2023 年 4 月

米国情報　2023 年 4 月分

日販グローバル株式会社
米山

● 米国におけるデータガバナンスを巡る政策動向と産業界への影響（DFFT、個人・産業データの取扱など）・ DFFT/データ主権確立に向けた政策動向（個人/産業データの越境流通制限・データローカライズ義務）

・ データ集積、産業・企業間連携に向けた取り組み（各国が産業・競争政策上で重要視している産業のデータ）

・ データ経済圏確立に向けた動き（域内共通ルール化、グローバルサウスとのデータ連携）／等

DFFT/データ主権確立に向けた政策動向（個人/産業データの越境流通制限・データローカライズ義務）

・ データ集積、産業・企業間連携に向けた取り組み（各国が産業・競争政策上で重要視している産業のデータ）

・ データ経済圏確立に向けた動き（域内共通ルール化、グローバルサウスとのデータ連携）／等

はじめに

インターネット黎明期の90年代の米国政府の政策はクリントン政権によるインターネットスーパーハイウェイ構想に象徴されるネットインフラの整備であったかと思われる。
ネット上の“データ”の収集と保護に関する感度が高まったのは9-11に伴う個人・企業情報への政府によるアクセスを可能にする愛国法の施行からかもしれない。

本稿ではそのあたりからのデータに関する米政府の政策や認識を時系列に見ていき、それに伴う個人や産業のデータ越境に関する問題や課題を考察していく。

１．データ主権について

①愛国者法（Patriot Act）とデータ主権　　ソース：　CloudCarib.com

9-11 のテロに対し、米政府は愛国者法を設けた。これにより連邦政府は米国内の如何なる情報へのアクセスも許され、また米国内にあるすべての企業の全ての情報を入手できる。

米国内で事業展開する場合はもとより、米国外での事業でも、クラウドサービスなどが米国でデータ保管を行う場合には米政府のデータ監視と法執行権が及ぶという前提で事業を行う必要がある。

②データ主権　　ソース：　ウィキペディア他

データはそれが収集される国の法体系と統治構造に従うという概念。それはデータセキュリティ、クラウドコンピューティング、ネットワーク主権及び技術主権という概念にも密接に絡む。

現状、１００以上もの国々が何らかの形のデータ主権法制を有している。
この議論のきっかけとしてスノーデンによる NSA の諜報活動の暴露がある。また愛国法によりアメリカにあるサーバーにて集められた海外の情報への米政府のアクセスを拒むことはできないこともこの議論にかかわる。

もう一つの出来事として２０１３年のマイクロソフトと米政府の訴訟事件がある。
アイルランドでホストされた Hotmail のアカウントからの麻薬密売に関する電子メールへのアクセスを米司法省がマイクロソフトに求め、同社がそれに従うことは EU のデータ・ローカライゼーションとデータ保護法に違反するとして司法省の要求を拒んだ。その結果訴訟となった本件は一審では米政府が勝訴し政府の家宅捜索権が尊重された。控訴審ではマイクロソフトに有利な判決で家宅捜索権は国外にて集められた情報には及ばないとした。

今後、クラウドコンピューティングサービスが世界中に広がると、そのデータの貯蔵場所のデータ主権の問題に抵触しかねない。あるデータがある国では違法で、別の国では合法と言うこともあり得る。

データ主権の名のもとに、データの囲い込みがなされると、データの普遍性が薄れ、データ分析による公共の利益が阻害されるとジョージワシントン大学のデジタルトレードとデータガバナンス部の創設部長のスーザン・アーロンソン教授は語る。

③アメリカのデータ主権に関する出来事　　ソース：CapacityMedia.com

2021 年 1 月 6 日の連邦議会襲撃事件の 2 日後、マイクロブログサービスを提供するパーカーのサービスがクラウドから落とされ、そのアプリがグーグルやアップルのショップから外された。理由は襲撃者の襲撃計画や様々な不法行為に用いられたため。

風前の灯火となったパーカーが同月 17 日に一部復活できたのはロシアのサーバーでホ

ストしてもらえるようになったため。
その１か月後に同社はアメリカのサーバーにホストしてもらえることとなり、フル機能で復活を果たした。　この一連の流れでアメリカのデータ主権の問題が意識されることとなった。

業界固有のデータ保護法や FTC による不正取引排除の取り締まりがあり、また愛国者法では連邦政府が指定する特定個人のデータを持つ企業にそのデータの開示を義務付け、クラウド法は愛国者法に基づく連邦政府のデータアクセスを在外のアメリカの主権が及ぶ企業にも適用可能としている。逆に、米国内のデータを国外でホストすることを直接禁止する法制はない。実際、アマゾンの AWS、マイクロソフトの Azure、そしてグーグルなどは米国のユーザーデータを国外に保存している。マイクロソフトの場合、ユーザーにデータの保管地のオプションを示して選択させてはいる。
但し愛国者法やクラウド法を回避するために意図的に国外に米国のデータを持ち出す行為は取り締まられるとみられる。

いずれにせよ、米国のデータ主権は、それにかかわる法律が侵され被害が出たときに FTC なりがアクションを取る形で発動するという事後対応型で EU や中露の事前取締とは異なる。

一方、連邦政府の海外個人情報アクセスの件ではトランプ前政権においてアメリカのクラウドサービス提供業者に対し海外ユーザーの氏名、住所、メルアド、国籍、支払方法、電話番号及び IP アドレスを保存し、サイバー犯罪発生の際に法執行機関がそのデータにアクセスできることを求める大統領令を発している。

２．プライバシーデータ保護とデータ・ローカライゼーションについて

①データ・ローカライゼーションの背景

エドワード・スノーデンが 2013 年に米国の諜報機関が対テロ活動の一環で国外のプライバシーデータまで監視していた事実が明らかとなってから欧州を中心にデータ・ローカライゼーションを通じた市民・住民のプライバシーデータ保護が強化された。中にはその名のもとに自国民を監視下に置いたり、国内経済活性化に利用したりする政府も出てきた。

ドイツやフランスが単独でデータ・ローカライゼーション法を整備する動きに出たところで EU として EU 全域のデータ・ローカライゼーションを行うものの、メンバー国の単位での法制化は EU 競争法違反とする形を取った。

②データ主権とローカライゼーション・データレジデンシー　　ウィキペディアほか

データが国境を越えて送られる前に地元のプライバシー法やデータ保護法に基づくユー

ザーの合意が求められること。

体系的にはデータ主権の概念の上にデータ・ローカライゼーションが成り立つ。

データ主権はデータの主題やそのデータを処理する人に適用される法律を規定する。データ主権はある国の市民や住民に関する記録が個人データや金融データを処理する法律に従うことを求めるが、データ・ローカライゼーションはさらに突っ込んでデータの最初の収集、処理、貯蔵がまず同国内で起こることを求めるもの。国によってはその国の市民や住民のデータを同国内の海外のシステムから削除しなければならない。

テックカンパニーや多国籍企業はデータ・ローカライゼーションに関する法規制に反対してきている。理由は地域のデータセンターの集合化や国境を越えたサービスの統一化を通じた効率化をそうした法規制が妨げるため。

EU を中心としたデータ保護の動きに対し、FTA を通じデータ・ローカライゼーションや越境のデータ移転を規制する動きを禁じる動きもある。

米国を含んだ当初の TPP にはそうしたローカライゼーションを禁じる文言が入っていた。そのあとの CPTPP にそれは引き継がれている。また米墨加の USMC 協定にも同様の文言が含まれている。

③米欧間のプライバシーデータ保護協定　　ホワイトハウス

昨年 10 月の大統領令 Enhancing Safeguards for United States Signals Intelligence Activities が発せられた。これは米-EU 間のプライバシーデータの移送の枠組みが EU 法に基づく EU 裁判所で否認されたことを受け、2020 年 3 月バイデン大統領と EU 大統領間で新たに合意された EU-U.S. Data Privacy Framework における米側の約束事項を履行するための大統領令。

この中で、米諜報機関による諜報活動の目的の限定、米諜報機関による個人情報収集に伴う責任、問題発生時の対応、個人情報漏洩に関する個人からの訴えのチャネルの確保などがうたわれた。

これにより米欧間でのデジタルビジネスに伴うデータ移送の欧州側の懸念を払しょくすると共に、米国民の不安も払しょくすることを狙う。

④米国は EU の GDPR に似た法制を採用すべきか　ソース：IS Partners LLC

米国には現状米国としての一貫したデータプライバシー法は存在しない。

ビジネス界は業界ごとの連邦政府の規制や州によって異なる規制と州法の混合の中からビジネスとして意味のある対応策を個別にとっている。

この連邦政府、州政府、業界ごとの規制の混合は規制をする方も受ける方にも混乱と非効率をもたらしている。そもそもその法制は下記の通り古いものばかりである。

1974 年　U.S. Privacy Act　連邦政府が保有するデータの権利と制限
1996 年　Health Insurance Portability and Accountability Act　医療関係の患者データのプライバシーとセキュリティを定める
1999 年　Gramm-Leach-Bliley Act　金融業界における消費者のプライバシー情報収集と利用に関する規制
2000 年　Children’s Online Privacy Protection Act　オンラインサービス企業が親の同意なしに 12 歳以下の子供のプライベート情報を収集することを禁じる

一方、規制当局として FTC がテックカンパニーやソーシャルメディア企業がユーザー情報の不当な収集、利用に対し罰則を科す形で規制している。

州政府ではカリフォルニア州の Californian Consumer Privacy Act やマサチューセッツ州の Massachusetts Data Protection Act が知られているが、他に以下の 14 州が同様のデータプライバシー規制を設けている。

アーカンソー州
コロラド州
コネチカット州
フロリダ州
インディアナ州
カンザス州
メリーランド州
ミネソタ州
ネバダ州
ニューメキシコ州
オレゴン州
ロードアイランド州
テキサス州
ユタ州

一方、2018 年 5 月に欧州から GDPR がやってきて米国の多国籍企業など欧州とのビジネスを継続するために GDPR に対するコンプライアンスを進めている。すなわち、EU 内の消費者から収集したデータの越境の規制要件であり、この規制は多国籍企業の関係会社全体に及ぶ。

そのため、ビジネス界にとってはデータプライバシーに関する今後のさらなる混乱を避けるべく、連邦政府がこの GDPR に近い内容の法制を定めることが望ましい。

すでに American Data Dissemination Act や Consumer Data Protection Act、Data

Care Act といった法案が議会に上程されたものの法制化には至っていない。

３．DFFT について

①DFFT について　　ソース：　WEF

DFFT はデータの越境での自由なやりとりに関するルール作りのための基本的原理として日本の安倍晋三元首相により最初に提言された。ダボス会議でその考え方のデビューを果たした後の 2019 年 6 月の G20 会議で加盟国の合意を得ている。

その後各国では DFFT の考えに沿ってデジタル取引のルールを立てている。例えば日本では日米貿易協定や日英 EPA においてはいスタンダードな電子商取引のルールを設けることに合意している。また EU との間でデータ関連のルール作りが進行中という。

RCEP においても同様の検討が進められている。また日本はシンガポール、オーストラリアとともに WTO において電子商取引に関する多国間の議論を推し進めている。

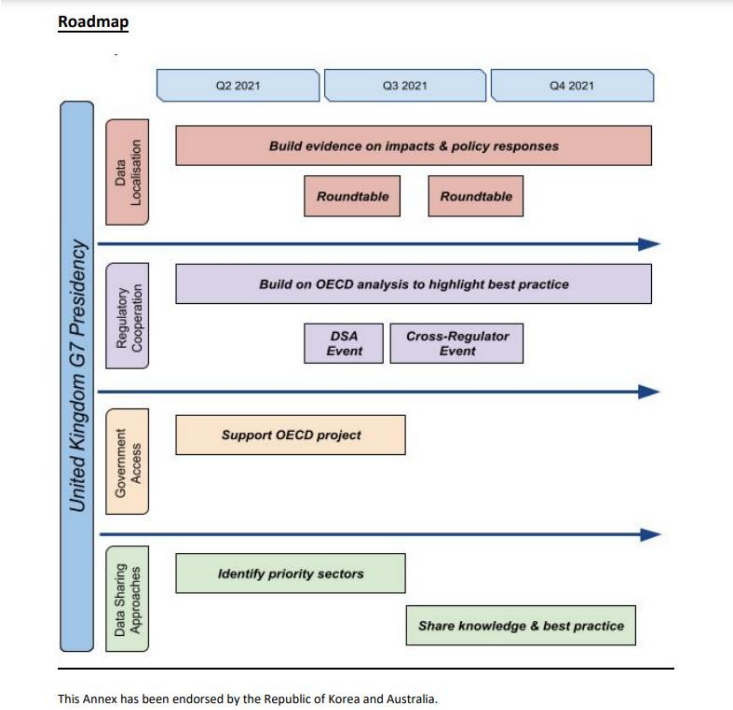
一方 DFFT の前に立ちはだかる障壁として各国独自のデータ保護とデータの信用の異なる方針がある。特に政府による民間セクターのデータへのアクセスの問題は大きな課題となっている。そこには国家安全保障の問題も関わってくる。

DFFT への１つの反論として、「もしある国が国内にしっかりしたデータのエコシステムを確立する前に越境データ移送の枠組みに参加するなら、その国のデータ資産はいずれ他国にはぎとられてしまう」というもの。一方で、座して何もしない代償も大きい。

広範な地域の国々の政策決定者はもとよりビジネスなど利害関係者の関心や懸念を網羅する形で様々に異なる政府のデータへのアクセスを分類することは DFFT への正しい議論への基盤づくりの第一歩となる。

OECD はその方向で準備を進めているがグローバルコンセンサスに至るにはまだ時間がかかる。当面は各国政府が取引相手国に自国のルールを個別に説明し理解を得ておく必要がある。

2021 年の G7 デジタル・技術閣僚会議で合意された DFFT ロードマップはこの認識を反映するものであり、さらにはデータ・ローカライゼーション、規制協力並びに優先分野でのデータ共有の 3 つの分野でのアクションプランを定めるロードマップとなっている。



2021 年 G7 サミットで合意された DFFT ロードマップ

求められるのはビジネスニーズに合致する DFFT への現実的でボトムアップのアプローチである。すなわち政府間のハイレベルな包括的ルール作りと並行して個別の問題を解決していく官民の間のパートナーシップは成り立たせることは可能である。

個別の問題の例として、IoT の機器を世界中に販売する企業がユーザーからのリアルタイムのデータを受領できてこそ維持整備のサービスが適切に提供できるものの、ユーザーの国の法制ごとにかかるデータの取得に制約があったりする（その他の具体的な問題も 6 点別紙 1 に示してある）。

次の DFFT のマイルストーンは 2023 年の G7 サミットとなる。2022 年のダボス会議で岸田首相は 2019 年に日本が提唱した DFFT をさらに推し進めると発言している。

②DFFT に関する日米合意の米側の認識と期待

ソース：U.S.-Asia Law Institute (USALI) of NYU School of Law

EU や中国のように自国・自地域内のデータの国外流出を規制する動きに対し、米国はインターネットを通じたグローバルな発展のために規制を最小化することを提唱してきた。米政府はデータ・ローカライゼーションの要求やデータサービスへの課税に反対してきている。それは　米国の多国籍企業の利害や同国の表現の自由の伝統そしてインターネットを通じた自由なデータの流れは世界に利益をもたらすという信念に沿っている。

DFFT を提唱した日本はアジアで最初に EU から GDPR に基づき両国・地域間の自由

なデータのやりとりを認めるに足る適切なレベルのデータ保護を行っているとの宣言を受けている。

DFFT における信用（Trust）を得るには、データを送る国のデータ保護の法体系がそのデータが越境することで悪影響を受けないことを確実にするためのデータを受ける国における法的なデータ保護が十分であるかを評価する必要がある。

データの受け手の国の保護が十分でかつ合理的であり、出し手と受け手で法的に相互運用可能な体系であると確認できる時、出し手はそのデータ管理の公共政策の目標がデータの越境取引によって台無しになることはないと信頼できる。

米国と日本は DFFT の推進のために緊密に連携している。日米間の Digital Free Trade Agreement（DFTA）は 2019 年の G20 大阪サミットから数か月後の 2019 年 10 月 7 日に署名されている。この合意では DFFT ということばは用いていないが、両国間の自由なデータの流れと、様々な分野での上述の「信用」のバランスがとられている。

この合意において、デジタル製品への課税を排除し、相手国のデジタル製品への差別的取引を禁じる一方で、電子的な情報の両国間の流れを制限することを禁じている。その情報には個人情報も対象となっている。

この合意はそれぞれの越境情報伝送に伴う個別の規制を例外的に認めるものの、その規制がこの合意の目的を超えることにはならず、また双方の法的規制の枠組みに互換性を保つことを狙っている。

この合意は全般的にデータ・ローカライゼーションを禁じている。同様に、ビジネス界にソフトウェアのソースコードを開示させあり暗号化方法やキーを開示させることを企業に強制することも禁じている。

日本以外では、米英自由貿易協定の交渉の中に DFFT が含まれる可能性が高い。
さらに上院外交委員会はバイデン政権に対し、APEC を通じアジア太平洋地域でのデジタルトレード協定を締結することを求めている。

今後 DFFT をさらに推進していくにあたっての最大の障害は米国に連邦レベルの統一したデータプライバシー法制が無いこと。現状は分野別、省庁別、州別に異なるルールがあってパッチワークとなっている。

４．米中対立とグローバルサウスの状況について

①ロシア―ウクライナ戦争に見るグローバルサウスの立場　ソース：　ワシントンポスト

ロシアーウクライナ戦争において欧米、カナダ、日本、豪州などウクライナ支援を行うグループと、ロシアを支える中国、イラン、北朝鮮、ベラルーシといったグループの他に、インド、ブラジル及び多くのアフリカの国々のいわゆるグローバルサウスがある。

冷戦時代の 2 極構造のバランスから、その後の米国一極、そして多極化の世界を経て

世界の秩序作りが安定を求めて動き出すところにある。

②対中囲い込みについて　ソース：　各種報道

今年世界で中国の偵察気球が波紋を広げる中、ハイテク技術の軍事転用を阻止するため、先端半導体や人工知能（ＡＩ）、監視技術などの投資を制限する大統領令を準備中。米国は同盟国を巻き込んだ「対中包囲網」の形成を目指している。

この大統領令では経済安全保障上重要なハイテク分野に限定し、米国企業による中国企業の合併・買収（M&A）やサプライチェーン（供給網）などを監視する「対外投資審査」の導入を宣言する予定。トランプ前政権時から検討が進められ、投資禁止も視野に入れる。

一方、中国経済への過度な依存からの脱却を念頭に「貿易」「供給網」「クリーン経済」「税・反汚職」の４分野で共通ルールを構築する枠組みとなる IPEF は加盟予定 14 カ国にて交渉中で、5 月下旬の APEC 貿易相会議までに 1 分野、11 月の APEC サミットで全分野の合意を目指している。

５．個人や産業へのインパクトについて

①個人データへのアクセス制限と個人データの価値の増大　　ソース：ワシントンポスト

アップルがその iOS のユーザーに広告会社による追跡を拒絶するオプションを与え、グーグルも同様にクッキーを削除するオプションを与えることで広告企業は個人データに従来のようには楽にアクセスしにくくなっている。

法制面でも GDPR や CCPA のように企業が個人データを収集することを制限してきている。これらの結果、Facebook は昨年広告収入が大幅に減少した。その結果、zero-party data と呼ばれる有償で個人データを収集する業界が生まれている。

Tapestri 社は個人の位置情報を継続的に提供することで対価として月に 8 ドル乃至 25 ドルを支払ってくれる。その結果、アメリカの消費者は個人情報の価値を意識するようになっている。従来は自分の個人データがある程度モニターされていると知りながらも具体的にどう利用されているかまでは気にしていなかったが、zero-party data においてはその目的を理解しつつ正当な対価を得るというある種公明正大な個人データの取引となっている。

とはいえ消費者の方は自分のデータがどう使われるかあるいはそれだけの期間保存されるかといったことは知らされない。例えば、Tapestri は収集した位置情報を第三者に売却するが、それが警備会社や保険会社はもとより勤務先の企業であることもありえる。

TIKI というアプリはそのアプリのユーザーに様々な広告企業からのコンタクトを紹介

し、ユーザーが合意すると広告対象のアプリを利用する金額を 10%割り引く代わりに、そのアプリ使用中のユーザーの振る舞いのデータへのアクセスを認めることになる。
個人データのなかでどのデータへのアクセスを許し、その対価としていくら報酬を得るかという感覚が生まれる市場ができつつある。

②産業データの越境とデータ・ローカライゼーションの問題　ソース：GSM Association

元々IoT が産業のデジタル経済インフラとして注目される中、5G の登場でその流れは加速している。
IoT の接続機器の数は年率 15%で増えており、2025 年には 250 億と、無線ネットワークに連接する個人携帯デバイス（スマホや PC 等）の数を上回る。
特に農業や基礎的製造業、運輸・ロジスティクス、医療及び教育業界への IoT 導入により生産性向上等のプラスの影響は大きく、その点で途上国の経済成長を加速させる。
データの流れは越境して広がるが、そこに各国のデータ・ローカライゼーションの規制が加わると、元々の潜在経済成長を下方に押しとどめてしまいかねない。
Global Trade Analysis Project モデルでグローバルサウスの経済に与える負の影響を試算すると、新興国のブラジルで想定される GDP 成長率の 59%、インドネシアで 61%、南アフリカで 68%もの割合が差し引かれてしまう。

③AI の進展と個人情報保護　　ソース：　各種報道

バイデン大統領は 4 月 4 日、チャット GPT に象徴される AI が社会に及ぼす影響について「国家安全保障への潜在的なリスクにも対処しなければならない」と述べ、利用者の個人情報を保護する法整備を目指すと語った。
米国では研究機関に対し AI の開発停止を求めるネット上の署名活動が起きている。
米国の NPO は FTC に対しオープン AI（別紙２参照）が開発する最新 AI「GPT-4」の商業利用を差し止めるよう要請している。

【考察】

経済原則として保護貿易より自由貿易の方が全体の利益が高まることは知られているが、途上国の国内産業保護や安全保障目的での国内調達には世界の同意がある。
同様にデータの自由な流れも全体としては便益が高まるであろうが、国家安全保障はもとより個人のプライバシーの理由から越境の壁を設けることも理解はできる。
米国は軍事技術を背景に半導体、コンピュータ、PC、インターネット、GPS を軍用に開発し、冷戦崩壊とともにそれらをスピンオフし、民活化を進め、デジタル社会における

グローバルスタンダードを築いていった。

その果実は米国として産業資本経済からデータ資本経済への進化をリードしつつ、GAFA のようなその頂点に立つプレーヤーを輩出してきている。

そうした経済面とは別に、エシェロンのような監視ゲートウェイを設けたりスノーデンが明かしたような他国のリーダーの情報すら抜くといった諜報活動のインフラも築いてきたりした。デジタル社会では比較的容易にそれができることがわかっているからこそ、逆に中国の半導体やソフト、そして TikTok のようなアプリの国内での利活用にまで神経をとがらせている。

いずれにせよ、データの自由な流れを保証していくことが米国の国益即ち安全保障と経済にとっても覇権を及ぼす点からも大切になる。

この点、中国はネット上の監視体制を確立し、独自の GPS など可能な限り独自のデジタルインフラを設けて米国の影響を排除しつつ経済力を中心に自らの影響力を一帯一路や AIIB を通じてアジアから中東、アフリカに及ぼそうとしている。

デジタル経済における要素技術では米国にまだ一日の長があり、今後、半導体供給や 5G 技術での中国排除の影響は要注目だが、データを生み出す人間や機械の数で圧倒的に上回る中国は一帯一路を通じたインフラ支援の名の下で中国のデジタルネットワークの傘を広げ、5G などのチャイナスタンダードを広げつつあると見られる。

今後グローバルサウスのネット化や 5G の浸透、IoT 化やスマートシティ化、クリプト・デジタルカレンシー化、メタバース化などで乗数的にデータは生まれてくるが、それを AI 等ビジネス目的や、政府・自治体による行政・福祉の発展目的で用いられることはさておき、覇権維持と安全保障対策の目的でデータ収集・監視を行う米国にとって、世界中のデータの入手は必要であり、特に米国への敵対意図を隠さなくなった習近平政権においてはなおさらであろう。

将来を見るならば、データ量は若い人口の増加が続くグローバルサウスがネット化とともに中心となっていく可能性も高いと考えられ、仮にデータにおいても米中それぞれが囲い込みを図る中で、インドを中心としたグローバルサウスの取り込みが米国にとっても大切になると考えられる。

以上

別紙１　データ越境に伴うビジネス上の問題点と越境管理技術

Cross-border data transfers and business pain points

	Types of of cross-border data transfers	Examples of Business Pain Points
1	**Product development by online app companies**	• Barriers to entry are too high for startups and SMEs as laws and regulations vary from country to country
2	**Transfer to a foreign third-country company for outsourcing**	• Unclear if data integration and data access among multiple regions across borders constitutes a "cross-border transfer" • Companies are required to ensure the same protection and management systems in the destination country as in the source country when transferring data across borders to a third country
3	**Real-time data analysis from abroad via IoT devices - no personal data is included**	• Growing regulations on non-personal data as new data categories such as "security information" emerge. Often vague in scope and prone to sudden change • Case-by-case review processes for data localization rules could undermine the advantages of real-time monitoring, a basic capability of IoT
4	**Real-time data analysis from abroad via IoT devices - personal data is included**	• "Personal data" definitions extend not only to laws but also to guidelines and administrative notices, making them difficult to implement and interpret
5	**Provide platform services and IaaS**	• Requirements for cross-border transfers are highly complex, requiring frequent customer agreement
6	**Providing cyber security services**	• Region-specific certifications may be required for security-related information, in addition to global rules and standards, imposing a significant cost burden

Regulatory technologies and potential applications

Technology	Example applications
Machine readable code	Automated processing of new regulations
Search functions	Identifying relevant regulations
Chatbots	Providing easy regulatory advice
Big data	Analysis and synthesis of data for reporting
(Robotic) process automation	Reducing manual, human tasks
Machine learning	Prioritizing and optimizing reporting, Horizon scanning
Blockchain/distributed ledger technology	Tracking and verifying data
Cloud-based platforms	Effective data management and storage
Natural language processing	Legislation scanning, information management, labelling
Surveillance/image recognition	Identify verification

別紙２　**米国で話題の ChatGPT**　　ソース：　ワシントンポスト

米国では **ChatGPT という AI に基づくコミュニケーション・情報サービス**が流行ってきているというニュースを**在ワシントンの法律事務所の DENTONS** から得た。

テスラのイーロンマスク等の共同出資でおよそ 2 か月前に米国で設立された OpenAI という AI のリサーチ会社が開発したもので、**その特徴は相手が AI とは思えない自然な応答であり、あたかも本当の人間とやりとりしている感覚になるという。**

ChatGPT も従来のチャットボットと同様、**ネット上の多くの情報に基づいて学習**していくが、**特に重視しているのが人間からのフィードバックのメッセージ**であるという。

これは**人間のフィードバックに基づく学習補強（Reinforcement Learning with Human Feedback: RLHF）テクニックに基づく機械学習**のようである。

期待される適用分野として営業の売込み、特に顧客の特性に応じたパーソナライズされたマーケティングや SNS でのポスティング、技術営業が期待されている。

また**創造的な業務としてエッセイを書いたり、書類を作成したり、ソフトウェアのコードを書いたりもする。**

その延長線上で、**既存のソフトウェアのコードのバグを特定し修正することもできる**という。

直接のビジネス以外でもたとえば**法律事務所でクライアントからの複雑な質問に応えたり、過去の関連事例を取りそろえたりしてくれる。**

一般の消費者は普段見るチャットボットの通り一遍の対応に不満を持つ者も多いが、**ChatGPT になるとその不満を解消するようなカスタマーサービスが可能になる**という。

ただし、その技術はまだ成熟しているわけではなく**問題やリスクも多々ある。**

例えば**知的所有権で守られているコンテンツを使ってしまったり、偏見を伴う不適切なコンテンツやデータを基に応答してしまうリスク**である。

さらには**この AI が提供した情報に従って損失が出た場合に、誰が賠償責任を負うのか、それを掲載した企業か、AI の開発企業か、ユーザーか、といった法的枠組みはまだ決まっていない。**

従い、**そうしたリスクや問題を意識して、注意深く活用していくというのが米国での現状**のようである。

即ち、**当分の間、人間の管理の下で活用範囲を広げていく**ということのようである。

AI が営業員や司法書士、弁護士に置き換わると言われて久しいが、その方向に一歩ずつ近づいてきていることも間違いないようである。