NPI 公益財団法人 中曽根康弘世界平和研究所
Nakasone Yasuhiro Peace Institute

IIPS Institute for International Policy Studies

米中覇権の相克における5G

US-China Rivalry and 5G

日本安全保障学会　第30回大会
テーマセッション　パート1
＜米中技術覇権の革新-5G-＞

2020年10月4日

公益財団法人　中曽根康弘世界平和研究所
主任研究員
大澤　淳

マッキンダーの地政学

•「歴史上の大戦争は、ことごとく直接または、間接的に国家間における成長の度合いの不均衡から端を発している。成長の不均衡の理由は、（中略）この地球上における資源の賦存状況や戦略上の有利不利に、かなりのむらがあることに求められる。」（『デモクラシーの理想と現実』（1919年））

•「回転軸となる国家に有利な地位を与えることは、やがてユーラシア大陸の諸地域に対するその勢力の膨張を促し、ひいてはまた莫大な大陸資源を艦隊の建設に役立てさせる結果にもなる。（中略）彼らは広い大陸の資源を背景にした上、さらにこれに加えて海の正面を持つ結果になる」

•シー・パワーがランド・パワーと均衡を保つためには、結局に於いて水陸両用的な性格を帯びるほかにない（中略）均衡こそ自由の基礎である。（「球形の世界と平和の勝利（1943年））

ハルフォード・マッキンダー(1861-1947)
イギリスの地理学者。ハートランド論を初めて提唱し、地政学の生みの親とされている。長年の大陸と海洋を巡る戦いの歴史を、ランド・パワーとシー・パワーの抗争として整理し、第一次世界大戦をハートランドを制しようとするランド・パワーとそれを阻止しようというシー・パワーの争いと分析した。

スパイクマンの地政学

•「リムランドはシーパワーとランドパワーとの間の広大な緩衝地帯なのだ。この地域の国々は、海と陸の両方を見つつ、両生類的に機能するのであり、この両方向の脅威から自分の身を守ろうとする。」

•「リムランドを支配するものがユーラシアを制し、ユーラシアを支配するものが世界の運命を制す」

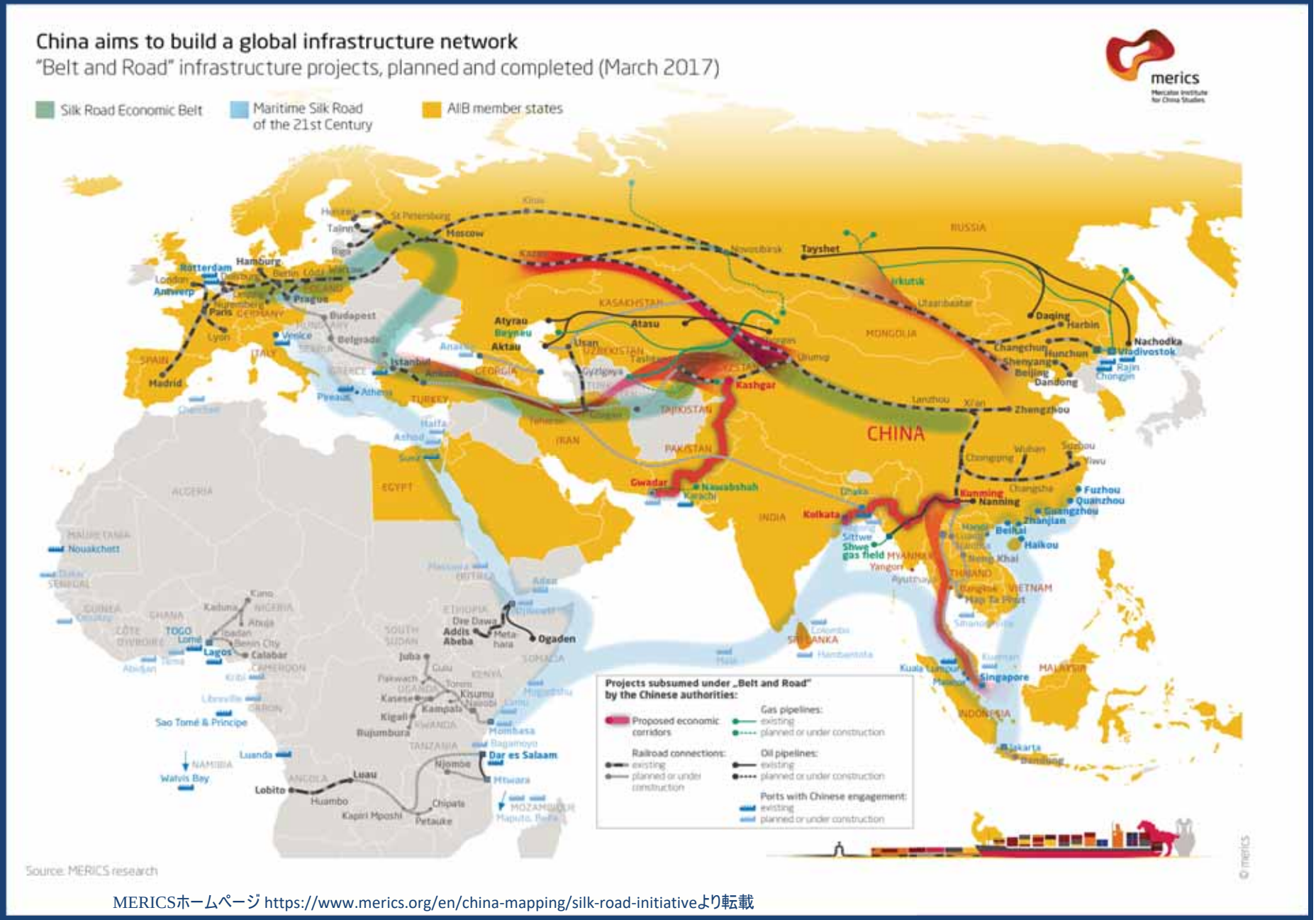
•「地理の現実が教えているのは、西半球のパワーの中心地であるアメリカの2．5倍の広さと10倍の人口を持つユーラシア全体の潜在力が、将来アメリカを圧倒する可能性がある、ということである」

•「アメリカが統一されたユーラシアのリムランドに直面することになれば、強力な勢力による包囲状態から逃れられないことになってしまう。よって平時・戦時を問わず、アメリカは、旧世界のパワーの中心が自分たちの利益に対して敵対的な同盟などによって統一されるのを防ぐことを目指さなければならない。」（『平和の地政学』（1944年））

ニコラス・スパイクマン(1893-1943)
アメリカの地政学者、国際政治学者。イェール大学教授。
地理が国際政治に与える影響を重視し、国際関係を「地理」と「パワー」の関係から分析した。マッキンダーのハートランド論を発展させ、ハートランドの周辺地域＝リムランドこそが重要であり、シーパワーであるアメリカは、リムランドへのアクセスを確保することによって、ランドパワーとの均衡を図るべきであると主張した。

中国の中長期国家発展計画と科学技術

一帯一路によるネットワーク確保



MERICSホームページ https://www.merics.org/en/china-mapping/silk-road-initiativeより転載

デジタルシルシルクロード:デジタル分野の優位性争い

デジタル分野の優越

経済優位

技術優位

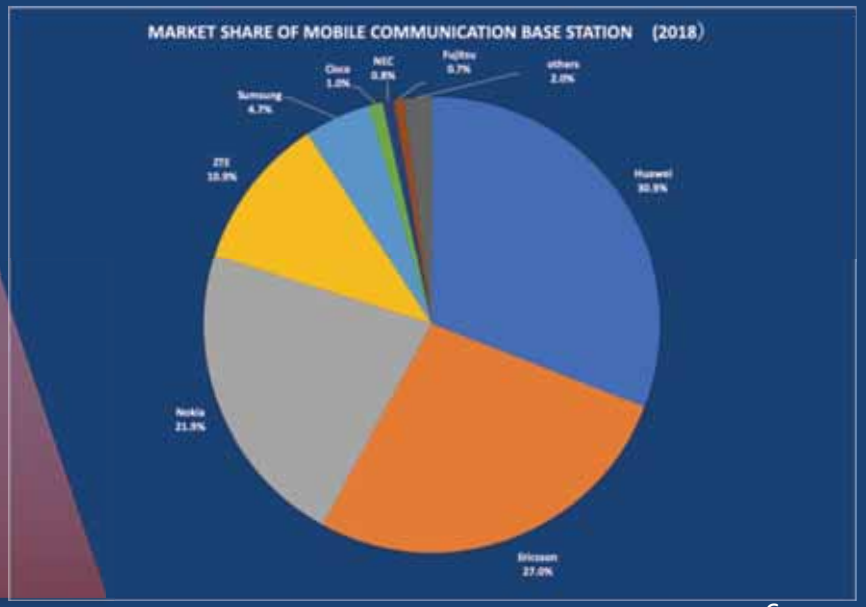
研究開発（R&D）
+
サイバー窃取による
先端技術獲得

デジタル優位
(デジタルシルクロード)

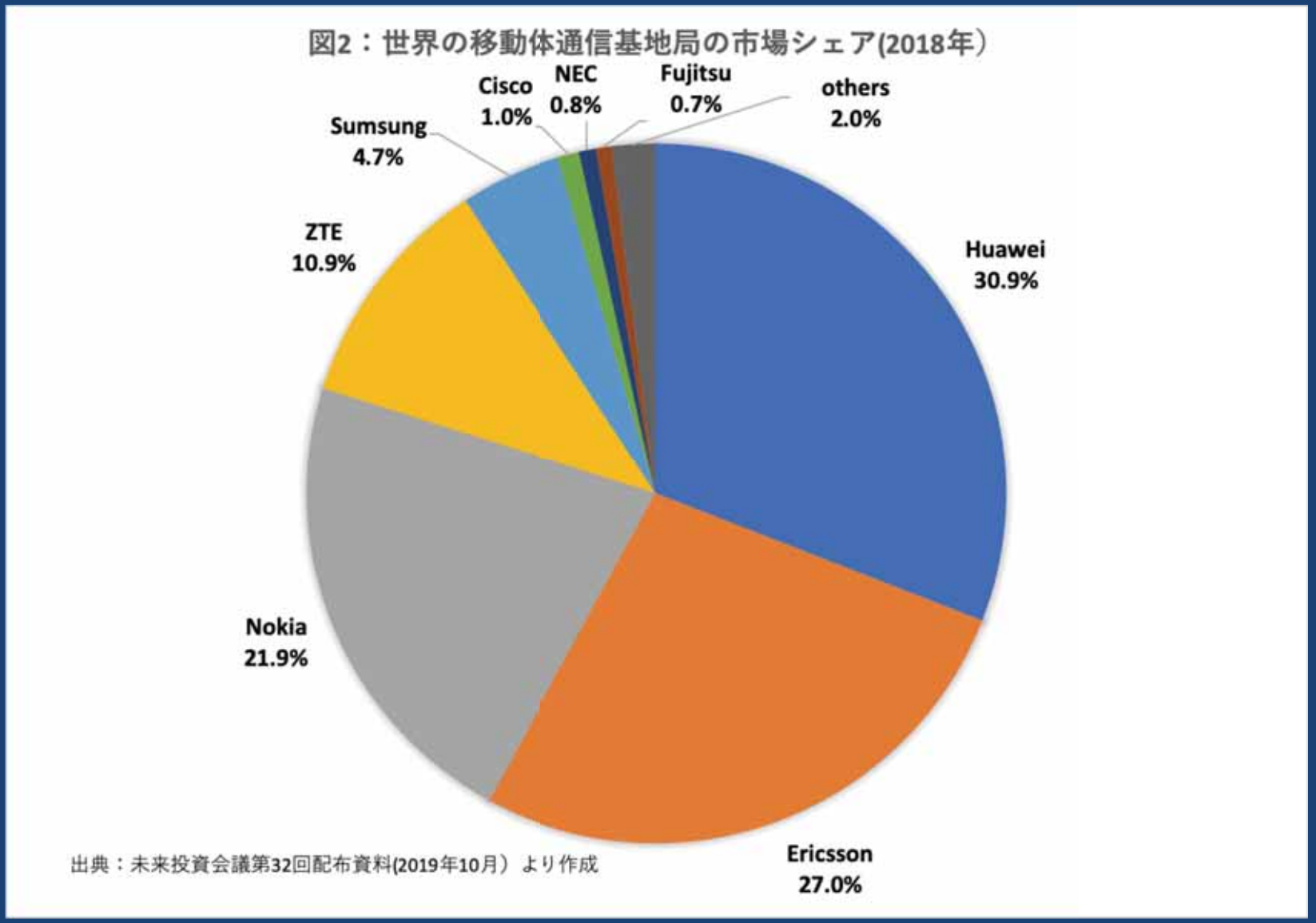
ソフトウェアの寡占
プラットフォーム優位
(電子商取引, デジタル決済, デジタル監視, SNS, etc.)

通信機器の寡占
情報通信基盤優位
(5G・海底ケーブル)

デジタルシルクロード: 中国が主導する海底ケーブルAAE-1



世界の移動体通信基地局のシェア



5Gの出願特許数

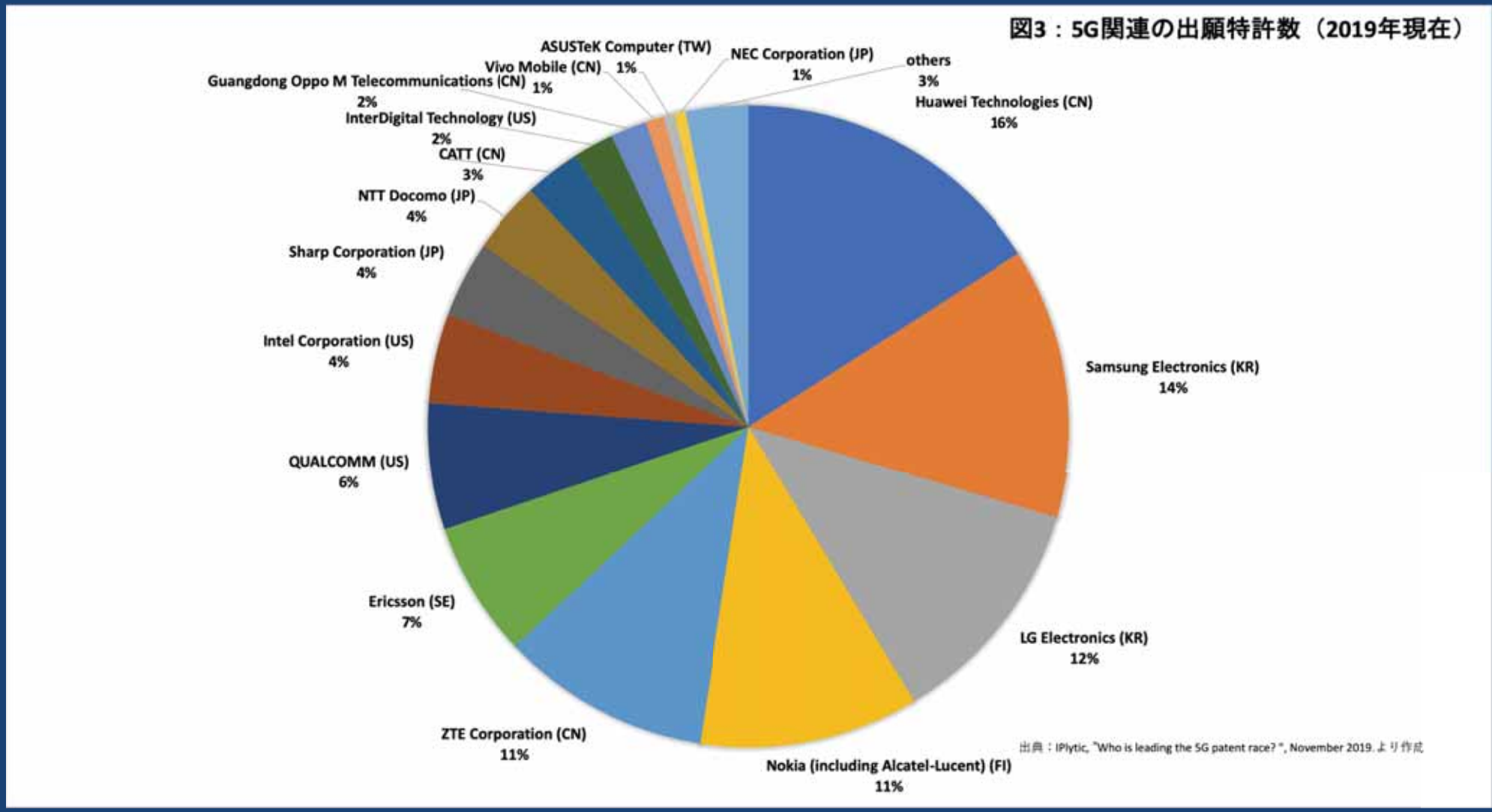


図3：5G関連の出願特許数（2019年現在）
Huawei Technologies (CN) 16%
Samsung Electronics (KR) 14%
LG Electronics (KR) 12%
Nokia (including Alcatel-Lucent) (FI) 11%
ZTE Corporation (CN) 11%
Ericsson (SE) 7%
QUALCOMM (US) 6%
Intel Corporation (US) 4%
Sharp Corporation (JP) 4%
NTT Docomo (JP) 4%
CATT (CN) 3%
InterDigital Technology (US) 2%
Guangdong Oppo M Telecommunications (CN) 2%
Vivo Mobile (CN) 1%
ASUSTeK Computer (TW) 1%
NEC Corporation (JP) 1%
others 3%
出典：IPlytic, "Who is leading the 5G patent race? ", November 2019. より作成

IoT時代のICT基盤　5G

<5Gの主要性能>　超高速／超低遅延／多数同時接続　⇒　最高伝送速度 10Gbps／1ミリ秒程度の遅延／100万台/km²の接続機器数

5Gは、AI/IoT時代のICT基盤

低遅延

移動体無線技術の高速・大容量化路線

2G 1993年　3G 2001年　4G 2010年

同時接続

5G 2020年

超高速

現在の移動通信システムより100倍速いブロードバンドサービスを提供

⇒ 2時間の映画を3秒でダウンロード（LTEは5分）

超低遅延

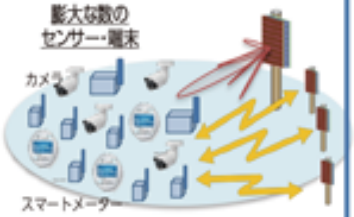
利用者が遅延（タイムラグ）を意識することなく、リアルタイムに遠隔地のロボット等を操作・制御

ロボットを遠隔制御

⇒ ロボット等の精緻な操作（LTEの10倍の精度）をリアルタイム通信で実現

多数同時接続

スマホ、PCをはじめ、身の回りのあらゆる機器がネットに接続



⇒ 自宅部屋内の約100個の端末・センサーがネットに接続（LTEではスマホ、PCなど数個）

社会的なインパクト大

出典：総務省　令和元年版　情報通信白書

中国製造2025と10重点分野

2015年5月中国国務院は「中国製造2025」と題する10カ年の産業政策を発表

2025
- 第一段階
- 製造強国の地位確立（仲間入り）

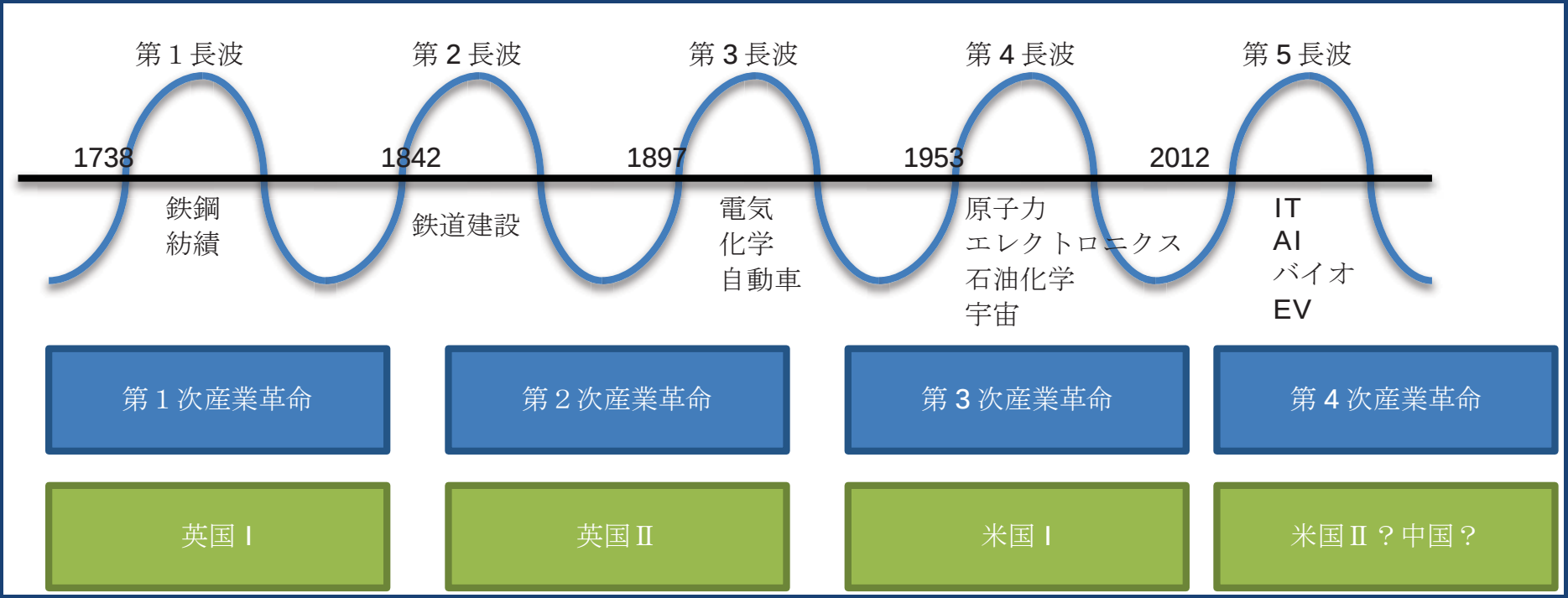
2035
- 第二段階
- 製造強国の中位レベルの達成（イノベーション牽引国）

2049
- 第三段階
- 製造強国の指導的地位の確立（大半の分野で競争優位を確立）

10重点分野

次世代情報技術	省エネ・新エネ自動車	航空・宇宙	海洋工学ハイテク船舶	先進鉄道
CNC工作機械ロボット	電力設備	新素材	バイオ医薬高性能医療機器	農業機械

IoTを制するものが第4次産業革命を制する？



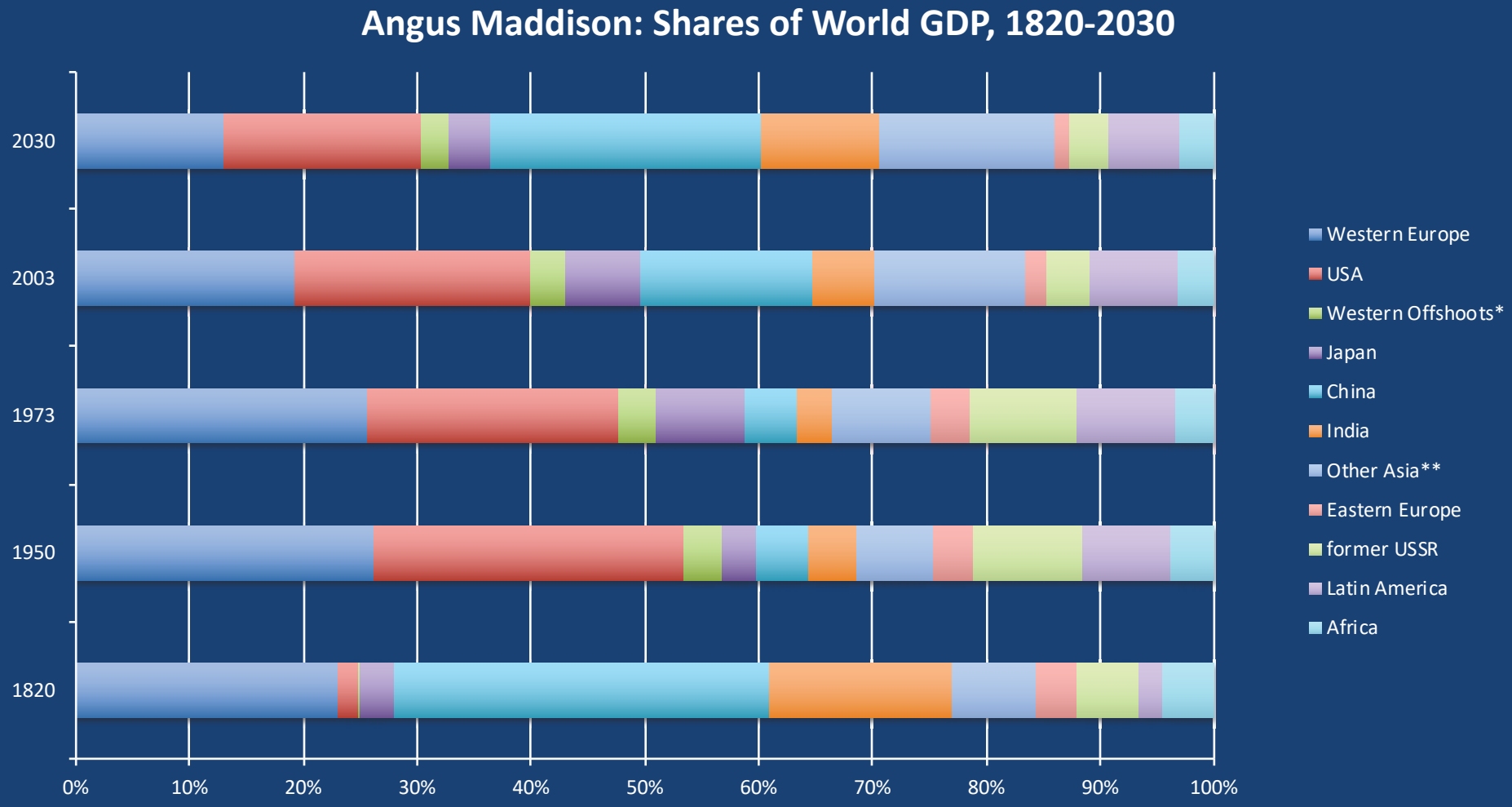
出典：著者作成

グローバルな政治システムの変遷と経済ネットワーク

国際システム（覇権国）	経済ネットワーク	国際システムを支えた制度革新	ネットワークの中心都市	ネットワークを支える情報基盤
ヴェネツィア	地中海貿易	造船（ガレー船）	ヴェネツィア	定期船による情報収集
(1381～1494)		航海パートナーシップ		大使館、外交使節による報告
		私的振替銀行		
		プレスティーティ債（国債）		
ポルトガル（スペイン）	遠隔地貿易（略奪貿易）	ガリオン船	アントウェルペン	取引所による価格情報
(1494～1609)		官僚制、軍隊の動員制度		豪商のネットワーク
		中継貿易・金融センター都市		（ウッガー家など）
オランダ	中継貿易	フライト船	アムステルダム	為替決済網
(1609～1713)		東インド会社		
		アムステルダム銀行（為替取引の制度化）		
		取引所		
英国Ⅰ	植民地貿易	重商主義	ロンドン	植民地と海軍
(1713～1815)		イングランド銀行とコンソル債（国債）		
		産業革命		
英国Ⅱ	大英帝国を中心とした自由貿易	自由貿易	ロンドン	郵便船
(1815～1914)		金本位制		電信技術
米国Ⅰ	GATT/IMF 緩やかな自由貿易体制	IMF、GATT（国際組織）	ニューヨーク	組織的な情報分析
(1914～1989)				
米国Ⅱ	自由な資本移動とグローバル競争	情報技術	ニューヨーク	インターネット
(1989～　　)		金融技術革命		

高橋琢磨『マネーセンターの興亡』（日本経済新聞社、1990年）p.64およびModelski, George, Long Cycle in World Politics, Macmillan Press, 1987. 浦野起央、信夫隆司訳『世界システムの動態：世界政治の長期サイクル』（晃洋書房、1991年）邦訳p.54などより作成

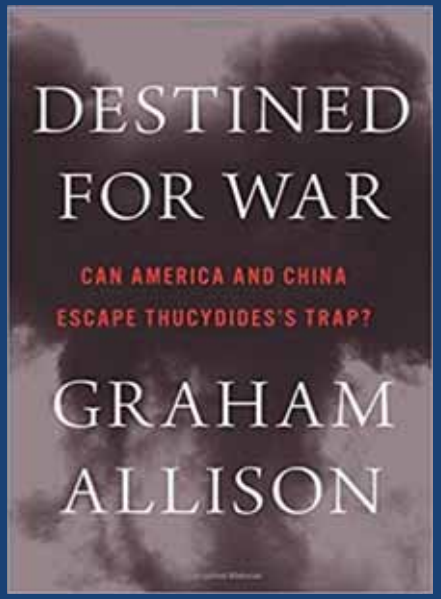
Share of World GDP



Source: Angus Maddison, "Shares of the Rich and the Rest in the World Economy: Income Divergence between Nations, 1820–2030", pp.8–9.

「トゥキディデスの罠」

- 米国の国際政治学者グレアム・アリソンは、覇権国米国と台頭する中国の相克を分析し、両国が「トゥキディデスの罠」に陥る可能性があると分析
- “I conceive to be the growth of the Athenian power, which putting the Lacedaemonians (Sparta) into fear necessitated the war.” Thucydides, History of the Peloponnesian War, Thuc.1.23
- 「トゥキディデスの罠」とは、紀元前５世紀にギリシャ全域を戦火に巻き込んだスパルタとアテネの「ペロポネソス戦争」を記録した歴史家トゥキディデスの分析にちなむ言葉で、「新興国が覇権国に取って代わろうとするとき、国際関係に構造的な摩擦が起こり、暴力的な衝突が発生する」というもの
- “(T)he peace was broken and that war was to be made, not so much for the words of the confederates as for fear the Athenian greatness should still increase.” Thuc.1.88



米国が恐れる中国の国家安全法/国家情報法

- 2015年7月　国家安全法
  - ✓ 第77条　いかなる組織や国民も下記の国家安全の義務を果たさなければならない。(5)国家安全機関、公安機関、軍事機関に対して必要な協力と支持を行うこと。
- 2017年6月　サイバーセキュリティ法
  - ✓ 第28条　ネットワークプロバイダは、公安機関及び 国の安全機関のため法により国の安全及び犯罪捜 査の活動を維持・保護し、技術サポート及び協力を提供しなければならない。
- 2017年6月　国家情報法
  - ✓ 第7条　いかなる組織や公民も、法により国の情報業務に協力しなければならず、知り得た国家情報業務の秘密を保持しなければならない。

中国から米国へのサイバー攻撃例（APT1=61398)

2013年1月30日　ニューヨーク・タイムズ　中国から同社のコンピュータネットワークに侵入があり、すべての従業員のパスワードが流出と発表
2013年1月31日　ウォールストリート・ジャーナル　同社のシステムに中国のハッカーが侵入と発表。ダウ・ジョーンズ社は中国報道の監視が目的とコメント。
2013年2月1日　　ワシントンポスト　過去3年間（08,09年～）にわたり中国からと見られるサイバー攻撃を受けていたと発表
2013年2月1日　　Twitterのサーバーに不正アクセスの痕跡、25万人分のメールアドレス、パスワード流出の恐れ
2013年2月12日　オバマ大統領一般教書演説でサイバー攻撃に対する危機感をあらわに"Now our enemies are also seeking the ability to sabotage our power grid, our financial institutions, our air traffic control systems."
2013年2月15日　Facebook、同社従業員のPCがウェブサイトを通じてマルウェアに感染と発表
2013年2月19日　Apple、社内のMacがマルウエアに感染と発表
2013年2月21日　ワシントンポスト、ワシントンのほぼすべての組織が中国からハッカー攻撃を受けていると報道
2013年2月22日　マイクロソフト社が不正侵入被害を発表（Mac事業部門を中心に複数のコンピュータが感染）
→Facebook、Apple、マイクロソフトとも、感染源はiOSアプリ開発者向けのサイト「IPhoneDevSDK」と見られる。同サイトが改ざんされ、Java脆弱制が使われた不正スクリプトが挿入されていた。

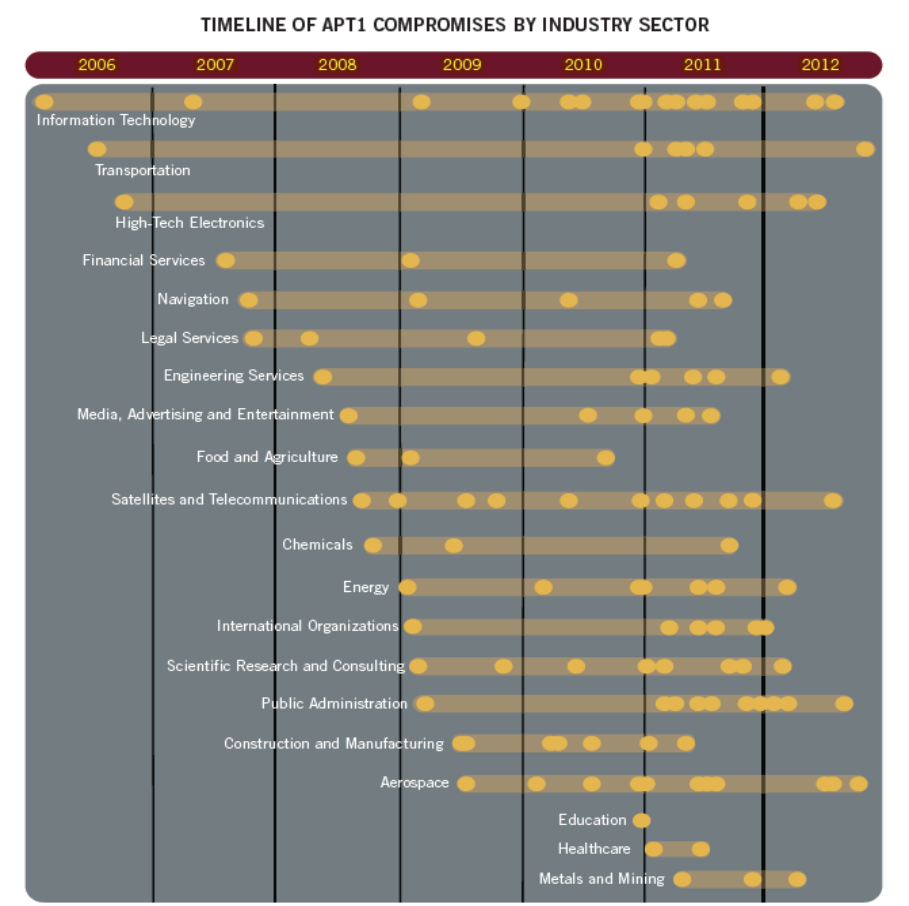


FIGURE 12: Timeframe of APT1's cyber espionage operations against organizations by industry. The dots within each bar represent the earliest known date on which APT1 compromised a new organization within the industry.

出典：Madiant, "APT1: Exposing One of China's Cyber Espionage Units"(2013.2), p.23.

産業競争力を奪うサイバー攻撃：欧米の事例

カナダの通信機器大手ノーテル社は、ベル研究所の流れを組み、いち早く光ファイバーや電話のデジタル化を模索。インターネット回線向けのコンピューター制御スイッチや通信機器製造のパイオニア的存在だった。

ノーテル社は、サイバー攻撃により、2000年から10年近く知財・ビジネス情報を窃取され、2009年に経営破綻した。中国のハッカーが2000年から、数年にわたって技術マニュアルや調査研究リポート、事業計画書、従業員の電子メールなどを含む文書をダウンロードしていたことが明らかになっている。

ノーテル社上級システムセキュリティ顧問たったBrian Shieldsは、「中国による広範なサイバー攻撃が企業崩壊の一因なった」とメディアのインタビュー で答えている。

Huaweiは、ノーテルが破綻した2009年に、同社のEthernetビジネスを400百万ドルで買い取ると持ちかけている。また、Huaweiの5Gイノベーションを支える「フェーウェイ・フェロー」の称号を与えられた童文（Tong Wen）博士はノーテルでワイヤレス技術研究に長年携わったのち、2009年にHuaweiに入社し、同社のワイヤレス・ネットワーク最高技術責任者である。また、同じ称号を与えられた朱佩英（Zhu Peiying）は、ノーテルで研究したのち2009年にHuaweiに入社し、5G研究のプログラムリーダーを務めている。

米コカコーラは、2008年9月、中国飲料メーカーの中国匯源果汁集団に買収を提案した。買収総額は24億ドルで、中国匯源果汁集団が香港市場に上場している発行済株式を12.2香港ドルで仏ダノン等の株主から買い付けるというものであった。しかし、中国の商務部は、この中国最大となる買収提案に対して、2009年3月18日に、前年施行された独占禁止法をたてに、「競争力が損なわれる」として承認しなかった。

この判断の背後には、中国政府がサイバー攻撃で得た情報が使われたと報道されている 。

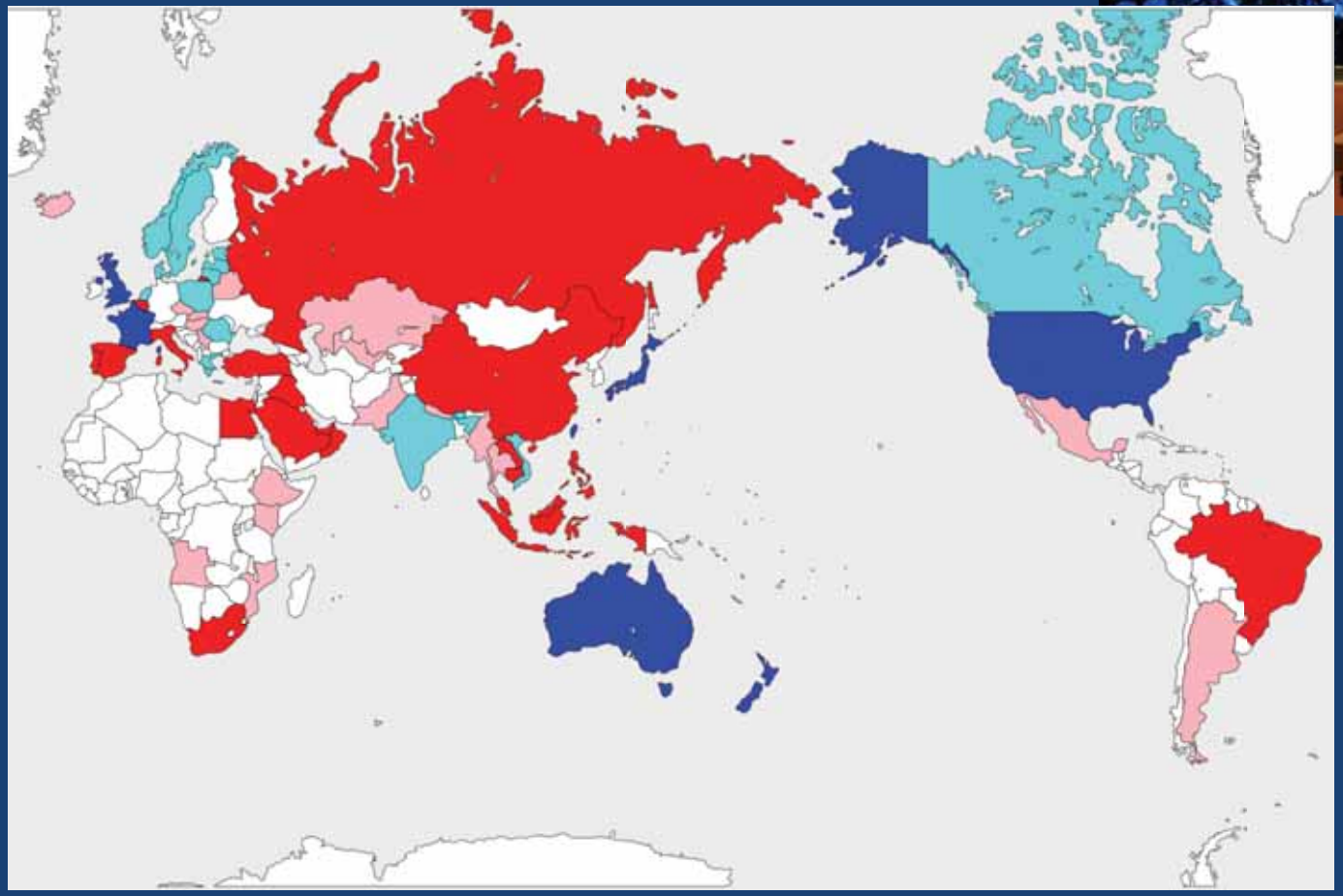
一連のサイバー攻撃は、コカコーラ太平洋グループのポール・エッチェルス（Paul Etchells）副社長への2009年2月16日の標的型メール攻撃から始まったとされる。エッチェルス副社長は当時、匯源果汁集団買収の総責任者であった。サイバー攻撃により、同副社長のコンピュータが乗っ取られ、最終的にはコカコーラ内部のネットワークへの侵入を許すことになった 。一度コカコーラのネットワークに侵入したハッカーは、以後1ヶ月間に渡って、FBIが警告するまで活動を続け、企業内の機密書類のほか、企業経営陣の送受信するメールを盗み見ていたと見られている。

結局大株主であった仏ダノンは2010年7月に、中国政府系の香港投資ファンドSAIFパートナーズにコカコーラが提示した額の半値の6ドル（総額2億ユーロ）で匯源果汁集団の22.98%を売却。

米国政府は、2018年10月、民間航空機向けのジェットエンジンの知的財産を窃取するため、フランスおよび米国の複数の民間企業にサイバー攻撃を行ったとして、2名の中国情報機関員を訴追。

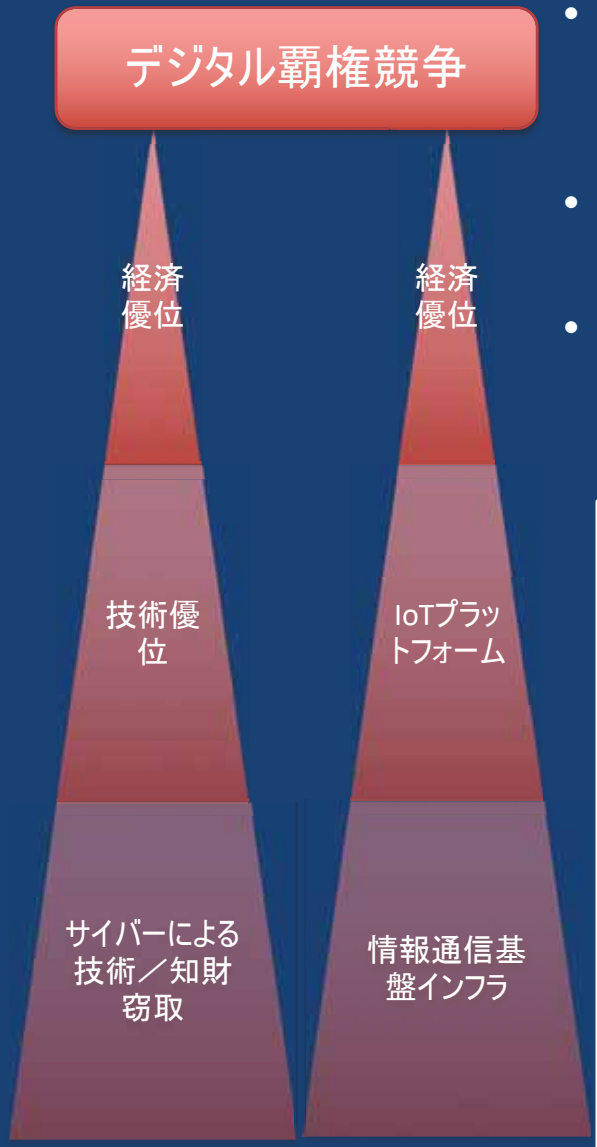
ウェスティング・ハウス・エレクトリックは原子力関連企業。2006年に東芝に買収された。2017年原子炉建設事業の赤字が原因でCh.11に基づく破産保護を申請し倒産。
同社の主力商品の加圧水型原子炉AP!000（第3世代）は、 2008～中国に輸出され、同社と中国国家核電技術公司は技術開発協力協定を締結。2010年中国のサイバー攻撃グループAPT1がAP1000に関する技術情報を窃取したとして、2014年米国司法当局はPLAの軍人5人を起訴。
AP1000の技術は中国に渡り、WHの競合製品としてCAP1400が登場。

5G Clean Path VS Digital Silk Road



出典：各種報道資料より著者作成

米国における総合的・横断的な対応



- 中国によるサイバー攻撃や世界各国における5G通信基盤への参画について、デジタル覇権競争を優位にするための中国の戦略的な行動と米国は認識。
- そのため、国家が関与するサイバー攻撃に対応するアクティブ・サイバー・ディフェンスのみならず、総合的・横断的な政策対応を実施。
- 米国では重要インフラについて分野横断的にサプライチェーンリスク対策をしており、日本でも政府調達や5Gに限らず、重要インフラ横断的にサプライチェーンリスク対策が必要。

- アクティブ・サイバー・ディフェンスの例
  - APT1 →分析レポート(2013.11)、PLA関係者5名訴追(2014.5)
  - APT10→分析レポート(2017.4)、国家安全部関係者2名訴追(2018.12)
  - ムーディーズ、GPS企業への攻撃→実行犯を訴追(2017.11)
  - GE等への攻撃→国家安全部高官2名訴追（2018.10）、実行犯訴追(2018.10)
- サプライチェーンリスクへの横断的対応
  - 不公正貿易・技術移転への対応：USTR報告書(2018)、通商法301条での対抗措置
  - Huaweiへの対応（懸念先リスト掲載、制裁違反での訴追）
  - 重要インフラからの排除：サプライチェーンから懸念国企業排除(大統領令2019.5)
  - 政府調達からの排除：2019年国防授権法
  - 米国への投資からの排除：CFIUS強化
  - 地域の通信網からの排除(FCC 2018.4)