、規制要件も記載した。

（輸出禁止部分）

1. 番号：217501J

技術名称：ヒトに用いる細胞クローンとゲノム編集

2. 番号：213301J

技術名称：希土の精製、加工、利用技術

規制要件：

1. 希土の抽出・分離工程技術
2. 希土金属及び合金材料の製造技術
3. サマリウムコバルト、ネオジム鉄ボロン、セリウム磁性体の調製技術
4. 希土類カルシウムオキシボレーートの調製技術

(輸出制限部分)

1. 番号：210105X

技術名称：農作物雑種強勢利用技術

2. 番号：213106X

技術名称：太陽光発電シリコンウェーハ製造技術

3. 番号：213509X

技術名称：バルク材料積み卸し輸送技術

4. 番号：214014X

技術名称：レーザーレーダーシステム

5. 番号：217501X

技術名称：CRISPR ゲノム編集技術

6. 番号：217502X

技術名称：合成生物学技術

7. 番号：053301X

技術名称：非鉄金属の冶金技術

規制要件：

- 1.無毒（シアン化物を含まない）ヒープリーチング法による金浸出技術と配合
- 2.酸化アルミニウム生産中の母液から原液中のガリウムを回収する「融解法」技術
- 3.強度が $\geq 520\text{MPa}$ のベリリウム材を製造する製粉、固結方法
- 4.次の特性を同時に持つ高温超伝導線、テープの製造技術
 - (1) 臨界温度 $> 77\text{k}$ 、長さ $> 100\text{m}$ 、臨界電流密度 $> 1 \times 10^4\text{A/cm}^2$ （77K、自分の電界強度で）
- 5.次の特性を同時に持つ高温超伝導薄膜の製造技術
 - (1) 臨界温度 $> 77\text{k}$ 、面積 $> 5\text{ cm}^2$ 、臨界電流密度 $> 1 \times 10^4\text{A/cm}^2$ （77K、電界強度0で）
6. 稀土類の採掘、選鉱、製錬技術（既に輸出禁止に掲載された技術を除く）
7. 稀土抽出剤の合成工程及び配合
8. 金属材料の稀土改質・添加技術

8. 番号：214006X

技術名称：コンピュータ中核ハードウェア製造技術

規制要件：

- 1.スパコン（演算回数 ≥ 97 兆回）の製造技術
 - (1) 全体設計技術
 - (2) 本体、OSの技術
 - (3) 本体、サブマシン、周辺設備の製造と開発技術
- 2.パラレルコンピュータマルチインタフェースメモリ高速通信メカニズムを実現

する技術

3. パラレルコンピュータ全対称マルチプロセッサのバスと中断制御の設計技術

○稀土（レアアース）関連については、2008年版では輸出禁止になっていたものが、今回の2023年版では輸出制限に移転されて緩和されているものもある一方、一部で輸出禁止対象が強化されたり、輸出制限部分にも、規制要件として新たに「希土類の採掘、選鉱、製錬技術」が追加されるなど、全体としては、強化されているように見える。

レアアースに関しては、レアアース管理条例案が2021年1月に募集されたものの、その後動きはないが、技術部分については、本リストで輸出規制を強化している形である。

○前掲の規制強化品目群を見ると、米国でウイグル強制労働防止法による輸入制限に関連して取り上げられる太陽光発電シリコンウェーハの製造技術が含まれている。また、以前よりあるコンピュータハードウェアの要件のスパコン製造技術については、今回、演算速度の閾値が大幅に高められ（130ギガ→97テラ）高性能化している。スパコンの2022年の世界最速は米国「フロンティア」であるが、中国はTOP500の内、173台が入っているなど存在感を発揮している。

また、イオン型稀土鉱からの浸出メカニズムも、稀土類資源のグリーンで高効率な採掘を実現するための優れた技術とされている。

「レーザーレーダーシステム」の規制要件は、「車載レーザー探測・測距システム技術」となっており、自動運転の測距システムや3次元地図作成等のモバイルマッピングシステム等が対象になると考えられる。

CRISPR ゲノム編集技術については、分子生物学の革命とも呼ばれる“CRISPR-Cas9”（クリスパー・キャス9。DNA内の狙った1文字だけをピンポイントで書き換えることを可能にし、従来技術に比べてはるかに安価で扱いやすいとされる）に関する中国の動きが注目されている。

このように、中国が優位性を追求し、米国の対中規制動向も念頭に置いて安全保障的関連からも重要視する品目分野が新たな対象となっている。

○なお、「ヒトに用いる細胞クローンとゲノム編集」が輸出禁止技術に追加されているが、中国では、2018～19年に南方科技大（広東省）の元教授が、“CRISPR-Cas9”のゲノム編集技術を用いて、HIV耐性をつけることを目的に、受精卵の遺伝子を改変し、3人（うち2人は双子）のベビーを誕生させて、世界に衝撃を与えた。同医師は厳しく刑事責任を問われたが、「デザイナー・ベビー」誕生可能性の危機感が強まったとされる。

○2020年の「輸出禁止・輸出制限技術リスト」追加の際には、総体国家安全観に基づいて検討するとされており、今回の改正で、従来型の産業分野の品目が削除され、先端技術品目を2020年に続いて更に加えている。

中国輸出管理法も総体国家安全観に基づくとされており、両法制の趣旨の差異が曖昧になってきている。中国輸出管理法に基づく軍民両用品目（大量破壊兵器関連以外）の国際輸出管理レジーム合意に準じた品目指定は現時点ではなされていない。

実質的には、(少なくとも当面は) 対外貿易法体系下の「輸出禁止・輸出制限技術リスト」による規制と、データ安全法体系下での「重要データ」の移転規制とが、輸出管理規制対象として機能していく可能性も考えられる。

【注】「総体国家安全観」は、2014年4月に開催された中央国家安全委員会第一次会議において習近平主席が提唱した国家安全に関する重要概念で、これに基づいて、多くの国家安全関係の法律のベースとなっている。

人民の安全を主目的とし、政治の安全を根本とし、経済の安全を基礎とし、軍事・文化・社会の安全を保証とし、世界の安全の促進に依拠して中国の特色ある国家安全の道を歩みだすことをいい、具体的な安全保障の対象として、①政治の安全、②国土の安全、③軍事の安全、④経済の安全、⑤文化の安全、⑥社会の安全、⑦科学技術の安全、⑧情報の安全、⑨生態の安全、⑩資源の安全、⑪核の安全の11項目が挙げられている。

2. 輸出管理法に基づく両用品リストの定例改正（2022.12.30）

- 輸出管理法に基づく両用品リストについては、例年、年末に改正が行われるが、昨年未の改正では、従来の大量破壊兵器関連規則を統合したもの以外の、(ワッセナーアレンジメント合意品目に準じたような) 軍民両用品目についての追加はなかった。
- 他方、独自規制品目の項である「11、特殊民生品及び技術」の項目に、高性能の高圧放水砲及び特別に設計された主要部品及び付属装置が追加された（「6」～「11」）。

従来、「11、特殊民生品及び技術」では、大型浚渫船が「1」～「5」に規制されていたが、昨2022年12月1日に施行された高圧放水砲の輸出管理に関する公告（商務部、海関（税関）総署、国防科技工業局連名）にて規制された高圧放水砲及び主要部品及び付属装置がそのまま追加されたものである。

3. データ安全法体系による「重要データ」の越境移転規制と輸出管理法の規制との関係

- 2021年11月に、データ安全法体系下の「ネットワークデータ安全管理条例（意見募集稿）」がパブコメ公開されたが、そこでは、「輸出管理データ」「輸出管理品目に関連する中核技術・設計構想・製造工程等に関連するデータ」が「重要データ」の定義に含まれていたため、輸出管理法体系とデータ安全法体系の重畳適用の懸念が生じた。

この点は、以下の資料を参照。

◎中国のデータ安全管理規制と輸出管理規制との重畳適用について

ーネットワークデータ安全管理条例案等を踏まえての考察（2021.12.23）

<https://www.cistec.or.jp/service/uschina/46-20211220.pdf>

- 同条例案については、その後の動きはない（別途の「データ国外移転安全評価弁法」は、2022年9月から施行済み）。

他方で、上記資料で密接に関連するものとして紹介した中国国家標準化管理委員会による「情報安全技術 重要データ識別ガイドライン（意見募集稿）」については、その後、2021年9月に、（2017年の案を修正した）新たな案が公表され、パブコメが募集された後、2022年に3回修正草案がパブコメ公開されている（1月、3月、5月）。なお、2022年3月以降の草案は、名称が、「情報安全技術 重要データ識別規則（意見募集稿）」となっている。

- 「情報安全技術 重要データ識別ガイドライン（意見募集稿）」の輸出関連部分は、次のように変遷してきている。

◇2021年12月時点

5.4 科学技術関連について

a) 輸出管理データに関わるもの。以下のデータは重要データに属する：

国の輸出管理リストに掲載される品目について、

これらの品目の設計原理、製造工程、製造方法等を説明する情報、およびソースコード、集積回路レイアウト、技術構想、重要パラメータ、実験データ、テストレポート。

◇2022年1月時点

d) 輸出管理品目に関わるもの

輸出管理品目の設計原理、製造工程、製造方法等を説明する情報、およびソースコード、集積回路レイアウト、技術構想、重要パラメータ、実験データ、テストレポートは、重要データに属する。

◇2022年3月時点、5月時点

g) 国の科学技術力に関わる、国際競争力に影響する、または輸出管理品目に関わるもの

例えば、国の科学技術イノベーションの重大な成果を反映するもの、または輸出禁止・輸出制限品目の設計原理、製造工程、製造方法等を説明する情報、およびソースコード、集積回路レイアウト、技術構想、重要パラメータ、実験データ、テストレポート等は重要データに属する。

※2022年3月、5月のものの名称は「情報安全技術 重要データ識別規則（意見募集稿）」となっている。

- 「データ国外移転安全評価弁法」は、前掲の通り 2022年9月から施行済みで、パブコメ

案通り、「法律・行政法規に別段の規定のある場合は、その規定に従う。」とある。他方で、輸出管理法では、「前項にいう管理品目には、品目に関わる技術資料等のデータを含むものとする。」とあるが、輸出管理法体系とデータ安全法体系のそれぞれの規制の関係が依然として曖昧となっている。

また、2022年3月、5月案では、「輸出禁止・輸出制限品目」の例示が加わっているが、それが、「国の科学技術力に関わるもの、国際競争力に影響するもの」の例示なのか、「輸出管理品目に関わるもの」の例示なのか、或いはその両方なのか、明確ではない。いずれにしても、「輸出禁止・輸出制限技術リスト」を規制する対外貿易法及びその下の技術輸出入管理条例に基づく規制と、データ安全法体系に基づく規制との関係も、同様に曖昧となってきている。

【「情報安全技術・重要データ識別ガイドライン（意見募集稿）」関連の解説サイト】

- ◎（日本語）「重要データの識別・認定～中国の安全保障貿易管理に関する制度情報 専門家による政策解説～」(JETRO 北京事務所海外調査部 2022年11月。環球律師事務所委託)
https://www.jetro.go.jp/ext_images/_Reports/01/5a02eed2b328b63b/20220046_02.pdf
- ◎（日本語）TMI 総合法律事務所中国最新法令情報 2022年2月号
https://www.tmi.gr.jp/uploads/2022/03/01/TMI_China_News_February_2022.pdf
- ◎（日本語）「データ域外移転の安全評価に対する新たな規制」（金杜律師事務所 2022年9月13日）
<https://www.kwm.com/cn/ja/insights/latest-thinking/new-regulations-on-safety-assessment-of-data-transfer.html>
- ◎（中国語）「浅析重要数据的识别与保护」（国楓律師事務所サイト 2022年6月24日）
<https://www.grandwaylaw.com/guofengshijiao/3786.html>

【参考1】《情報安全技術 重要データ識別規則（意見募集稿）》における「重要データ」等について（抄訳）

【参考2】《情報安全技術 ネットワークデータ処理安全要求》（2022年11月1日実施）（抄訳）

巻末に掲載。

4. 学術論文データベース企業「知網」に対する独禁法及び国家安全法等による調査

- 中国国家市場監督管理総局は、昨 2022 年 12 月 26 日に、学術文献等のデータベースを扱う「同方知網北京技術（知網）」とその関連会社に対し、独占禁止法違反で 8760 万元（約 17 億円）の罰金を科すと発表した。

同社に対しては、別途、ネットワーク安全審査弁公室が、2022 年 6 月より、国家安全法その他の一連の法令違反の疑いで調査している。

- 独禁法違反については、2022 年 5 月に立件され調査が行われてきたもの。当局の発表では、次のように説明されている。

中国知網（CNKI）は中国国内の中国語の学術文献オンラインデータベースサービス市場において支配的地位をもっていた。2014 年以降、中国知網（CNKI）は支配的地位を濫用して独占行為を実施した。

第一に、サービス価格を継続的に大幅に引き上げる、データベースを分割して形を変えて価格を引き上げるなどの方法を通じて、データベースサービスを不当な高価格で販売するなどの行為を実施した。

第二に、独占的強力協議を締結するなどの方法を通じて、学術定期刊行物の出版団体、大学が学術定期刊行物、博士・修士学位論文などの学術文献データを第三者に使用する権限を与えることができないよう制限し、さらにさまざまな賞罰措置を講じて独占協力の実施を確保した。

調査によって明らかになったことは、中国知網（CNKI）は不当な高価格、取引を制限する行為を実施し、中国語学術文献オンラインデータベースサービスの市場競争を排除・制限し、ユーザーの合法権益を侵害し、関係市場のイノベーション・発展と学術交流の伝播に影響を及ぼし、《独占禁止法》第二十二条第一項（一）、（四）で禁止する“不当な高価格で商品を販売する”、“正当な理由なくして、取引の相手方が取引相手としか取引できないよう制限する”などの市場の支配的地位を濫用する行為を構成した。

なお、知網側は当局による是正要求を受けて、2022 年 12 月 26 日に、15 項目の是正措置を公表している。

- 他方、ネットワーク安全審査弁公室が、2022 年 6 月より、国家安全法違反などの疑いで調査については、当局の発表として以下があるのみで、詳細は不明である。

○中国知網（CNKI）の安全審査開始に関する中国国家互聯網信息弁公室の発表（2022 年 6 月 24 日）

ネットワーク安全審査弁公室の関係責任者は、国家データセキュリティのリスクを防止し、国家安全を守り、公共の利益を保障するため、《国家安全法》、《サイバーセキュリティ法》、《データセキュリティ法》に基づき、《ネットワーク安全審査弁法》に照らして、2022 年 6 月 23 日、ネットワーク安全審査弁公室は同方知網（北京）技術有限公司の責任者を事情聴取したことを明らかにし、中国知網（CNKI）に対してネットワーク安全審査を始動させたことを発表した。

知るところによれば、中国知網（CNKI）は大量の個人情報と国防、工業、電信、交通運輸、自然資源、衛生健康、金融等の重点産業分野の重要データ、および我が国の重大プロジェクト、重大科学技術成果と重要技術動態などの機微情報を掌握している。

○これらの動きは、以下の3つの点から注視されるところである。

第一は、中国の独禁法は、昨 2022 年 8 月 1 日に改正法が施行されている。それまでは、外国企業（コカコーラ、クアルコム等）に対する調査が目立っていたが、ネットの台頭に伴って「プラットフォーム」と呼ばれる企業が出現したことから、中国政府が 2019 年に独禁政策を担う国家市場監督管理総局に対してネット大手を厳しく取り締まるよう指導し、独禁法改正の検討を進めたという経緯がある（日経新聞 22.8.1 付）

2021 年以降、民間プラットフォームであるネット大手に対する立件が強化され、2021 年の独禁法違反の没収を含む罰金額は 235 億元で、2020 年の約 50 倍に急増したが、このうちネット大手が市場での支配的な地位を乱用した案件などの罰金が 217 億元にのぼり、罰金全体の 92%に達したとのことである（2021 年にはアリババ、美团に罰金）。他方で、政府系シンクタンクは、「(当局は) 長期にわたって国有企業の独占や寡占の問題に触れておらず、鉄道、石油や通信、航空、金融など多くの領域で様々な形で独占や寡占が存在する」と指摘したという（同上）。

アリババなどは、独禁法で巨額の罰金を課された後、政府・共産党の影響が高まっている。昨 2022 年秋以降、テンセント、アリババ、京東の主要な中国デジタル企業国有企業との提携を発表したほか、中国政府が、傘下の事業体を通じアリババグループとテンセント・ホールディングス（騰訊）の子会社のいわゆる「黄金株」を取得する見込みと報じている。具体的には、国家インターネット情報弁公室が政府系投資基金の下で設立した事業体が、アリババのデジタルメディア子会社の株式 1%を今年 1 月 4 日に取得し、同弁公室幹部と思われる 1 人が同日に新しい取締役役に指名されたとのことである。テンセントについても政府の事業体が同程度の株式を取得する協議が進行しているという（ブルームバーグ 2023.1.14 付他）

中国知網も学術文献データベースのオンラインサービスを提供するプラットフォームの一つであり、上記の流れの中で同様の展開になるのか注目される（15 の是正策のうち、「コンプライアンス建設の全面的強化（⑭コンプライアンス管理システムの整備 ⑮コンプライアンスリスク管理の強化）がある）。

○第二の注目点は、ネットワーク安全審査弁公室による国家安全法その他一連の違反の容疑が、具体的にどういうものかという点である。

違反容疑の法令として、「《国家安全法》、《サイバーセキュリティ法》、《データセキュリティ法》に基づき、《ネットワーク安全審査弁法》に照らして」とある。

そして、知網が「重要データ」と「機微情報（「敏感情報」）」を把握しているとしてい

る。

ネットワーク安全審査弁公室によるプラットフォームに対する同様の法令に基づく処罰としては、滴滴 (DiDi) グローバルに対して、2022 年 8 月に、80 億元強 (約 12 億ドル) の罰金を科したと発表している。《サイバーセキュリティ法》《データ安全法》《個人情報保護法》《行政処罰法》等の法律法規に基づいて、大別して 8 つの情報について 16 件の違法事実が存在したとされている。具体的には、以下の資料参照。

◎滴滴グローバルに対する罰金に関する中国国家インターネット情報弁公室による発表 一具体的な違法事実 16 件を指摘 (CISTEC ジャーナル 2022 年 9 月号)

https://www.cistec.or.jp/journal/data/2209/05_tokusyuu02sankou01.pdf

前掲のように、「重要データ」の定義について、国レベルでの明確な内容、ガイドライン等が未だ定められていない中でどのように適用されるのか、「機微情報」としてどういふものが該当するとされるのか、管理上どのような点が問題とされるのか、といった点が注目されるところである。

○第三の注目点は、従来の学術文献等の公開の流れとの関係である。

知網は学術文献や産業分野の成果等についてのデータを有しており、それらを有料で一般に提供している以上、それらは基本的には公開される性質のものと考えられる。これまでも、学術論文等は一般的には積極的開示が奨励されてきた。独禁法違反の調査結果を見ても、学術データの公開を前提として、それが広く共有されるべきところを阻害しているとの観点から問題視している。

他方で、公開・移転に当局の承認が必要な性格の「重要データ」「機微情報」を扱っているとネットワーク安全審査弁公室は述べており、公開対象と非公開・移転管理対象の峻別とをどのように当局として判断しているのか、という点を窺う上で、その調査結果は重要な材料になると思われる。換言すると、通常であれば公開されるはずの学術データその他の研究成果等が、国家安全の観点から非公開の方向に向かう要素が出てくるかどうかという点である。

これに関連し、例えば次のような点が懸念材料となっている。これらの動向と、知網への国家安全法、データ安全法等の観点からの調査が同根のものであるのか注視されるところである。

(1) 前掲の 2021 年 9 月の「ネットワークデータ安全管理条例案 (意見募集稿)」や「情報安全技術 重要データ識別ガイドライン (意見募集稿)」の当初案では、「暗号・生物・電子情報・人工知能等の分野で国の安全・経済競争力に直接影響を与える科学技術成果データ」が挙げられ、後者では更に「主要な発明の発見を含む。科学研究や産業実践の過程で生まれた論文、報告書、実験データなどは、戦略的または経済的価値」が挙げられていた。

その後の改訂過程で、その表現はかなり変わってきているが、「国の科学技術力に関

わるもの、国際競争力に影響するもの」は「重要データ」に属するとされている。
(2) また、データ安全法が施行された後の 2021 年 12 月に、WSJ は、次の記事で中国の「データ封鎖」の諸局面について報じているが、その一つに、「学術分野の承認手続きの厳格化」が挙げられている。最近、西側諸国の研究者による中国の研究資料へのアクセスが閉ざされてきていることを報じている。

◎中国経済の実態、データ規制でさらに不透明に

—新データセキュリティ法、海外からの情報入手を阻む (WSJ 2021.12.7 付)

<https://jp.wsj.com/articles/china-increasingly-obscurer-true-state-of-its-economy-to-outsiders-11638847730>

学術分野の承認手続きも厳格化

中国の開放姿勢が逆転した最も劇的な項目の 1 つが学術分野だった。同分野はかつて、中国と西側との関与の度合いを示す指標とみなされていた。中国は西側の学者による中国の研究資料へのアクセスを着実に閉ざしてきており、中国の大学は国際会議を主催するのが一段と難しくなっている。

中国教育省が今年 (2021 年) 8 月に公表したデータでは 2018、19 両年に中国と外国の大学との連携プログラムのうち 286 件が打ち切られたことが示されており、同省によれば、これらプログラムの一部は同省の教育、指導基準に合致していなかった。公開された公式ウェブサイトの 2021 年 9 月以降のアーカイブ版によれば、停止されたプログラムの大半は英国、ロシア、米国の学校とのもので、これにより影響の大きかった分野はコンピューターサイエンス、バイオテクノロジー、国際経済、貿易などだった。

もっと最近には、国際関係・中国史研究分野の学者が海外出張や外国の学者とのズーム会議に参加することに対し、大学側は一段と厳しい承認手続きを適用している。(中略)

北京大学国際関係学院の元院長、賈慶国氏は今年 3 月の全国人民代表大会 (全人代) に提出した請願書の中で、学術分野への規制が厳しくなっていることを指摘した。同氏は、一部の政府機関が「多様な検討案件」に対し管理を強める措置を講じていると付言した。(中略) 一部の大学では、研究者は、少なくとも他の同僚 1 人が同席している場合にしか外国人と交流することが認められていないと指摘した。

5. 政府調達における国産品優先／外国製品排除の動向

○政府調達等において、中国国内での設計・開発・生産等を国家規格等の形で要求したり、国内市場へのアクセスの条件として技術内容の当局への開示を条件にするなどの動きが報じられており、内外無差別原則との抵触、強制技術移転の一種として WTO でも議論になっている。

中国は内外企業の差別を禁じる WTO の政府調達協定を締結していないが、2001 年の

WTO 加盟時に政府調達の透明性の確保と将来の協定への加盟を約束している。

○複合機等のオフィス設備に関する国内設計・開発・生産要求の国家規格案の動向

- ・昨 2021 年 7 月に、中国政府が、日本を含めた外国オフィス機器メーカーに対し、複合機などの設計や製造の全工程を中国国内で行うよう定める新たな国家規格を制定する方針が報じられたが、WTO でも「市場アクセス」の観点から問題視され、議論がなされるようになった。

同報道等によれば、国家市場監督管理総局が「情報セキュリティー技術オフィス設備安全規範」の名称で 2022 年 4 月に草案を策定したもので、政府などが入札で購入するオフィス設備について「(中国) 国内で設計、開発、生産を完成すべきだ」と明記し、オフィス設備の安全評価についても「中国国内で設計、生産が完成されていることを証明できるかどうかを検査する」と規定しているとのことだった（読売新聞 2022.7.23 付）。

- ・同草案の概要と外国企業の懸念については、以下の昨 2022 年 8 月の資料で解説されている。

◎「設備調達の国産優先戦略の動き（中国）」

(NO&T Asia Legal Update ～アジア最新法律情報～ No.119 (2022 年 8 月))

川合正倫、万鈞剣（共著） 長島・大野・常松法律事務所

<https://www.noandt.com/publications/publication20220825-1/>

- ・その後、本年 1 月の報道によれば、「ジュネーブの交渉筋によると昨 2022 年 10 月 18、19 日に開かれた WTO の市場アクセス委員会で、複合機を巡る国家規格が議論された際、中国政府担当者は『近い将来、プリンターやコピー機に関する国家規格を見直す計画はない』と説明し、『国家規格を扱う当局もいかなる規格見直しの指示も受けていない』と明言した。中国側は、昨 2022 年 11 月 24～25 日の WTO 物品貿易理事会の場でも同じ説明を繰り返した。」

という。しかし、「所管の『全国情報安全標準化技術委員会』は、昨 2022 年 10 月 30 日、オフィス機器の全面国産化の国家規格を規定する『情報セキュリティー技術オフィス設備安全規範』を公示し、規格導入を進めていく方針を打ち出した。」とのことである（読売新聞 2023.1.13 付）。

○医療機器についても、同様の問題が報じられている。

主要医療機器について、地方政府が病院に国産機器を調達するよう求め始めたほか、中央政府は設計開発や重要部品の調達を中国に移すための法改正案を公表した（2022 年 7 月に政府調達法の改正草案を発表し、中国で付加価値を高めた製品の調達を優遇する項目を追加）。

◎中国、医療機器も外国製排除 世界市場の分断深まる（日経新聞 2022.9.14 付）

<https://www.nikkei.com/article/DGXZQOGM07AIV0X00C22A9000000/>

○2020年の改正化粧品監督管理条例による化粧品の成分全面開示要求の問題も報じられている。

- ・化粧品メーカーに対し、原料の全成分や比率を明記した調合表の提出を義務づけ、原料メーカーにも成分比率の開示（登録）を今年4月末までに求め、登録しなければ、中国内販売ができなくなるとのこと。長年培ってきた企業秘密である成分組成情報の開示要求に、外国メーカーに大きな懸念が生じているとのこと。

◎中国、今度は化粧品標的…繰り返される大国の要求と摩擦（読売新聞 2023.1.4 付）

<https://www.yomiuri.co.jp/world/20230103-OYT1T50148/>

- ・同条例については、以下の中国政府サイトに掲載されている。

http://www.gov.cn/zhengce/content/2020-06/29/content_5522593.htm

6. 「信頼できないエンティティ・リスト」に米国2社を初掲載

○中国商務部は、2月26日に、「信頼できないエンティティ・リスト」に、台湾への武器販売を理由として、米国の防衛関連2社を掲載した。2社は、ロッキードマーティンとレイセオン・ミサイルアンドディフェンスカンパニー。

○同リストは、2020年9月に制度としては施行されていたが、掲載されるのは今回が初めてとなる。

○制裁内容は、商務部発表によれば、

- ・中国に関連する輸出入活動への従事を禁止
- ・中国への新規投資を禁止
- ・当該企業の上級管理職の入境を禁止
- ・当該企業の上級管理職の労働許可、滞在、在留資格の承認取消し・拒否
- ・「信頼できないエンティティ・リストに関する規定」の実施以来、台湾に対する各企業の武器販売契約の2倍の罰金を科す。この発表の公布日から15日以内に、関連する法律および規制に従って支払いを行うものとする。この決定が期限内に履行されない場合、法律に従って追加の罰金を課す。
- ・この発表に含まれていない事項は、信頼できないエンティティ・リストの規定に従って実施されるものとする。

○ロッキードマーティンとレイセオン・ミサイルアンドディフェンスカンパニーはこれまでも、同様の理由で「反外国制裁法」で指定され（2022年2月）、それ以前にも「制裁」を科したと発表されている（制裁内容は不明）。

○「信頼できないエンティティ・リスト」制度については、以下の資料を参照。

◎中国における「信頼できないエンティティ・リスト」、「輸出禁止・輸出制限技術リスト」の施行について（2020.9.23）

<https://www.cistec.or.jp/service/uschina/30-20200923.pdf>

◎「信頼できないエンティティ・リスト」規定の仮訳

<https://www.cistec.or.jp/service/uschina/31-20200923-2.pdf>

7. 「反スパイ法」修訂草案二審稿が公表

○全人代常務委において、2022年12月27日に「反スパイ法」（「反間諜法」）の修訂草案二審稿が公表された。2014年版（現行法）は全五章40条であったが、全6章71条に大幅に増補されている。

○全人代常務委の動向を報じる「法治日報」（2022.12.28付）によれば、以下の通り。

修訂草案二審稿では反スパイ宣伝教育をより一層強化し、全人民の反スパイ意識を向上させるため、立法の指導思想と基本原則の中に“堅固な国家安全人民防衛線を建設する”という規定が追加され、同時にニュースメディアなどの団体は社会に向けて反スパイ宣伝教育を行わなければならないとの規定を追加し、（これによって）全人民の国家安全の素養を強化し、重点団体は秘密に関わる人員の反スパイ安全防止教育を強化することを明確にした。

修訂草案ではスパイ行為の定義を規定した。（中略）修訂草案二審稿ではスパイ行為の実施援助の法律責任のなかで処罰することを明確にした。さらに、ネットワーク上における機密窃取、攻撃、破壊はスパイ行為の新たな形態であり、サイバースパイにかんする規定を追加するよう提案するなどの意見が提出された。修訂草案二審稿ではスパイ組織とその代理人に重要情報インフラにおけるネットワークセキュリティの脆弱性などの情報を提供する行為をスパイ行為と規定している。

修訂草案二審稿ではさらに反スパイ活動の支援をより一層強化するために、反スパイ活動において重大な貢献を果たした個人と組織に対して国の関連規定に基づいて表彰と奨励を与える；重点団体は秘密に関わる事項、場所、媒体などの反スパイの物理的予防措置を強化する；反スパイ分野の科学技術イノベーションを奨励し、反スパイ活動における科学技術の役割を發揮させる；国家安全機関は反スパイ活動のための人材チーム建設と専門訓練を強化しなければならないことを明確にするなどの規定が追加された。

反スパイ活動と個人・組織の合法権益保護との関係をしっかり処理するため、国家安全機関の反スパイ活動に対する監督を強化しなければならないとの提出された意見について、修訂草案二審稿では第四章の章名を“保障と監督”に改め、国家安全機関による調査・情報収集、差押え・拘留、凍結などが執行任務の範囲と限度を超えてはならないことを明確にし、国家安全機関が人身、物品、場所に対して実施する検査および出国禁止の決定などを承認するためのレベルを明確にした。（以下略）

○修訂草案二審稿では、法律制定の目的に「人民の利益の保護」（第1条）、「総体国家安全観の堅持」（第2条）が追加された上で、スパイの定義が次のように規定されている。

※下線部分が、現行法からの追加箇所。

第四条 本法に言うスパイ行為とは以下のものを指す。

- (一) スパイ組織とその代理人が実施あるいは他人に指示、資金援助して実施する、あるいは国内外の機構、組織、個人がそれと結託して実施する中華人民共和国の国家安全に危害を及ぼす活動；
- (二) スパイ組織に参加する、あるいはスパイ組織とその代理人の任務を引き受けるもの、あるいはスパイ組織あるいはその代理人に身を寄せる；
- (三) スパイ組織とその代理人以外のその他の国外の機構、組織、個人が実施する、あるいは他人に指示・資金援助して実施する、あるいは国内の機構、組織、個人とそれが結託して実施する国家秘密あるいは情報およびその他の国家の安全と利益に関わる文書、データ、資料、物品を窃取、偵察、買収あるいは不法に提供する、あるいは国家の職員が裏切るよう策動、誘惑、脅迫、買収する活動；
- (四) スパイ組織とその代理人に重要情報インフラのネットワークセキュリティの脆弱性等の情報を提供する；
- (五) 敵に攻撃目標を指示するもの；
- (六) その他のスパイ活動を行うもの。

スパイ組織とその代理人が中華人民共和国の領域内において、あるいは中華人民共和国の公民、組織あるいはその他の条件を利用して、第三国に対するスパイ活動に従事し、中華人民共和国の国家安全に危害を及ぼすものは、本法を適用する。

参考 1

「重要データ識別規則（意見募集稿）」における「重要データ」等について（仮訳）

※旧名称「情報安全技術 重要データ識別ガイドライン（意見募集稿）」

《情報安全技術 重要データ識別規則》の重要データについて

- 《情報安全技術 重要データ識別ガイドライン Information security technology - Guideline for identification of critical data》（意見募集稿）（2022年1月7日稿）¹
- 《情報安全技術 重要データ識別規則 Information security technology – Rules for

¹ 「关于国家标准《信息安全技术 重要数据识别指南》征求意见稿征求意见的通知」（全国信息安全标准化技术委员会网站 2022年1月13日）
https://www.tc260.org.cn/front/bzzqyjDetail.html?id=20220113195354&norm_id=20201104200036&recode_id=45625；（本体）<https://www.tc260.org.cn/file/2022-01-13/bce09e6b-1216-4248-859b-ec3915010f5a.pdf>；（作成説明）
<https://www.tc260.org.cn/file/2022-01-13/e3ea82f4-051e-4f8b-ba56-008f877c8a49.pdf>

identification of key data》(意見募集稿)(2022年3月16日稿)²

○《情報安全技術 重要データ識別規則 Information security technology – Rules for identification of key data》(意見募集稿)(2022年5月12日稿)³

→2022年3月16日稿で名称が「重要データ識別ガイドライン」から「重要データ識別規則」に変更された。

◆重要データ識別規則(旧・重要データ識別ガイドライン)における重要データの定義

2022年1月7日稿	3.1 重要データ(critical data): 電子方式で存在する、ひとたび改ざん、破壊、漏洩または不法取得、不法利用されたならば、国家安全、公共の利益を損なう恐れのあるデータ。注:重要データに国家秘密と個人情報に含まれないが、膨大な個人データによって形成される統計データ、派生データは重要データとなる可能性がある。
2022年3月16日稿	3.1 重要データ(key data): 特定の分野、特定の集団、特定の区域または一定の精度と規模に達したデータで、ひとたび漏洩、改ざん、破損されたならば、国家安全、経済運営、社会の安定、公共の健康と安全を直接損なう恐れがあるもの。注:重要データに国家秘密は含まれない。
2022年5月12日稿	3.1 重要データ(key data): 特定の分野、特定の集団、特定の区域または一定の精度と規模に達したデータで、ひとたび漏洩、改ざん、破損されたならば、国家安全、経済運営、社会の安定、公共の健康と安全を直接損なう恐れがあるもの。

※2022年5月12日稿では「注:重要データに国家秘密は含まれない」が削除されている。
→なお、2022年11月1日に施行されたGB/T41479-2022《情報安全技術 ネットワークデータ処理安全要求》では、「重要データ(important data)」とは、「ひとたび漏えいすれば国家安全、公共の安全、経済の安全と社会の安定に直接影響するおそれのあるデータ。注:重要データには未公開の政府情報、数量が一定規模に達する遺伝子、地理、鉱物資源情報などが含まれる。原則として個人情報、企業内部の経営管理情報などは含まない。」と定義している⁴。

◆《情報安全技術 重要データ識別規則 Information security technology – Rules for

² 「国标《重要数据识别指南》又有重大修改了」(微信・小貝說安全 2022年4月26日)
<https://mp.weixin.qq.com/s/KD1UtgdUcarUDtiw3VS31A>

³ (道客巴巴 2022年8月18日) <https://www.doc88.com/p-57547039110914.html>

⁴ <http://www.powertime.cn/uploadfile/2022/06/10/20220610061405457.pdf>

4. 重要データ識別の基本原則

重要データ識別で準拠する原則は以下の通り。

- a) 安全への影響に焦点を当てる：国家安全、経済運営、社会の安定、公共の健康と安全などの観点から重要データを識別する。組織自身あるいは公民個人にのみ影響するデータは一般に重要データとしないが、膨大なデータマイニングの分析結果は考慮する必要がある；
- b) 保護の重点を際立たせる：データの等級分けを通じて、重点的に保護する対象を明確にし、安全保護要求を満たすという前提の下で重要データを秩序をもって流動させる；
- c) 既存の規定との整合：地方にすでにある管理要求と産業の特性を十分に考慮し、地方・部門がすでに制定実施している関連するデータ管理政策と標準規範と緊密に連携させる；
- d) リスクを総合的に考慮する：データの所在する分野、カバーしている集団、用途、直面している脅威などのさまざまな要素に基づいて、データの改ざん、破壊、紛失、漏洩、不法取得、不法利用などのリスクを総合的に考慮し、保密性、完全性、可用性、真実性、正確性など多くの観点からデータの重要性を分析し判断する；
- e) 定量・定性の結合：定量と定性を結合させた方式で重要データを識別し、かつ具体的なデータのタイプ、特性に基づいてさまざまな定量または定性の方法を採る。
- f) 動的識別と再評価：データの用途、共有方式、必要性などの変化に伴って、重要データを動的に識別し、定期的に重要データの識別結果を再評価する。

5. 重要データの識別要素

重要データを識別する際、以下の要素を考慮すべきである：

- a) 国の主権、政権の安全、政治制度、イデオロギーの安全に直接影響する。たとえば社会動員の実施に用いるデータ等は重要データに属す；
- b) 領土の安全と国家統一に直接影響する、あるいは国の自然資源の基礎状況を反映する。たとえば未公開の領陸、領水、領空データ等は重要データに属す；
- c) 他の国家や組織の我が国に対する軍事攻撃に利用されるおそれがある、または我が国の戦略備蓄、緊急動員、作戦などの能力を反映する。たとえば一定精度の指標を満たす地理情報や戦略物資の生産能力、備蓄量の情報などは重要データに属す；
- d) 市場秩序あるいは国家経済の命脈の安全に直接影響する。たとえば重要インフラの所在する産業、分野の核心業務の運営あるいは重要経済分野の生産を支えるデータ等は重要データに属す；
- e) 我が国の言語文字、歴史、風俗習慣、民族の価値観などの特質を反映する。たとえば歴史文化遺産情報などは重要データに属す；

- f) 重点目標、重要場所の物理安全保護状況または未公開の地理目標の一を反映し、テロリスト、犯罪分子の破壊活動の実施に利用されるおそれがある。たとえば重点安全保護団体、需要生産企業、国家重要資産（鉄道、送油パイプラインなど）の施工図、内部構造、安全防護などの情報、および未公開の専用道路、空港の情報などは重要データに属す；
- g) 国の科学技術力に関わる、国際競争力に影響する、あるいは輸出管理品目に関わる。たとえば国家科学技術イノベーションの重大成果を反映する、または我が国の輸出禁止・輸出規制品目の設計原理、プロセスフロー、製作方法などの情報、およびソースコード、集積回路のレイアウト、技術ソリューション、重要パラメータ、実験データ、検査報告などは需要データに属す；
- h) 重要情報インフラ全体の運行、開発と安全保護の状況を反映し、重要情報インフラのサイバー攻撃の実施に利用される恐れがある。たとえば重要情報インフラのシステムは位置情報、コアソフト/ハードウェアの設計情報、システムトポロジー、緊急対策、評価、監査などの状況を反映するデータは重要データに属す；
- i) 重要設備、システムコンポーネントのサプライチェーンを破壊し、高度で持続的な脅威などのサイバー攻撃に利用される恐れがある。たとえば政府や軍工団体の顧客リスト、未公開の製品とサービスの調達状況、未公開の重大な脆弱性などは重要データに属す；
- j) 自然環境、生産生活環境の基礎状況を反映する、あるいは環境安全事件を引き起こすのに利用される恐れがある。たとえば未公開の土壌データ、気象観測データ、環境保護監視データなどは重要データに属す；
- k) 水資源、エネルギー資源、土地資源、鉱物資源などの資源備蓄と開発・供給状況を反映する。たとえば未公開の水文観測結果、未公開の耕地面積や品質変化状況などは重要データの属す；
- l) 核物質、核施設、核活動の状況を反映する、または核破壊やその他の核安全事件を引き起こすのに利用される恐れがある。たとえば原子力発電所の設計図、原子力発電所の運行データなどは重要データに属す；
- m) 海外エネルギー資源の安全、海上戦略航路の安全、海外の公民と法人の安全に関わる、あるいは我が国が参加している国際経済貿易、文化交流活動の破壊または我が国に差別的禁止・規制やその他の類似措置の実施に利用される恐れがある。たとえば国際貿易における特殊品目の生産取引および特殊装備の配備、使用状況などは重要データに属す；
- n) 我が国の宇宙、深海、極地などの戦略的新領域の現実または潜在的な利益に関わる。たとえば未公開の科学調査、開発利用データと人員の安全な出入に影響するデータなどは重要データに属す；
- o) バイオテクノロジーの研究、開発と応用状況を反映する、エスニックグループの特徴、

胃炎情報を反映する、重大突発伝染病、動植物の疫病流行に関わる、生物実験室の安全に関わる、あるいは生物兵器の製造に製造、バイオテロリズムの実施に利用される恐れのあるもの、外来種の侵入と生物多様性に関わる。たとえば重要生物資源データ、薬剤耐性菌の基礎研究データなどは重要データに属す；

p) 未公開の政務データ、インテリジェンスデータと法執行司法データ。たとえば未公開の統計データ重要データに属す；

q) 大局的あるいは重点分野の経済運営、金融活動状況を反映する、産業競争力に関わる、公共安全事故を引き起こし公民の生命の安全に影響する恐れがある、集团的活動を引き起こす、あるいは集団の感情や認知に影響する。たとえば未公開の統計データ、重点企業の商業秘密および危険化学品の製作プロセス、危険化学品の備蓄地点などは重要データに属す；

r) 国または地域の集団の健康・生理状況を反映する、疾病の伝播と予防・治療に関係する、食品・薬品の安全に関係する。健康・医療資源データ、膨大な人々の診療と健康管理データ、疾病管理・防疫データ、健康救援保障データ、特定薬品の実験データ、食品安全トレーサビリティ標識情報などは重要データに属す；

s) その他の国の政治、国土、軍事、経済、文化、社会、科学技術、ネットワーク、生態、資源、核、海外における利益、宇宙、極地、深海、生物などの安全に影響する恐れのあるデータ。

以上の要素の一つをもつものは、重要データあることを考慮すべきである。

参考 2

GB/T41479-2022 《情報安全技術 ネットワークデータ処理安全要求》
(2022年11月1日実施) (抄訳)⁵

目次

- 1 範囲
- 2 規範性引用文書
- 3 専門用語と定義
- 4 データ処理における安全の総体要求
 - 4.1 データの識別
 - 4.2 分類・等級分け
 - 4.3 リスクの予防制御
 - 4.4 監査・追跡

⁵ <http://www.powertime.cn/uploadfile/2022/0610/20220610061405457.pdf>

5 データ処理における安全の技術的要求

5.1 総則

5.2 収集

5.3 保存

5.4 使用

5.5 加工

5.6 伝送

5.7 提供

5.8 公開

5.9 プライバシー情報と転送可能情報の処理方式

5.10 個人情報のリファレンス、訂正、削除およびユーザーアカウントの取消

5.11 苦情の申し立て、通報の受理・処置

5.12 アクセス制御と監査

5.13 データの削除と匿名化処理

6 データ処理の安全管理要求

6.1 データ安全の責任者

6.2 人材資源の保障と審査

6.3 事件の応急処置

付録 A（規範性）突発公共衛生事件における個人情報の保護要求

参考文献

3 専門用語と定義

3.9 重要データ important data

ひとたび漏えいすれば国家安全、公共の安全、経済の安全と社会の安定に直接影響するおそれのあるデータ。

注：重要データには未公開の政府情報、数量が一定規模に達する遺伝子、地理、鉱物資源情報などが含まれる。原則として個人情報、企業内部の経営管理情報などは含まない。

（中略）

5.6 提供

5.7.1 他人への提供

ネットワーク事業者は他人にデータを提供する前に、安全影響分析とリスク評価を行わなければならない。国家安全、公共の安全、経済の安全と社会の安定を損なうおそれのあるものは、他人に提供してはならない。要求は以下の通り。

- a) 他人に個人情報を提供するには、個人情報対象者にデータ受信者の名称、連絡方法、処理目的、処理方法、個人情報の種類、保存期間を通知し、かつ個人情報対象者の同意を得なければならない；
- b) 重要データを共有・譲渡するには、データ受診者と契約などの形式を通じて双方のデータ安全保護の責任と義務を明確にし、暗号化、マスキングなどの措置を講じ重要データの安全を保障しなければならない；
- c) 第三者に委託してデータ処理活動を行うには、契約などの形式を通じて委託処理の目的、期限、処理方法、データの種類、保護措置、双方の権利と義務、および第三者がデータを変換あるいは削除する方式等を明確に取り決め、第三者に契約中に取り決めた形式で受信・生成したデータを返却・削除するよう要求し、かつデータ処理活動に対して監督を行わなければならない；
- d) 買収、合併、再編、倒産が発生した場合、データ受信者は引き続き関連するデータ安全保護義務を履行しなければならない；データ受信者がいなくなったならば、データを削除しなければならない。

5.7.2 データの越境

ネットワーク事業者が個人情報あるいは重要データを国外に提供するには、国の関連規定と関連標準の要求を従わなければならない。国内のユーザーが国内で国内のネットワークにアクセスするには、そのトラフィックは国外にルーティングしてはならない。

5.8 公開

ネットワーク事業者が管理しているデータ資源を利用して、市場予測、統計などの情報を公開するさい、国家安全、公共の安全、経済の安全と社会の安定を損なってはならない。

(以下略)

以上