

データ駆動社会の実現に向けて

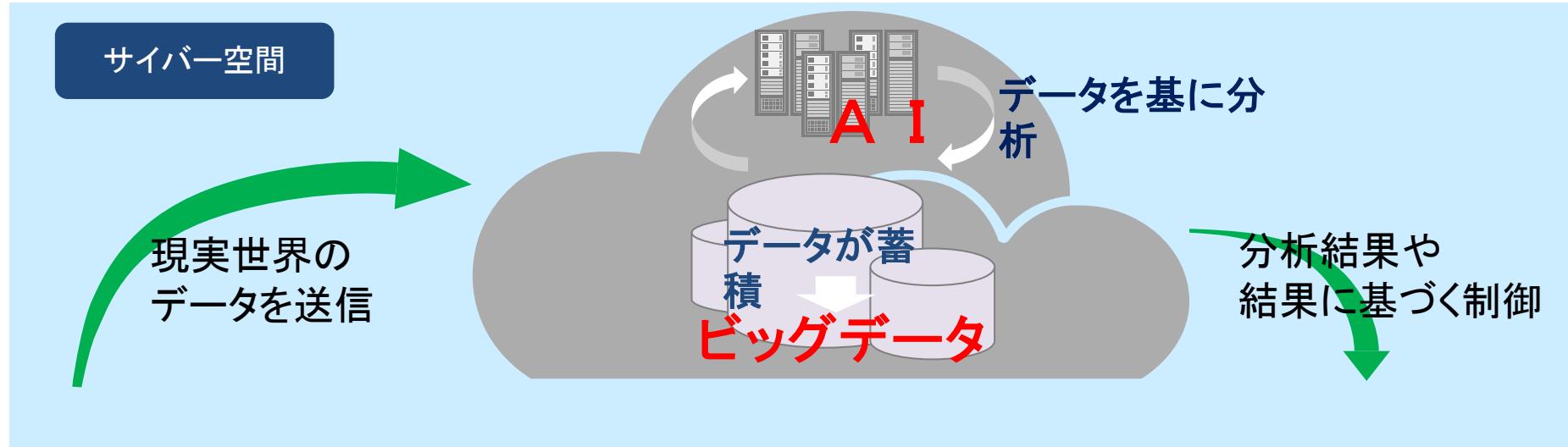


2023年11月10日

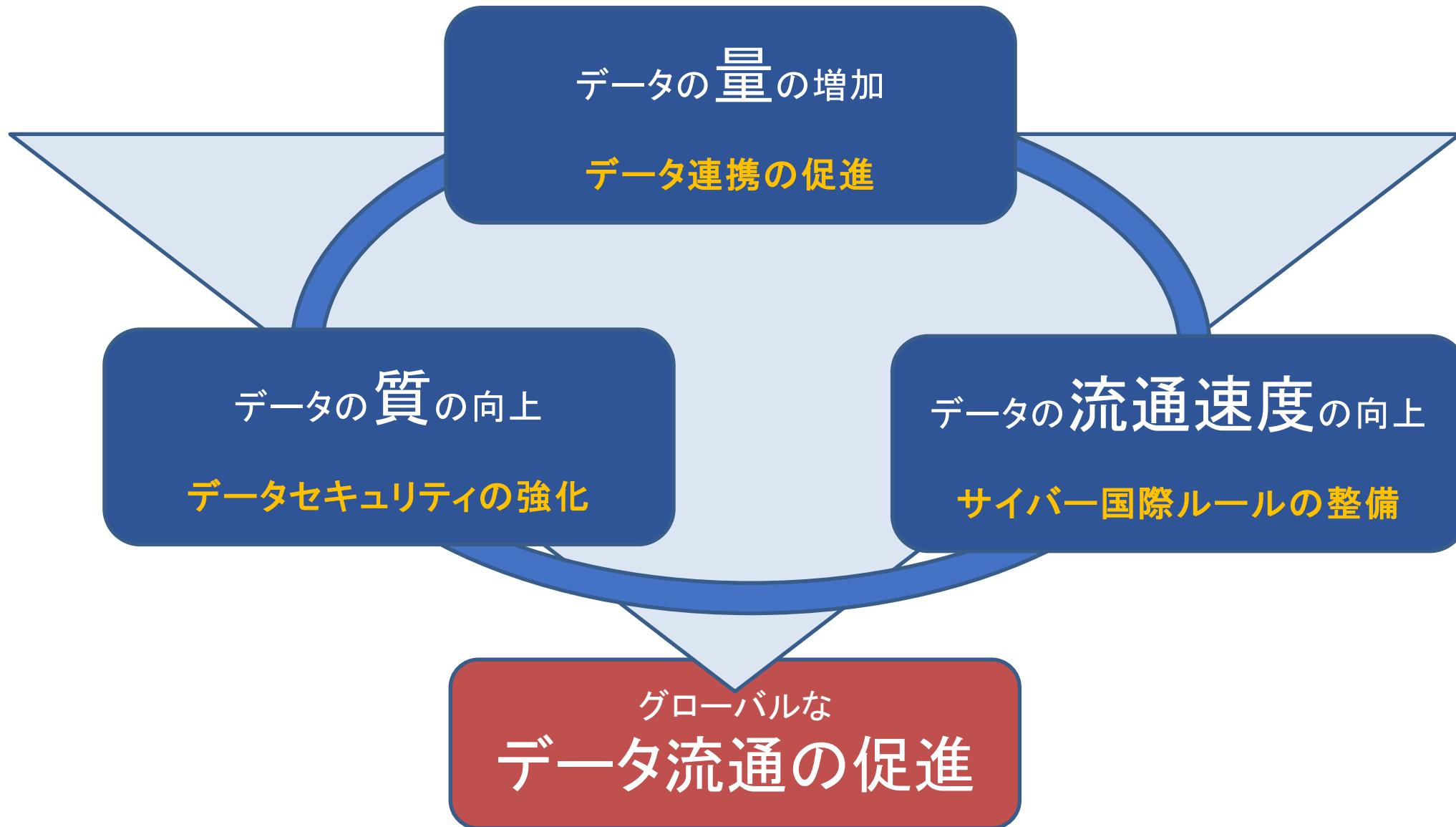
株式会社インターネットイニシアティブ
取締役副社長

谷脇 康彦

データ駆動社会 (Data Driven Society)



データ流通を促進するために



加速化する欧州データ戦略



データ法(2023年2月、欧州委員会決定)

- ◆ IoTデータの(適正な対価での)共有促進
- ◆ 大企業と抽象企業との間のデータ契約の適正化を確保
- ◆ クラウドサービス間の円滑な乗り換えを義務化

データガバナンス法(2023年9月施行)

- ◆ データ仲介事業者(情報銀行、データ取引市場、データ協同組合)を届出制とし、データのセキュリティ確保を要件化。

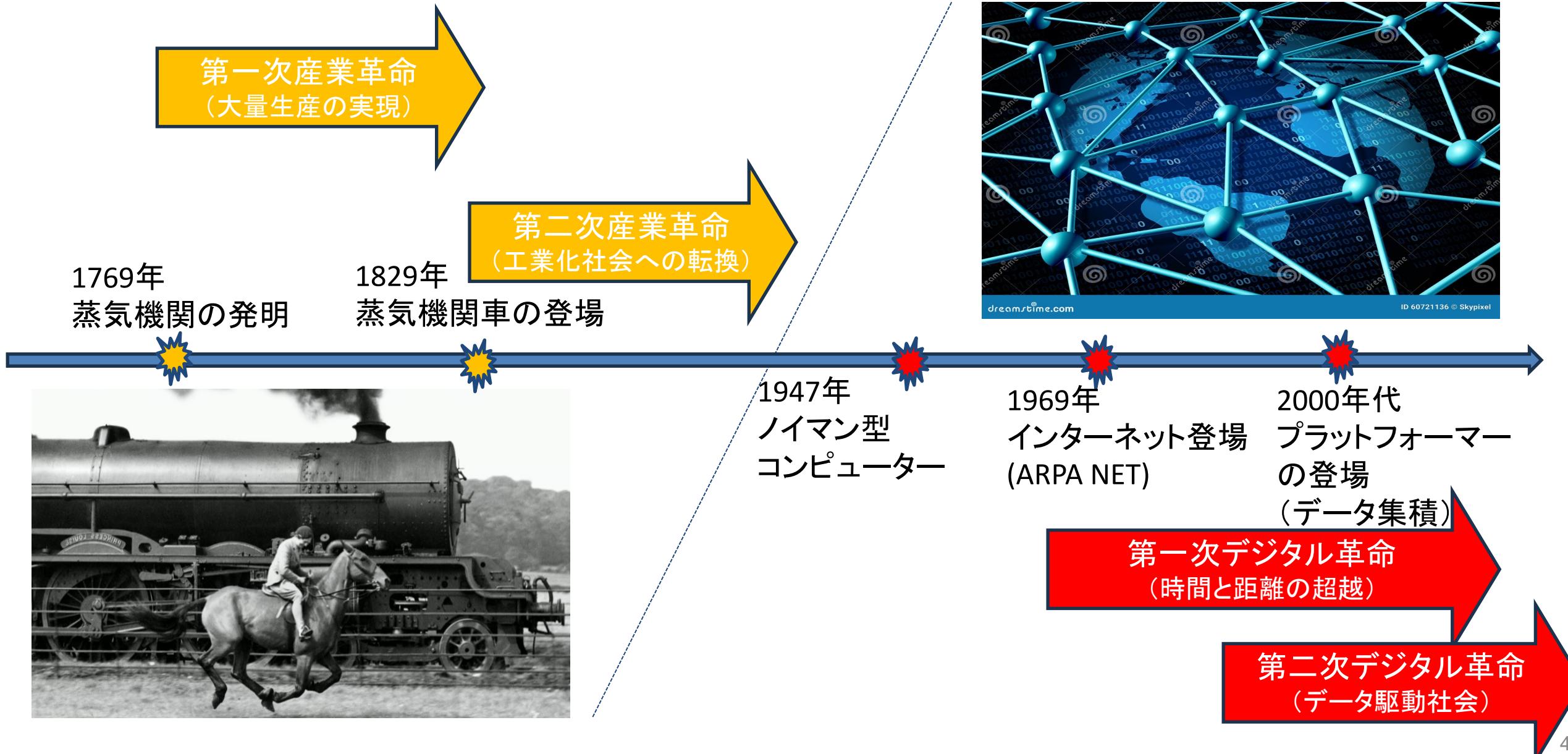
AI法制定の動き

- ◆ AIの危険度(リスク)を4段階評価し、必要な規制を適用。



データ活用やデータセキュリティを確保するための法制度を早急に検討すべき。

産業革命とデジタル革命



サイバー空間における新たなルールの必要性

ロシアによるウクライナ侵攻、そしてイスラエルにおける戦争で必要性がより明確に…

■ 民間の重要インフラ等への国境を越えたサイバー攻撃、偽情報の拡散等を通じた情報戦等が恒常に生起し、**有事と平時の境目はますます曖昧**になってきている。

(グレーゾーン事態)

■ 国家安全保障の対象は、経済、技術等、これまで非軍事的とされてきた分野にまで拡大し、**軍事と非軍事の分野の境目も曖昧**になっている。 (ハイブリッド戦争)

(注)「国家安全保障戦略」(2022年12月)より引用。



インターネットに対する**国家関与**はどこまで許容されるのか

インターネットの**基本精神** (自律・分散・協調)は守られるべき



インターネット運営(internet governance)のあり方が問われている

サイバー空間に適用される国際法についての合意はない (GGE, 2015年6月)

国家主権、平和的紛争解決、内政不干渉については具体的

に守るべき規律(must)として記載。

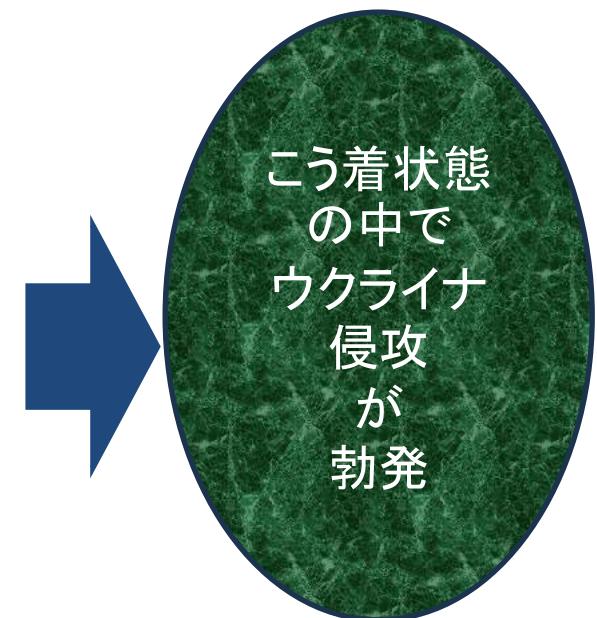
国際法の適用はあくまで適用可能(applicable)とのみ記載。

自衛権の行使や国際人道法の適用は記載されず。

・**軍事目標主義**(武力の行使は相手の軍事力を破壊する目的のみに行使可能)

・**害敵手段の制限**(武力行使の際に使ってもよい武力を制限)

許容されるサイバー攻撃の範囲は不明



ウクライナ侵攻とデジタル技術

フェイクニュースの流布



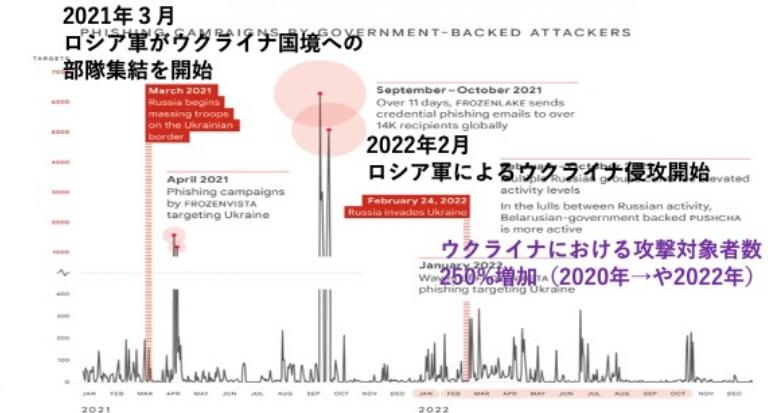
AIによる偽アカウント自動生成



偽動画（ディープフェイク）



ロシアによるフィッシング攻撃



ファクトチェック機関の活躍

bellingcat

Investigations Results Guides Journals Webpage Q E-mail Contact

Latest investigations

Russia's Bucha "Facts"
Versus the Evidence



Latest resources

How to Archive Telegram Content
to Document Russia's Invasion of
Ukraine

March 2022

Help Bellingcat Decide Which Open
Source Tools to Build
Russia's

Radar Interference Tracker: A New
Open Source Tool to Locate Active
Military Radar Units

March 2022

Tracking Russian Military Vehicles

偽ファクトチェック機関の登場

PROPUBLICA

Фейк от Украинских СМИ

Pro-Russian fake "fact-check" video debunked by Clemson's Media Forensics Hub and ProPublica

On March 2, 2022, a Russian-language video went viral on social media, falsely claiming that a missile strike had hit a hospital in Kyiv. This is an example of how Russian disinformation can spread rapidly through fake news outlets and social media platforms.

Photo: AP

Пожар в г. Первомайске 2021 г.

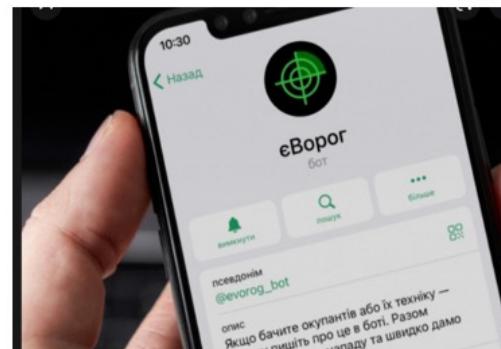
Огонь из российской ракеты разорвало центр в Киеве

2021 г.

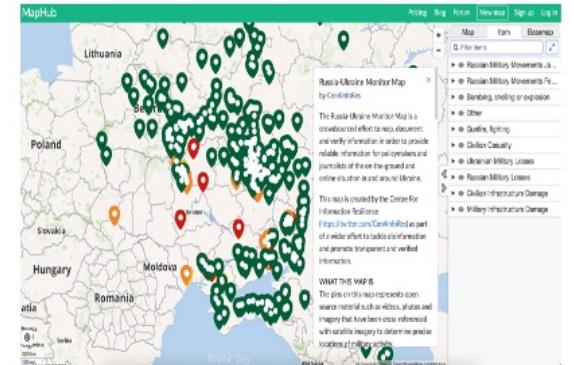
Source: ProPublica

Text at the bottom: "This image is from a Russian-language video that falsely claimed a missile strike had hit a hospital in Kyiv. There is no evidence the video was created by a Russian government or military entity. The video was posted on social media and widely shared by pro-Russian accounts. It has since been debunked by researchers at Clemson's Media Forensics Hub and ProPublica. The video is a doctored version of a video shot on fire after being hit by a Russian missile. Taken attributing the event to Ukrainian media. The original video can be seen here: [link]."

SNSを活用したロシア軍の動向把握 (eEnemy) IT軍(約32万人の民間人材、大半がウクライナ国籍)

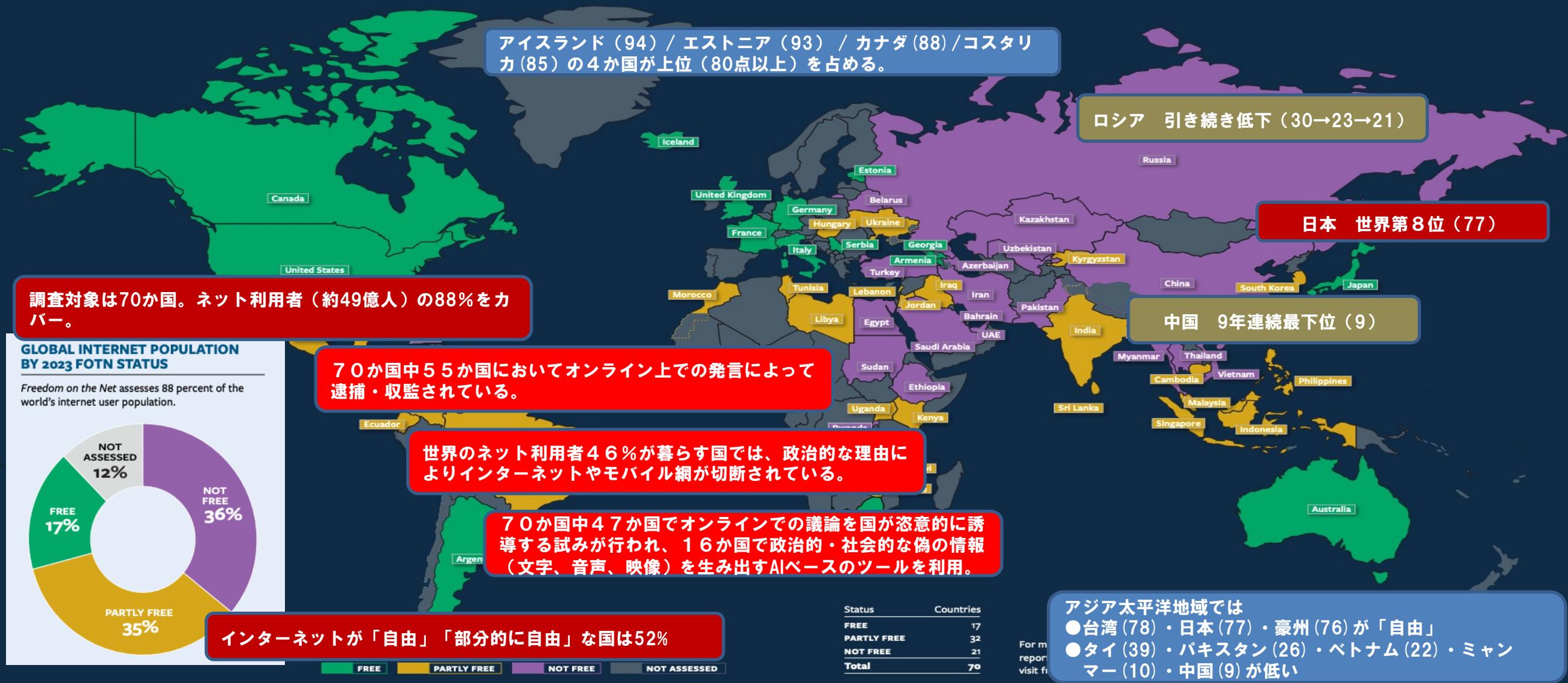


OSINT情報のマッピング



ネットの自由 (Freedom on the Net)

FREEDOM ON THE NET 2023



ネットの自由 (Freedom on the Net)

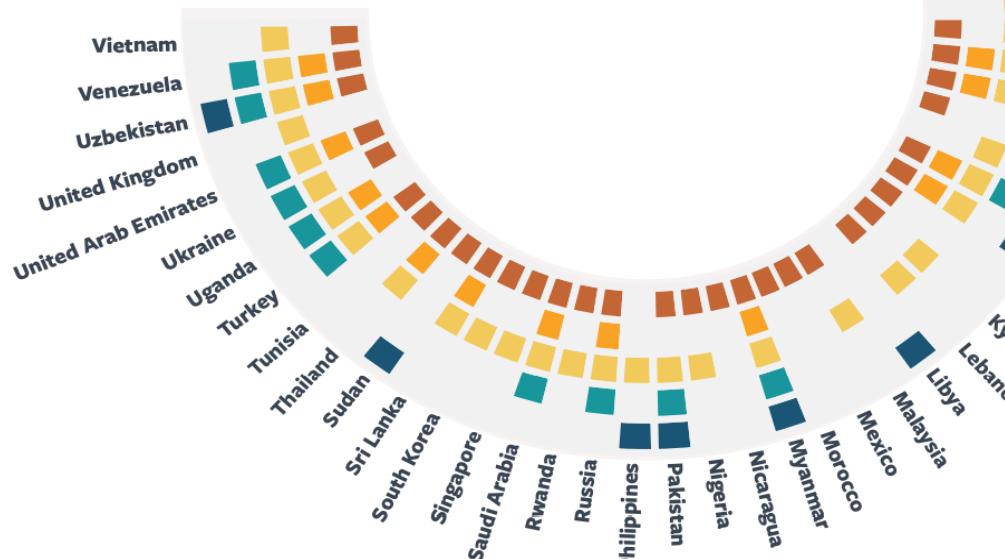
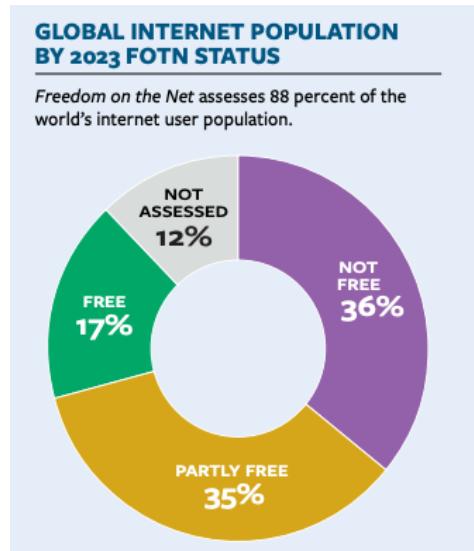
ネット上における検閲

インターネット接続を規制(16)
ソーシャルメディアをブロック(22)
ウェブサイトをブロック(41)
VPNをブロック(19)
コンテンツの削除(45)

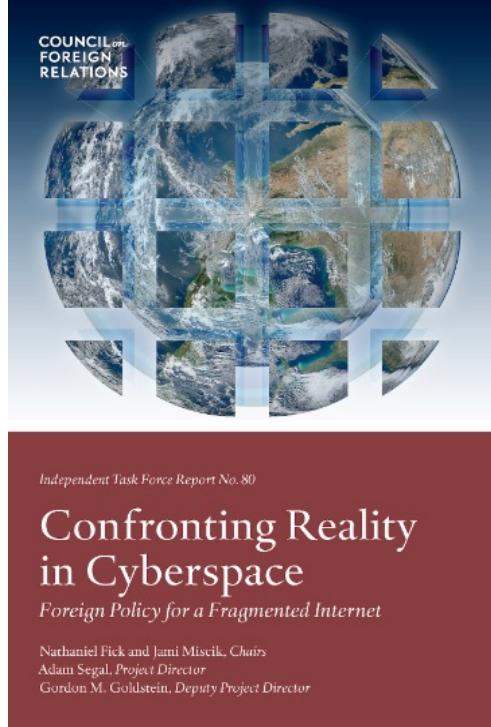
INTERNET CONNECTIVITY RESTRICTIONS	16
BLOCKS ON SOCIAL MEDIA PLATFORMS	22
BLOCKS ON WEBSITES	41
BLOCKS ON VPNs	19
FORCED REMOVAL OF CONTENT	45



41か国において、政府は政治的・社会的・宗教的なコンテンツをホストするウェブサイトをブロックしている。



米外交問題評議会報告書（2022年7月）



- グローバルインターネットの時代は終わった
(*The era of the global internet is over*)。
- オープンでグローバルなインターネットを促した
米国の政策は失敗。
- 米国は敵対国(adversaries)に対して
十分なコスト(訴追、経済制裁)を払わせることに失敗。

(出典)Council on Foreign Relations (CFR) “Confronting Reality in Cyberspace : Foreign Policy for a Fragmented Internet”
(Independent Task Force Report No. 80)(July 2022) <https://www.cfr.org/report/confronting-reality-in-cyberspace>

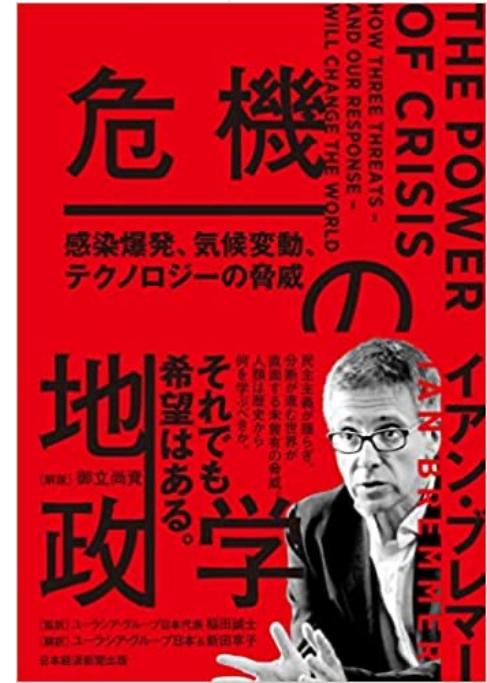
デジタル冷戦の可能性

“米中以外の国々には、**デジタルのベルリンの壁**がいずれ築かれていくのが見えていて、どちらかの側につかなければならぬのだろうかと注視している状況だ。かつての冷戦を鏡写しにしたような、新しい冷戦の一つの形がこの壁であり、少なくとも新技術をめぐっては、**各国は米中どちらかの陣営に足並みを揃えるしか選択肢がない**だろう。”(P268)

“我々全員、すなわち、政治指導者、産業界のリーダー、思想的指導者、そして市民が連携して協力し合い、こうした変化にどうすればいちばんうまく対処できるのかについて、**妥協点を探る意思が必要**になる。それに向けて第一歩を踏み出すには、まず、**新たな冷戦が起きれば、破壊ばかりで無益なのだと認識しなければならない。**”(P271)

“世界の民主国家は新技术の開発と利用を統制するための**包括的な国際制度**(注:世界データ機関)を築く必要がある。”(P278)

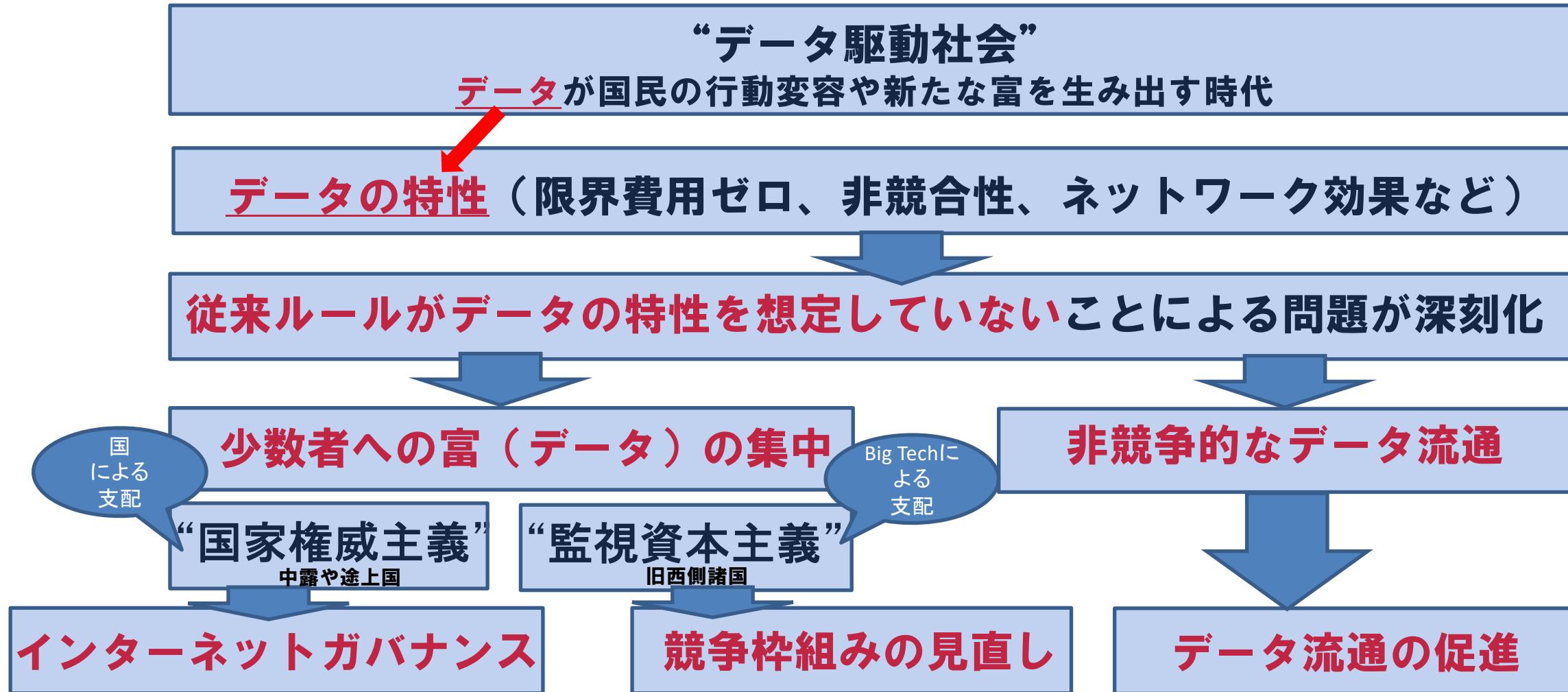
(出典)イアン・ブレマー「危機の地政学」(2022年、日本経済新聞出版)



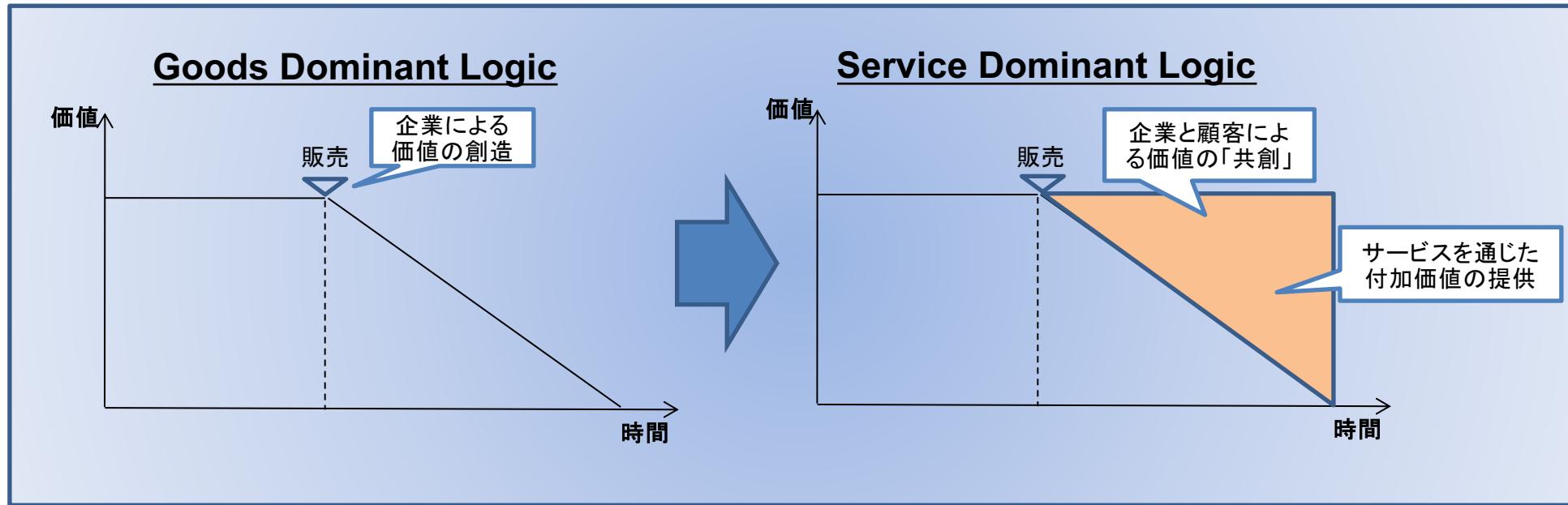
インターネットを巡る10の論点



1. 有形資産と無形資産



2. モノ中心主義とサービス中心主義



“競争優位の原動力は製品からデータへ紛れもなくシフトしている。いまやデータが製品を支えるのではなく、製品がデータを支えている。なぜならセンサーやIoTなどの先進デジタル技術により、製品がユーザーのインタラクティブデータを運ぶ導管として機能するようになったからだ。”

(出典)モハン・スプラマニアム著「デジタル競争戦略」(ダイヤモンド社、2023年8月)

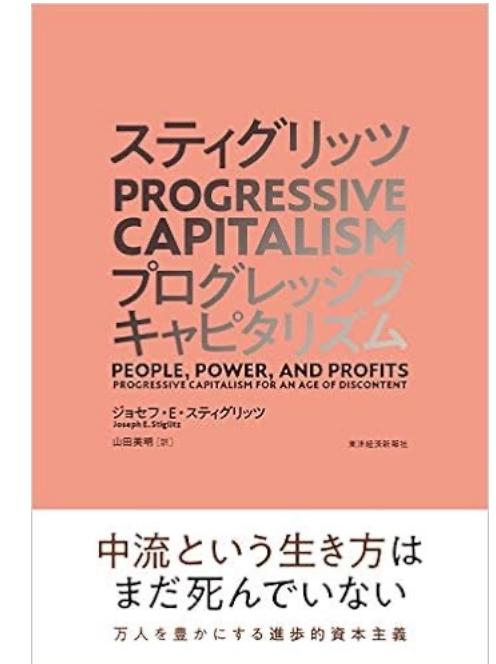
3. 新自由主義と修正資本主義

“レント増加の最大の要因は、**超過利潤**、すなわち競争経済で手に入れられる利益をはるかに超越した利益にある。”

”**上場企業の時価総額のおよそ80%はレントによるものであり、それが付加価値総額の4分の1近くを占めており、その大半がIT部門に集中**している。そしてこれらすべてが、30年前から起きた著しい変化の結果だという。”

”実際アメリカでは、きわめて収益性の高い最新の「イノベーション」として、この堀をつくり、広げる能力、その結果手に入れた**市場支配力を利用する能力を高めるイノベーション**が生み出されている。」”

ジョゼフ・E・スティグリツ「プログレッシブキャピタリズム」(2020、東洋経済新報社)



4. 事前規制と事後規制

- ✓ 事前規制から事後規制への流れ(非対称規制を除く)
 - プラットフォーム規制は事前規制
(市場支配力濫用の結果を回復するのが困難)
- ✓ 経済的規制の最小化、社会的規制の増大
 - 両者の差異は明確か。
 - (各法にいう)「公共の利益」とは何か。
- ✓ ルールベースと原則ベース

5. ハードローとソフトロー

- ✓ 技術革新とハードローの限界
- ✓ ソフトローとしての共同規制(coregulation)の可能性
 - 偽情報対策
 - ネット中立性
- ✓ “行政の不作為”としてのソフトローの懸念

6.差別と区別

- ✓ 人口減少社会-----自動化・個別化が必要
- ✓ 個別化の時代---差別との違い

“企業は価格を差別化し、その製品を特に重視する顧客や、ほかに選択肢がない顧客に対して、高い料金を設定することが可能になる。”

ジョゼフ・E・スティグリツ「プログレッシブキャピタリズム」(2020、東洋経済新報社)



7.国内ルールと国際ルール

- ✓サイバー空間には国境がない。
- ✓域外適用は、ルールの重畠適用を通じて規制の最大化を招く。
- ✓国内ルールによる保護主義的な動きを防ぐことが必要。

ルールの国際的な整合性を確保するための努力が必要。



8. 自由主義国家と権威主義国家

旧西側諸国



ICANN/IETF
(コンセンサスアプローチ)

民間主導原則
(自律・分散・協調を基本)

自由(資本)主義
(監視資本主義である面も)

TCP/IP
(IETF)

(民主的統治力は相対的に弱い)

中国・ロシア



ITU
(国に投票権)

サイバー主権
(国による統治ルールの確立)

国家覇権主義
(国による情報統治)

New IP
(ITU)

(中央統制的統治力は相対的に強い)



9. マルチラテラル主義とマルチステークホルダー主義



中国・ロシア “共同声明” (2022年2月)

■両国(中国及びロシア)はインターネットガバナンスの国際化を支持し、各國がガバナンスについて同等の権利を有していることを確認し、インターネットの国内セグメントを規制することで国内の安全を確保する主権的権利を制限しようとしないとするいかなる試みも容認できない。

■これらの問題に取り組む上で国際電気通信連合 (ITU) がより大きく参加することに関心がある。

(出典) “Joint Statement of the Russian Federation and the People’s Republic of China on the International Relations Entering a New Era and the Global Sustainable Development” (February 4, 2022)
<http://en.kremlin.ru/supplement/5770>

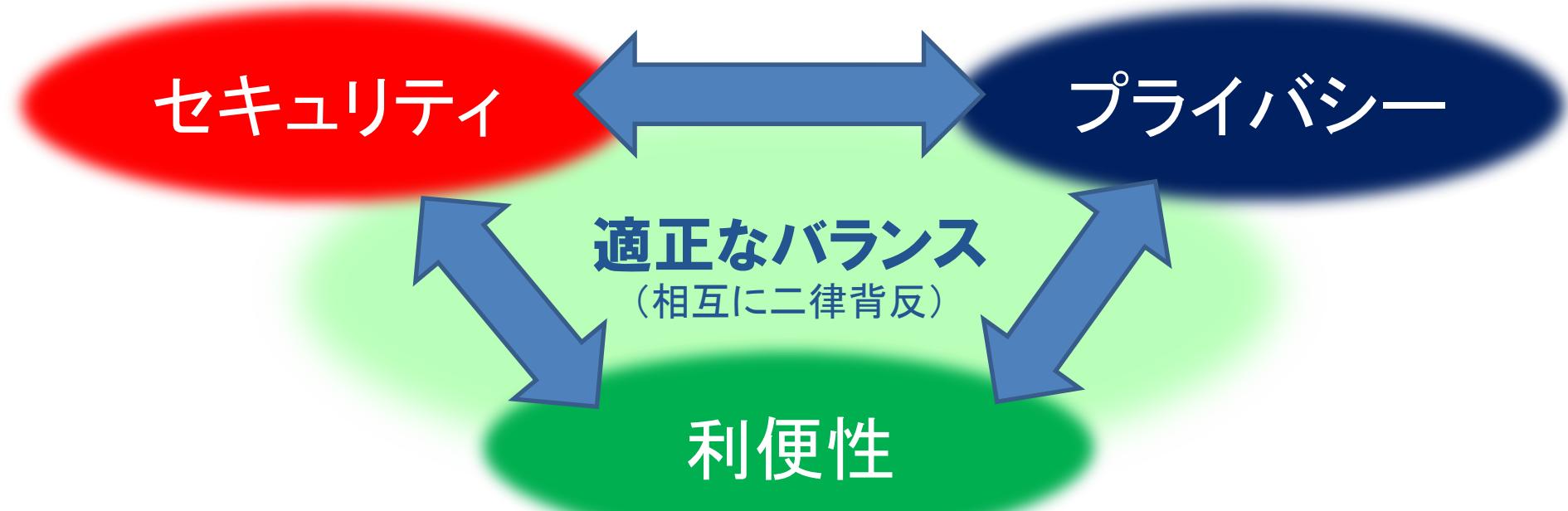
日米欧等 “インターネットの未来に関する宣言” (2022年4月) (米国、日本、欧洲連合、豪州、カナダほか計60か国・地域)

■開かれたインターネットへのアクセスが、一部の権威主義的な政府によって制限されており、オンラインプラットフォームやデジタルツールが表現の自由を抑圧し、その他の人権や基本的自由を否定するためにますます使用されるようになっている。

■インターネットの未来に関する5原則---①人権及び基本的自由の保護、②グローバル（分断のない）インターネット、③包摂的かつ利用可能なインターネットアクセス、④デジタルエコシステムに対する信頼、⑤マルチステークホルダーによるインターネットガバナンス

(出典) US Department of State “Declaration for the Future of the Internet” (April 28, 2022) https://www.soumu.go.jp/menu_news/s-Ne/01tsushin06_02000235.html
(総務省報道資料)

10. セキュリティと利便性とプライバシー



AIによって三者のバランスが急速かつ劇的に変化しようとしている

AIガバナンスの具体的ルール
を早急に確立することが必要

サイバー空間におけるトラスト(信頼)



日本のインターネットは1992年、IIJとともにはじまりました。以来、IIJグループはネットワーク社会の基盤をつくり、技術力でその発展を支えてきました。インターネットの未来を想い、新たなイノベーションに挑戦し続けていく。それは、つねに先駆者としてインターネットの可能性を切り拓いてきたIIJの、これからも変わることのない姿勢です。IIJの真ん中のIはイニシアティブ
—— IIJはいつもはじまりであり、未来です。



本書には、株式会社インターネットイニシアティブに権利の帰属する秘密情報が含まれています。本書の著作権は、当社に帰属し、日本の著作権法及び国際条約により保護されており、著作権者の事前の書面による許諾がなければ、複製・翻案・公衆送信等できません。本書に掲載されている商品名、会社名等は各会社の商号、商標または登録商標です。文中では™、®マークは表示しておりません。本サービスの仕様、及び本書に記載されている事柄は、将来予告なしに変更することがあります。