令和３年度内外一体の経済成長戦略構築にかかる国際経済調査事業

デジタル経済発展に向けた諸外国におけるデータ流通関連制度等に関する調査　報告書

株式会社野村総合研究所

〒100-0004　東京都千代田区大手町1-9-2
大手町フィナンシャルシティ グランキューブ

2022年3月18日

NRI

Share the Next Values!

目次

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

本調査の背景と目的

■ 背景

- 社会のデジタル化・グローバル化が進みデータの重要性が高まる中、データがもたらす価値を最大限引き出すには、国境を越えた自由なデータ流通を確保することが重要である。
- 一方で、近年、プライバシー侵害や情報セキュリティ上の問題、当局による国内データ保護政策、競争上の課題等の負の側面も顕在化している。またこうした課題と相まって、諸外国のデジタル保護主義の動きが拡大傾向にあり、国境を越えたデータの円滑な利用が妨げられる恐れが増大している。これらはグローバルなデータガバナンスの規律が不在であることにも起因している。このため、日本がG20大阪サミットで提唱したDFFT(Data Free Flow with Trust)の具体化を国内及び世界で実現していくことが急務である。
- 日本はこれまでCPTPPをはじめ、データの越境移転に係る規律を含むデジタル貿易ルールを締結してきており、今後もデータ流通に関するハイレベルな規律を実現していくことが望まれる。

■ 目的

- こうした観点から、本事業では、諸外国とのデータ流通に係る議論の前提となる情報として、日本がデータの越境移転等に関する協定を有していないヨーロッパ諸国におけるデータ流通・越境移転に係る規制や、データ戦略等のデータ利活用に係る政策の方向性等について整理を実施した。

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

本調査の実施タスク

本調査の実施タスクの全体像

①データ流通や人工知能に関する政策方針についての調査
⇒ 特に問題となり得る規制等を把握

②データ・人工知能等に関する主要企業・業界団体等
⇒ 現地の主要企業、日系企業の進出状況を把握

③各種政策が企業活動に与え得る影響
⇒①で調査した規制・政策が②の日系企業等にどのような影響を与えるかを分析

④データ政策に関する主要マスコミ・有識者の論調
⇒③で影響ありと分析した規制・政策の評価や将来動向を分析

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

①データ流通や人工知能に関する政策方針についての調査

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

調査項目と調査の視点

■ 調査対象国において、データの越境移転に関連する制度、特にプライバシー保護などのデータの越境移転に関連しうる制度や個人情報を含むデータの越境移転を制限するもの、サーバ・コンピュータ設備等のローカライゼーション要求、当局によるデータへのアクセスを強制するような措置を伴う規制や制度の前提となる政策方針や国家戦略、今後制度化等の可能性がある政策方針等、人工知能の研究開発等を念頭に置いたデータ収集・蓄積に係る政策方針等を調査し、現行制度との関係を整理した。

■ 以上について、具体的には下記の調査項目と調査の視点に基づいて調査を実施した。

区分	調査項目	調査の視点	制度・政策の検討例
データの越境移転に関連する制度	(1)−1　個人情報保護	• 基本的には直接効果を持つGDPRが規律する。 • ただし、通信や金融、医療について上乗せ規制がある可能性あり	• EU一般データ保護規則(GDPR) • 各国のデータ保護法 • 上記の特則となる分野個別の法令・ガイドライン(通信・金融・医療に絞って調査)
	(1)−2　データローカライゼーション*	• 基本的にはローカライゼーション義務はないが、通信や金融、医療については可能性あり(通信のメタデータの保存義務等)	• 分野個別の法令・ガイドライン(通信・金融・医療に絞って調査)
	(1)−3　ガバメントアクセス**	• 諜報活動に関する法令はEUの規律範囲外のため、各国独自の法令・運用がある。	• 各国の諜報法制(仏、国内安全法(Internal Security Code)や独・BND法など)
AI関連制度・政策	(1)−4　データ収集・蓄積に関する制度・政策	• ソースコード等の開示義務があるかやデータ流通の促進に向けた政策の動向	• 各国の国家AI戦略 • 各国の国家データ戦略

注）*データローカライゼーションとは、一般には、事業を遂行するための要件として、自国にコンピュータ関連設備を設置させる義務を指す（CPTPP第14.13条等に規定される）。
しかし、本調査では、上記の意味におけるデータローカライゼーションの他、運用によってはデータの越境移転が禁止される政策を幅広く調査した。
**ガバメントアクセス（GA）とは、政府機関等の公的機関による、民間部門が保有する情報への強制力を持ったアクセスを意味する。アクセス対象となるデータの種類（非個人と個人データ）や、アクセスの目的を問わず幅広く調査した。

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

（１）−１　個人情報保護(分野横断)

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

EU加盟国のGDPRの適用状況

■ 各国のデータ保護に関する国内法の整備状況

- GDPRは直接効果を持つ規則であり本来国内法の整備は不要であるが、GDPRに加えて越境移転に付加的な条件が付されている可能性があった。
- しかし、下記の調査の通り、越境移転について、各国法においてもGDPRに追加した越境移転規制(上乗せ規制)は確認されなかった。したがって、ここではGDPR上の越境移転規制を調査することとした。

加盟国名	フランス	ドイツ	オランダ	チェコ
データ保護に関する国内法	Law No. 78-17 of January 6, 1978 on information technology, data files and civil liberties	Federal Data Protection Act (BDSG)	The Dutch GDPR Implementation Act (Uitvoeringswet Algemene Verordening gegevensbescherming) (“UAVG”)	Act of 12 March 2019 on personal data processing
GDPRとの差異(越境移転)	なし	なし	なし	なし

以降、GDPRの移転規制を見る

■ 上記弊社調査結果について、例えばWhite & Case法律事務所も上乗せがないとの見解をとる；

- (b) Does national law restrict the transfer of specific categories of personal data to third countries?
  - In the absence of an Adequacy Decision, EEA Member State law may, for important reasons of public interest, expressly set limits to the transfer of specific categories of personal data to a third country.
    - most of the EEA Member States have not implemented any restrictions beyond those set out in the GDPR;
    - Cyprus and Denmark, under certain conditions, apply certain additional restrictions to the transfer of sensitive personal data to third countries; and Liechtenstein applies certain additional restrictions to the transfer of personal data by banks or telecommunication companies to third countries. Slovakia applies certain additional restrictions to law enforcement authorities that transfer personal data relating to criminal offences and convictions to third countries.

出所)White & Case “GDPR Guide to National Implementation”
(https://www.whitecase.com/publications/article/gdpr-guide-national-implementation)

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

GDPRにおける越境移転の概要

■ GDPRにおいては越境移転が原則として禁止されている。この例外についてGDPRは主に5つを規定しているが、EU域内と同等以上のデータ保護をどの単位で担保しているかという観点から理解するとわかりやすい。

■ まず、国レベルの保護を担保する十分性認定については日本法と同様である。日本以外にも、スイスや英国、南米等複数の国が指定されている点に特徴がある。また、相手国の法制度が不十分であっても、国際協定等の実装行為をもって補完することで十分性を認めることがあり、かつての米国への十分性認定はこの例であった。なお、EUから日本への移転データについて、EUからの十分性認定に依拠するには個人情報保護委員会が定めたEUからの移転データに対する補完的ルールを遵守する必要がある点に注意すべきである。

■ 次に、組織単位の担保について、GDPRは日本法よりも豊富な選択肢を規定している。まず、主にグループ企業を一体として策定したルールである拘束的企業準則(BCR)に基づく移転がある。これは、グループ単位のポリシーを現地のデータ保護を担当するEU加盟国の政府機関、データ保護監督機関(DPA)に対して提出し、審査を経て認められるものである。現状、楽天やKUMON、Internet Initiative Japan(IIJ)等の日本企業がこれを取得している。ただし、これはグループごとに起草する必要があり、自由度が高い分、認可に至るやり取りが複雑であるため、実務上はグループ単位での移転が活発な企業に限定されると思われる。他方、このように複雑なやり取りを規制当局と行うため、その過程で現地の規制当局の問題意識の把握や職員との関係づくりが行いやすくなり、規制当局にコストをかけてGDPRを遵守する姿勢を目に見える形で示せるため信頼関係が構築できるとのメリットも指摘されている。

出所)渡辺翔太「2021年に大きな変更　EU・GDPR上の越境移転対応の最新事情」
(https://xtrend.nikkei.com/atcl/contents/18/00538/00003/)を加筆修正

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

GDPRにおける越境移転の概要

■ 次に、組織単位の十分性を担保する手段のうち、最も実務的に利用頻度が高いのが、標準契約条項(SCC)である。SCCは従来、あらかじめEU当局から提示されたひな形にサインするだけで利用できるため(サインの手間などはあるものの)、実務上利用頻度がもっとも高かった。しかし、特に2021年の改正において大幅に改訂が行われ、かつ旧来のSCCが無効になることも決定された。

■ BCRとSCCはGDPR以前から存在していたが、GDPRで新たに加えられたものが認証(Certification)と行動規範(Code of Conduct)である。認証や行動規範はGDPR施行後、数年を経ても活用されることがなかったが、2021年に入って英国において認証と認証機関の設定が行われ(これは英国法に基づくことであり同国に限られる)、同じく2021年6月、ベルギーDPAがクラウドサービスプロバイダに対する行動規範を承認している。今後活用が進むことが期待されるが、現時点では事例が限られるため詳細な記述は割愛したい。

■ 最後に、同意についても例外の1つとされているものの、日本の個人情報保護法と大幅に位置づけがことなる点に留意しておく必要がある。日本法では同意は上記の国あるいは組織単位の例外と同様の位置づけだが、GDPRは十分性を担保することが原則とされ、同意はこれらに依拠できない例外的な場面でのみ活用されるべきであり、反復継続的に行われるシステミックなデータ移転等には適用できないとされる。また、そもそもGDPRにおいて同意は真正である必要があり、例えば雇用主が雇用関係にある者(従業員等)から得た同意は力関係の非対称性からその真正性が否定される。

出所)渡辺翔太「2021年に大きな変更　EU・GDPR上の越境移転対応の最新事情」(https://xtrend.nikkei.com/atcl/contents/18/00538/00003/)を加筆修正

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

GDPRにおける越境移転の概要

越境移転の根拠		概要	実務上の留意点
国単位の十分性認定	国単位の審査	欧州委員会が一定の基準に沿って外国の制度を審査し、十分性を認定する。	どの国を対象とするかは政府判断であり、企業側で対応できることは限定される。 民間部門のみ等、一定の制約が付される場合がある。
	実装行為による補完	十分性認定について、個別の政府間協定において補完	
組織単位の十分性認定	標準契約条項(SCC)	ひな形に基づいてデータ移転先・移転元間で移転データの取扱いに関する契約を締結	2021年の改訂を経て事業者が判断すべき要素や義務が拡大されている。
	拘束的企業準則(BCR)	企業グループ単位のポリシーを現地のDPAに提出し、審査を経て認められる。	自由度が高い分、締結に手間と時間が必要となる 現地当局へデータ保護への姿勢を見せ良好な関係が構築できる可能性がある
	認証	認証を実施する組織やその手法について規定	(事例が限定されるため今後の分析にゆだねる)
	行動規範	業界団体等が策定する行動規範をDPA等が評価・認証を行う	
例外	同意	真正な同意の取得がある場合	反復継続しない例外的な移転に対して依拠できる。 同意は従業員に対しては利用できない。
	契約の履行	データ主体との契約の履行に基づく場合	
	公共の利益	データ主体の生命・身体の保護等に基づく場合	

出所)渡辺翔太「2021年に大きな変更　EU・GDPR上の越境移転対応の最新事情」(https://xtrend.nikkei.com/atcl/contents/18/00538/00003/)を加筆修正

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

GDPRにおける越境移転の概要

■ 実務上最も使い勝手の良かったSCCであるが、2021年に内容が大幅に改訂された。2021年6月にSCCの改訂決定が公示され、2021年9月に改訂前のSCCが廃止されることが決定された。また、既に締結済の改訂前のSCCについても、2022年12月27日に廃止されることが決定している。SCCを締結済みの企業も移行期間の終わる2022年12月27日までに2021年決定に準拠した形で既存のSCCを改訂する必要がある点に注意すべきである。

■ 改訂版SCCの具体的な内容に入る前に、改訂の背景についても説明しておきたい。2000年代前半からGDRR施行を経ても変わることなく継続してきたSCCがなぜ突然改訂されるに至ったのか、そのきっかけは2020年に欧州司法裁判所で判断が下されたSchrems II事件である。同事件は米国へ移転された個人データについて、特に米国の政府機関による民間企業(SNSサービス等)への監視活動を念頭に、米国のデータ保護水準がGDPR上の保護水準と比較して不十分であり、それゆえプライバシーシールドを無効にした事件として著名である。裁判所は同時にSCCの有効性についても示したが、それはSCCが移転先のリスク、同事件の文脈では米国のガバメントアクセスのリスクに応じてデータ移転を実施する事業者が追加的な保護措置を講じられること、DPAはいつでも苦情処理の権限に基づいて移転を停止させ得ることから、条件付きで有効性が認められた判断であったといえる。この条件付の司法判断をSCCに明示的に導入することが、SCCの2021年改訂の目的といえよう。

出所)渡辺翔太「2021年に大きな変更　EU・GDPR上の越境移転対応の最新事情」
(https://xtrend.nikkei.com/atcl/contents/18/00538/00003/)を加筆修正

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

GDPRにおける越境移転の概要

■ 2021年の改訂版SCCの具体的な内容に入るが、ここではSCCの改訂部分を中心に扱う。改訂の趣旨から明らかであるが、SCCに移転先のデータ保護上問題となるガバメントアクセスの対応が規定されている。まず、移転先国においてSCCに規定する権利義務に影響を与えるガバメントアクセスが法令上存在しないことを確認させている(14条)。ここでは、関与する主体の数や移転の経路等、これを確認する上での考慮要素が列挙されており、企業にはこれらの要素を適切に検討したことを示せるような準備(検討内容の書面化等)が求められるだろう。また、データの移転先となる事業者がガバメントアクセスの要請を受けた場合には、それをデータの移転元に通知するといった義務が課されることとなる。

■ 以上に加え、SCCで担保すべきデータ保護の水準について、GDPRの施行に合わせてGDPR水準への向上が図られている。具体的には以下の表の内容が盛り込まれている；

主な追加点	説明
管轄監督当局	• 管理者からの移転、又は処理者間の移転に適用 • 当局はEU域内に拠点がある場合には当該拠点のDPA、ない場合には代理人の設置場所等のDPAとなっている。
GDPR上のデータ取扱いにおける基本原則の明記	• 目的の限定、透明性、データ最小化、正確性、記録保持が明記
移転先が講じるべき技術的・組織的措置	• 移転先国のリスクを踏まえて講じるべき安全管理措置の導入 • 安全管理において考慮すべき詳細な手段が列挙
移転先のデータ漏えい等対応	• 移転元、管轄監督当局、データ主体への通知が義務化 • 移転先での記録の作成が義務化
再移転(Onward Transfer)の規律強化	• 処理者に移転する場合にも越境移転規制が適用 • 移転先での取り扱いの文書作成が義務化

出所)渡辺翔太「2021年に大きな変更　EU・GDPR上の越境移転対応の最新事情」(https://xtrend.nikkei.com/atcl/contents/18/00538/00003/)を加筆修正

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

スイス現行連邦データ保護法における越境移転規制

■ スイス連邦においては、個人情報の保護に関する包括的な法令として、1992年6月19日のデータ保護に関する連邦法(The Federal Act on Data Protection of 19 June 1992)(以下「DPA」という)及び1993年6月14日のデータ保護に関する連邦法規則(The Ordinance to the Federal Act on Data Protection of 14 June 1993)(以下「ODPA」という)が存在する。DPAの最新の改正は2013年7月1日に施行されている。

- スイス議会は、2020年9月25日に、GDPRによる個人データの保護水準に合わせること等を目的とする全面的改正案を可決し、2022年下半期に施行される見込みである。また、ODPAも改正案が2021年10月14日まで意見募集手続に付されており、今後改正がなされる可能性がある。

■ 以降の分析は上記現行法令に基づいて実施する。

■ 越境移転規制についてはDPAの第6条が規律し、同条1項にある通り原則としてスイス法と同等以上の保護を与えていると認められた国のみに移転できるとされ、そのリストが公表されている。

(https://www.edoeb.admin.ch/dam/edoeb/fr/dokumente/2021/20211115_Staatenliste_f.pdf.download.pdf/20211115_Staatenliste_f.pdf)

- なお、日本については十分性が認められていない。他方、EU加盟国については十分性を認めており、スイス連邦もEUの十分性認定を2000年7月に取得している。

■ 十分性が認められない国に対しても、個別に移転を認める事由が列挙され(同条2項)、EUと同様に契約関係の締結(同項a)や企業グループ内の移転(同項g)、特定の場合の同意(同項b)といった事例が挙げられている。ただし、契約の履行や訴訟に係る理由など、GDPRよりも広い範囲で越境移転を認めている。

- 同条3項にある通り、SCC又はBCRに類似する契約関係についてはDPAへの通知がもとめられる。

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

スイス現行連邦データ保護法における越境移転規制

■ 上記のうち、契約関係の締結についてはEUのSCCを用いることが認められている。最新の動向では、SCCがSchrems II事件を受けて改訂されたことに合わせて、スイスにおいても改訂版のSCCに基づくべきことが2021年7月にスイスDPAから公表されている。(https://www.sidley.com/-/media/publications/the-transfer-of-personal-data-to-a-country-with-an-inadequate-level-of-data-protection.pdf)

■ なお、上記の契約関係の締結に基づく移転に関しては、企業が遵守すべきチェックリストが公表されている。(https://www.edoeb.admin.ch/dam/edoeb/en/dokumente/2021/Anleitung%20f%C3%BCr%20die%20Pr%C3%BCfung%20von%20Daten%C3%BCbermittlungen%20mit%20Auslandbezug%20EN.pdf)

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

(参考)スイス現行連邦データ保護の越境移転規制(抜粋)

■ Art. 6 Cross-border disclosure

- 1 Personal data may not be disclosed abroad if the privacy of the data subjects would be seriously endangered thereby, in particular due to the absence of legislation that guarantees adequate protection.
- 2 In the absence of legislation that guarantees adequate protection, personal data may be disclosed abroad only if:
  - a. sufficient safeguards, in particular contractual clauses, ensure an adequate level of protection abroad;
  - b. the data subject has consented in the specific case;
  - c. the processing is directly connected with the conclusion or the performance of a contract and the personal data is that of a contractual party;
  - d. disclosure is essential in the specific case in order either to safeguard an overriding public interest or for the establishment, exercise or enforcement of legal claims before the courts;
  - e. disclosure is required in the specific case in order to protect the life or the physical integrity of the data subject;
  - f. the data subject has made the data generally accessible and has not expressly prohibited its processing;
  - g. disclosure is made within the same legal person or company or between legal persons or companies that are under the same management, provided those involved are subject to data protection rules that ensure an adequate level of protection.
- 3 The Federal Data Protection and Information Commissioner (the Commissioner, Art. 26) must be informed of the safeguards under paragraph 2 letter a and the data protection rules under paragraph 2 letter g. The Federal Council regulates the details of this duty to provide information.

出所) Swiss Confederation, “Federal Act on Data Protection”
(https://www.fedlex.admin.ch/eli/cc/1993/1945_1945_1945/en)

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

スイス改正データ保護法の越境移転規制は、同意が例外と位置づけられるなどよりGDPRを反映し変化しているが、認証や行動規範は規定がない。

越境移転の根拠		GDPR	スイスデータ保護法(2021改正)
国単位の十分性認定	国単位の審査	欧州委員会が一定の基準に沿って外国の制度を審査し、十分性を認定する。	16条1項
	実装行為による補完	十分性認定について、個別の政府間協定において補完	16条2項a
組織単位の十分性認定	標準契約条項(SCC)	ひな形に基づいてデータ移転先・移転元間で移転データの取扱いに関する契約を締結	16条2項d
	拘束的企業準則(BCR)	企業グループ単位のポリシーを現地のDPAに提出し、審査を経て認められる。	16条2項e
	認証	認証を実施する組織やその手法について規定	(該当なし)
	行動規範	業界団体等が策定する行動規範をDPA等が評価・認証を行う	(該当なし)
例外	同意	真正な同意の取得がある場合	17条1項a
	契約の履行	データ主体との契約の履行に基づく場合	17条1項b
	公共の利益	データ主体の生命・身体の保護等に基づく場合	17条1項c, d

出所)後掲英語参考訳を元にNRI分析

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

(参考)スイス改正データ保護法の関連条文

Section 3 Cross-Border Disclosure of Personal Data

Art. 16 Principles

- 1 Personal data may be disclosed abroad if the Federal Council has determined that the legislation of the relevant State or international body guarantees an adequate level of protection.
- 2 In the absence of such a decision by the Federal Council under paragraph 1, personal data may be disclosed abroad only if appropriate protection is guaranteed by:
  - a. an international treaty;
  - b. data protection provisions of a contract between the controller or the processor and its contracting partner, which were communicated beforehand to the FDPIC;
  - c. specific safeguards prepared by the competent federal body and communicated beforehand to the FDPIC;
  - d. standard data protection clauses previously approved, established or recognised by the FDPIC;
  - e. binding corporate rules on data protection which were previously approved by the FDPIC, or by a foreign authority which is responsible for data protection and belongs to a state which guaran-tees adequate protection.
- 3 The Federal Council can provide for other adequate safeguards in the sense of paragraph 2.

出所) Walder Wyss法律事務所による非公式英訳

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

(参考)スイス改正データ保護法の関連条文

■ Art. 17 Exceptions

- 1 By way of derogation from Article 16 paragraphs 1 and 2, personal data may be disclosed abroad if:
  - a. The data subject has explicitly consented to the disclosure;
  - b. The disclosure is directly connected with the conclusion or the performance of a contract:
    - 1. between the controller and the data subject, or
    - 2. between the controller and its contracting partner in the interest of the data subject;
  - c. Disclosure is necessary:
    - 1. in order to safeguard an overriding public interest, or
    - 2. for the establishment, exercise or enforcement of legal claims before a court or another competent foreign authority;
  - d. Disclosure is necessary in order to protect the life or the physical integrity of the data subject or a third party and it is not possible to obtain the consent of the data subject within a reasonable period of time;
  - e. The data subject has made the data generally accessible and has not expressly prohibited its processing;
  - f. The data originates from a register provided for by law which is accessible to the public or to persons with a legitimate interest, provided that the legal conditions for the consultation are met in the specific case.
- 2 The controller or the processor informs, upon request, the FDPIC of disclosures of personal data under paragraph 1, letters b, nr 2, c and d.

出所) Walder Wyss法律事務所による非公式英訳

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

（１）－２　個人情報保護(個別分野：金融、医療、通信)

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

フランスにおける決済データのローカライゼーション動向

- フランス経済・財務大臣Bruno Lemaireは2019年6月、業界団体や政府機関等へのヒアリングを経て、省内で決済データのローカライゼーションに関する報告書を起草するよう指示し、有識者や産業界の代表者等からなる起草委員会が組織された。
- 本報告書の狙いはデータローカライゼーションの実現可能性や予想される結果、制約を評価することであった。ローカライゼーションについては一部の外国事業者から反対があったものの、反対が受け入れられることはなかった。
- フランス経済・財務省は2020年2月に入って報告書を公表した。この報告書においては、決済データがフランス国内にとどめ置かれるべきであること、およびフランスとしてこれをEUレベルの規制とするよう働きかけることを提案している。
- 以降、報告書の概要を記載する。

出所)フランス経済・財務省報告書(https://www.economie.gouv.fr/files/files/directions_services/cge/donnees-paiement.pdf)よりNRI作成

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

フランスにおける決済データのローカライゼーション動向

■ 報告書はまず、過去の複数のデータに対して影響を与えた司法判断やインシデント事案を挙げる；

- SWIFT事件：米国財務省によるトランザクションデータへの大量アクセスに関する事件
- スノーデン事件
- 米国対Microsoft事件(2017年・2018年)
- アマゾンAWS breakdown(2017年)
- Cambridge Analytica事件(2018年)

■ 以上の事例に対する分析から、委員会はフランスの決済データについて下記のリスクに対処する必要があるとした；

- 決済プロバイダーが政府からサービスを停止するよう命じられうる場合の政治的リスク
- 非EU政府当局の、国際法及び相互司法共助条約の規則の外側の裁判所決定(召喚状)に基づくデータアクセス
- 非EUオペレーターがEU消費者の決済データに関するデータに対して十分な水準の保護をしていない場合、とりわけ、運用地国で諜報機関から法的拘束力ある開示要請がなされた場合(米国の制裁など)の諜報活動のリスク
- EUの利益のためでない目的の決済データの販売
- 不公正な手法(価格の引下げなど)を通じて地元の競争者を排除するような、非EUオペレーターによる支配的地位濫用のリスクなどの経済的考慮
- 決済に関する国際基準を設定する主体にEUのプレイヤーが参加しないことは、EUのプレイヤーが不利益を被ることがあるが、こうした不参加などを含む、国際決済システムにおけるガバナンスリスク
- EEA全体の警察及び司法当局の捜査権限の縮小、非EUオペレーターが当局の要請に応えないということが起こり得る可能性

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

フランスにおける決済データのローカライゼーション動向

以上の分析を元に、委員会は報告書において下記を勧告した；

1. GDPRの枠組において、EEA内決済のために、EEAレベルでの厳格なデータローカライゼーションを強いること(決済者と被決済者の両方がEEA内にある場合の取引など)。データは直接又は間接的に自然人に関連づけられる。これは、決済者/消費者と被決済者/商品販売者の間の決済取引に付属する全てのデータに、当該データが、個人のアカウントIDが隠されているか明確にされているかに関わらず、個人のアカウントID、カード又はなんらかの他の決済方法を通じて識別可能な個人に直接または間接的に関連付けられる限りで及ぶ。報告書は、商品販売者の詳細、位置情報、IPアドレス、購入者の詳細などの例を挙げている。特に重要なのはこの義務が厳格であることで、たとえば決済データはEEA外に移転されてはならないし、すべてのプレイヤーに、彼らが(決済関連の法令で)規律されていようがいまいが、適用される。

2. インターチェンジフィー規則(IFR)の次なる改正にデータローカライゼーションを含み、IFR第7条の意味における決済処理組織(スキーム組織とは区別されなければならない)は、EEAにおける決済データをローカライズすることが求められるとすること。

3. モバイルデバイスでのクロスペイ・ソリューション(AppleペイやGoogleペイなど)において、EEA外へ決済データが移転されないことを確保すること。

4. 共同バッジカード(二つの決済スキームを組み合わせたカードなど)が、たとえばモバイルデバイスで、トークン化されたとき、そのカードの二つのブランド間での厳格な同価値性を尊重するために、二つの決済トークンが発行されること。たとえばそれぞれのスキームにひとつ発行されることを確保すること。さらに、報告書は、この点をIFRの今次改正に含めることを勧告した。

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

フランスにおける決済データのローカライゼーション動向

5. 欧州データ保護会議(EDPB)は、(i)名称の効果と共に、データコントローラ又はデータプロセッサとしての、ペイメント・チェーンにおける当事者の法的地位、(ii)決済データの商業的利用の合法性、(iii)決済代行者に適用される保持期間に関するガイダンスを発行するべきである。

6. クラウドにおける決済データの保管と処理をアウトソースしているEU金融機関が、(i)EEAベースのクラウドサービスプロバイダーを使うこと、又は(ii)少なくとも非EEAクラウドサービスプロバイダーに対する、EEAにおけるデータのローカライズの、契約による義務付けを求めることを奨励されるよう確保すること。さらに、(iii)決済データが、クラウドサービスプロバイダーがエンジニアにデータを変えさせることができないような方法で暗号化されるよう求めること。

次なるステップとして、報告書は、データローカライゼーションの要請を、IFRの改正版、EDPBの会議、EBAからの新しいガイドラインの発効、そして最終的にはGDPR自体の改正に含めることを勧告した。

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

（1）−２　個人情報保護(個別分野：医療)

医療データ共有PFにおける米系クラウドの排除

- フランスでは、医療関連の学術研究を推進するため、政令に基づいてHealth Data Hub (HDH)と呼ばれるデータ共有PFが構築されている。これはAI関連の政策(後述)と結びついており、医療分野においてAIにおけるデータ解析を進めるためのインフラとなるものである。
- このデータ共有PFのインフラとして、米国のマイクロソフト社が提供するクラウド基盤Azureが用いられることとなっているが、CNILはこの点に懸念を表明している。すなわち、CJEUが2020年に判断を下したSchrems II判決において、米国における政府の監視活動がEU法上の十分な保護を与えていないと判断された点から、追加的な保護措置が講じられていない限り、米国へのデータの移転が許容されない。
- データの機微性と件数の多さから、本PFはデータ保護について、第三国当局の直接のアクセスを防止することを含め、最高水準の技術的・法的措置が取られるべきであり、CNILは本PF上にあるデータのホスティングや管理が、EUの管轄のみに服する主体によって提供されるべきであると推奨している。

- 国務院も同様の立場に立っており、CNILはHDHを所管する保健省に対して、一定の期間内に上記リスクを除去する技術的措置をとることを求めた。結果、同省は12~18カ月以内にこのような技術的措置を導入し、いかなる理由があっても2年を超えないことを約束した。
- CNILは以上の移行期間がデータ保護と学術研究の推進を調和させる適切なバランスの取れたものであると評価し、受け入れた。

- (NRI注：ただし、CNILの上記見解はあくまで米国企業が提供するクラウドへの懸念に基づくものであって、一般にEU域外のクラウドサービスを排除することまで求めているわけではないと考えられる)

出所)CNIL, ” La Plateforme des données de santé (Health Data Hub)” (https://www.cnil.fr/fr/la-plateforme-des-donnees-de-sante-health-data-hub)

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

医療分野における認証制度

- フランス公衆衛生法(2017年オルドナンスによって改正)L.111-8は 、第三者(ヘルスデータ・コントローラ、リサーチ・スポンサーなど)を代表して、ヘルスデータをホストする企業の義務的認証を規定している。
- この認証は、フランス認証委員会によって認証された専門組織が二段階調査を行って与える。二段階調査は、第一に、認証枠組の遵守に関するホストの書類作成の評価、第二に、ホスト企業の作業監査から成る。

出所)Bird＆Bird, “Processing health data in France: What to look out for after GDPR?”
(https://www.twobirds.com/en/news/articles/2019/France/processing-health-data-in-France-what-to-look-out-for-after-gdpr)

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

通信記録の保存を定めたデータ保存指令に基づく仏国内法について、CJEUで審理されているが、これがEU法上違法とされる可能性が生じている(独法は既に違反と判断)。

■ この事案は、違法なインサイダー取引とされた二つの嫌疑に対するフランスでの捜査に関係する。検察は主に、フランス金融市場庁(AMF)が集めた電話線の利用に関するパーソナルデータに基づいていた。破棄院は、国内の立法府に、行政当局によるEU指令2003/6及び規則596/2014の履行を可能にするため、一時的だが一般的な接続データを保持することをデータ電気通信オペレーターに求める独立した義務があるか否かという質問を付託した。この市場における不正行為に関するEU二次法は、行政当局に対し、「既存の電話及び既存のデータトラフィックレコードを要求する」権限を与えている。

■ Sánchez-Bordona法務官によると、市場における不正行為に関する上記EU指令と規則が発効していたとしても、*La Quadrature du Net*における判例が適用可能である。同法務官は、市場における不正行為に関するEU立法の外で作成されたデータトラフィックレコードの処理は、e-プライバシー指令に照らして解釈されなければならないとした。e-プライバシー指令は、これに関する参照標準を設定している。市場における不正行為に関するEU指令も規則も、データを保持する特別かつ自律的な権限を与えていない。それらは単に、これらデータへのアクセスを認めているのみである。他の事例におけるように、フランスのシステムは、犯罪との闘いのためのデータ保持に関係するが、予防的、一般的かつ無差別であるがゆえに、*La Quadrature du Net*でCJEUが支持した均衡を欠いている。二つの嫌疑に対する刑事捜査について、同法務官は改めて、国内裁判所はその不適合性の効果を限定的に解することはできないと強調した。

出所)併合事案C-339/20、C-397/20 (*VD and SR*):
(https://curia.europa.eu/juris/documents.jsf?num=C-339/20)

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

ドイツにおいては、ヘルスケア分野のデータについて、ドイツ国内、EEA又は同水準のデータ保護の国で保管すべきことを定める法令が存在する。

■ ヘルスケアの分野におけるデータについて、ドイツ国内、EEA圏内又は同水準のデータ保護の国に保存すべき旨を定めた法令として、Sec. 80 (II) of the German Social Code No. 10 (“SGB X”)が存在する。

- なお、日本は2019年に欧州委員会からGDPR上の十分性認定を取得しており、上記における「同水準のデータ保護の国」として認められるというのが、現地弁護士の見解である。

出所)データ保護を専門とする弁護士へのヒアリングよりNRI作成

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

ドイツにおいても、電気通信法における通信メタデータの国内保管義務が存在するが、これがCJEUで無効とされる可能性が生じている。

■ 本件は、電気通信法(TKG113条以下)で規律されるドイツのデータ保持規制の適合性に関する事件である。本件では、ドイツで公開のインターネットサービスを提供する二つの企業が、連邦行政裁判所(Budesverwaltungsgericht)において、交通及び位置データを保持するTKG上の義務に対して訴えを起こした。同連邦行政裁判所は、ドイツ法は、データ保持にいくつかの制約を課しており、そこには、特定の電気通信の方法に関する特定のテレコムデータのみを保存しておくことや、保存期間の大幅な短縮(位置データには 4 週間、その他のデータには10週間)があることを強調した。

■ サンチェス・ボルドナ法務官は、ドイツの立法過程はCJEUの判例に従おうという意図があったことを示していたとした。しかし、ドイツの規則は、広範囲の交通及び位置データの保管義務を含む、一般的で無差別なデータ保持レジームを構築している。期間の限定は、こうした状況を解決するものではなく、電気通信の管理はもっとターゲットを絞って行われなければならない。したがって、同法務官は、ドイツのデータ保持立法は支持しえず、(保存期間に関わらず)プライバシー及びデータ保護の権利に対する不正で深刻な介入であるとした。

出所)CJEU併合事案 C-793/19 及び C-794/19 (SpaceNet 、Telekom Deutschland)

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

(２)データローカライゼーション

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

データローカライゼーションの指す範囲

- データローカライゼーションとは、一般には、企業などに対し、事業を遂行するための要件として、自国にコンピュータ関連設備を設置させる義務を指す（CPTPP第14.13条等に規定される）。
- しかし、EUにおいては上記の厳密な意味におけるローカライゼーションは必ずしも多くなが、上記に至らないものの企業活動に影響を与えうる措置が確認された。
- そのため、本調査では、上記の意味におけるデータローカライゼーションの他、運用によってはデータの越境移転が禁止される政策を幅広く調査した。例えばEUデータ法案は、上記の意味でのデータローカライゼーションに該当しないが、特定の場合においてはデータの移転を制限するものであるため、ここに含めている。

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

国家クラウド戦略を2021年5月に公表し、信頼できるクラウドの認証システム、政府機関のクラウド中心の推進、クラウドサービス開発に向けた産業戦略の3つを規定した。

データ主権強化のための信頼できるクラウドラベル	• 技術・法律レベルの両方で運用される。技術的特性によってサイバー犯罪のリスクに対抗することは可能だが、法的レベルでもEUの価値観に適合しない域外法の適用リスクから守らなければなりません。 • Cloud of Trustラベルは、フランスの企業、行政、市民のデータを保護するという明確な目的を持って、この2つの問題に取り組む。信頼できるクラウドラベルは、特にANSSIが発行したSecNumCloud認証に基づいてサービスプロバイダーに授与される。 • 世界で最も効果的なクラウドサービスは、海外特に米国企業から提供されている。信頼できるクラウドラベルは、欧州企業による株式保有と外国技術のライセンスを組み合わせた企業の設立など、新しい組み合わせを可能にする。このポリシーは、高いレベルのセキュリティを保証しつつ、最高レベルのサービスへのアクセスを提供するという明確なニーズに応えるものである。
クラウド中心	• 政府はサイバーセキュリティと市民・企業のデータ保護を厳守した上で、政府内のすべての新たなデジタルプロジェクトの前提条件としてクラウドを導入する。クラウドの採用で行政のデジタル化に向けた取り組みを加速できる。 • 行政機関のデジタルサービスは、政府内クラウドの1つ、または厳格なセキュリティ基準を満たす事業者が提供すうクラウドサービスでホストされる。特にセンシティブデータを扱うデジタル製品は、国民の個人データ、企業に関する経済データ、公務員に関するビジネスアプリケーションのいずれに関するものであっても、国の内部クラウドまたはANSSIがSecNumCloudと認定した産業クラウド上でホストされ、共同体外の規制から保護される。
野心的産業戦略	• フランスにおけるクラウド技術開発のための産業プロジェクトを特定し支援する。ＡＩ・ビッグデータを展開するためのPaaSソリューションや、共同作業用ソフトウェアスイートなどの重要技術を対象として、ＥＵやフランスが技術的主権を進展させることができる。 • 関心表明の募集では、1億ユーロ以上の価値がある5つのプロジェクトが決定しており、大企業、中小企業、スタートアップ、研究機関が参加してしている。共同作業プラットフォーム、エッジコンピューティング(特にIoT)、セキュアな通信の分野をカバーする。 • 最初のプロジェクトは今後数ヶ月以内に開始されますが、最大のプロジェクトは、現在、フランス、ドイツ、など11のEU加盟国が参加している欧州主要プロジェクト(PIEEC)の一部として資金提供され、エッジ・コンピューティングなどの技術的ブレークスルーの分野で、グリーンな欧州クラウドの提供を目指している。

出所)フランス政府プレスリリース(https://minefi.hosting.augure.com/Augure_Minefi/r/ContenuEnLigne/Download?id=B32CFA9B-74D2-411D-A501-82041939FC67&filename=1002%20-%20Le%20Gouvernement%20annonce%20sa%20strat%C3%A9gie%20nationale%20pour%20le%20Cloud.pdf)よりNRI作成

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

フランス政府は、政府や重要サービスのサイバーセキュリティ基準において、米系クラウドサービスを排除する動きを見せている。

- フランスのサイバーセキュリティ当局機関「国家情報システムセキュリティ庁(ANSSI)」は2016年に、公的機関や重要な部門を担う企業に対し、どのクラウドサービスが「信頼ある」かを示すラベルとしてサイバーセキュリティ認証制度とラベリングプログラム(SecNumCloud)を始動した。
- 公的機関や社会的に重要なサービスの提供者等は、SecNumCloud認証サービスの利用を義務づけられる。
- ANSSIは現在、(SecNumCloud)の改正に取り組んでいる。改正案においては後述の通り、外国企業に現地でのデータ保存や、現地の技術支援と技術スタッフのみの使用を強いる。外国のオーナーシップや企業の取締役会の代表に対しても厳格な制限が課せられる。

項目	主な義務
クラウド運営者の外国所有及び管理	クラウドサービスプロバイダーは非EU法の免除要件を定める19.6条で、同条は企業所有構造に制限を課している。とくにEU外の個人株主は25％以上所有することができないなどの基準をおいている。
強制的ローカライゼーションとローカルスタッフ	データローカライゼーション規定として、クラウドプロバイダーは全ての顧客データをEU内で保管し処理しなければならないこと、サービスの運営と監督はEU内から行われなければならないこと、サービスプロバイダーは技術的データをEU内で保管処理しなければならないことを定めている。

出所) NIGEL CORY, ""SOVEREIGNTY REQUIREMENTS" IN FRANCE—AND POTENTIALLY EU—CYBERSECURITY REGULATIONS: THE LATEST BARRIER TO DATA FLOWS, DIGITAL TRADE, AND DIGITAL COOPERATION AMONG LIKEMINDED PARTNERS" (https://www.crossborderdataforum.org/sovereignty-requirements-in-france-and-potentially-eu-cybersecurity-regulations-the-latest-barrier-to-data-flows-digital-trade-and-digital-cooperation-among-likemi)よりNRI作成

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

(２)データローカライゼーション　SecNumCloud

ANSSI長官は米国CLOUD法等のリスクを念頭に、米系クラウドサービスへの依存度低下によるEUの戦略的自立性を強調し、前述の動きを擁護している。

- 欧州ではサイバーセキュリティ当局が、Amazon、Microsoft、Googleなどのクラウドプロバイダーに対する規則を発展させている一方で、ANSSIのGuillaume Poupard長官は、外国法の射程から重要なサービスを遮断することで、さらに踏み込もうとしている。
- 米国のCLOUD法によって米国企業は、当局の求めに応じて、米国当局に外国のデータを提出する義務を負っている。Poupard長官の方策が実現すれば、欧州の法のみが適用され、米国当局に重要なデータが渡ることを妨げることになる。
- 欧州各国の政府は、「戦略的自立性」(欧州は科学技術政策に対する制御を維持する必要があるとする考え方)への前進の一部として、米国のクラウドサービスへの依存度の低い成長を試みている。
- 米国のCLOUD Actは、2018年に可決されたもので、EUがアメリカのデジタルサービスに依存しないよう取り組む動機となった。とりわけクラウド市場における「科学技術主権」と呼ばれる戦略が打ち立てられ、EUはEUのクラウド標準を設定するGaia-Xと呼ばれるプロジェクトを始動させている。
- EUのサイバーセキュリティ機関ENISAは、新たなクラウドサイバーセキュリティ認証の仕上げに取り組んでいる。しかしPoupard長官は、米国政府による特定のデータへのアクセスを妨げるためには欧州のリーダーたちの更なる政治的支援が必要であるとしている。
- 米国のクラウドプロバイダーはフランスやドイツと共に、CLOUD Actに晒されないよう取り組んでいる。米国企業は、グーグルのサービスを提供するがデータに対しては地域のコントロールに服する「主権クラウド」を発表するなど、各社がこうした雰囲気に応じている。

出所)ANSSI長官インタビュー：戦略的自立性(https://www.politico.eu/article/france-wants-cyber-rules-to-stop-us-data-access-in-europe/)

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

フランスでは、2021年5月、CapgeminiとOrangeがMicrosoftと提携し、Bleuと呼ばれる新しいANSSIのSecNumCloud認証に合致したクラウドサービスの提供を公表した。

- 本提携について、ANSSI長官は、フランスクラウド戦略に合致する動きであり、この提携を歓迎すると表明している(クラウド戦略は5月17日に、本提携は同月27日に公表されている)。
- また、本取り組みは将来的にGAIA-Xに合流するとの計画が記載されている。

【Bleu設立に関するOrange社プレスリリースより抜粋】
本日、CapgeminiとOrangeは、信頼あるクラウド（Cloud de Confiance）サービスを提供する会社「Bleu」社を設立した。同社は、政府機関、行政機関、重要インフラ企業のSovereign要件に対応し、フランス政府が定めるプライバシー、セキュリティ、レジリエンスの要求を満たすサービスを提供することを目的としている。
このプロジェクトでは、フランスを代表するグローバルデジタル企業2社の専門知識をマイクロソフトと組み合わせることで、特定の企業群に固有のニーズを満たすフランスのクラウドサービスプロバイダーを作り上げることができる。Bleuは、重要なデータや業務を扱うため、それぞれのニーズに合わせたCloud de Confianceプラットフォームを必要とするフランス政府、公共機関、病院、地方公共団体、OIV（重要業務運営者）等に対してソリューションを提供する。
Bleu社は、Microsoft 365の最新のコラボレーションおよび生産性ソリューション、Microsoft Azureクラウドプラットフォームで利用できるサービスなど、マイクロソフト社の安全なクラウド技術を独立した環境を通じて提供し、顧客が最新の技術革新の恩恵を最も幅広く受けられるよう配慮する。
フランスとEUの管轄下にあるクラウドBleuは、フランス顧客のニーズを満たすため、機密データに関する重要な要件に従う。Bleuはデータ移転の要件を満たし、フランス国内にあるデータセンターを利用した隔離されたインフラ内で、クラウドベースのアプリケーションを完全に制御できるようにする。このデータセンターはマイクロソフト社のグローバルデータセンターと厳密に分離され、運用の自律性が保証されている。また、Bleuは、すべてフランスにいる自社のスタッフによって運営される予定である。

出所)Orange社プレスリリース(https://www.orange.com/sites/orangecom/files/2021-05/2021_05_27_Capgemini_Orange_Bleu_EN.PDF)

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

ドイツ法令はVATに係るインボイスを国内保存することを求めている。

- ドイツ付加価値税法は、インボイスは、電子的に保存されるときを含め、国内で保存されなければならないとしている。
- 電子的に保存されるとき、完全なオンラインアクセスとダウンロードができるよう確保されていれば、EU領域内でも保存しておくことができる。この場合、所轄税務当局へ書面にて、電子的に保存されているインボイスの場所を通知することが求められており、当該税務当局は当該データにアクセスでき、それをダウンロードできる。
- ドイツでは税法上、帳簿や記録の保持義務が課せられる税の支払いに責任を負う自然人、企業はすべて、ドイツでそれらの記録を保持しなければならない。多国籍企業にはいくつか例外がある。ドイツ商法によれば、会計書類や商用書簡はドイツで保存されなければならない。

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

ドイツ連邦データ戦略(2021年2月)

■ 非個人データについてドイツ連邦政府は、ドイツ経済は価値創造の大きな可能性を有していると述べた。販売市場に加えて、この可能性はますます、いわゆるアフターマーケット(メンテナンス、修理、改修など)に存在している。

■ 特に以下の措置が計画されている。

- データアクセス、データ相互運用性及びポータビリティの定義による、データ収集の標準化と、データ経済を促進
- 経済において共有された価値創造を促進するための、データプールとデータ収集の発展への支援
- 競争法を調整して、経済のデジタル化の要請に適合したプロアクティブ及びデジタル競争法4.0、規制枠組を創設
- 欧州デジタル市場法(特定の条件下でデジタルプラットフォームによるデータアクセスに対する規制を禁止する)を支援し、特定のデータを享有する義務が特定のデータドリブン市場に必要か否かを検討
- デジタル単一市場指令実施の一部として、著作権法に目的自由テキスト及びデータマイニングへの新しい許可を導入
- デジタルイノベーションにおける経済(とりわけスタートアップ及び企業)に向けた、欧州イノベーション委員会(European Innovation Board)に、データ保護問題のためのアドバイザリーコンタクトとして貢献

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

(２)データローカライゼーション

ドイツ連邦データ戦略(2021年2月)

■ 改善された欧州規則はまた、データ及びITセキュリティの強化をし、デジタル化がもたらす機会が活用され、革新的なデータに基づくビジネスモデルをもって企業が自らの競争力を拡大させることができるようにすることを意図している。

■ 特に以下の措置が計画されている。

- 新しい10年間のサイバーセキュリティにおける基盤を置くためのサイバーセキュリティ戦略の評価と更新と共に、ITセキュリティ法2.0を通じたIT及びサイバーセキュリティの促進
- クラウドコンピューティングサービスに対する企業の権利の強化と、技術仕様を通じたクラウドプロバイダの変更を単純化(欧州クラウドサービスプロバイダを強化することによっても可能)
- 越境データ流通に対する不当な制約からドイツ企業を保護
- 欧州及びアフリカのテック企業によるそれぞれのデジタル市場へのアクセスと、欧州標準の国際的な強制

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

ドイツ連邦データ戦略(2021年2月)

■ 新しいデータスペースの創設

■ 革新的なデータに基づく信頼あるビジネスモデルの中心的要素は、部門横断型の解放性のある、新しいデータスペースであるべきである。特に以下の措置が計画されている。

- 革新的なデータサービスやデータに基づくビジネスモデルを導くことができる、斬新なデータプロダクト及びシステムを発展させる、様々な産業からのプロジェクトに対する資金提供
- 企業、顧客及びサプライヤー間の協力に関する動態的な価値創造ネットワークでの協業(インダストリー4.0)
- 経済における機械及び製造設備のパフォーマンスと機能性を向上させるため、製造業における人工知能の可能性を解き放つこと
- 2021年10月までに、国内レベルでの、モビリティデータの提供と、革新的で包括的なデータネットワークの構築(データルーム「モビリティ」)のための、法的枠組みを詳述し拡大すること
- また国際的な競争力を保つためにも、行動計画「モビリティにおけるデジタル化および人工知能」を発展させること

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

(２)データローカライゼーション

(参考)前述のフランスと同様の考えのもと、ドイツにおいてはドイツテレコム子会社とGoogle Cloudが合弁事業としてSovereign Cloudの提供を開始した。

MEDIA | 09-08-2021 | FRANK LEIBIGER | 0 COMMENTS

T-Systems and Google Cloud Partner to Deliver Sovereign Cloud for Germany

Share Print Read out

- Strategic, long-term partnership will provide a next-generation sovereign cloud solution
- Both companies to invest in technology solutions and co-innovation to serve local customer needs

Sovereign Cloud from Google Cloud and T-Systems.

T-Systems and Google Cloud today ann
deliver sovereign cloud services for Germ
sector, and healthcare organizations. Brea
companies will jointly innovate to develop
generation sovereign cloud solutions and
customers to host their sensitive workloac
continuing to leverage the scalability, elas
cloud services. Service management and
cloud will be supervised by T-Systems.

"Our joint strategic goal is to support the
companies and the public sector as they r
explained Adel Al-Saleh, member of the Te
and CEO of T-Systems. "Together with Google Cloud, we will build a sovereign cloud s
clients with full control over their data, software and operations whilst leveraging the

Full sovereignty, full functionality

Initially, T-Systems will roll out the sovereign cloud offering to German organizations in several industries, including healthcare, automotive, public transport, and the public sector. Clients will benefit from:

- A full spectrum of highly innovative and scalable cloud technology at various levels of sovereignty
- Google Cloud's open-source expertise that provides freedom of choice and prevents lock-in
- Increased openness and transparency for clients
- Easy integration with existing IT landscapes
- Help complying with existing European sovereign cloud policies, including GDPR (European General Data Protection Regulation)
- Full public cloud scale as well as version and feature parity to global network

出所)ドイツテレコム(https://www.telekom.com/en/media/media-information/archive/sovereign-cloud-from-t-systems-and-google-cloud-635314)

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

(２)データローカライゼーション　公文書

オランダにおいては、公文書のオランダ国内における保管が定められている。

■ オランダのPublic Records Actは、公文書はオランダ国内の特定のアーカイブに保存することとしている。

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

スイスにおいては、マネーロンダリング対策として関連書類を国外のサーバーに保存する場合には、国内にハード又は電子的なコピーを保管する義務がある。

- スイスでは、マネーロンダリング対策のため、金融規制を所管するスイス連邦金融市場監督機構(FINMA)が様々な既成を導入している。
- うち、FINMA Anti-Money Laundering Ordinanceの第74条は、金融事業者に一定の書類の整備が求められている。そして、同条第4項は、このような書類はスイス国外のサーバーに電子的に保存することを妨げられていない。ただし、スイス国外のサーバーに書類を保存する場合には、当該事業者は書面の最新のハードコピー又は電子的なコピーをスイス国内に保管する義務を負うと定めている。

出所) FINMA, “Anti-Money Laundering Ordinance” (https://www.fedlex.admin.ch/eli/cc/2015/390/de)

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

(２)データローカライゼーション

データ処理サービス事業者の外国政府へのデータ提供制限

- EUデータ法案は、データ処理サービス事業者が行う、非個人データの外国政府への提供(越境移転)について一定の制約を課している。
- まず第27条1項は、データ処理サービスの提供者に対して、EU法との法の抵触を生じうる外国からのデータ提供要求を防止する、技術的、法的及び組織的な措置をとることを求める。
- ついで、同条第2項は、外国の裁判所や行政機関のデータ提供命令に基づくEU域外への非個人データの移転は、既存の当該命令を発出した国家とEU又はその加盟国間に締結された刑事共助条約等に基づくもののみが認められるべきであることを定める。
- 同条第3項は、上記の命令に従うことがEU法又は加盟国法と抵触を生じうる場合には、第三国の要求が比例性等を満たしていることや、当該命令について司法審査等の救済があること、といった条件が満たされる場合にのみ移転が認められることを定める。
- 同条第4項は上記の第2項又は第3項が満たされる場合には最小限のデータが提供され得る事、また第5項はその場合にデータの管理者に対して通知を行うべきことなどを定めている。

出所)EUデータ法案よりNRI作成

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

データ処理サービス事業者の外国政府へのデータ提供制限

■ 第７章　国際的な文脈における非個人データのセーフガード

■ *第27条 国際的なアクセス及び移転*

- 1. データ処理サービスのプロバイダーは、連合における非個人情報への国際移転又はガバメンタルアクセスが連合法又は関係締約国の国内法との抵触を生じさせるようなとき、それを妨げるため、第2項又は3項に影響を及ぼすことなく、すべての合理的な技術的、法的、組織的措置をとらなければならない。
- 2. データ処理サービスのプロバイダーに対し、連合における本規則の射程内にある非個人情報からの移転又はアクセス許可を要請する第三国の裁判所の決定又は判決、並びに行政当局の決定はすべて、要請する第三国と連合との間で有効な、相互司法共助条約などのような国際合意、又は要請する第三国と締約国との間で有効な同様の国際合意に基づいた方法においてのみ承認又は執行されうる。
- 3. そのような国際合意がない場合、データ処理サービスのプロバイダーが、連合における本規則の射程内にある非個人情報からの移転又はアクセス許可を求める第三国の裁判所の決定又は行政当局の決定の名宛人であり、そのような決定の遵守により当該名宛人が連合法又は関係締約国の国内法に抵触する危険を有するとき、第三国の当局によるそのような非個人情報への移転又はアクセスは次の場合にのみ実施される。
  - (a) 当該第三国の制度が、下される決定又は判決の理由と均衡性を求めており、及び、そのような決定又は判決に、場合により、特定の疑いをかけられている個人又は違反との十分な関連性を立証することなどにより、性質上特定的であることを求めているとき
  - (b) 名宛人による合理的な異議申立てが、第三国の権限ある裁判所の審査に服するとき
  - (c) 決定又は判決を発する又は行政当局の決定を審査する権限ある裁判所が、当該国の法に基づいて、EU法又は関係する締約国の国内法で保護されるデータのプロバイダーの関連する法的利益を適切に考慮に入れる権限を有しているとき
  - 当該決定の名宛人は、これらの条件が満たされているかを決定するために、とりわけ、当該決定が商業的にセンシティブな情報に関連する可能性がある、又はEU若しくは締約国の国家安全保障若しくは国防上の利益を害する可能性があるとき、本規則に基づいて、関係する権限ある主体又は当局に意見を要請することができる。
  - 規則[xxx - DGA]に基づいて設立された欧州データイノベーション委員会は、欧州委員会がこれらの条件が満たされているかの評価に関するガイドラインを発展させる際に助言し支援する。

出所)EUデータ法案よりNRI作成

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

データ処理サービス事業者の外国政府へのデータ提供制限

- 4. 第2項又は3項の条件が満たされたとき、データ処理サービスのプロバイダーは、合理的な解釈に基づいて、要請に応じて許容可能なデータの最小量を提供しなければならない。
- 5. データ処理サービスのプロバイダーは、第三国の行政当局からデータへのアクセス要請がなされているということについて、それに応じる前に、データホルダーに知らせなければならない。ただし当該要請が法執行目的でなされており、法執行活動の効率性を保護するのに必要な限りにおいてなされている場合を除く。

出所)EUデータ法案よりNRI作成

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

データ処理サービス事業者の外国政府へのデータ提供制限(前文)

(77) 第三国は、連合を含む、自国国境外に位置する非個人情報の移転またはそれへの政府によるアクセスの提供を直接的に目的とする法、規則及びその他の法律行為をとることができる。そのような非個人情報への移転又はアクセスを要請する第三国の法執行当局を含む、裁判所の判決又はその他の司法若しくは行政当局の決定は、要請する第三国と連合又は締約国との間で有効な、相互司法共助条約などの国際合意に基づいているときにのみ執行可能であるべきである。その他の場合、第三国法による非個人情報への移転又はアクセス許可の要請が、EU法又は国内法に基づいてそのような情報を保護する義務、特に、安全保障に対する権利、実効的救済を受ける権利などの個人の基本的人権、又は国家安全保障若しくは国防に関連する締約国の基本的利益の保護、企業秘密の保護など商業的にセンシティブなデータの保護、知的財産権の保護、そこにはこれらの法に従った守秘義務に関する契約上の義務を含むが、そのような義務と抵触する状況が起こり得る。この問題を規律する国際合意がない場合、移転又はアクセスは、第三国の法制度が下される決定の理由と均衡性を求めていること、裁判所の命令又は決定が性質上特定的であること、名宛人の合理的な異議申立てが第三国の権限ある裁判所の審査に服し、その裁判所がそのようなデータのプロバイダーの関連する法的利益を適切に考慮に入れる権限を有していることが証明されたときにのみ許される。第三国の当局のデータアクセス要請の条件のもとで可能なときは常に、データ処理サービスのプロバイダーは、そのようなアクセスと、企業秘密及び知的財産の保護、並びに守秘義務に関する契約上の義務を含む商業的にセンシティブな情報の保護に関する規則など、EU又は国内規則との潜在的な抵触の存在を明らかにするため、要請されたデータの所有者である顧客に通知することができるべきである。

出所)EUデータ法案よりNRI作成

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

(３)ガバメントアクセス

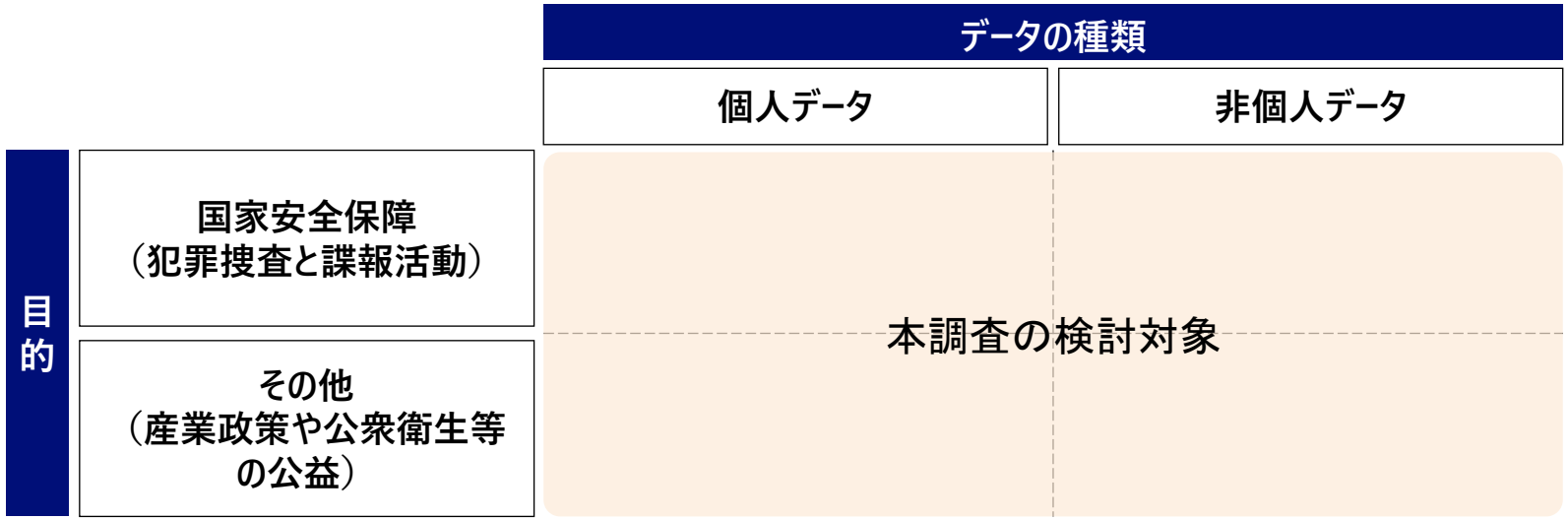
Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

(3)ガバメントアクセス

ガバメントアクセスの指す範囲

- ガバメントアクセス（GA）とは、政府機関等の公的機関による、民間部門が保有する情報への強制力を持ったアクセスを指す。
- 一般的に、ガバメントアクセスは、目的及びアクセス対象となるデータの種類（個人データと非個人データ）に基づき類型化される。
- 上記類型に基づきつつ、本調査は国家安全保障（犯罪捜査と諜報活動）以外にも産業政策や公衆衛生等の公益を目的としたデータへのアクセスも検討対象とした。

ガバメントアクセスの指す範囲（本調査）



参考) 渡辺翔太　ガバメントアクセス（GA）を理由とするデータの越境移転制限―その現状と国際通商法による規律、そしてDFFTに対する含意―（https://www.rieti.go.jp/jp/publications/dp/19j067.pdf）

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

(３)ガバメントアクセス

ガバメントアクセス概要

フランス	諜報機関 (intelligence service)	捜査機関 (law enforcement authority)
GAに関する法制度の根拠法	国内安全法(Internal Security Code)	刑事訴訟法(French Code of Criminal Procedure)
GAに関する手続き(特に司法の関与)	司法による事前許諾は必要なし。 ⇒諜報活動計画(surveillance program)の導入には、CNCTRによる拘束力のない助言(non-binding recommendation)に基づいた首相による事前許諾が必要。	司法による事前許諾が必要。
適用対象(データ、企業)	適応対象の限定なし	適応対象の限定なし
特に個人/非個人の区別があるか	個人・非個人データの区別は不明(区別なし)	個人・非個人データの区別は不明(区別なし)
どの程度広範であるか	比較的広範 ⇒フランスの経済的利害・集団犯罪の予防等を含む幅広い目的に対して諜報活動を許可。比例性についても疑問が生じている。	比較的限定的 目的・比例性に制限が存在
権利保障の確保	• 刑法(French Criminal Code)が通信の秘密(secrecy of correspondences)に対する権利を保障 • 民法(French Civil Code)が(私的第三者・政府機関に対する)プライバシー権を規定 人権と基本的自由の保護のための条約(ECHR)が、(政府機関に対する)プライバシー権を規定 • データ保護法(French Data Protection act, hereafter LIL)	
第三者監査	CNCTR及び首相	司法機関

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

ガバメントアクセス　根拠法(法令の変遷)

年	GAに関わる法令	関連内容
NA	Internal Security Code (国内安全法・治安法)	**フランスの諜報活動の全体を規定：** 2015年以前、同法は刑事手続きに比べて保護の水準が低く、特に第三者による監査が一部の諜報活動について及ばないという問題が存在していた。
2015	Surveillance Law/Intelligence Act (諜報活動法)	**国内安全法(Internal Security Code)の大幅改正：** 諜報活動に法的な原理原則・フレームワークに関わる新章を追加。具体的には 、監督(oversight)基準だけでなく1) proportionality 2) subsidiarity3) individualisation4) centralisation5) territorialityに原則を規定。 一方、リアルタイムでのメタデータに対するアクセスや「アルゴリズムに基づく諜報活動algorithmic surveillance」も規定された。
2016	Law of June 3 2016 strengthening the fight against organized crime, terrorism, and their financing, and improving the efficiency and guarantees of the criminal procedure	**諜報可能主体の拡大：** 司法省(Ministry of Justice)部門は行政最高裁判所(Administrative Supreme Court)のデクレ(Decree)に基づき、CNCTRのコンサルテーション実施後に、諜報手段を使用可能とした。(Articles L.811-4 CSI治安法)が規定。 司法省(Ministry of Justice)は、諜報手段の許諾を求める要求書をCNCTRに提出することを可能にした。(Articles L. 821-2 CSI治安法)
2016	Law of July 21 related to the state of emergency and strengthening counter-terrorism measures	**諜報活動の適応対象の拡大：** 脅威を及ぼすと特定された個人(imposing a threat)⇒脅威に関連する可能性がある個人(likely to be related to a threat)。リアルタイム情報の取集に関しても、関連する個人(related person)⇒persons closely related to him/her に拡大。(Article L. 851-2 CSI)他には、Article L.852-1, L.863-2 CSI治安法の適応対象拡大。
2016	Ruling of the constitution Council of October 21 2016	**無線傍受の承認廃止：** 無線傍受に対する法体制が違憲となる。よって無線傍受関連のモニタリングは手続きの対象外。また、モニタリングの実施に際しての保証提供も不要となる。
2017	Law of February 28 2017 on public safety	**諜報可能主体の拡大：** 同法は治安法に(within Book Ⅷ of the CSI)刑務所管理の諜報活動に関する項目を追加。 (Article L.855-1 CSI)
2017	Law of 30 October 2017	**サンセット条項の延長：** 「アルゴリズムに基づく諜報活動 algorithmic surveillance」 (L.851-3)は、2018年12月31日を期限とするサンセット条項であったが、その期限が同法により延期された。

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

ガバメントアクセス　根拠法　諜報活動法(Surveillance Law/Intelligence Act)

■ 諜報活動法(Surveillance Law/Intelligence Act)：(１/２)

2015年に導入され、法改正が実施。以下３点が主要な変更内容。

- **監視機関(CNCTR)の設置：**
  第三者監査のために諜報手段の監督に関する国家委員会(CNCTR)が設立
  - 諜報活動計画(surveillance program)の導入には、CNCTRによる拘束力のない助言(non-binding recommendation)に基づいた首相による事前許諾が必要(治安法L821条1項)。
    - 情報収集は、首相による書面の事前許諾を必要とするが(治安法L821条1項)、司法による事前許諾は必要ない。
    - CNCTRは首相に判断のための意見を治安法の基準に基づいて提示するが、首相の判断を拘束しない(治安法L821条1項)。
    - CNCTRの意見は、要請から24時間以内(72時間以内まで延長可能)提示する(治安法L821条3項)。
  - 委員は9人で、上院2人、下院2人、コンセイユ・デタ2人、破棄院2人、通信監督庁(ARCEP)1人で構成(治安法L831条1項) 。
  - CNCTRの判断は、防衛機密の対象となる(治安法Article L832条5項)
- **メタデータ情報等へのアクセス保障：**
  - **メタデータに対するアクセス：**
    情報機関は通信事業者やホスティング・プロバイダーが保有するメタデータへのアクセス権を要求するだけでなく保存されたメタデータをリアルタイムで収集することができる。(Article L851- 1, 治安法)リアルタイムでのデータ収集は、テロ防止目的にのみ認められ、CNCTRの事前許諾が必要である。(Article L851- 2,治安法)また通信事業者とホスティング・プロバイダーは、幅広いカテゴリーのメタデータを12ヶ月間保持することを義務づけられている。
  - **非対象データ主体に対するメタデータ分析(アルゴリズムに基づく諜報活動)：**
    諜報機関が通信事業者やホスティングプロバイダーにアルゴリズムを導入を要求可能とする規定。首相の許諾に基づき、諜報機関はアルゴリズムを通じてフランスの電気通信サービスやホスティングサービスの利用者のメタデータを分析してテロの脅威を示す疑わしいパターンを特定が可能。政府はメタデータは匿名であり、分析はプライバシーを脅かすものではないと主張。⇔**CJEU Digital Rights Ireland判決では、その国の全ユーザーのトラフィックデータを記録することは、プライバシーの不均衡な侵害にあたるとされており、本決定に抵触する可能性がある。**

参考)Baker＆McKenzie. Global Data Privacy ＆ Security Handbook(https://resourcehub.bakermckenzie.com/en/resources/data-privacy-security)、Fred H. Cate; James X. Dempsey　Bulk Collection: Systematic Government Access to Private-Sector Data　Systematic Government Access to Private- Sector Data in France

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

ガバメントアクセス　根拠法　諜報活動法(Surveillance Law/Intelligence Act)

■ 諜報活動法(Surveillance Law/Intelligence Act)：(２/２)

- **諜報活動を正当化できる目的範囲の規定：**
  “国家の基本的利益の防衛と促進 (defense and promotion of the fundamental interests of the nation)の為に必要な場合にデータを収集することを可能としている。

  - 国家の独立、領土保全および国防
  - 外交政策における主要な利害、フランスによる欧州・国際義務の履行、あらゆる形態の外国からの干渉の防止
  - フランスの経済・産業・科学における主要な利害
  - テロ防止
  - 共和制関連機関への攻撃、解体された結社の継続または再結成を目的とした行動の防止(Article L. 212-1 刑法)
  - 公共の平和に重大な損害を与える可能性のある集団的暴力、組織犯罪および非行の防止
  - 大量破壊兵器の拡散の防止

参考)Baker＆McKenzie. Global Data Privacy ＆ Security Handbook(https://resourcehub.bakermckenzie.com/en/resources/data-privacy-security)、Fred H. Cate; James X. Dempsey　Bulk Collection: Systematic Government Access to Private-Sector Data　Systematic Government Access to Private- Sector Data in France

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

ガバメントアクセス　諜報機関・組織

■ 国内・国外の諜報活動が許諾されている機関・組織は、６つ存在(L.811-2, L.854-2-III and R. 811-1 CIS治安法)。

1. **対外治安総局：the General Foreign Security Office(DGSE)**
   ⇒フランス国外の諜報活動を実施する情報機関
2. **国防治安局：the Defense Intelligence and Security Office (DRSD)**
   ⇒防諜・カウンターテロリズムの為の情報取集を実施する情報機関。軍事省(Ministry of Defense)の一部。
3. **軍事偵察局：the Military Intelligence Office (DRM)**
   ⇒軍事省(Ministry of Defense)の為の情報収集を行う情報機関
4. **国内治安総局：the General Domestic Security Office (DGSI)**
   ⇒フランス国内の情報機関
5. **関税情報調査局：the National Intelligence and Customs Investigation Office (DNRED)**
   ⇒関税に関する諜報活動を実施する情報機関
6. **対資金洗浄情報課：(TRACFIN)**
   ⇒intelligence processing and action against clandestine financialと名付けられた国家部門

■ 上記に追加して、「非特化型の(non-specialized)」諜報活動が定義されている(R. 811-2 CIS治安法)。

- 内務省(Ministry of Justice)と軍事省(Ministry of Defense)内の29部門が関連する。
- その他の非特化型(non-specialized)の情報機関は司法省(Ministry of Justice)経済省(Ministry of Economy)のデクレ(政令)内包される。
- 非特化型(non-specialized)の情報機関は限定的な目的に対して、限定的な手段が付与されている。

出所)Baker＆McKenzie. Global Data Privacy ＆ Security Handbook
(https://resourcehub.bakermckenzie.com/en/resources/data-privacy-security)

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

ガバメントアクセス　ガバメントアクセスに関する手続き(特に司法の関与)

■ 第三者監督機関CNCISは権威を有しておらず、諜報活動は独立した機関より監視されていない状況であった(2015年以前)。

■ 第三者監査機関CNCTR：第三者監査のために諜報手段の監督に関する国家委員会(CNCTR:Commission Nationale de Controle des Techniques de Renseignement)が設立した。

- 諜報活動計画(surveillance program)の導入には、CNCTRによる拘束力のない助言(non-binding recommendation)に基づいた首相による事前許諾が必要(治安法L821条1項)。
- 情報収集は、首相による書面の事前許諾を必要とするが(治安法L821条1項)、司法による事前許諾は必要ない。
- CNCTRは首相に判断のための意見を治安法の基準に基づいて提示するが、首相の判断を拘束しない(治安法L821条1項)。
- CNCTRの意見は、要請から24時間以内(72時間以内まで延長可能)提示する(治安法L821条3項)。

ガバメントアクセス実施に関する手続き

	CNCTRによる意見	首相による許諾	
実施事項	• 治安法原則(目的範囲と手段)との適合性について意見を表明 • 諜報機関の活動内容との合理性と比例性に基づき審査例えば、リアルタイムでのデータ収集は、テロ防止目的にのみ認められる(Article L851- 2,治安法)	• 特定ケース毎に首相により許諾を行う CNCTRの意見を無視した場合には、首相は意見書の提出義務を負う。また、CNCTRはコンセイユ・デタ (Conseil d'État)に対して訴訟可能	以下３つに該当する場合、CNCTRの意見は不要 • 緊急事態(テロ等) • 国際的なデータ収集に関連(International data collection) • 無線通信の一般的な監視

出所)Baker＆McKenzie. Global Data Privacy ＆ Security Handbook
(https://resourcehub.bakermckenzie.com/en/resources/data-privacy-security)

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

ガバメントアクセス　権利保障の確保

救済措置として、データ主体(Data subject)は、諜報機関が実施した監視措置について裁判所の審査を要請することができる。(国際的な電子通信監視措置の場合を除く)

■ 一般的に、データ主体は、諜報措置の検証・保障を含む救済措置を要求することができる。

- 監視されていると疑うデータ主体は、CNCTRに諜報措置の規則性(regularity)を検証するよう要求することができる。CNCTRは適切な検証に基づき、データ主体に対する監視の有無を明かすことなく、検証実施完了の旨をデータ主体に共有する。(L. 833-4 CSI)。データ主体は、CNCTRから回答を得た後、コンセイユ・デタ(Conseil d'État)に監視活動の合法性の見直しを求めることが可能。(L. 841-1 CSI)。
- 監視活動が違法に行われたと裁判所が判断した場合、裁判所は監視活動を行う権限を取り消し、収集したデータの破棄を命じることが可能(L. 773-7 Code of Administrative Justice、Code de la justice administrative 以下「CAJ」と言う)。
- 行政最高裁判所は、監視措置の違法性が刑事犯罪を構成する可能性があると判断した場合、共和国検察官に通知CNCTRに事件要素を提供し、CNCTRが首相に当該要素の機密解除の可能性について勧告を行い、共和国の検察官に転送させることが可能(L. 773-7 CAJ)。
- データ主体は、フランスのDPA(art. 40 Loi informatique et libertés)に連絡することで、個人データ保護に関する権利を行使することも可能。この場合、最高行政裁判所は、データが不正確、不完全、曖昧、古いものである場合、またはデータの収集もしくは処理が禁止されている場合、データ主体に通知しなければなりません。裁判所は、当該データの修正、更新又は消去を命じることができる。裁判所は、データ主体に補償を行うことを決定することができます(L. 773-8 CAJ)。

■ ただし、データ主体は、国際的な電子通信監視措置(International electronic communications surveillance measures)について裁判所の審査を受ける権利は存在しない。

- 国際監視措置に対して不服を申し立てることができると規定することで司法救済を受ける権利と国防の秘密との間に、明らかに不均衡が生じる為(Constitutional Council, 2015-722 DC of Nov. 26, 2015 及びCouncil of State, no. 397623 of Oct. 19, 2016参照)。

出所)Baker＆McKenzie. Global Data Privacy ＆ Security Handbook
(https://resourcehub.bakermckenzie.com/en/resources/data-privacy-security)

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

ガバメントアクセス　権利保障の確保

データ主体(data subject)が保障されているプライバシー権は以下の通り。

- 刑法(French Criminal Code)が通信の秘密(secrecy of correspondences)に対する権利を保障(Articles 226-15 432-9)。
- 民法(French Civil Code)が(私的第三者・政府機関に対する)プライバシー権を規定(Article 9)。また、人権と基本的自由の保護のための条約(ECHR)が(政府機関に対する)プライバシー権を規定(Article 8)。
- データ保護法(French Data Protection act)が私的・公的機関によるデータ処理の際、個人データの保護を保証する。
  - いかなる個人は自身の個人データの処理または商業的利用に異議を唱えることができる。しかし、明示的な規定により、これらの規定が除外される場合が存在(Article 38)。
  - 個人はどのような目的にて何のデータが収集・処理されているかについての情報に関してデータ管理者に対して開示請求できることを規定(Article 39)。
  - いかなる個人は、自身の個人データが不正確・不完全・最新ではない、また、データの収集や処理が適切でない、禁止されている場合においては、個人データの修正、完全、更新、ブロック、または消去を求めることができる (Article 40)。
  - Article39・40の例外として国家安全保障、国防また公共の安全を目的にデータが処理される場合、個人はCNILに対して情報を確認、(必要に応じて)修正を依頼しなければならない。データ管理者の同意を得た場合に限り、データは申請者に開示される(Article 41)。
  - 間接アクセス権 (Article 41)は公的機関の予防・捜査措置の為の処理に対しても適応対象である(Article 42)。

出所)Baker＆McKenzie. Global Data Privacy ＆ Security Handbook
(https://resourcehub.bakermckenzie.com/en/resources/data-privacy-security)

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

(参考)ガバメントアクセス　捜査機関

■ GAに関する制度の根拠法：刑事訴訟法(French Code of Criminal Procedure)が規定。
- フランスの捜査活動を規定しているのは刑事訴訟法(French Code of Criminal Procedure)

■ GAに関する手続き(特に司法の関与)：司法機関に対して事前許諾が必要である。
- 被疑事件ごとに、個別・事前に司法機関の許諾を得る必要がある。盗聴、メール等データの傍受は、刑事訴訟法(French Code of Criminal Procedure)に基づき、司法による事前許諾が必要(Articles 100、706- 95)。

■ 適用対象(データ、企業)：適応対象の限定はなし。
- コンピュータデータの完全取得：PC端末を複製してリモートで監視するなどが該当。重大な犯罪についてのみ許され、司法による事前許諾が必要(Article 706- 102- 1)。
- コンピュータデータの開示要求など：犯罪が進行している疑いがある場合、同時に司法職員に通知さえすれば、被疑者に対して開示を要求できる。但し、予備捜査の段階では、予審判事の判断を仰ぐ(Articles 57- 1, 60- 1, 60- 2) 。
- 通信事業者は、ログ保持の義務化を負う。
- 9.11後、通信事業者およびホスティング事業者に対して、ログ等のメタデータ(identification data)を12ヶ月保持する義務を追加。

■ 特に個人/非個人の区別があるか：個人/非個人の区別は不明。

■ どの程度広範であるか：一定の限定が存在。

■ 第三者監査：司法機関の事前許諾が必要。

出所)Baker＆McKenzie. Global Data Privacy ＆ Security Handbook
(https://resourcehub.bakermckenzie.com/en/resources/data-privacy-security)

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

ガバメントアクセス　近年の事例

〇Global security law法案可決(2020年)

- 2020年11月24日、仏議会は、「Loi relative à la sécurité globale(global security law)」を可決。
- 同法案は、フランスの監視国家体制を強化するとして、AMNESTY Internationalから批判されている。
- 同法案内容(抜粋)は、以下の通り。
  - 第21条：警察による「歩行者用」カメラの設置を増やし、人々を監視する可能性を拡大すること。
  - 第22条：少数の例外(住宅内部等)を除いて、警察によるドローンの使用を予見していること。
  - 第24条：ジャーナリスト等が警察官や憲兵を特定できるかたちでの映像を放送した場合、その映像が「身体的・心理的完全性を脅かす」目的である場合、最高で1年の禁固と4万5000ユーロの罰金を科すと定めること。
    ※第24条は最も物議を醸し、後にフランス上院の法委員会によって修正が為された。

〇2015年のシャルリー・エブド襲撃事件を契機に、Law of June 3 2016等、安全保障を優先する法令が継続して採択・可決されている。

〇2020年のGlobal security law法案に関しても、一部条項を除き、安全保障を優先する条項が維持されたまま法案が可決された。

出所)AMNESTY International　New security law risks dystopian surveillance state
(https://www.amnesty.org/en/latest/news/2021/03/france-new-security-law-risks-dystopian-surveillance-state/)

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

ガバメントアクセス概要

ドイツ	諜報機関(intelligence service)	捜査機関(law enforcement authority)
GAに関する法制度の根拠法	基本法10条を制約する各法： G-10法　例えば、信書、郵便及び通信の秘密の制限のための法律等 (the Act to Restrict the Privacy of Correspondence, Mail, and Telecommunications) 各諜報機関の設置法： 連邦憲法擁護法(BfV法)、軍事防諜法(MAD法)連邦情報庁法(BND法)	刑事訴訟法・連邦刑事警察局に関する法律・ 連邦警察に関する法律・税関調査局及び税関調査事務所に関する法律
GAに関する手続き(特に司法の関与)	司法による事前許諾は不要 ⇒諜報活動の類型別に第三者監査の事前許諾が必要	司法による事前許諾が必要
適用対象(データ、企業)	適応対象の限定なし	適応対象の限定なし
特に個人/非個人の区別があるか	個人・非個人データの区別は不明(区別なし)	個人・非個人データの区別は不明(区別なし)
どの程度広範であるか	比較的広範 ⇒しかし、国内と国外を結ぶ通信からの情報収集は違憲となる(2020年BND法違憲)	比較的限定的
権利保障の確保	• 通信、郵便、通信のプライバシーに関する憲法上の権利。(ドイツ基本法第10条) • 住居不可侵(ドイツ基本法13条) • 憲法上のプライバシー権(情報的自己決定権)(ドイツ基本法第2条第1項) • 私生活および家族生活、自宅、通信手段を尊重する権利(欧州人権条約「 ECHR 」第8条)	• テレメディア法　第11条から第15a条 • 連邦データ保護法第27条から第35条 • 刑法第201条から第206条 • 電気通信法　第88条以下参照
第三者監査	G-10委員会(G-10 commission)・PKGr(the Parliament Control panel)・ 独立機関(Independent body)	司法機関

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

ガバメントアクセス　諜報機関と根拠法の全体像

ドイツにおける諜報機関と根拠法

諜報機関 (設立年)	連邦憲法擁護庁 BfV (1950)	連邦軍事防諜庁 MAD (2017)	連邦情報庁 BND (1990)
設置法	連邦憲法擁護法 (BfV 法)	軍事防諜法 (MAD 法)	連邦情報庁法(BND 法)
根拠法	G-10法： ドイツ基本法10条を制約する各法 例)信書、郵便及び通信の秘密の制限のための法律　等 スノーデン事件後の2016年、BKA Act of 2016によりG-10法の大幅改正が実施された		

近年の主な争点

- 過去、ドイツ基本法の適応外として、外国人に対する諜報活動に対する制限が限定的であった。
- 2020年、ドイツ国内を出発地または目的地としない通信データの戦略的・非標的諜報活動(foreign-foreign surveillance)を実施するBNDの権限が基本的な憲法上の権利を侵害しているとの判決が下る
  - ⇒BNDによる海外で大規模な監視(Mass Surveillance)を禁止
  - ⇒外国人市民や国境を越えた通信に関連してもドイツ憲法(基本法)に拘束される

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

ガバメントアクセス　諜報機関・組織と設置法

■ 憲法擁護庁(BfV)、連邦情報局(BND)、軍事保安局(MAD)の3つの情報機関が存在
- 連邦軍事防諜法が、MADに情報収集権限を付与
- 連邦憲法擁護法が、戦闘的民主主義に基づく活動権限をBfVに付与
- 通信傍受法(2016年)が、初めてBNDに国外における外国人の通信を傍受する権限を付与(⇒BKA act of 2016)

■ 近年、諜報活動について法整備が繰り返されてきた
- 1990年以前は、個人情報の収集が基本権を制約するとは認識されず、諜報に明確な法的根拠はなかった。しかし、1983年の連邦最高裁判決(BverfGE 65, 1)が国勢調査における個人情報の収集も、一般人格権(憲法2条)から導かれる情報自己決定権を侵害すると判示して転機を迎えた。
- 以降、情報機関による諜報活動は、基本権に対する制約であるため法的根拠に基づかなければならず、情報機関の活動が民主主義国家で受け入れられるために透明性を確保する必要があるとの議論が主流となり、1990年のMAD法およびBND法制定で明文化された。
- さらに、国外の外国人に対する傍受についても、法的根拠が整備された。(⇒BKA act of 2016)
- これまで実施していた外国人に対する広範な諜報活動(strategic[untargeted]surveillance)制度の運用が原則禁止へ。標的諜報活動も厳しい制限を受ける(⇒BND法違憲判決2020年)

	連邦憲法擁護庁(BfV)	連邦軍事防諜庁(MAD)	連邦情報庁(BND)
設置年	1950 年	1956 年： 連邦軍軍事防諜局 2017 年：連邦軍事防諜庁	1956 年
設置法	連邦憲法擁護法(BfV 法)(1950)	軍事防諜法(MAD 法)(1990)	連邦情報庁法(BND 法)(1990)
任務	国内の極右・極左主義及びイスラム主義の団体活動の監視	軍事防衛分野の諜報。主にドイツ国内で活動するが、連邦軍が 海外派遣されている場合には、外国でも活動する。	ドイツの外交及び安全保障政策上重要な外国に関する情報の収集及び分析

参考)Baker＆McKenzie. Global Data Privacy ＆ Security Handbook(https://resourcehub.bakermckenzie.com/en/resources/data-privacy-security)、Fred H. Cate; James X. Dempsey　Bulk Collection: Systematic Government Access to Private-Sector Data　Systematic Government Access to Private- Sector Data in Germany

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

ガバメントアクセス　根拠法(主要な法令)

■ドイツ基本法10条を制約する各法はG-10法と呼ばれる

- 信書、郵便及び通信の秘密の制限のための法律(the Act to Restrict the Privacy of Correspondence, Mail, and Telecommunications)G-10条の制限

■G-10 法改正により、情報機関(BND)は反テロ・データバンクを構築・運用できるようになった。

- 以前は、ドイツに対する武力攻撃のおそれがある場合、ドイツにおける国際的なテロ攻撃のおそれがある場合、薬物取引や資金洗浄等の組織犯罪のおそれがある場合等に限られてきた。
- 安全保障上の諜報活動(strategic[untargeted] surveillance)の対象となる行為類型(改正法5～8条)を限定しつつ、該当した場合には広範な情報の収集が可能。(10条)
  - 諜報活動(strategic [untargeted] surveillance)を正当化する危機の性質(nature of danger)は以下通り。(5条１)ドイツに対する武力行使、ドイツに直接関連する国際テロ攻撃、兵器の国際不法取引、麻薬違法取引、及びその他の重大な危険(限定的)ドイツに関わる重大な利害に関わる経済関連(economic-relates surveillance)についても許可されている。
  - 経済目的での偵察(経済スパイ)は禁止される(5条)
  - 光ファイバーなどへの物理接続、スマートフォンへのマルウェア埋め込みも可能
  - ただし、国内と国外を結ぶ通信からの情報収集は、監視する通信網の容量の 20% 以下に制限されている
- 通信偵察(外国での傍受)においては、個人のプライバシー情報は、いかなる場合でも収集が許されない(5a条)。
- BNDは、収集した情報が目的に即して必要か自己検証し、不要な場合には直ちに消去する。
- 通信偵察には、事前に連邦首相府が具体的に対象・期間等を指定する必要。

■G-10関連の情報収集活動は、連邦議会に設置された議会監視委員会と傘下の基本法第10条審査会が監査する

- 議会監視委員会は、連邦議会議員9名で構成され、年4回以上開催される。
  - ただし、情報機関の申告に対する審査のみであって、自主調査権をもたないため申告されないケースは監査できないとの欠陥も指摘される。

参考)Baker＆McKenzie. Global Data Privacy ＆ Security Handbook(https://resourcehub.bakermckenzie.com/en/resources/data-privacy-security)、Fred H. Cate; James X. Dempsey　Bulk Collection: Systematic Government Access to Private-Sector Data　Systematic Government Access to Private- Sector Data in Germany

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

ガバメントアクセス　諜報機関・組織と設置法

BND諜報活動権限と法的根拠(2020年時点)

BNDの諜報活動範囲	根拠法
ドイツ国民個人、ドイツ国内の居住者および法人の通信データの監視	ドイツ基本法 第10条セクション３
外国領内における外国個人の通信データの監視	成文化なし、秘密の行政命令による ⇒2020年：厳しい制限
ドイツ国内を出発地または目的地とする通信データの戦略的・非標的諜報活動(Foreign-Domestic strategic[untargeted] surveillance)	ドイツ基本法　第10条セクション５
ドイツ国内を出発地または目的地としない通信データの戦略的・非標的諜報活動 (Foreign-Foreign strategic[untargeted] surveillance)	BND法 第6条 ⇒2016年：改正(⇒BKA act of 2016) ⇒2020年：違憲判決
コンピューターネットワーク搾取(Computer Network Exploitation)	成文化なし、秘密の行政命令による
データのバルク取得(Bulk Data Acquisition)	成文化なし、秘密の行政命令による

出所)Thorsten Wetzling　Germany's intelligence reform June 2017 Policy Brief
(https://www.stiftung-nv.de/sites/default/files/snv_thorsten_wetzling_germanys_foreign_intelligence_reform.pdf)

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

ガバメントアクセス　2020年BND法判決について

■ 2020年5月19日、ドイツ連邦憲法裁判所(Bundesverfassungsgericht)は、ドイツ国内を出発地または目的地としない通信データの戦略的・非標的諜報活動(foreign-foreign surveillance)を実施する連邦情報庁(BND)の権限が基本的な憲法上の権利を侵害していると判断する画期的な判決を下した。
⇒ドイツ連邦憲法裁判所は、BNDは海外で大規模な監視(Mass Surveillance)を行うことはできず、外国人市民や国境を越えた通信に関連してもドイツ憲法(基本法)に拘束されることを明らかにした。

- “Do foreigners deserve privacy?” (Marko Milanovic氏)
  ⇒普遍的な人権の保護法令順守と自国内の市民の安全を調整することが可能か？という問いに関連する。

■ BND法判決は、以下の３点により注目されるべき事象である。

- ドイツ連邦憲法裁判所が foreign-foreign surveillanceの使用について直接的に言及した点
  - ドイツ憲法の基本的権利は、(特に公的機関が行う活動に関して)ドイツ国内だけでなく、国家管轄外の外国人との関係においても拘束力を持つことを明らかにした
  - しかし、本結論は、海外に居住する外国人に、自国民やドイツ法の管轄下にある外国人と同等の保護を与えることと同一視すべきではなく、裁判所は、適切な法的保護措置が適用されている場合には、原則として、バルクインターセプションは、外国諜報において憲法上正当化される措置である可能性があると指摘している
- 判決はEU加盟国の憲法裁判所が下したものである。その為、EU法(EU law)と欧州人権条約(the European Convention on Human Rights)の両方に由来する基本権の保護(protection of fundamental right)を考慮された判決となっている点
- ドイツ連邦憲法裁判所が国際的な諜報活動連携に関する問題を詳細に取り上げ、保護措置を提案した点
  - 外国人に対する追加保護措置の導入を要請
  - 国家間のデータの授受に適用される一連の法的保護措置策定に有用なガイドラインを提供

参考) Marcin Rojszczak　Extraterritorial Bulk Surveillance after the German BND Act Judgment(https://www.cambridge.org/core/journals/european-constitutional-law-review/article/extraterritorial-bulk-surveillance-after-the-german-bnd-act-judgment/D6B51E73049E18D9EEB563F36CEB679E）Marko Milanovic　Foreign Surveillance and Human Rights, Part 1: Do Foreigners Deserve Privacy?(https://www.ejiltalk.org/foreign-surveillance-and-human-rights-part-1-do-foreigners-deserve-privacy/)

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

ガバメントアクセス　2020年BND法判決について

■ 2021年末までにドイツ連邦憲法裁判所は、外国人に対する追加保護措置(safeguard)の導入を要請
⇒本改正は欧州におけるシギント基準の調和に貢献する可能性がある。

■ また、「データの海外授受に対する、別途前提条件として、外国当局が送信されたデータをどのように取り扱うかについて、法の支配の下で保証されていることが必要である」と規定した(Para233)

保護措置(抜粋)

1. それぞれの伝送チャネルから取り出されるデータ量と監視対象の地理的領域に対する制限が設けられる。
2. Foreign-foreign strategic surveillanceが連邦政府による決定準備目的だけに使用される場合、目的変更や他団体へのデータ転送は一般的に除外されなければならない。
3. 外国諜報活動を目的とした情報取集に際して全トラフィックデータを保存・保持する権限は収集可能なデータ量に応じて制限されなければならない。また6ヶ月以上のデータ保存はできない。
4. 専門家集団及び通信の秘密性を高める必要がある人物集団の保護には、特別な要件が適用される。
5. 高度に個人的な領域に関連する情報は使用してはならず、直ちに削除しなければならない。(Highly-personal)
6. データ削除に際しての重要ステップは、独立監視機関のために合理的かつ必要である限りにおいて、文書化されなければならない。

国際的な諜報協力とデータ転送に関する法的根拠

- a ：データ保護に対しての保証を尊重すること
- b：受領国が情報を使用する際に、人権を尊重すること。
- c：aとbの両方について、連邦情報局が十分に保障される様な明確な規制が必須となっていること
- d： さらに戦略的モニタリングからのデータの送信については、受信国による強い保証を取得することで、送受信制限が維持されなければならない。

出所)Thorsten Wetzling　Try harder, Bundestag! Germany has to rewrite its foreign intelligence reform
(https://aboutintel.eu/german-constitutional-court-bnd-ruling/)

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

ガバメントアクセス　ガバメントアクセスに関する手続き(特に司法の関与)・監査

■ G-10委員会(G-10 commission)：

- 連邦議会によって任命された４名で構成される。いかなる機関にも縛られることなく独立して、諜報手段可否を決定する。

■ PKGr(the Parliament Control panel)：

- 構成員は連邦議会より議会メンバーが任命される。議会はPKGr構成員数・構成・活動方法を決定できる。PKGr討議は秘密裏に実行される。(Parliamentary Control Panel Act 2・4・10条)

■ 独立機関(Independent body)：

- 1名の議長、２名のメンバー、３名の補欠で構成。最高裁判所長官・連邦検察庁総長の提案に基づいた任期6年の連邦政府に選出された最高裁判所判事・連邦検察庁検事がメンバーの対象。いかなる機関にも縛られることなく独立して、諜報手段可否を決定する。

ガバメントアクセス実施に関する手続き

類型	命令	許諾 事後許諾可能(差し迫った危機の場合)
諜報手段 (全般)	• 連邦内務省による命令(order)が必要(Sec.10 G-10)	• G-10委員会(G-10 Commission)による事前許諾が必要(Sec.15 G-10)
国外-国内戦略的諜報手段 (Foreign-Domestic strategic/ untargeted surveillance ,BND)	• 特定個人・組織に対する事前疑惑に基づかない集団的な傍受(G-10 5～8条)に該当する場合場合、連邦内務省は、どの国または地域が特定の非標的傍受措置に含まれるかの決定が必要	• G-10委員会(G-10 Commission)・PKGrによる承認が必要
国外-国外戦略的諜報手段 (Foreign-Foreign strategic/ untargeted surveillance ,BND)	違憲判決 (違憲判決後の動向は調査中。2021年に追加保護措置等を含む対応方針を提出予定)	

諜報活動を許諾するケースは以下の通り(詳細は次頁)

- BND法(セクション6.1)の３つの許諾ケース
- ドイツ基本法10条(Section 5.1)の８つの許諾ケース
  (Section 5.1)の９つの許諾ケース

参考)Baker＆McKenzie. Global Data Privacy ＆ Security Handbook(https://resourcehub.bakermckenzie.com/en/resources/data-privacy-security)、Fred H. Cate; James X. Dempsey　Bulk Collection: Systematic Government Access to Private-Sector Data　Systematic Government Access to Private- Sector Data in Germany

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

ガバメントアクセス　ガバメントアクセスに関する手続き(特に司法の関与)・監査

ドイツ諜報法における諜報活動措置を正当化できるケース

Three warranted cases of Section 6.1 BND Law
• Risks to the internal or external security of the Federal Republic of Germany; • Germany's ability to act; • Information on developments of foreign and security policy significance that relate to the National Intelligence Priority Framework
Eight warranted cases of Section 5.1 Art. 10 Law
• An armed attack against the nation • Intent to carry out acts of international terror • International proliferation of military weapons • Illegal import or sale of narcotics • Counterfeiting • International money laundering • Smuggling or trafficking of individuals • The international criminal, terrorist or state attack by means of malicious programs on the confidentiality, integrity or availability of IT systems
Nine warranted cases of Section 3.1 Art. 10 Law
• Crimes of treason • Crimes that are a threat to the democratic state • Crimes that threaten external security • Crimes against national defense • Crimes against the security of NATO troops stationed in the Federal Republic of Germany • Crimes against the free democratic order as well as the existence or the security of the country. • Crimes under the Residence Act • Crimes under Sections 202a, 202b and 303a, 303b of the Criminal Code, in so far as they are directed against the internal or external security of the Federal Republic of Germany, in particular against security sensitive bodies of vital institutions • Crimes under Section 13 of the Criminal Code

出所)Thorsten Wetzling　Germany's intelligence reform June 2017 Policy Brief
(https://www.stiftung-nv.de/sites/default/files/snv_thorsten_wetzling_germanys_foreign_intelligence_reform.pdf)

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

ガバメントアクセス　ガバメントアクセスに関する手続き(特に司法の関与)・監査

2017年BND法改正前後の諜報活動規定

2017年BND法改正前

Table 2: Pre-reform framework for the BND's strategic surveillance

Practice	**Foreign-Domestic Strategic Surveillance** (Strategische Fernmeldeaufklärung)	**Foreign-Foreign Strategic Surveillance** (Ausland-Ausland-Fernmeldeaufklärung)
Law	Section 5 Art. 10 Law	Section 2.1 BND Law and secret interpretations
Surveillance Orders	BND requests them through the Interior Ministry	unregulated
Review Body & Composition	G10 Commission (4 honorary members, 4 deputies)	Only executive control (if at all)
Warrants	Default standard: Ex ante authorization with full knowledge of search terms	n/a
Oversight Mandate	Legality & necessity review; can prompt immediate end of measures deemed unlawful or unnecessary	n/a
Investigation Powers	Full access to premises & documents	n/a
Effective Remedy Procedure	Default standard: Ex post notifications	n/a
Data Minimization	DAFIS Filter System	DAFIS Filter System
Quantity Restriction	20 percent rule in Section 10.4 Art.10 Law	None

2017年BND法改正後

Table 3: Post-reform framework for the BND's strategic surveillance

Practice	Foreign-Domestic Strategic Surveillance (Strategische Fernmeldeaufklärung)	Foreign-Foreign Strategic Surveillance (Ausland-Ausland-Fernmeldeaufklärung)
Law	Art. 10 Law	BND Law
Surveillance Orders	BND requests them through Interior Ministry	BND requests them through Chancellery
Review Body & Composition	G10 Commission (4 honorary members, 4 deputies)	Independent Committee (UG) (3 members, 3 deputies)
Characterization	Judicial oversight by quasi-judicial body	Restricted judicial oversight by administrative body
Review Sessions	Once a month	Once every three months
Warrants	Default standard: Ex ante authorization with full knowledge of search terms	Default standard: Ex ante authorization with limited knowledge of search terms
Oversight Mandate	G10 Commission can prompt immediate end of measures deemed unlawful or unnecessary	UG can prompt immediate end of measures deemed unlawful or unnecessary
Investigation Powers	Full access to premises & documents	Not specified.
Effective Remedy Procedure	Default standard: Ex post notifications	No notifications.
Data Minimization	DAFIS Filter System	DAFIS Filter System
Quantity Restriction	20% rule in Section 10.4 Art.10-Law	None

出所)Thorsten Wetzling　Germany's intelligence reform June 2017 Policy Brief
(https://www.stiftung-nv.de/sites/default/files/snv_thorsten_wetzling_germanys_foreign_intelligence_reform.pdf)

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

ガバメントアクセス　権利保障の確保

救済措置として、データ対象者(Data subject)は、諜報機関が実施した監視措置について裁判所の審査を要請することができる。

■ ドイツ基本法第10条第2項は、通信、郵便、電気通信のプライバシーに関する憲法上の権利が制限され、その制限が自由民主主義の基本秩序、ドイツ連邦またはそのいずれかの国の存在または安全を保護するのに役立つ場合、裁判所に対する訴訟の代わりに、立法府によって任命された機関および補助機関が、案件の審査を実施すると規定している。

■ G-10 に基づき BND、MAD または BVD が発行した監視命令に異議を唱えるため、データ対象者は以下の措置を講ずることが可能である(Sec. 2 para. 1 G-10)

- データ対象者は行政裁判所に異議申し立てが可能
- ただし、G-10に基づく監視措置の場合、裁判所の審査は影響を受けるデータ対象者がこれらの措置について公式に通知された場合にのみ可能である。(Sec.13 G-10)

出所)Baker＆McKenzie. Global Data Privacy ＆ Security Handbook
(https://resourcehub.bakermckenzie.com/en/resources/data-privacy-security)

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

ガバメントアクセス　権利保障の確保

■ 政府に対する個人のプライバシー権は特に以下に記載

- 基本的人権：
  - 通信、郵便、通信のプライバシーに関する憲法上の権利。(ドイツ基本法第10条)
  - 住居不可侵(ドイツ基本法13条)
  - 憲法上のプライバシー権(情報的自己決定権)(ドイツ基本法第2条第1項)
  - 私生活および家族生活、自宅、通信手段を尊重する権利(欧州人権条約「 ECHR 」第8条)

*一方で、通信の秘密は、安全保障目的での制約を受けると明記(1968年改正で規定)

- ドイツ基本法第10条 (通信の秘密)
- (1) 信書の秘密ならびに郵便および電気通信の秘密は、不可侵である。
- (2) 制限は、法律に基づいてのみ行うことができる。その制限が、自由で民主的な基本秩序の擁護、または連邦およびラントの存立もしくは安全の擁護のためのものであるときは、法律により、その制限が当事者に通知されないこと、および裁判上の方法に代えて、議会の選任した機関および補助機関によって事後審査を行うことを定めることができる。

- 連邦データ保護法　第12条-第26条(Bundesdatenschutzgesetz、”BDSG”)
- 傍受に対し、判例が具体的危険を要求して制約している
  - 国家は個人の情報を根拠なく収集してはならず(1983年憲法裁判所判決)、国家による通信傍受(通信の秘密に対する侵害)は、「具体的かつ現在の危険」を要件とする判例があり、ガバメントアクセスを強く規律している

■ 個人データを政府と共有する企業に対する個人のプライバシー権は特に以下に記載

- テレメディア法　第11条-第15a条(ドイツ語：Telemediengesetz, "TMG")
- 連邦データ保護法　第27条-第35条(Bundesdatenschutzgesetz、”BDSG”)
- 刑法　第201条-第206条(ドイツ語：Strafgesetzbuch、”StGB”)
- 電気通信法　第88条以下参照(ドイツ語：Telekommunikationsgesetz “TKG”)

出所)Baker＆McKenzie. Global Data Privacy ＆ Security Handbook
(https://resourcehub.bakermckenzie.com/en/resources/data-privacy-security)

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

(参考)　ガバメントアクセス　捜査機関

■ GAに関する制度の根拠法：

- 刑事訴訟法：
  the Code of Criminal Procedure.
- 連邦刑事警察局に関する法律：
  the Act on the Federal Criminal Police Office
- 連邦警察に関する法律：
  the Act on the Federal Police
- 税関調査局及び税関調査事務所に関する法律：
  the Act on the Customs Investigation Bureau and the Customs Investigation Offices

■ GAに関する手続き(特に司法の関与)：司法機関に対して事前許諾が必要

■ 適用対象(データ、企業)：適応対象の限定はなし

■ 特に個人/非個人の区別があるか：個人/非個人の区別は不明

■ どの程度広範であるか：一定の限定が存在

■ 第三者監査：司法機関の事前許諾が必要

出所)Baker＆McKenzie. Global Data Privacy ＆ Security Handbook
(https://resourcehub.bakermckenzie.com/en/resources/data-privacy-security)

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

ガバメントアクセス　非個人データ　次世代自動車に関連する法案

■ドイツで、次世代自動車に関連する法案が2021年5月20日に連邦議会(下院)で、5月28日に連邦参議院(上院)で可決、7月28日に発効した。
- 公道でのレベル4の自動運転を可能にする道路交通法(StVG)改正案(自動運転法)

■当該法案の内、連邦政府が閣議決定した法案から、連邦議会で一部修正がされた内容かつ、非個人データに対するガバメントアクセスに係るものは以下の通り。
- 自動運転車両の製造者に対する、自動運転車両利用時に利用者個人のデータと自動運転に必要なデータを収集・保存する際のルールをさらに詳細化した。
- 非個人データは、デジタル化・自動化に関する研究、交通事故の分析など公共の利益のために、政府機関が提出を要求できるケースについて明確化した。

道路交通法 (StVG)改正　ガバメントアクセスに関連する規定は以下；
According to Sec. 1d (II) StVG, certain vehicles shall be able to drive fully autonomously in defined areas (e.g. highways), which are opened for autonomous driving by the federal states. According to Sec. 1g StVG, certain data (e.g. in case of accidents) listed in the section must be stored for this purpose and transmitted to the Kraftfahrt-Bundesamt upon request. Pursuant to Sec. 1g (5) StVG, the Kraftfahrt-Bundesamt is authorized to make certain data available to research institutions for the purpose of scientific research in the area of digitalization, automation and networking, as well as for the purpose of road traffic accident research.

参考)JETRO　次世代自動車のための自動運転と急速充電インフラ整備に関する2法案が可決(ドイツ)
(https://www.jetro.go.jp/biznews/2021/06/c1b16d24eee741b6.html) 、データ保護を専門とする弁護士へのヒアリングよりNRI作成

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

ガバメントアクセス概要

オランダにおけるガバメントアクセス：

■ 通信機器等の傍受

- the Dutch Telecommunications Act
- **the Dutch Intelligence and Security Services Act(2002)**

■ 職場監視

- GDPR(General Data Protection Regulation)
- the Works Council Act

※無許可のハッキング、監視、傍受は刑事犯罪であり、the Dutch Criminal Codeにて規制されている。

出所)Baker＆McKenzie. Global Data Privacy ＆ Security Handbook
(https://resourcehub.bakermckenzie.com/en/resources/data-privacy-security)

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

ガバメントアクセス　根拠法

- 根拠法：the Dutch Telecommunications Act及びThe Dutch Intelligence and Security Services Act(2002年)により、オランダ総合情報保安局(AIVD)は、通信の傍受、保存、検索、およびコンテンツへのアクセスを行う特別な権限が付与されている。
- 主体：
  オランダ総合情報保安局(Algemene Inlichtingen- en Veiligheidsdienst： AIVD)
- 承認：

傍受対象	Mass interception of　telecommunications (通信の集団傍受)	Targeted interception of telecommunications (標的型通信傍受)
関連大臣による事前承認	**不要**	**必要**
データ主体	特定なし	特定有り (個人又は組織の特定の通信)
データ内容	(内容を含まない)通信のメタデータ	通信の内容

通信の集団傍受は、その通信の内容の処理が行われないため、関連大臣の承認は必要なく、法律上、通信の秘密に対する侵害に該当しない。一方、集団傍受によって取得されたバルクデータの中から、ある特定の個人または組織に関する電気通信トラフィックを分離することも可能である。このような場合は、プライバシー権を侵害するため、大臣の承認が必要である。また、通信の内容は開示される可能性がある。(The Dutch Intelligence and Security Services Act(2002年)第27条)

参考)General Intelligence and Security Services　Interception of telecommunications by the AIVD: rules and regulations(https://english.aivd.nl/latest/news/2013/11/29/interception-of-telecommunications-by-the-aivd-rules-and-regulations)よりNRI作成

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

ガバメントアクセス　承認、監督

■ 承認：

Targeted interception of telecommunications(標的型通信傍受)を実施する場合、AIVDは大臣に根拠のある要請(request)を提示しなければならない。
このような要請には、以下を明記する必要がある。

- 必要性(necessity)：本権限を用いることが必要かどうか
- 比例性(proportionality)：プライバシーの侵害がGAの結果に見合うかどうか
- 補完性(subsidiarity)：より侵害度の低い別の方法で情報を取得できないかどうか

■ 監督：

- 独立した監督機関として、情報セキュリティサービス規制委員会(CTIVD)が設置されている。
  CTIVDは、AIVD(および、オランダ軍情報保安局(MIVD)の活動が合法的かどうかを監督する。また、CTIVDはAIVDとMIVDが大量傍受(Signal Intelligence)を行う方法についても調査している。この件に関する報告書は、委員会のサイトで閲覧できる。
- さらに、議会下院の情報・治安サービス委員会(CIVD)は、情報・治安サービスに対する議会監督責任を負う。委員会は、各議会の下院議長によって構成される。

出所)General Intelligence and Security Services　Interception of telecommunications by the AIVD: rules and regulations
(https://english.aivd.nl/latest/news/2013/11/29/interception-of-telecommunications-by-the-aivd-rules-and-regulations)

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

ガバメントアクセス概要

チェコにおけるガバメントアクセスと根拠法：

■ 安全保障関係

- Constitutional Act No. 110/1998 Coll., on the Security of the Czech Republic(安全保障に係る憲法条項)
- Subsequent defense and crisis legislation (acts and implementing regulations)(防衛・危機管理法制)
- Act No. 153/1994 Coll., on the Intelligence Services of the Czech Republic(情報機関に関する法律)
- Act No. 154/1994 Coll., on the Security Information Service(治安・諜報サービスに関する法律)
- Constitutional Act No. 23/1991 Coll., Introducing the Charter of Fundamental Rights and Freedoms as a Constitutional Act of the Federal Assembly of the Czech and Slovak Federal Republic(表現の自由等に係る憲法条項)

チェコ共和国の安全保障システム：

■ チェコ共和国の安全保障に関する憲法第110/1998改正法は、チェコ共和国の主権と領土の一体性、民主主義の基盤の保護、生命、健康、財産の保護を確保することが国家の基本的義務であると定めている。この法律は、チェコ共和国の安全を、その軍隊、武装治安部隊、救助隊、緊急サービスによって確保することを規定している。国家機関、自治領の機関、自然人および法人は、チェコ共和国の安全保障に参加する義務がある。情報機関は、チェコ共和国の安全保障に不可欠な情報を取得、収集、評価し、安全保障上の脅威とリスクを迅速に特定することによって、チェコ共和国の安全保障システムにおいて重要かつかけがえのない役割を果たす。個々の情報機関の地位を規定する法律上の規定は、例えば長官の任命や解任の方法などに関して、それぞれ異なっている。しかし、チェコの情報機関は、その任務およびその他の義務の遂行に関する限り、対等なパートナーである。政府はすべての情報機関に任務を与え、その活動を調整し、任務の遂行を監督している。チェコ共和国の安全保障戦略は、国家の安全保障政策にとって不可欠な概念文書である。チェコ共和国の安全保障戦略は、チェコ共和国の重要な、戦略的な、その他の重要な利益、一般的な安全保障上のリスク、長期計画、チェコ共和国の発展と繁栄、国民の安全のための良好な条件の確保を目的とした措置について定義している。

出所)Petr ZEMAN　INTELLIGENCE SERVICES OF THE CZECH REPUBLIC：CURRENT LEGAL STATUS AND ITS DEVELOPMENT
(http://connections-qj.org/system/files/3006_zeman.pdf)
Security Information Service (BIS)　Security system of the Czech Republic
(https://www.dcaf.ch/sites/default/files/publications/documents/zeman_intelligence-services-czech.pdf)

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

ガバメントアクセス　根拠法

根拠法	主体	補足
No. 153/1994 Coll. on Intelligence Services of the Czech Republic	N/A	■ アンブレラ法として機能しており、チェコ共和国の３つの諜報機関の位置づけ等を明記 ● 各諜報機関の権限、任命の仕組み ● 調整、統制、国内外の諜報に係る争点 ● 個々の情報機関の内部規定を前提にしている点も明記
Act No. 154/1994 Coll. on the Security Information Service (internal civilian service)(BIS)	BIS (安全保障に係る諜報機関)	■ BISは国防省ではなく文民による情報機関である。 ■ BISは一人の大臣に報告するのではなく、15～19人のメンバーから成立するキャビネットに対する報告義務を負う。
Act No. 289/2005 Coll. on the Military Intelligence. (VZ)	VZ (軍事に係る諜報機関)	■ VZは、国防省の一部である。 ■ 責任者は、防衛大臣により任命され、政府の同意を得る。
設置法は、アンブレラ法に依拠 (独立した設置法は存在しない)	UZSI (文民外交に係る諜報機関)	■ UZSI は、国防省ではなく文民による情報機関である。 ■ その設置法はNo. 153/1994 Coll. on Intelligence Services of the Czech Republicで定義されている。 ■ 海外から発信された重要な情報を提供を担う。

参考)Petr ZEMAN　INTELLIGENCE SERVICES OF THE CZECH REPUBLIC：CURRENT LEGAL STATUS AND ITS DEVELOPMENT
(http://connections-qj.org/system/files/3006_zeman.pdf)
Security Information Service (BIS)　Security system of the Czech Republic
(https://www.dcaf.ch/sites/default/files/publications/documents/zeman_intelligence-services-czech.pdf)よりNRI作成

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

ガバメントアクセス　法的根拠

■ 2015 年 9 月 25 日の諜報活動に関する連邦法(The Federal Act on the Intelligence Service of 25 September 2015「以下IntelSAという。」)が、**個人データに係るガバメントアクセス**を根拠法となっている。

法的根拠(1/2)

項目	概要
目的	ガバメントアクセスに係る、以下 4 つの目的が規定されている。 ① スイスの民主的及び憲法的原則の保障及び住民の自由の保護に貢献すること ② スイス住民及び外国にあるスイス国民の安全を増進すること ③ スイスの行動能力を支えること ④ 国際的な安全保障上の利益の保障に貢献すること
実施主体	連邦諜報機関(Service de renseignement de la Confédération / Nachrichtendienst des Bundes)(以下FISという。)
取得される個人データの種類に関する限定の有無	存在しない。
手続規定の有無	存在しない。
制限及びその例外に係る規定の有無	次項にて詳細説明。

出所)西村あさひ法律事務所「外国における個人情報の保護に関する制度等の調査結果報告書」
(https://www.ppc.go.jp/files/pdf/offshore_DPA_report_R3_12.pdf)

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

ガバメントアクセス　法的根拠

法的根拠(2/2)

項目	概要
制限及びその例外に係る規定の有無	**【連邦諜報機関(FIS)の権限】** ● その任務の遂行のため、**公開又は非公開の情報源から情報を収集することができる**(IntelSA5 条 1 項)。 ● **許諾を得る必要のある情報収集手段も許諾不要の情報収集手段も使用することができる**(IntelSA5 条 2 項)。 ● **関係者に注意喚起をすることなく情報収集**をすることができる(IntelSA5 条 4項)。 ● 以下の場合に、民間事業者に情報の提供を要求できる(IntelSA25 条)。 ①FIS が要求することのできる情報は、**国内外の安全に対する特定の脅威を特定、予防又は排除するために必要**な場合 ②(i)商業的利益のために運輸事業を行い、又は運輸手段の提供若しくは手配を行う自然人又は法人、 あるいは、(ii)特に映像送信又は映像録画装置等のセキュリティインフラストラクチャを運営する民間事業者に対して**のみ**要求する場合 (i)の場合には提供するサービスに関する情報、(ii)の場合には記録の移転(公の場所におけるイベントの記録を含む)の提供を求めることができる。 **【連邦諜報機関(FIS)に権限に対する制限】** ● 以下、2 つの条件を満たす報収集手段を選択しなければならない。(IntelSA5 条 3 項)。 ①特定の情報収集目的を**達成するために最も適切かつ必要** ②**関係者の基本権を最も阻害しない**情報収集手段を選択しなければならない ● **政治活動又はスイスにおける言論、集会又は結社の自由の行使に関する情報を収集又は処理することができない***(IntelSA5 条 5 項)

*例外として、組織又は個人がテロリズム、諜報又は暴力的過激主義の活動を実行するためにその権利を行使する場合という特定の証拠がある場合、FIS はかかる組織又は個人のIntelSA5 条 5 項に定める情報を収集することができ、個人に関連する当該情報を記録することができる(IntelSA　5 条 6 項)。
また、IntelSA72 条の監視リストに記載された組織又は集団によりもたらされる脅威を情報収集等により評価できる場合、かかる組織若しくは集団又はその構成員の IntelSA5 条 5 項に定める情報を収集及び処理することができる(IntelSA5 条 8 項)。

出所)西村あさひ法律事務所「外国における個人情報の保護に関する制度等の調査結果報告書」
(https://www.ppc.go.jp/files/pdf/offshore_DPA_report_R3_12.pdf)

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

ガバメントアクセス　取得された個人データの取扱いに対する制限

取得された個人データの取扱いに対する制限

項目	概要
保管期間の定めの有無	IntelSA 上、**特定の保管期間の定めはない。** ※ただし、IntelSA45 条において、FIS は全ての情報システムにおいて個人データの記録が任務の遂行に未だ必要なものかを定期的に確認し、必要のなくなったデータの記録については削除することとされている。
データの取扱者に関する制限	個人データ(センシティブデータ及び人格プロファイルを含む)を処理できるのは、FIS 及びカントン*47の執行当局に限定される(IntelSA44 条 1 項)。 FIS には、定期的に多様な監査を行う内部品質保証部門が存在する(IntelSA45 条 5 項)。
安全管理措置に関する定めの有無	存在しない。

*カントン ：スイスの地方自治組織の単位。スイスの地方行政区画は、カントンと呼ばれる州からなる。

出所)西村あさひ法律事務所「外国における個人情報の保護に関する制度等の調査結果報告書」
(https://www.ppc.go.jp/files/pdf/offshore_DPA_report_R3_12.pdf)

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

ガバメントアクセス　正当な目的の追求、承認の要求

正当な目的の追求

- IntelSA に基づき連邦機関が行った判断については、連邦行政裁判所に対して**提訴可能**であり、さらに連邦最高裁判所に対する上訴が可能である(IntelSA83 条)。
- 基本権に対する制限は、以下の 3 つの要件を満たさなければならない(スイス連邦憲法 36 条) 。
  ①法令上の根拠を有していること。
  ②公益又は他人の基本権の保護によって正当化されていること。
  ③比例原則上適切でなければならないこと。
- 民間事業者が保有する個人データに対するガバメントアクセスは、IntelSA 25 条が許容するものに限られる。

承認の要求

項目	概要
事前承認及び事後承認、保護措置	FIS の判断に従わない場合は、裁判手続が可能である(IntelSA83 条)ため、承認を求める規制は存在しない。また、FIS によって情報が取得されたと思料する者が FIS 又はデータ保護当局から情報提供を受ける権利が定められている。
暗号復号強制、保護措置	存在しない。

出所)西村あさひ法律事務所「外国における個人情報の保護に関する制度等の調査結果報告書」
(https://www.ppc.go.jp/files/pdf/offshore_DPA_report_R3_12.pdf)

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

ガバメントアクセス　透明性

透明性

項目	概要
ガバメントアクセスの事実の通知義務の有無	存在しない。
ガバメントアクセスの実施状況の公表・公的機関に対する報告	諜報活動監督局（Autorité de surveillance indépendante des activités de renseignement / Unabhängige Aufsichtsbehörde über die nachrichtendiensten Tätigkeiten。以下「**OA-IA**」という）は、FIS を監督する独立機関である。 **FIS は、OA-IA に対する報告義務を負う。**しかし、それ以外の機関に対する報告義務や公表義務は負わない。
監督機関による監督状況の公表	OA-IA は、連邦国防・市民防衛・スポーツ省に対し、その活動を記載した年次報告書を提出しなければならず、この報告書は公表される(IntelSA78 条 3 項)。 当該報告書はインターネット上で誰でも閲覧可能である。

出所)西村あさひ法律事務所「外国における個人情報の保護に関する制度等の調査結果報告書」
(https://www.ppc.go.jp/files/pdf/offshore_DPA_report_R3_12.pdf)

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

ガバメントアクセス　救済

救済

項目	概要
違法なガバメントアクセスに対する救済制度の有無等	データ保護機関(連邦データ保護・透明性コミッショナー)に基づく救済を求めることが可能である。 IntelSA 上、データ主体に追加的な情報提供を受ける権利が定められており、これに基づき FIS が自己に関するデータを処理しているかについて情報提供を求めることができる。
救済を提供する行政機関・裁判所	通常の民事及び刑事の裁判所が救済について審理する。
外国人の救済の可否	可能である。
ガバメントアクセスによって取得された情報に基づき訴追された者の権利	一般手続法に基づき異議を述べることが可能である。

出所)西村あさひ法律事務所「外国における個人情報の保護に関する制度等の調査結果報告書」
(https://www.ppc.go.jp/files/pdf/offshore_DPA_report_R3_12.pdf)

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

ガバメントアクセス　監督・調査・審査の仕組み

監督・調査・審査の仕組み

項目	概要
監督・調査・審査の仕組みを規定する法令の有無	● IntelSA75 条 ● OA-IA の内部規則：諜報活動監督規則(Ordonnance sur la surveillance des activités de renseignement du 16 août2017 / Verordnung über die Aufsicht über die nachrichtendienstlichen Tätigkeiten vom 16. August2017)
監督機関の名称・権限・独立性ディレクターの任命プロセスと身分保障	● OA-IA は、連邦国防・市民防衛・スポーツ省に所属しており、主要な事項については連邦参事会も監督権限を有している。 ● OA-IA は独立した機関であり、他の当局の指示に拘束されない(IntelSA77 条 1 項)。 ● OA-IA は、独立した予算、職員を有し、自らその組織、勤務形態及び内部手続を定めている(IntelSA77 条 2 項、3 項)。 ● OA-IA のディレクターは、連邦国防・市民防衛・スポーツ省の推薦に基づき、連邦参事会が任命し、その任期は 6 年間である。連邦参事会が現任のディレクターが適切でないことを客観的に合理的な理由を付して現任のディレクターの任期終了の 6 か月前までに決定しない限り、現任のディレクターは次の 6 年間の任期について再任される。現任のディレクターが故意若しくは重過失により職務上の義務に違反し、又は職務の遂行が恒常的に不可能となった場合、連邦参事会は現任のディレクターをその任期終了より前に解任することができる。
調査形態	● OA-IA は、FIS が行う諜報活動を監督する(IntelSA78 条)。 ● OA-IA は、FIS の活動の適法性、有用性及び実効性を評価する。OA-IA は、関連する全ての情報及び文書、並びに FIS の全ての施設に対するアクセスが可能である。OA-IA は文書の写しを提出することを要求できる。監督活動の範囲内で、OA-IA は、他の連邦及びカントンの当局から情報を求め、かかる当局が保有するファイルを検査することができる(ただし、かかる情報が当局間の協力及び FIS に関連することを条件とする)(IntelSA78 条 4 項)。 ● OA-IA は、監督活動を目的として、FIS が保有する全ての情報システム及びデータの集合体(機微データを含む)に対するアクセスが可能である。OA-IA は、監督が完了するまでの間に限り、取得したデータを保存することができる。データの集合体の所有者は、データの集合体に対するアクセスを記録しなければならない(IntelSA78 条 5 項)。 ● OA-IA は、その監査の結果に関する報告書を連邦国防・市民防衛・スポーツ省に提供する(IntelSA78 条 6 項)。 ● OA-IA は勧告を出すことができ、連邦国防・市民防衛・スポーツ省は勧告の実施を確保するか、勧告を拒否する場合には勧告を連邦参事会に提出し、判断を仰ぐ(IntelSA78 条 7 項)。
GAによって取得された情報に基づき訴追された者の権利	● OA-IA は、その監査の結果に関する報告書を連邦国防・市民防衛・スポーツ省に提供する(IntelSA78 条 6 項)。 ● OA-IA は勧告を出すことができる。連邦国防・市民防衛・スポーツ省は、連邦参事会に対し定期的に脅威及び FIS の活動について報告する(IntelSA80 条 1項)

出所)西村あさひ法律事務所「外国における個人情報の保護に関する制度等の調査結果報告書」
(https://www.ppc.go.jp/files/pdf/offshore_DPA_report_R3_12.pdf)

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

ガバメントアクセス　非個人データ　デジタルサービス法(欧州議会案)

■ デジタルサービス法案において、違法情報に関する当局へのデータ提供義務が規定されている。

	欧州議会　修正案　対応箇所	仲介サービス	ホスティングサービス	オンラインプラットフォーム	超巨大オンラインプラットフォーム
1 命令を受けた国家当局との協力とサービスの受け手の救済措置	第8条、第9条、第9a条	●	●	●	●
窓口および必要な場合は法定代理人	第10条、第10a条、第11条	●	●	●	●
基本的人権を考慮した利用規約の要求事項	第12条	●	●	●	●
透明性のある報告	第13条	●	●	●(第23条も追加)	●(第23条、第33条も追加)
オンライン・インターフェースの設計と構成	第13a条	●	●	●	●
ユーザーへの告知・対応と情報提供義務	第14条、第15条		●	●	●
2 犯罪行為の報告	第15a条		●	●	●
内部苦情処理システムと裁判外紛争解決	第17条、第18条			●	●
信頼できるフラガー(flaggers)	第19条			●	●
オンラインに関するアクセシビリティ要件	第19a条			●	●
不正使用に対する対策と保護	第20条			●	●
オンラインプラットフォームを利用する取引業者のトレーサビリティ	第22条			●	●
3 違法な製品・サービスに関する消費者・当局への情報提供	第22a条			●	●
オンライン広告のユーザー向け透明性	第24条			●	●
リコメンダーシステムの透明性	第24a条			●	●(第29条も追加)
ユーザーが作成したポルノコンテンツへの対策	第24b条			●	●
リスク管理義務とコンプライアンス・オフィサー	第26条、第27条、第32条				●
外部リスク監査と説明責任	第28条				●
情報へのアクセスに対するユーザーの選択	第30条				●
ディープフェイクの透明性	第30a条				●
4 当局や研究者とのデータ共有	第31条				●
行動規範	第35条、第36条				●
危機対応協力	第37条				●

参考)European Parliament Texts adopted - Digital Services Act(https://www.europarl.europa.eu/doceo/document/TA-9-2022-0014_EN.pdf)
張睿暎 EUにおけるプラットフォーム規制と「デジタルサービス法」規則案の意義獨協法学第115号(2021年8月)211-244頁

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

ガバメントアクセス　非個人データ　デジタルサービス法(欧州議会案)

■ デジタルサービス法案において、違法情報に関する当局へのデータ提供義務が規定されている。

	条項	項目	内容
1	第9条	情報提供の命令	• 仲介サービスのプロバイダは、サービスの1人以上の特定の個人の受領者に関する特定の項目の情報を提供する命令を、安全な通信チャネルを介して受領した場合、関連する国の司法又は行政当局から、適用されるEU又は国の法律に基づいて、EU法に準拠して、不当に遅延なく、その命令の発行機関に、受領とその命令に与えられた効果を通知しなければならない。
2	第15a条	刑事犯罪の疑いの届出	• ホスティングサービスのプロバイダは、人の生命または安全に対する差し迫った脅威を伴う重大な犯罪が行われた、行われている、または行われる予定であるという疑いを生じさせる情報を知った場合、その疑いを加盟国または関係加盟国の法執行機関または司法機関に速やかに知らせ、その要請に応じて、利用できるすべての関連情報を提供しなければならない。
3	第22a条	違法な製品・サービスに関する消費者・当局への情報提供義務	• 消費者が販売者との遠隔契約を締結できるオンラインプラットフォームが、そのプラットフォームのインターフェース上で販売者が提供する製品またはサービスが連合法または国内法の適用要件に照らして違法であることを認識した場合、使用する手段に関わらず、そのプラットフォームは以下のことを行わなければならない。 (a) インターフェースから違法な製品またはサービスを迅速に削除し、必要に応じて市場監視当局または税関当局などの関連当局に決定事項を通知する。 (b) オンラインプラットフォームがサービスの受領者の連絡先を知っている場合、当該製品またはサービスを取得したサービスの受領者に、違法性、取引者の身元、救済を求めるための選択肢を通知すること。 (c) 過去12ヶ月間にプラットフォームから削除された違法な製品及びサービスに関する情報を含むリポジトリを編集し、アプリケーションプログラミングインタフェースを通じて一般に利用可能にすること。
4	第31条	データアクセスおよび精査	• 非常に大規模なオンラインプラットフォームは、設立のデジタルサービスコーディネーターまたは委員会に対し、その合理的な要求があり、合理的な期間内に、要求で指定された遅延なく、本規則の遵守を監視し評価するために必要なデータへのアクセスを提供するものとする。そのデジタル・サービス・コーディネーターと委員会は、それらの目的のためにのみ、そのデータを要求し、アクセスし、使用するものとする。

参考)European Parliament Texts adopted - Digital Services Act(https://www.europarl.europa.eu/doceo/document/TA-9-2022-0014_EN.pdf)

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

ガバメントアクセス　非個人データ　デジタル市場法(欧州委員会案)

デジタル市場(DMA)法案は、大手プラットフォーム事業者を規制することで参入退出自由で公正なデジタル市場を確保し、問題となる行為を取りしまる執行についてを扱い、欧州デジタル市場における競争と調和を確保するものである。また、本規則に定める規則の監視、実施および執行の目的とした情報提供要求(第19条)が定められている。

DMA法案概要

1. **規律対象(ゲートキーパー)の認定(法案 3 条)**
   - ① EEA での過去 3 年間の年間売上高 65 億ユーロ以上、又は直近会計年度の株式時価総額 650 億ユーロ以上で 3 以上の加盟国でサービスを提供。
   - ② ＥＵ域内の一般利用者が月間 4500 万人以上及び事業利用者が年間 1 万社以上。
   - ③ ②の基準が過去 3 年間適合すること。
2. **ゲートキーパーの主な禁止事項(法案 5 条、6 条)※後述**
3. **欧州委による市場調査目的**
   - ①ゲートキーパーを特定する(ゲートキーパー認定に漏れはないか)
   - ②デジタル市場におけるサービスを見直しする(対象デジタルサービスに漏れはないか)
   - ③ゲートキーパーが組織的違反を行った場合の追加制裁措置を考える
4. **欧州委の権限**
   - **①情報提供要求(法案 19 条)**、事情聴取(法案 20 条)、②立入検査(法案 21 条)、③法案 5 条及び 6 条違反に対する緊急措置(法案 22 条)、④確約(法案 23 条)、⑤モニタリング(法案 24 条)、⑥違反決定(法案 25 条)、⑦制裁金(法案 26 条～29 条)：違反に対して売上額 10％までの制裁金、情報提供懈怠等に対して売上額 1 ％までの制裁金
     ⑧異議申立(法案 30 条)、⑨秘匿特権(法案 31 条)、⑩デジタル市場委員会からの支援(法案 32 条)

出所)ジョン・フランソワ ベリス、亀岡 悦子(バンバール・アンド・ベリス法律事務所)　EU 競争法の最新動向
(https://www.koutori-kyokai.or.jp/description/reserch/2020/202101gaikoku.pdf)

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

ガバメントアクセス　非個人データ　デジタル市場法(欧州委員会案)

■ 第19条 情報提供の要請

- 1.欧州委員会は、簡単な要請または決定により、事業者および事業者団体に対し、本規則に定める規則の監視、実施および執行の目的を含め、必要なすべての情報を提供するよう求めることができる。また、欧州委員会は、単純な要求または決定により、事業者のデータベースおよびアルゴリズムへのアクセスを要求し、これらに関する説明を求めることができる。

- 2.欧州委員会は、第14条に基づく市場調査または第18条に基づく手続きを開始する前にも、第1項に基づき事業者および事業者団体に情報を要求することができる。

- 4.欧州委員会が事業者及び事業者団体に対し、決定により情報の提供を要求する場合、要求の目的を述べ、必要とされる情報を明示し、提供する期限を定めるものとする。欧州委員会が事業者に対し、そのデータベースおよびアルゴリズムへのアクセスを要求する場合、法的根拠および要求の目的を述べ、提供すべき期限を定めなければならない。また、第26条に規定する罰則を示し、第27条に規定する定期的な罰金の支払いを示し、又は課さなければならない。さらに、その決定を司法裁判所に再審理してもらう権利も示さなければならない。

出所)ジョン・フランソワ ベリス、亀岡 悦子(バンバール・アンド・ベリス法律事務所)　EU 競争法の最新動向
(https://www.koutori-kyokai.or.jp/description/reserch/2020/202101gaikoku.pdf)

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

ガバメントアクセス　非個人データ　デジタル市場法(欧州委員会案)

ゲートキーパーに対する義務(第５-６条)

	条項	概要
	第５条(a)	PF上のデータと他から得たデータの突合禁止
	第５条(b)	PF外でPF上の条件と異なる条件での販売を抑制することの禁止
	第５条(c)	事業者にPF上で獲得したEUとのPF外取引を認めるべきこと
	第５条(d)	事業者による公的機関への苦情申し立てを禁止しないこと
	第５条(e)	事業者にPFの識別サービス利用を強制することの禁止
	第５条(f)	消費者にPF利用の条件として、他のPFへの登録等を要件としないこと
1	第５条(g)	広告主が支払った対価と媒体社が受領した報酬についての情報開示
	第６条(a)	PF上で得た情報を利用して事業者と競争することの禁止
	第６条(b)	消費者がプレインストールされたアプリ削除を許容すること
	第６条(c)	OS上で第三者アプリや第三者アプリストアを利用することの許容
	第６条(d)	ゲートキーパー自身等が有利となるランキング条件設定の禁止
	第６条(e)	OS上でユーザーが別のアプリへ乗り換えるための技術的制限の禁止
	第６条(f)	事業者と付随サービス提供者へのOSへの公平なアクセスの確保
	第６条(g)	広告効果測定ツールへの広告主・媒体社のアクセス確保
2	第６条(h)	データポータビリティを確保する
3	第６条(i)	事業者に事業者や消費者がPF利用により生じた情報を無償で提供
4	第６条(j)	検索サービスの消費者により生成されたランキング等情報の提供
	第６条(k)	事業者に対してアプリストアへの非差別的なアクセスの確保

義務内容の詳細

1. 広告サービスに関して、広告主とパブリッシャーに対し、要求に応じて、支払い価格情報等を提供しなければならない。

2. 事業者又は消費者の活動を通じて生成されたデータの効果的なポータビリティを提供し、特に消費者に関して、継続的かつリアルタイムでのアクセスを含め、GDPRに沿い、データポータビリティの行使を促進するツールを提供しなければならない。

3. 事業者又は消費者に承認された第三者に対して、中核プラットフォームサービスの利用に関して提供・生成されたデータ(集計・非集計両方)への、継続的かつリアルタイムのアクセスを提供しなければならない。(個人データの場合は本人の同意がある場合のみ)

4. オンライン検索エンジンのサードパーティプロバイダに対して、要求に応じて、公正で合理的かつ非差別的な条件で、検索に関連するランキング、クエリー、クリック、および表示データへのアクセスを匿名化した形で提供しなければならない。

参考)
ニッセイ基礎研究所　提案された EU のデジタル市場法案
(https://www.nli-research.co.jp/files/topics/68328_ext_18_0.pdf)
生貝直人　欧州におけるデータ関連政策の状況
(https://www.jftc.go.jp/cprc/conference/index_files/201221da4.pdf)

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

ガバメントアクセス　EUデータ法案 公共部門機関等に対するデータ提供義務　概要

■ データ法は、公共部門が特定の公益目的のために必要な民間部門が保有するデータにアクセスし利用すること(ガバメントアクセス)に係る調和された枠組みを規定している。このようなガバメントアクセスの例として、企業の負担を最小限に抑えながら、公共の緊急事態に迅速かつ安全に対応するための洞察を導くこと等が挙げられる。

■ まず、第14条及び15条は、本枠組みが、データを使用可能にする義務に基づいており、公共部門機関が特定のデータを使用する例外的な必要性があるにもかかわらず、新しい法律の制定又は既存の報告義務によって適時にそのようなデータを市場で取得できない場合にのみ、適用されることを定めている。

■ 第17条及び19条は、データを要求する権利が乱用されないため、また、公共部門が当該データの使用について説明責任任を果たす為に、データの要求は比例的である必要があり、達成すべき目的を明確に示し、データを利用可能にする企業の利益を尊重する必要があることを定めている。また、管轄当局は、すべての要請に係る透明性と一般への公開を保証すること、また、その結果として生じるあらゆる苦情にも対応することを定めている。

■ 第20条1項は、公衆衛生上の緊急事態、大規模な自然災害や人為的災害等の公共の緊急事態に対応するための例外的な必要性がある場合、データは無料で使用可能であることを定めている。また、同条2項は、その他の例外的な必要性(公的緊急事態の予防、緊急事態からの回復支援等)の場合、データを使用可能にするデータ保有者は、関連データを使用可能にするための費用に合理的なマージンを加えた補償を受ける権利を有することを定めている。

参考)European Commission Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on harmonised rules on fair access to and use of data (Data Act) (https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=COM:2022:68:FIN) よりNRI作成

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

ガバメントアクセス　EUデータ法案 公共部門機関等に対するデータ提供義務　概要

概要

GAが正当化されるケース

■ **第15条　データの使用に係る例外的な必要性**

- 例外的な必要性の例(以下の状況のいずれかに該当する場合)：
  - (a)公共の緊急事態に対応するために要求されたデータが必要である場合
  - (b) 公共の緊急事態を防止するため、または公共の緊急事態からの回復を支援するために必要な、時間および範囲が限定されたデータの要求がある場合
  - (c)利用可能なデータの不足により、公共部門機関、連合機関、政府機関が、法律で明示的に規定されている公共の利益のための特定の任務を遂行することができない場合

GA主体の義務

■ **第17条　データ提供の要請**

- １．データ提供の要請に係る公共部門機関、連合機関、政府機関の手順：
  - (a) どのようなデータが必要であるかを明示すること。
  - (b) データが要求される例外的な必要性を示すこと
  - (c) 要求の目的、要求されたデータの使用目的、及びその使用期間を説明すること。
  - (d) データを要求する法的根拠を明記すること。
  - (e) データが利用可能になる期限、またはデータ保持者が公共部門機関、連合機関、政府機関に要求の修正または撤回を要求できる期限を指定すること。
- ２．データ提供の要請に係る公共部門機関、連合機関、政府機関の義務内容：
  - (a) データ保有者が理解できるように、明確、簡潔かつ平易な言葉で表現されていること。
  - (b) 要求されたデータの粒度、量及び要求されたデータへのアクセスの頻度において、例外的な必要性に釣り合ったものであること。
  - (c) 企業秘密の保護及びデータを利用可能にするために必要なコストと労力を考慮した上で、データ保有者の合法的な目的を尊重すること。
  - (d) 可能な限り、非個人データに関するものであること。
  - (e) 要求に従わない場合、第31条に言及する管轄当局が第33条に従って課すべき罰則を情報保有者に通知すること。
  - (f)(データ提供の要請が) 不必要な遅滞なく、オンラインで一般に利用可能とすること。

■ **第19条　公共部門機関、連合機関、政府機関の義務**

- １．第14条に基づく要請に従って、データを受領した公共部門機関、連合機関、政府機関は、以下を遵守しなければならない。
  - (a) データを要求された目的と相容れない方法で使用しないこと。
  - (b) 個人データの処理が必要な限りにおいて、データ主体の権利及び自由を保護する技術的及び組織的な措置を実施すること。
  - (c) 明示された目的に対して必要でなくなった時点でデータを破棄し、データ保有者に破棄されたことを通知すること。

参考)European Commission Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on harmonised rules on fair access to and use of data (Data Act) (https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=COM:2022:68:FIN)よりNRI作成

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

ガバメントアクセス　EUデータ法案 公共部門機関等に対するデータ提供義務　概要

概要

データ主体の義務・権利

■ **第14条　例外的な必要性に基づいてデータを利用可能にする義務**

- ２．本章はレコメンデーション 2003/361/EC の附属書第 2 条に定義される中小企業及び零細企業には適用されないものとする。

■ **第18条　データ提供要請への遵守**

- ２．データ保有者は、部門別法令に定められたデータの利用可能性に関する特定のニーズを阻害することなく、公共緊急事態に対応するために必要なデータ提供に係る要請を受領してから5 営業日以内、その他の例外的な必要性のある場合には 15 営業日以内に、以下のいずれかの事由により要求を拒否、又はその変更を求めることが可能である。
  - (a) データが入手できない場合。
  - (b) リクエストが第17条第1項および第2項に定める条件を満たしていない場合。

補償

■ **第20条　例外的な必要性がある場合の補償**

- １．第15条(a)に基づき、利用可能とされたデータは、無償で提供される。
- ２．第15 条 (b) 又は (c) に基づき、利用可能とされたデータについて、その補償は、必要に応じて匿名化および技術的適応の費用を含む要求に従うために生じた技術的および組織的費用を超えないものとし、これに妥当なマージンを加算するものとする。データを要求した公共部門機関、連合機関、政府機関の要求に応じて、データ保有者は、費用および妥当なマージンの計算の根拠に関する情報を提供するものとする。

その他

■ **第16条　公共部門機関、連合機関、政府機関がデータを利用可能にする他の義務との関係性**

- １．本章は、報告、情報要求への対応、法的義務の遵守の実証又は検証を目的とした、欧州連合法又は、国内法に定められた義務に影響を与えない。

参考)European Commission Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on harmonised rules on fair access to and use of data (Data Act) (https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=COM:2022:68:FIN)よりNRI作成

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

ガバメントアクセス　EUデータ法案　第５章　条文

第５章　例外的な必要性に基づく、公共部門機関、連合機関、政府機関に対するデータ提供；

■ *第14条 例外的な必要性に基づいてデータを利用可能にする義務*

- １.データ保有者は、要求があれば、公共部門機関又は、要求されたデータを使用する例外的な必要性を示す連合機関、政府機関にデータを提供するものとする。
- ２.本章はレコメンデーション 2003/361/EC の附属書第 2 条に定義される中小企業及び零細企業には適用されないものとする。

■ *第15条　データの使用に係る例外的な必要性*

- 本章の意味におけるデータ利用に係る例外的な必要性は、次のいずれかの場合に存在するとみなされるものとする。
  - (a)公共の緊急事態に対応するために要求されたデータが必要である場合
  - (b) 公共の緊急事態を防止するため、または公共の緊急事態からの回復を支援するために必要な、時間および範囲が限定されたデータの要求がある場合
  - (c)利用可能なデータの不足により、公共部門機関、連合機関、政府機関が、法律で明示的に規定されている公共の利益のための特定の任務を遂行することができない場合
    かつ、
    - (１)公共部門機関または連邦機関、代理店または団体が、市場価格でデータを購入する、またはデータを利用可能にする既存の義務に依存するなどの代替手段によって当該データを入手することができず、新たな立法措置を採用しても当該データの適時利用が確保できない場合　又は、
    - (２)本章に定める手続きに沿ってデータを取得することが、データ保有者又は、その他の企業の事務的負担を実質的に軽減することになる場合。

■ *第16条　公共部門機関、連合機関、政府機関がデータを利用可能にする他の義務との関係性*

- １．本章は、報告、情報要求への対応、法的義務の遵守の実証又は検証を目的とした、欧州連合法又は国内法に定められた義務に影響を与えない。
- ２．本章による権利は、公共部門機関、連合機関、政府機関が、刑事若しくは行政犯罪の予防、捜査、探知、訴追、刑事罰執行のための活動、税関又は税務行政のための活動を行うために行使してはならないものとする。本章は、刑事上若しくは行政上の犯罪の予防、捜査、探知、訴追、刑事罰、行政罰の執行、税関又は税務行政のために適用される同盟法及び国内法に影響を与えない。

出所)European Commission Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on harmonised rules on fair access to and use of data (Data Act) (https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=COM:2022:68:FIN)

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

ガバメントアクセス　EUデータ法案　第５章　条文

■ *第17条　データ提供の要請*

- １．第14条第1項に従ってデータを要求する場合、公共部門機関、連合機関、政府機関は、以下を行うものとする。
  - (a) どのようなデータが必要であるかを明示すること。
  - (b) データが要求される例外的な必要性を示すこと。
  - (c) 要求の目的、要求されたデータの使用目的、及びその使用期間を説明すること。
  - (d) データを要求する法的根拠を明記すること。
  - (e) データが利用可能になる期限、またはデータ保持者が公共部門機関、連合機関、政府機関に要求の修正または撤回を要求できる期限を指定すること。
- ２．同条第1項の規定によるデータの請求は、以下の通りとする。
  - (a) データ保有者が理解できるように、明確、簡潔かつ平易な言葉で表現されていること。
  - (b) 要求されたデータの粒度、量及び要求されたデータへのアクセスの頻度において、例外的な必要性に釣り合ったものであること。
  - (c) 企業秘密の保護及びデータを利用可能にするために必要なコストと労力を考慮した上で、データ保有者の合法的な目的を尊重すること。
  - (d) 可能な限り、非個人的データに関するものであること。
  - (e) 要求に従わない場合、第31条に言及する管轄当局が第33条に従って課すべき罰則を情報保有者に通知すること。
  - (f)(データ提供の要請が) 不必要な遅滞なく、オンラインで一般に利用可能とすること。
- ３．公共部門機関、連合機関、政府機関は、本章に従って取得したデータを指令(EU)2019/1024の意味における再利用のために利用可能にしてはならない。指令(EU)2019/1024*は、本章に従って取得した公共部門機関が保有するデータには適用されないものとする。
- ４．同条第3項は、公共部門機関、連合機関、政府機関が、第15条の業務を完了する観点から、本章に従って得られたデータを他の公共部門機関、連合機関、政府機関と交換すること、又は公開された契約により技術検査その他の業務を当該第三者に委託している場合に当該データを第三者に利用させることを妨げるものではない。第19条に基づく公共部門機関、連合機関、政府機関に対する義務が適用される。
  公共部門機関、連合機関、政府機関が本項に基づきデータを送信し又は利用可能にする場合には、当該データの受領元であるデータ保有者に通知するものとする。

*指令(EU)2019/1024：オープンデータ指令(オープンデータおよび公共部門情報の再利用に関する指令(EU)2019/1024)

出所)European Commission Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on harmonised rules on fair access to and use of data (Data Act) (https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=COM:2022:68:FIN)

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

ガバメントアクセス　EUデータ法案　第５章　条文

■ *第18条　データ提供要請への遵守*

- １．本章に基づくデータへのアクセス要求を受けたデータ保有者は、要求元の公共部門機関、連合機関、政府機関に対し、データを不当に遅滞なく提供するものとする。
- ２．データ保有者は、部門別法令に定められたデータの利用可能性に関する特定のニーズを阻害することなく、公共緊急事態に対応するために必要なデータ提供に係る要請を受領してから5営業日以内、その他の例外的な必要性のある場合には15営業日以内に、以下のいずれかの事由により要求を拒否、又は、その変更を求めることが可能である。
  - (a) データが入手できない場合。
  - (b) リクエストが第17条第1項および第2項に定める条件を満たしていない場合。
- ３．公共緊急事態に対応するために必要なデータの要求の場合、データ保有者は、他の公共部門機関、連合機関、政府機関が、以前に同じ目的で提出された要求に応じて、要求されたデータを既に提供し、データ保有者が第19条第1項(c)に従ってデータの破棄を通知されていない場合も、要求の拒否又は、変更を求めることができる。
- ４．データ保有者が、第3項に従って要求を拒否し、又は、その変更を求めることを決定した場合、データ保有者は、以前に同じ目的で要求を提出した公共部門機関又は連合機関若しくは団体の身元を示すものとする。
- ５.公共部門機関、連合機関、政府機関に対してデータを利用可能にする要求の遵守のために個人データの開示が必要な場合、データ保有者は仮名化されたデータで要求を満たすことができる限り、そのデータを仮名化する合理的な努力をするものとする。
- ６.公共部門機関、連合機関、政府機関が、データ保持者による要求されたデータの提供の拒否に異議を唱えたい場合、要求の変更を求めたい場合、又は、データ保持者が要求に異議を唱えることを希望する場合においては、このような問題は、第31条にて言及された管轄当局に持ち込まれるものとする。

出所)European Commission Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on harmonised rules on fair access to and use of data (Data Act) (https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=COM:2022:68:FIN)

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

ガバメントアクセス　EUデータ法案　第５章　条文

■ *第19条　公共部門機関、連合機関、政府機関の義務*

- １．第14条に基づく要請に従って、データを受領した公共部門機関、連合機関、政府機関は、以下を遵守しなければならない。
  - (a) データの提供を要求された目的と相容れない方法で使用しないこと。
  - (b) 個人データの処理が必要な限りにおいて、データ主体の権利及び自由を保護する技術的及び組織的な措置を実施すること。
  - (c) 明示された目的に対して必要でなくなった時点でデータを破棄し、データ保有者に破棄されたことを通知すること。
- ２．公共部門機関、連合機関、政府機関に対する営業秘密、又は、いわゆる営業秘密の開示は、要請の目的を達成するために厳密に必要とされる範囲でのみ要求されるものとする。この場合、公共部門機関、連合機関、政府機関は、これらの営業秘密の秘密を保持するために適切な措置を講じるものとする。

■ *第20条　例外的な必要性がある場合の補償*

- １．第15条(a)に基づき、公共の緊急事態に対応するために利用可能とされたデータは、無償で提供されるものとする。
- ２．第15 条 (b) 又は (c) に基づき、利用可能とされたデータについて、その補償は、必要に応じて匿名化および技術的適応の費用を含む、要求に従うために生じた技術的および組織的費用を超えないものとし、これに妥当なマージンを加算するものとする。データを要求した公共部門機関、連合機関、政府機関の要求に応じて、データ保有者は、費用および妥当なマージンの計算の根拠に関する情報を提供するものとする。

出所)European Commission Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on harmonised rules on fair access to and use of data (Data Act) (https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=COM:2022:68:FIN)

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

ガバメントアクセス　EUデータ法案　第５章　条文

■ *第21条　例外的な必要性の下での研究機関や統計機関の貢献*

- １．公共部門機関、連合機関、政府機関は、本章に基づき受領したデータを、データが要求された目的に適合する科学的研究、分析を実施する観点、又は、公的統計の作成のために国家統計機関及びEurostatに提供する観点から、個人又は組織と共有する権利を有するものとする。
- ２．第１項に従ってデータを受領する個人又は組織は、非営利ベース又は欧州連合法若しくは欧州連合加盟国の法で認められた公益的な使命のもとで行動するものとする。また、営利事業が決定的な影響力を持つ組織や、研究結果への優先的なアクセスをもたらす可能性のある組織を含んではならない。
- ３．第1項の規定によりデータの提供を受ける個人又は組織は、第17条第3項及び第19条の規定を遵守するものとする。
- ４．公共部門機関、連合機関、政府機関が同条第1項の規定によりデータを送信し又は利用可能にする場合、当該データの受領元のデータ保有者に通知するものとする。

■ *第22条　相互扶助および国境を越えた協力*

- １．公共部門機関、連合機関、政府機関は、本章を一貫して実施するため、相互に協力・支援するものとする。
- ２．同条第1項に従って要求され提供された援助の文脈で交換されたいかなるデータも、要求された目的と相容れない方法で使用してはならない。
- ３．公共部門機関が他の加盟国に設立されたデータ保有者にデータを要求しようとする場合、当該機関はまず第31条に言及される当該加盟国の権限ある管轄当局にその意図を通知しなければならない。この要件は、連合機関、政府機関による要請にも適用されるものとする。
- ４．第3項に従って通知された後、関係する管轄当局は、データ保有者が要求に応じる際の事務的負担を軽減する目的で、データ保有者が設立されている加盟国の公共部門機関と協力する必要がある場合、要求元の公共部門機関にその旨を通知するものとする。要請する公的部門機関は、関連する管轄当局の助言を考慮しなければならない。

出所)European Commission Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on harmonised rules on fair access to and use of data (Data Act) (https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=COM:2022:68:FIN)

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

ガバメントアクセス　EUデータ法案　前文

(64)公共部門機関、連合機関、政府機関に対して利用可能とされるデータに、個人データを含めることが厳密な意味でに必要となる場合、個人データ保護に係る適用規則を遵守し、データの提供及び、その後の使用は、そのデータに関係する個人の権利と利益の為に、保護措置を伴う必要がある。データを要求する機関は、データ処理の厳密な意味での必要性及び、具体的かつ限定的な目的を提示しなければならない。データ保有者は、データを利用可能とする前に、データを匿名化(anonymize)するための合理的な努力をする、又は、匿名化が不可能であると判明した場合は、仮名加工や集計(pseudonymization and aggregation)等の技術的手段を適用する必要がある。

(67)公共的な緊急事態に対応する場合の様に、重要な公益の保護が危機に瀕している場合には、公共部門機関、連合機関、政府機関は、取得したデータについて企業に補償を求められるべきではない。公共的な緊急事態は稀な出来事であり、そのような緊急事態のすべてが企業の保有するデータの利用を必要とするわけではない。したがって、公共部門機関、連合機関、政府機関が本規則を利用することにより、データ保有者の事業活動に悪影響が及ぶ可能性は低い。しかし、公共的な緊急事態への対応以外の、公共緊急事態の予防又は復旧を含む例外的な必要性が、より頻繁に発生する可能性があるため、そのような場合、データ保有者は、要求に応じるために発生した技術的・組織的コスト及び、公共部門機関、連合機関、政府機関に対してデータを利用可能にするために必要な合理的マージンを超えない補償を受ける権利を有するべきである。この補償は、データそのものに対する支払いであると理解されるべきではなく、又は、強制的なものであってはならない。

出所)European Commission Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on harmonised rules on fair access to and use of data (Data Act) (https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=COM:2022:68:FIN)

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

ガバメントアクセス　EUデータ法案に対する報道情報

報道内容

■ Reuters　EU rules take aim at illegal data transfer to non-EU governments(2022/2/23)

- **(データ法の下で)企業は、洪水や山火事などの公共的な緊急事態の際に、特定のデータを政府に提供することが義務づけられることになる。**
- 2013年にスノーデン氏が米国の大規模な監視を暴露して以来、データ移転に係るEUの懸念は高まっている。
- 欧州司法裁判所は、何千の企業がクラウドインフラ、給与計算、財務情報等の様々なサービスに依存していたプライバシーシールド(データ転送協定)を非合法化することになっている。

■ Bloomberg　EU Unveils Rules to Force Firms to Share Product Usage Data(2022/2/23)

- データ法では、以下のような新しい規則が定められている。
  - 企業は、中小企業とのデータ共有を阻害するような不公正な契約は禁止される。
  - **企業は緊急時に公共部門がデータを利用できるようにしなければならない。**
  - 企業は、コネクテッドデバイスの利用者がそのデバイスで生成されたデータにアクセスできるようにしなければならない。
- また、EU域外の政府によるデータへのアクセスを阻止するための保護措置の導入を企業に求めている。

出所)　Reuters　EU rules take aim at illegal data transfer to non-EU governments
(https://www.reuters.com/technology/eu-rules-take-aim-illegal-data-transfer-non-eu-governments-2022-02-23/)
Bloomberg　EU Unveils Rules to Force Firms to Share Product Usage Data
(https://www.bloomberg.com/news/articles/2022-02-23/eu-unveils-rules-to-force-firms-to-hand-over-product-usage-data)

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

(4)AI関連制度・政策

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

フランスのAI関連制度・政策　(i) AI関連制度・政策の概要

■ 2018年3月エマニュエル・マクロン大統領は、自身のビジョンと５ヵ年国家AI戦略を公表した。フランスAI戦略は、「人間のためのAI(AI for humanity)」と題され、「AI政策報告書」に基づいて発展してきた。同報告書はフランス議会の議員が準備したもので、数学者であるセドリック・ヴィラニがこれを仕上げた。大統領が強調したように、フランスAI戦略の主たる目的は以下のものである。

- 世界レベルのAIの人材を育成し、確保し、誘致するためのAI教育及び訓練エコシステムを向上させること
- AIのアプリケーション及び資産のプーリングを共に実施するためのオープンデータ・ポリシーを構築すること
- AIアプリケーションの透明かつ公正な利用のための倫理的な枠組みを発展させること

■ この目的のため、フランス政府は2022年末までにAIの発展に15億ユーロを費やす予定である。うち7億ユーロは研究に充てられる。

■ 2021年ジャン・カステックス首相は新たな公開かつ共有されたデータ戦略を発表した。また、将来のための多年国民投資計画の第四世代の枠組みが2022年作成された。一つのプログラムがAIに設けられ、他にもいくつか国家AI戦略に関連する行動を含むと想定される。これによって国家AI戦略の資金調達の更新が可能となり、EUで更新される連携計画に対応した予算枠を確保することができる。

出所)European Commission “AI Watch - National strategies on Artificial Intelligence: A European perspective, 2021 edition”
(https://publications.jrc.ec.europa.eu/repository/bitstream/JRC122684/ai_watch_report_national_ai_strategies.pdf)よりNRI作成

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

フランスのAI関連制度・政策　(ii) 人的資源

■ 労働市場におけるAI、データサイエンス、ロボットに関するスキルギャップを減らすために、フランスのAI戦略は、高等教育及び研究機関に対し、職業訓練、中級及びエキスパートのデュアルプログラム、人材の確保と育成を行う財政的インセンティヴを与え続けることになる。

- 修士課程相当卒業者の数を2016年から二倍にし、新たな二倍目標を設定する。
- 職業訓練及びパートタイム社会人教育、夏期又は冬期スクール、エクゼクティブプログラムにおける様々な訓練コースが、2019年から2021年にかけて急激に上昇してきた。
- 「アルゴリズムチェーン」に関する全てのプレイヤー(設計者、専門家、市民)の育成教育は、市民一人ひとりが機械の内部構造及びAIの利点をより理解するためのデジタルリテラシーを向上させる。

■ AI技術の発展は求人市場に影響を与える。フランスのAI戦略は、将来の労働需要と技能需要をより理解することに特別の注意を払っている。プロフェッショナル転換に首尾よく備えるためである。以下の政策提言は、増大した労働市場インテリジェンスと将来の技能予測を対象としている。

- 自動化が職業に影響を与える態様に関する検討を奨励し、プロフェッショナル転換への支援を提供するための、ワークトランスフォーメーションの公的な研究所の設立

出所)European Commission “AI Watch - National strategies on Artificial Intelligence: A European perspective, 2021 edition”
(https://publications.jrc.ec.europa.eu/repository/bitstream/JRC122684/ai_watch_report_national_ai_strategies.pdf)よりNRI作成

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

フランスのAI関連制度・政策　(iii) 研究開発と社会実装

- 国家AI戦略の目標は、応用研究とイノベーションに依拠している。研究面を調整する責任を担うのはフランス国立情報学自動制御研究所(inria)である。同研究所は、フランスのAI部門全体を強化し、科学技術のスピンオフ又は移転を促進し、産業との協力計画を発展させるという明確な目的を有している。とりわけ、同研究所は戦略の実施を調整し、科学的及び技術的専門知識を提供し、とくにドイツとの間の二国間協力構想を発展させる。
- 大学内における学際的AI研究機関のネットワークはなんらかの専門化に依拠している。直接的には地域のアカデミック及び経済的なエコシステムに関連している。奨励計画は進展し、集団的R&D&I(研究・開発・イノベーション)計画におけるプライベートパートナーの投資1ユーロが、結果的に国家の財政を1ユーロ増加させることとなる。
- これまで国家AI戦略は、AI分野において180席の教授職と300のPhDを増やすことに役立った。他の非営利組織の多くはイノベーションに好都合なエコシステムの創設と戦略の実行に貢献している。
  - 16ある科学技術研究機関(IRT)又はエネルギー移転機関(ITE)のいくつかが、AIにおける主要な提携プロジェクトを支援する。IRTとITEの連携は、EngageAIと呼ばれる、機関横断型のAI計画を発展させた。
  - 53あるフランスの部門別「競争力の核(poles de compétitivité)」(イノベーションクラスター)もまた、産業にAIを普及させるという観点から、AIエコシステムの活性化に貢献している。
  - Teralab Instituteは、技術的資源と専門企業のエコシステム全体を提供し、データ開発及び実験と技術移転の促進を望む団体が直面する科学的技術的障壁を取り除いている。

出所)European Commission “AI Watch - National strategies on Artificial Intelligence: A European perspective, 2021 edition”
(https://publications.jrc.ec.europa.eu/repository/bitstream/JRC122684/ai_watch_report_national_ai_strategies.pdf)よりNRI作成

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

フランスのAI関連制度・政策　(iii) 研究開発と社会実装

■ 人間のためのAI戦略は、主要なAIトランスフォーメーションへの対応に十分な成熟性が見られる特定の部門―衛生、運送、環境、防衛及び安全保障―についての研究及びイノベーションを支援する政策を優先している。したがって、このためには部門特化型のデータプラットフォームなど部門特化型の政策が必要である。これらの多くはインフラストラクチャーに関連するが、フランス政府は、AI技術の設計及び配備を円滑に進めるためのテストエリアの設置を推奨している。

- 現実世界の条件下での実験を可能にするための実施テストエリア及びイノベーションサンドボックスは一時的に、規制負荷を低減させる。
- 経済的国家運営業者であるbpifrance(フランスの政府系投資銀行)もまた、毎年一般的資金調達を行い、全体としてデジタル移転をターゲットとするが、AIプロジェクトのシェアは安定して上昇しているスキームを重要視し、分類する。

出所)European Commission “AI Watch - National strategies on Artificial Intelligence: A European perspective, 2021 edition”
(https://publications.jrc.ec.europa.eu/repository/bitstream/JRC122684/ai_watch_report_national_ai_strategies.pdf)よりNRI作成

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

フランスのAI関連制度・政策　(iii) 研究開発と社会実装

■ 以下のイニシアティヴは、AIにおけるネットワークと協業を促進させると想定される。

- Inriaは「人工知能学際機関(Interdisciplinary Institute of Artificial Intelligence: 3IA)」の発展、及び他の結果重視型集団的支援メカニズムによって、AIに関するフランスの専門知識のネットワークを調整する。
- フランス、日本、ドイツの三ヶ国からなるAI研究プロジェクトは、AIに関する研究計画を初めて三ヶ国で提案した。この提案は、3年間、三ヶ国の研究チームによる集団的プロジェクトを支援し、フランス、ドイツ、日本からの研究パートナーを団結させることを意図している。
- 官民研究室、いわゆるLabComsを、集団的AI研究及びイノベーションを奨励するために促進させる。
- InriaとDFKIは、フランス・ドイツ間のAI戦略パートナーシップを創設するために了解覚書を結んだ。目的は、衛星、サイバーセキュリティ、ロボット及び産業分野における障壁を克服するための力を管理することである。
- AIグローバルパートナーシップ(Global Partnership on AI: GPAI)への参加。フランス・カナダ間で、人権、包摂(inclusion)、多様性、イノベーション及び経済成長を完全に尊重して、AIの合理的な発展及び利用を奨励する国際的なインセンティヴを創設するプロジェクトを始めるために宣言が表明された。

■ フランスにおけるAIの国際的な誘致を促進させるため、フランスの戦略は、研究者の労働条件及び給与を向上させることで、国外移住者及び外国の人材に向けたアピールを促進させる政策の必要性を訴えている。

出所)European Commission “AI Watch - National strategies on Artificial Intelligence: A European perspective, 2021 edition”
(https://publications.jrc.ec.europa.eu/repository/bitstream/JRC122684/ai_watch_report_national_ai_strategies.pdf)よりNRI作成

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

フランスのAI関連制度・政策　(iv) 規制

■ AI技術及びアルゴリズムの公正かつ透明な利用を確保するという倫理的問題は、フランスAI戦略の中心である。これに関して、セドリック・ヴィラニはAI政策報告書において、「透明なかたちで行われる公的な議論の先導に責任を負い、法律によって組織され規律されるデジタル技術及びAI倫理委員会」の創設を提案したが、これが実際に2020年初頭の「パイロット国家デジタル倫理委員会(Pilot National Digital Ethics Committee: CNPEN)」設立へと至った。このパイロット段階には、AI倫理の約３分野の仕事が割り当てられているが、今後段階的に拡大されていく予定である。

出所)European Commission “AI Watch - National strategies on Artificial Intelligence: A European perspective, 2021 edition”
(https://publications.jrc.ec.europa.eu/repository/bitstream/JRC122684/ai_watch_report_national_ai_strategies.pdf)よりNRI作成

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

フランスのAI関連制度・政策　(v) インフラ

■ フランスの戦略は、以下のデータ政策構想を強調している。

- AI特化型高性能コンピューターインフラストラクチャーJean ZAY：2020年初頭に始動し、現在28ペタフロップスの処理能力を発揮している(始動以来X2)。
- CASDセキュアデータハブ：公益団体が国家代表機関を連携させ、R&Dプロジェクトのために機密性の高いものを保護されたデータにおいて安全に交換する。
- 民間部門におけるデータシェアリング：フランス政府は、スポンサーが、スタートアップや他のイノベーターと協力して、AIを通じたデータ・バロリゼーション及び問題解決に取り組むことができるよう、多くのAIチャレンジに資金を提供してきた(2020年第3期)。また政府は、いくつかのデータハブプロジェクトにも、完全に欧州データ空間と統合できる部門別データ空間(とりわけ農業、栄養、物流、衛生、スポーツ)の設置と発展を促進するため、資金提供を行ってきた。
- AI時代に適合したデータコモンズの創設の奨励：ここでいうデータコモンズは、オープンデータセット、更にリアルタイムなオープンデータの提供を含む。
- データポータビリティの向上：データポータビリティの権利は支援されるべきで、つまり、データ履歴を損なうことなくあるサービスエコシステムから他への移動が可能になるべきである。

■ 機械学習及びAIアルゴリズムの発展を奨励するためのデジタル及び電気通信インフラストラクチャーに関しては、フランスの戦略は「GAIA-Xプロジェクト」を強く支援し、それに参加している。同プロジェクトはドイツとフランスによって、イノベーションを促進しながらも、デジタル主権(digital sovereignty)に関する高い基準に合致する、安全で一体化したデータシステムを創設するために開始された。

出所)European Commission “AI Watch - National strategies on Artificial Intelligence: A European perspective, 2021 edition”
(https://publications.jrc.ec.europa.eu/repository/bitstream/JRC122684/ai_watch_report_national_ai_strategies.pdf)よりNRI作成

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

フランスのAI関連制度・政策　(vi) 社会課題の解決：気候及び環境

- セドリック・ヴィラニが起草したAI政策報告書には、「よりエコロジカルな経済の実現に役立つAIの利用」と題された章があり、以下の提言を行っている。
  - グリーンなAIの促進：この領域において公的機関は、よりグリーンなバリューチェーンと欧州クラウド産業の経済的移転を支援することが求められる
  - エコロジカルデータの普及の促進：オープンエコロジカルデータ(天気、農業、運輸、エネルギー、バイオダイバーシティー、気候、ごみ、土地登記、エネルギーパフォーマンス評価などに関するデータ)は、グリーンなAI技術が経済的な移転を発展させ促進する際に重要なポイントとなる
- 2019年に公表された、フランスにおけるAIの将来に関する別のAI政策報告書は、類似の警鐘を鳴らしている。同報告書は、エネルギー部門及び環境の利益になるようなAIの利用という国家目標を強調する必要性を説いている。とりわけ、(スマートメーター及びスマート家電に基づいた)スマートグリッドの利用を通じた、インテリジェントなエネルギーネットワークの発展が必要だとした。また、高水準のデジタル化及び遠隔制御介入を用いた監督制御及びデータ取得(supervisory control and data acquisition: SCDA)の新たな創設も求められた。最先端のインフラストラクチャーは、エネルギー消費、ネットワークにおける高クオリティサービス、よりよいエネルギー保管能力の最適化のために、AIアプリケーションの発展を強化できる。
- 環境についてはAIの利用が、天然資源の使用減少、環境リスクの予想、再生可能エネルギー支援の効率と統合化の向上においてAIの利用が有用である。
- Inriaリール-北欧州の、最適化及びAI研究者らは、Pref-AIという、欧州ホライズン2020の枠組みにおいて実行された研究プロジェクトを成功裏に完成させた。同プロジェクトは航空科学部門からのスタートアップと共同で実施され、フライトデータ分析に基づいており、フライトプランの最適化を可能にするデジタル航空モデルの発展を導いた。すなわち、Pref-AIは民間航空におけるエネルギー消費削減に対する解決策を提供したのである。

出所)European Commission “AI Watch - National strategies on Artificial Intelligence: A European perspective, 2021 edition”
(https://publications.jrc.ec.europa.eu/repository/bitstream/JRC122684/ai_watch_report_national_ai_strategies.pdf)よりNRI作成

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

フランスのAI関連制度・政策　(vi) 社会課題の解決：COVID-19パンデミック

■ COVID-19パンデミックに対するAI関連政策については、以下の構想が準備中である。

- GPAIの枠組みにおいて、AI及びパンデミック対策(AI and pandemic response: AIPR)作業部会が、この分野における部門及び国境横断型の共同を促進するために設置された。2020年11月同作業部会は報告書を公表し、そのマンデートを概括し、AIが可能にするCOVID-19 及び将来のパンデミックに対応する解決策の責任ある発展と利用を促進し支援する勧告を行った。
- 連帯・保健省(Ministère des Solidarités et de la Santé)と高等教育・研究・イノベーション省(Ministère de l'Enseignement supérieur, de la Recherche et de l'Innovation)は、COVID-19 と闘うため、20の研究プロジェクトを支援している。そのうちの一つは、COVID-19 の複製プロセスを再構成し、そのモデルを構築し、最終的には適切な阻害剤を実験するのにAIを利用している。

■ さらに、COVID-19パンデミックとの戦いにおいて、フランス国立保健医学研究所(French National Institute of Health and Medical Research: INSERM)とパリ大学の研究者らが、インテリジェントデジタルアシスタントで運営する国営電話回線を創設した。このサービスはAlloCOVIDと名付けられ、同時に千人以上に対応できるAIに基づいたバーチャル電話アシスタントによって運用される。さらに、フランス当局は新しいAIツールをパリの地下鉄における防犯カメラにも搭載した。それによって他の公共交通手段が拡大した。フランスのスタートアップDatakaLabは、当局がCOVID-19 の今後の発生を予想するのに役立つ匿名のデータを作成するソフトウェアを開発した。

出所)European Commission "AI Watch - National strategies on Artificial Intelligence: A European perspective, 2021 edition"
(https://publications.jrc.ec.europa.eu/repository/bitstream/JRC122684/ai_watch_report_national_ai_strategies.pdf)よりNRI作成

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

フランスのAI関連制度・政策　(vii) モニタリングと今後のアップデート

- Inriaは、国家AI戦略のコーディネーターとしての重要な役割を果たしてきた。その実施、とりわけ研究及びイノベーションに責任を負っていた。
- 3年間で8億ユーロの予算が充てられたAI国家戦略は、第一段階が2018年に始まった。同戦略は、研究の促進を強く強調し、学際機関3IAの創設、180のPhDのための追加の資金調達、ペタスケールスーパーコンピューティング施設の開業を行った。
- 同戦略の第二段階(2021-2022)は、AIによるデジタル及びエコロジカル企業移転を加速させながら、国家の産業基盤を強化するため、教育及び訓練、組込みAI、クリティカルシステムにおいて信頼できるAIの質の向上に主たる優先を置いた。

出所)European Commission “AI Watch - National strategies on Artificial Intelligence: A European perspective, 2021 edition” (https://publications.jrc.ec.europa.eu/repository/bitstream/JRC122684/ai_watch_report_national_ai_strategies.pdf)よりNRI作成

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

ドイツのAI関連制度・政策　(i) AI関連制度・政策の概要

- 2018年11月、ドイツ連邦政府は「国家AI戦略(National AI strategy)」を始動した。同戦略はドイツにおけるAIの進歩を示し、将来達成すべき目標とその実現のための政策行動の具体的な計画を明らかにしている。様々な政策構想が概説されているが、それらは以下の目標達成を目指している。
  - ドイツ及び欧州を、AIを先導する中心地とすることで、ドイツにおける将来の競争力を上昇させ、強化させること。
  - 社会のためのAIの、信頼できる発展と配備を確保すること
  - 倫理、法、文化、制度的な意味で、広い社会対話及び積極的政治措置の文脈にAIを統合すること

- ドイツ連邦政府は、2019年11月、1年後に実施するドイツAI戦略の主たる措置を提案する暫定報告書を公表した。同報告書は戦略実施、行動領域、今後の見込みに関する事実と数字を表した。
- 2019年10月、ドイツデータ倫理委員会は、倫理ガイドラインとAI、アルゴリズムに基づく意思決定及びデータの利用に関する特別の勧告を公表した。
- 2020年10月、ドイツ連邦議会第19会期「AI-社会責任及び経済、社会、生態学的ポテンシャルに関する研究委員会(Study Commission on Artificial Intelligence – Social Responsibility and Economic, Social and Ecological Potential)」が最終報告書と行動のための特別勧告を公表した。
- 2020年12月、ドイツ連邦政府は「新AI戦略(Updated AI strategy)」を採択した。暫定的な均衡を作成し、国内、欧州、国際レベルでの関連する発展を示し、2022年までに実施する具体的な措置を設定した。これは、研究、知識や専門知識、移転と応用、基本的枠組み、社会という行動領域に焦点を当てている。更に、とりわけ持続可能性、環境/気候保護、パンデミック制御、国際/欧州協力にも注目している。
- 景気刺激と将来のパッケージを用いて、ドイツ連邦政府はAIの促進のために計画していた30億ユーロの支出を、20億ユーロ増額し、これによって2025年までに総額50億ユーロつぎ込まれることとなった。

出所)European Commission “AI Watch - National strategies on Artificial Intelligence: A European perspective, 2021 edition”
(https://publications.jrc.ec.europa.eu/repository/bitstream/JRC122684/ai_watch_report_national_ai_strategies.pdf)よりNRI作成

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

ドイツのAI関連制度・政策　(ii) 人的資源

- ドイツの戦略は、正式な訓練及び教育のための政策改革やイニシアティヴをいくつか提案している。AI教育の高水準を保つために、特に教育者、訓練者、一般公衆の構造に着目している。
  - 講座、ビデオ、ポッドキャスト、知識交換を通じた、AIのしっかりとした知識基盤発展のため、学習プラットフォームを拡大すること。
  - 高等教育システムにおいてAIが強固な足場を確保するためにAI領域における教授職を最低100増加させること。
  - STEM教科に関わる学生を獲得すること。
- 形式的な教育及び訓練改革の頂点に、ドイツ連邦政府は、全労働力におけるAI関連技能の拡大及び向上のための広範囲にわたる方策を提案した。個人に求められる技能はAI技術によって大きく変わるため、ドイツ連邦政府は、生涯学習や、キャリア全体を横断する従業員の再教育及び技能アップへ注目し、大規模な資格イニシアティヴをいくつか開始した。
  - デジタルおよびAI関連の応用職業訓練を促進するための国家技能戦略を策定。
  - 革新的でユーザー志向で、一貫したデジタル社会人教育と訓練のためのINVITE(Digital Platform for Continuing Vocational Training)イノベーション競争計画の着手。
  - AI労働環境における労働力を研究し構築し、必要な技能をマネジメントや全労働者へ提供する、地域的な労働研究拠点の設置。
  - AI教育プログラムの拡大。
- 他の政策手段は、今後の技能需要を特定し、労働需要のデジタル及び人口統計的変化に柔軟に対応することを目的としている。したがって以下の構想は労働者と企業双方のニーズを満たし架橋することを目指している。
  - 熟練労働者戦略の策定：将来必要とされる技能を特定する技能管理システム。
  - 変化を起こすため、適合した情報及びイノベーション学習アプローチをもって企業と従業員に対応する、将来的地域ハブの形成
- ドイツ連邦政府はまた、文化およびメディア部門におけるAIの可能性とインパクトに注意を払っている。

出所)European Commission “AI Watch - National strategies on Artificial Intelligence: A European perspective, 2021 edition” (https://publications.jrc.ec.europa.eu/repository/bitstream/JRC122684/ai_watch_report_national_ai_strategies.pdf)よりNRI作成

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

ドイツのAI関連制度・政策　(iii) 研究開発と社会実装

■ AI領域における研究を促進するための資金提供及び支援は以下の通りである。

- AI研究のためのコンピテンス・センターの創設：AIに関する国内研究ネットワークへと拡大、発展させるため、当局は2022年までに同センターへの資金提供を二倍に増やした。
- 国家安全におけるAIリアリティ・ラボの始動：同ラボは、安保研究共同体、AI研究者、産業に接点を提供する。また、AIの研究及び発展を実務家の需要と結び付ける。同研究所の目的は、AIに基づく科学技術を実務家がアクセス・利用できるようにする策を実験し、発展させることである。他の主要なタスクとして、データ収集構想の発展がある。
- グランダープラットフォーム：スタートアップを初期研究から具体的なAIアプリ研究まで支援するオンラインのプラットフォームである。
- 産業集団的研究計画：基礎研究と産業での応用との間のギャップをなくすため、集団的なAIプロジェクトに関するビジネスと科学研究の結合を促進する。
- ベンチャーデッドなどを用いたAIスタートアップの成長を促進させるための顧問業及び資金調達業：ヒューマン・マシン・インタラクションの一流研究における会社創業を促進させる政策もここに含まれる。

■ イノベーション及び実験に対する支援には以下のものがある。

- AIに注力した画期的イノベーションのための機関に対する資金提供
- デジタル化への革新的解決を促進するため共同イノベーション空間の発展
- 「SMEのための中心イノベーションプログラム(ZIM: Zentrales Innovationsprogramm Mittelstand)」の強化：個人及び集団的R&Dプロジェクトをターゲットとした SMEへの資金提供計画
- いわゆる移転イニシアティヴ、デジタルテストベッド、レギュラトリー・サンドボックスの着手、AIに関するパイロットプロジェクト及びフラグシッププロジェクトの促進によって、AIイノベーションの過程を加速化

出所)European Commission “AI Watch - National strategies on Artificial Intelligence: A European perspective, 2021 edition”
(https://publications.jrc.ec.europa.eu/repository/bitstream/JRC122684/ai_watch_report_national_ai_strategies.pdf)よりNRI作成

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

ドイツのAI関連制度・政策　(iii) 研究開発と社会実装

■ また、特定の部門及び地理的区域においてAI政策に熱心なエリアを特定し、そこでの研究及びイノベーション支援プログラムがある。2020年版更新AI戦略は、ヘルスケア、環境及び気候、航空科学、モビリティに注目している。こうした政策の例は以下と、(vi)社会課題の解決を参照。

- ヘルスケアシステムにおける患者中心ケア向上のためのデジタルイノベーション
- 農業、健康栄養、食物連鎖、農村地域におけるAI技術研究
- デジタルモビリティのためのリアルワールド・テストフィールド：ドイツ連邦政府は、古典的な交通計画の要素をモビリティ及びイノベーションマネジメントと結び付ける大規模な研究計画に資金を供給し、ここでAIを使用している。
- データ空間モビリティ・ドイツ：2021年末までに包括的な「データ空間モビリティ・ドイツ」を共に作るため、ステークホルダーダイアログが現在実施されている。とりわけ、ドイツにおける自動運転の発展を促進するために、信頼できるAIアルゴリズムの研究、発展、検証、認定を行う様々な競争者が利用可能なモビリティデータ(リアル及び合成訓練及び実験データ)を、入手可能とすることを目的としている。

出所)European Commission “AI Watch - National strategies on Artificial Intelligence: A European perspective, 2021 edition”
(https://publications.jrc.ec.europa.eu/repository/bitstream/JRC122684/ai_watch_report_national_ai_strategies.pdf)よりNRI作成

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

ドイツのAI関連制度・政策　(iii) 研究開発と社会実装

■ ドイツの戦略は、ビジネス共同体、アカデミア、公共研究センターを越えたネットワーク及び協業を促進させるための政策を様々提言している。ネットワーキングの目的は、学際的な最先端研究とイノベーションプロジェクトを奨励することと、知識の拡散及び移転を促進することによる相乗効果や多様性を完全に開発することにある。

■ 協業を奨励する支援政策には次のものがある。

- 仏独R&Dネットワーク(「バーチャルセンター」)：特定の産業における二国間のAIクラスターを伴う、二国間の資金調達及び訓練計画。
- 科学、ビジネス共同体、市民社会及び政府間の対話とネットワーキングを行うため「Platform Lernendeシステム」をAIのプラットフォームに拡大する。ネットワーキングを促進させ、ドイツAI研究の国際的な認知を高めるため、ドイツ連邦政府はAIマップに着手。このマップによって、AIに関する革新的なアプリケーションやプロジェクトが発見され、AIについて研究しているあらゆる研究機関を特定し情報を集めることができる。
- プラットフォーム・インダストリー4.0：デジタルエコシステムを形作る全体論的アプローチを備えたプラットフォームである。デジタル経済におけるイノベーションや協業を支援し促進することを目的としており、現在AI科学技術に特に注目している。
- ネクストジェネレーション・クラスターの発展：最先端研究から得られた、重大で開発可能な成果を商品やサービスに移転することを目的としている。
- ドイツにおけるデジタルハブ構想と将来的ハブ構想の更なる発展：とりわけAI、サイバーセキュリティ、その他AI関連の領域におけるそれである。
- 「シビックコーディング―公共財のためのイノベーションネットワークAI」の設立：より大きな社会全体の善の為のAIを促進することを目的としたイノベーションエコシステムを発展させる。ノウハウ、AIプロジェクトへの財政的支援、スタートアップ、NGO、科学者、政府機関を結合させるマッチングプラットフォーム、非営利組織及び市民社会のための集団的データ交換インフラストラクチャーの提供を目的としている。ドイツ連邦政府は、持続可能で広範囲アクセスが可能なITインフラストラクチャーとツールを発展させることに注力する「緑のためのシビックテックラボ(Civic Tech Labs for Green)」を設立する予定である。また、それによって市民社会の中でのデータ交換を促進させる。「シビックイノベーションプラットフォーム」は、公共財のためのAI技術の利用に関するアイディアの市場を提供し、資金調達機会へのアクセスを促進させる。

出所)European Commission “AI Watch - National strategies on Artificial Intelligence: A European perspective, 2021 edition” (https://publications.jrc.ec.europa.eu/repository/bitstream/JRC122684/ai_watch_report_national_ai_strategies.pdf)よりNRI作成

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

ドイツのAI関連制度・政策　(iii) 研究開発と社会実装

■ AIにおける国際協力については次のものがある。

- ドイツ連邦政府は、AIの更なる発展及び利用が、持続可能な開発目標(SDGs)に合致することを確保するため動いている。発展途上国及び新興国との間の国際的なネットワーキングや協業は、全ての人のAI技術利用参加を可能にすること、持続可能な経済、生態学、社会的発展のためにAIアプリケーションを発展させることに重要な役割を果たしている。
- ドイツ連邦政府は、AI領域におけるネットワーキング及び協業のための国際的及び多国間構造の構築を支援している。ドイツは、AIグローバルパートナーシップ(GPAI)の創設メンバーの一つである。GPAIは、産業からの専門家、市民社会、政府、学問の世界を共にさせる。
- ドイツ連邦政府はまた、現在進行中のAIに関するOECDの作業にも貢献している。AIはデジタルトランスフォーメーションにおけるOECDでの作業の重要な分野である。2019年5月、OECDは政府間で合意した初のAIに関する国際基準である、AI原則を採択した。ドイツ連邦政府は、OECDの、仕事、イノベーション、生産性、技能に係るAIプログラムを支持している。

■ 国際的誘致を高めるための努力として、ドイツ連邦政府は、最も聡明な才能を引き込み、確保し、誘致するために労働条件と俸給を向上させようとしている。また、ドイツの戦略は、熟練労働者の移住手続を円滑にする法改正を提案している。

- Alexander von Humboldtプロフェッサーシップ：500万ユーロに相当する同プロフェッサーシップはドイツにおいて最も才能ある研究賞で、このためにトップレベルの国際研究者たちはドイツ大学に集う。2020年から2024年にかけてAI分野における賞が更に送られ得る。
- 若手女性AI研究者への支援：ドイツのAI研究への助成の参加を増やすため、主要な学際研究グループにおいて女性は促進される

出所)European Commission “AI Watch - National strategies on Artificial Intelligence: A European perspective, 2021 edition”
(https://publications.jrc.ec.europa.eu/repository/bitstream/JRC122684/ai_watch_report_national_ai_strategies.pdf)よりNRI作成

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

ドイツのAI関連制度・政策　(iii) 研究開発と社会実装

■ 現在のAIの進歩や理解を監視するため、及びデジタル化及びAIについての全国的な情報を普及させるためのイニシアティヴとして次のものがある。

- 社会及び将来の仕事におけるAIの理解とインパクトを監視するため、「仕事と社会におけるAI観測所(Observatory for Artificial Intelligence in Work and Society: AI Observatory)」が強化される。
- 経済、高等教育及び教授、仕事と社会におけるAIの利用についてのインディケーターを蓄積することでAIの全体像を監視する。
- AIなどのデジタル科学技術分野で情報及び政策キャンペーンを計画し、学際的な社会的科学技術デザインを促進するために「デジタルワーク及び社会の将来基金(Digital Work and Society Future Fund)」を設立する。

出所)European Commission “AI Watch - National strategies on Artificial Intelligence: A European perspective, 2021 edition”
(https://publications.jrc.ec.europa.eu/repository/bitstream/JRC122684/ai_watch_report_national_ai_strategies.pdf)よりNRI作成

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

ドイツのAI関連制度・政策　(iv) 規制

- AI研究委員会(Study Commission on Artificial Intelligence)はその最終報告書で行動勧告を行った。とりわけ同委員会はAIについて部門特化型規制枠組みを要求する一方で、均衡性と責任原則の確保を説いた。
- この勧告に沿って、ドイツ連邦政府は、とりわけ情報マネジメント、データオーナーシップ、自由なデータ流通、標準化に関連する問題に取り組む政策を開始した。法改正は多くの領域に及んだ。
- 以下はAIのための立法枠組みに向けた最初のステップである。
  - 競争法4.0に基づく委員会が、競争法及び著作権法をいかにしてこれから発展させるかについての議論のための政治的プラットフォームとして始動した。2019年同委員会は「デジタル経済のための新しい競争枠組み」に関する報告書を公表した。2020年9月9日に採択された「競争及びデジタル化法」は委員会の勧告のいくつかを扱い、これを実施している。
  - 連邦データ保護法はデータ保護規制、プライバシー、EU法との適合性を規定した。
  - 非個人データ及び著作権の使用に関する法のレビューを行い、必要に応じて改正した。
  - サイバーセキュリティ指令を実施した。この指令は「ネットワーク及び情報システムの安全(NIS)」に関する指令として知られている。締約国は国家サイバーセキュリティ戦略を採択しなければならず、ドイツにおいては2017年6月にNIS実施法によって実施されている。

出所)European Commission “AI Watch - National strategies on Artificial Intelligence: A European perspective, 2021 edition”
(https://publications.jrc.ec.europa.eu/repository/bitstream/JRC122684/ai_watch_report_national_ai_strategies.pdf)よりNRI作成

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

ドイツのAI関連制度・政策　(iv) 規制

■ ドイツ連邦政府は、AIベースのアプリケーションのあらゆる開発段階と利用を通じた「設計による倫理(ethics by design)」アプローチの活用を提言した。AIに関する共同ガイドラインと倫理基準の合意を形成するための対話を勧告した。したがってドイツの戦略は、欧州ガイドラインに合致した法及び倫理的枠組みへの取組を想定し、適切な場合は国家データ倫理委員会の勧告を考慮に入れる。ドイツにおけるAIの倫理ガイドラインの規定に取り組む政策として次のものがある。

- AIシステム発展及び利用のためのガイドライン：データ倫理委員会(DEC)は2019年10月に、データ及びアルゴリズムシステムの倫理的設計と利用に関する勧告を表明した。
- AIシステムの透明性、検証可能性、予測可能性を確保するための倫理的要件

■ 標準化についてドイツ連邦政府は、次のものを提案している。

- AIに関するドイツ標準化ロードマップ
- EU全域における協業を奨励することを目的とした、データ標準及びフォーマットの発展のための財政的支援
- SME及びスタートアップの国際標準化プロセスへの参加を支援するための、SME及びスタートアップからの専門家への財政的支援

出所)European Commission “AI Watch - National strategies on Artificial Intelligence: A European perspective, 2021 edition”
(https://publications.jrc.ec.europa.eu/repository/bitstream/JRC122684/ai_watch_report_national_ai_strategies.pdf)よりNRI作成

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

ドイツのAI関連制度・政策　(v) インフラ

■ インフラストラクチャーについては、最先端のAIアプリケーションの発展に最適な条件を備えるために、現在のデータインフラストラクチャーを拡大することが想定されている。データインフラストラクチャー投資は、AI研究を強化し、より柔軟なデータ相互運用性のための交換を奨励するために、信頼あるデータ及び分析環境を整えることを目的としている。さらに、ドイツAI戦略は現在の電気通信及びデジタルインフラストラクチャーを発展させて、ネットワークの接続性をよりよくし、サイバーセキュリティを向上させることを目指している。さらに、ドイツ連邦政府は、教育システムにおけるデジタルインフラストラクチャーを改善することで、AIの学習能力と実験を促進させるための資金提供を計画している。

■ とりわけ、ドイツの戦略はAIインフラストラクチャーの向上のために次のイニシアティヴを想定している。

- 政府のデータへのオープンアクセスを提供すること、地球観測データへのアクセスのためのインフラストラクチャーを改善することによって、データ共有設備を向上させる。
- クラウドプラットフォームとアップグレード版の記憶容量とコンピューター能力に基づく信頼あるデータ及び分析インフラストラクチャーを構築する。
- 研究者共同体へ科学主導型のデータサービスを提供すべく、国家研究データインフラストラクチャー(NFDI)を設置する。
- 情報セキュリティ及び情報のパフォーマンス、並びにコミュニケーションシステムを向上させる。とりわけ攻撃を受けた場合のAIシステムのレジリエンスに注目する。
- 学校におけるデジタルインフラストラクチャーを向上させるために、学校のためのデジタル協定プログラムからの資金提供を行う。
- 「学習型工場4.0」政策を拡大する。同政策により職業用の工場が設置され、学生たちがAI学習のためにそれを自由に使用できる。
- PLAINを導入する。政府のビックデータとAIアプリケーションの見取り図としてのプラットフォーム分析と情報システムである。

出所)European Commission “AI Watch - National strategies on Artificial Intelligence: A European perspective, 2021 edition”
(https://publications.jrc.ec.europa.eu/repository/bitstream/JRC122684/ai_watch_report_national_ai_strategies.pdf)よりNRI作成

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

ドイツのAI関連制度・政策　(v) インフラ

■ 次世代データインフラストラクチャーのための準備における重要な政策は、GAIA-Xプロジェクトと連邦政府データ戦略である。GAIA-Xプロジェクトはドイツとフランスが始めたもので、イノベーションを促進させながらも、デジタル主権の高い水準にかなう安全で統合されたデータシステムを創設することを目的としている。連邦政府のデータ戦略は、４つの具体的な行動領域を特定している。すなわち、データの供給及びアクセスの向上、信頼あるデータ利用の促進、社会におけるデータコンピテンスの上昇、データシェアリングとデータ利用といったデータ文化の発展である。

■ AIアプリケーションの発展を促すデータインフラストラクチャーを整備するための支援計画には次のようなものがある。

- mCloud：モビリティ、地理、天候に関するデータへの自由なアクセスを供給するオープンデータプラットフォームである。行政、研究、ビジネスからの利用者を第一のターゲットとしている。
- モビリティ・データ・マーケットプレイス(Mobility Data Marketplace: MDM)：モビリティに関するデータの供給者と利用者に、渋滞関連のオンラインデータを共有、調査、購読するB2Bプラットフォームを提供する。データ供給者から提供されたデータを変更せずにクライアントへ届ける。
- スマートデータイノベーションラボ(Smart Data Innovation Lab: SDIL)：研究者に幅広いビックデータとインメモリ技術への特別なアクセスを提供する。産業と科学が密接に連携して、ビックデータで価値を見出し、そこからスマートデータを生み出す。産業4.0、エネルギー、スマートシティ、個別化医療といった戦略的研究領域に焦点を置いている。
- ドイツ連邦医薬品医療機器研究所のリサーチデータセンター(Research Data Centre: FDZ)：研究者や衛生政策立案者に、ドイツの全ての法定被保険者のレセプトデータへのアクセスを提供する。

■ ICTインフラストラクチャーと高性能コンピューティングについてドイツ連邦政府は、AIアプリケーションや大容量データ分析の需要が将来ピークになることを特に考慮して、州政府と共同のうえ、国立スーパーコンピューティングセンター(National Supercomputing Centre: NHR)の発展に加え、ガウス・スーパーコンピューティングセンター(Gauss Centre for Supercomputing: GCS)をエクサスケールまで拡大することを促進する。エネルギー効率、資源効率、産業利用可能性に特に注意が払われる。

出所)European Commission “AI Watch - National strategies on Artificial Intelligence: A European perspective, 2021 edition”
(https://publications.jrc.ec.europa.eu/repository/bitstream/JRC122684/ai_watch_report_national_ai_strategies.pdf)よりNRI作成

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

ドイツのAI関連制度・政策　(vi) 社会課題の解決：気候及び環境

■ 国家AI戦略は明確に、人と環境への利益をもたらし、環境や気候に利益あるAIアプリケーションへ資金提供しようとしている。そのため、ドイツ連邦政府は気候変動への取組におけるAIの役割を促進させる様々な支援計画や行動計画をうちたてている。

- 環境、気候、自然、資源のためのAIの灯台：2019年8月ドイツ連邦政府は資金提供計画(4千万ユーロ)を発表した。AIを使って環境変動を解決し、環境保護と気候保護にAIを戦略的に利用する機会を促進させるソリューションへ資金を提供する。デジタル生態学的領域において活動しているアプリケーション志向の研究計画をターゲットにしている。3年間で最大300万ユーロの資金提供が行われ得る。
- 遠隔感知： 国家AI戦略は、各観測データへのアクセス可能性を向上させるために高性能インフラストラクチャーを提供する必要性を強調している。そのために連邦政府は、AIを用いた遠隔感知データの分析及び評価への資金提供を行っている。遠隔感知は、遠方の活動のモニタリングを可能にしてくれる。
- モビリティにおけるデジタル化及びAIのための行動計画：ドイツ連邦政府は「モビリティにおけるデジタル化とAI」という行動計画を策定した。これは、モビリティにおけるデジタルイノベーションとAIの高い効率を実現する将来性を開発することで「モビリティ4.0」を実効的かつ持続可能にすることを目的としている。とりわけドイツ連邦政府は、モビリティの新しい形態、自動運転やコネクテッド・ドライブへのAIイノベーション、そしてデータに基づく資金提供計画mFUNDを通じたAIイノベーションを促進している。ドイツ連邦政府はまた、ドイツモビリティAIセンター(AI centres for mobility)を設立し、全ての参加者のための最適なネットワークの提供、モビリティ部門におけるAIアプリケーションの促進、研究者から実務への急速な移転の促進、そしてそれによってこの領域における競争力の強化をさせようとしている。

出所)European Commission “AI Watch - National strategies on Artificial Intelligence: A European perspective, 2021 edition” (https://publications.jrc.ec.europa.eu/repository/bitstream/JRC122684/ai_watch_report_national_ai_strategies.pdf)よりNRI作成

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

ドイツのAI関連制度・政策　(vi) 社会課題の解決：COVID-19パンデミック

■ ドイツ連邦政府は、COVID-19パンデミックと闘う際、健康な社会環境を創設する際の、AIの役割を向上させるための幅広い政策に現在資金提供している。

- HiGHmedユースケース感染制御：HiGHmedコンソーシアムの感染制御ユースケースは、潜在的に危険な細菌を可能な限り早く発見するために、病院からの様々なデータソースを分析するソフトウェアシステムを発展させている。自動化され早期に警告を発するシステムであり、新たな感染症から患者を守っているだけでなく、その発生と拡大の理解にも役立っている。SARS-COV-2ウィルスパンデミックを感知するのに適している。ドイツ連邦政府は「医療情報イニシアティヴ」の一部として、HiGHmedコンソーシアムに資金提供を行っており、現在2018-2022の発展とネットワーキング段階で約4100万ユーロ提供している。
- ドイツ関税行政におけるチャボット/ボイスボット：ドイツ関税行政は、情報発信の領域においてAIモジュールの搭載を計画している。これにより企業や私人から様々寄せられる質問に答えようとしている。中央情報局からのホットラインによって受けた電話に自動で答えるボイスチャットを活用することと、関税行政のインターネット上のプレゼンスにチャボットを利用することを計画している。このプロジェクトはドイツ関税のデジタルインフラストラクチャーの向上全般に重要な貢献となるが、不必要な人との接触を避けることにも役立ち、現在続いているパンデミックにおいて必要なソーシャルディスタンスを維持するのにも役立つ。2020年6月に開始し、技術的な構想は2020年12月に完了した。最終的なシステム導入は2021年6月に予想される。
- AIグローバルパートナーシップ(GPAI)への参加：GPAIの枠組みの中で、AIとパンデミック対策(AIPR)に関する作業部会は、この分野での部門横断型、国境横断型の協業を促進するために設置された。2020年11月、同作業部会は、その任務を概括した報告書を公表した。そこで、COVID-19と将来のパンデミックに対応するAIによるソリューションの信頼ある発展と利用を促進し支援するための勧告を行った。
- AI利用イメージに関する集団的プロジェクト：ドイツのいくつかの病院もまた、COVID-19・AIイメージに関する集団的プロジェクトに参加している。AIを用いることでCOVID-19の診察におけるコンピューター断層撮影法(CT)を強化することを目的としている。これによってCTスキャンでのCOVID-19の自動感知と自動分類のため、肺病変の数量化による患者の重病度の評価のためのディープラーニングモデルが開発される予定である。
- AIや衛星を含むEUプロジェクトへの参加：ドイツはEXSCALATE4COVというEUのプロジェクトに参加している。EXSCALATE4COVは、コンピューター支援医薬品設計(Computer-Aided Drug Design)の正確さと予測可能性を高めながら、スマート・インシリコ医薬品設計(smart in-silico drug design)を促進させる、最も強力なコンピューティングリソースを開発している。ヨーロッパ中の製薬会社や生物学、生命分子動態に関する主要な機関もこれに参加している。

出所)European Commission “AI Watch - National strategies on Artificial Intelligence: A European perspective, 2021 edition” (https://publications.jrc.ec.europa.eu/repository/bitstream/JRC122684/ai_watch_report_national_ai_strategies.pdf)よりNRI作成

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

ドイツのAI関連制度・政策　(vii) モニタリングと今後のアップデート

■ ドイツ連邦政府は、現在の政策行動及び将来の実施のための具体的なステップの再検討を含む、国家AI戦略の定期的なアップデートを行っている。

出所)European Commission “AI Watch - National strategies on Artificial Intelligence: A European perspective, 2021 edition”
(https://publications.jrc.ec.europa.eu/repository/bitstream/JRC122684/ai_watch_report_national_ai_strategies.pdf)よりNRI作成

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

チェコのAI関連制度・政策　(i) AI関連制度・政策の概要

■ 2019年5月、チェコ共和国は「国家AI戦略(National AI strategy)」を発表した。同戦略は、「改革戦略2019-2030(Innovation strategy 2019-2030)」及び「デジタルチェコ共和国(Digital Czech Republic)」戦略に基づいている。本AI戦略の目的は、以下の手段を用いてAIにおける国内の経済成長と競争力を促進することにある。

- 信頼できる確かなAIエコシステム
- 企業、とりわけSMEのデジタル化
- AIにおいて社会の経済発展を高める公正な機会及び利益

■ これらの目的を達成するため、チェコ政府は、教育、R&D支援、金融、産業、社会的インパクト、規制、及び国際協力などのカギとなる領域にわたる政策を想定している。本AI戦略は、公的及び民間機関における雇用とAIアプリケーションに関する事実と数字、更にAIの公的調査チームに係る資金調達の見積もりを提示しているが、国家AI戦略実行のための予算配分についてはこれを示していない。しかし、本AI戦略の開始以来、チェコ共和国科学技術機構(Technology Agency)は、様々なAIプロジェクトに対して総額1億2000万ユーロの支援を行った。

出所)European Commission “AI Watch - National strategies on Artificial Intelligence: A European perspective, 2021 edition”
(https://publications.jrc.ec.europa.eu/repository/bitstream/JRC122684/ai_watch_report_national_ai_strategies.pdf)よりNRI作成

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

チェコのAI関連制度・政策　(ii) 人的資源

- チェコ共和国は、初等、中等及び高等教育をAI教育のために改革する行動を想定している。
- 「2030年までのチェコ共和国教育政策のための戦略(Strategy for the education policy of the Czech Republic up to 2030+)」もまた、デジタル技術による教育課程の質向上において教育者を支援することを目的としている。2021年、初等教育のための新たな教育課程が支持され、コンピューターサイエンスクラスの数は二倍になり、新たな重要なデジタルコンピテンスが導入された。
- チェコの戦略は、生涯学習、職業訓練、技能再教育の機会の重要性を強調している。教育改革は労働市場の動態性を確認しなければならないため、チェコ政府は、AIに関する雇用の創出と喪失を予測するための分析を委託することで労働市場を厳重に監視することとなる。将来の労働力需要の予測は、キャリアガイダンス、労働者の流動性及び技能再教育の機会を用いた最新式の仕事の組織的な促進のため、「国家職業登録(National Register of Professions)」及び「中央技能データベース(Central Competence Database)」に送られる。

出所)European Commission “AI Watch - National strategies on Artificial Intelligence: A European perspective, 2021 edition” (https://publications.jrc.ec.europa.eu/repository/bitstream/JRC122684/ai_watch_report_national_ai_strategies.pdf)よりNRI作成

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

チェコのAI関連制度・政策　(iii) 研究開発と社会実装

- AI領域における基礎研究及び応用研究を十分に支援することは、AIの配備を成功させるために重要である。そのため、チェコ政府は、AIが経済に与えるインパクトを分析する、「AI調査におけるCoE(Centre of Excellence in AI Research)」、「デジタル改革ハブ(Digital Innovation Hubs: DIHs)」、及び「人文学及び社会科学センター(Centre for Humanities and Social Science)」の構築に働きかける予定である。2021年4月、チェコ共和国は、8つの地域において運用する、完全に運転可能な8DIHsと、準備段階である4DIHsを想定に入れた。
- 効率的なAI起業家のエコシステムを通じた、AIにおける躍進的イノベーションを促すことは、チェコ政府よって重要視されている。とりわけ、AIにおける改革ハブ(IHAI)、チェコインベストによる共同設立されたスタートアップ支援プログラム、及び加速装置は、AI経済活動及びイノベーションを促進させるだろう。
- チェコ政府は「イノベーション戦略2019-2030」に、戦略的マネジメント(教育及と研究など)、デジタル技術及び技能の潮流に関するイノベーションシステムを向上させるためのロードマップを導入した。「将来の国家(The Country for the Future: CFF)」計画は産業貿易省によるもので、同改革戦略を実施するためのツールである。それは、61億チェコ・コルナ(約2億3269万ユーロ)の予算を、企業、デジタルサービス、R&Dベース改革の支援に充てている。
- チェコの戦略は、官民両セクターにおけるAIの支援については金融商品が有用だと考えている。「デジタルチェコ共和国」計画は、「AI調査におけるCoE」にプラハ及び民間のパートナーからのリソースをつぎ込む予定である。長期的にはチェコ政府はAIへの補助金計画を計画しており、AIビジネスの資金調達は市場ベースの金融商品にまで拡大される予定である。チェコ政府はまた、SME、スタートアップ、スピンオフへの特別の補助金及び投資計画を発展させる予定である。

出所)European Commission “AI Watch - National strategies on Artificial Intelligence: A European perspective, 2021 edition”
(https://publications.jrc.ec.europa.eu/repository/bitstream/JRC122684/ai_watch_report_national_ai_strategies.pdf)よりNRI作成

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

チェコのAI関連制度・政策　(iii) 研究開発と社会実装

- チェコの戦略は、国家及び国際パートナーシップの両方を促進させる政策提言を想定している。チェコ政府は、ポーランド、チェコ共和国、スロヴァキア、ハンガリーを横断するこの分野の連携を強化するため、V4(4か国)の優先事項の中にAIを含めることを提案している。二国間の連携も非常に重要である。
- SME、スタートアップ、科学研究センターの間の連携には、「知識移転パートナーシップ」などの特定のプログラムから支援が与えられる。チェコ共和国はまた、学際的チームにおいてもAI改革の発展を促進させる入札の呼びかけを始める予定である。加えて、アカデミア、研究センター及び民間部門からの代表者からなる専門家集団が、AIにおける共同投資計画を支援する。
- チェコ政府は、チェコの国際的なアピールを高め、海外のAIに関する人材を誘致し、確保する政治行動を見越している。例えば、チェコの戦略には外国人居住及び科学研究者への長期在留資格に関する法律を見直す狙いがある。
- チェコ共和国はチェコ内外におけるチェコのAIエコシステムの促進を奨励する。経済におけるAIの普及と利用を強化するためである。

出所)European Commission “AI Watch - National strategies on Artificial Intelligence: A European perspective, 2021 edition”
(https://publications.jrc.ec.europa.eu/repository/bitstream/JRC122684/ai_watch_report_national_ai_strategies.pdf)よりNRI作成

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

チェコのAI関連制度・政策　(iv) 規制

- 人間中心のAIのためには、人権を保護するために実効的な規制が必要である。チェコの戦略は、AI技術の発展を不必要な規制上の制約から解放する倫理的及び法的規制を規定している。第一に、チェコ共和国は、AIの研究や発展の努力が不適切な立法にほとんど妨げられている部門を特定することを予定している。データアクセス、データオーナーシップ、(個人)データ保護の全ての問題が、部門特定型アプローチで厳格に検討されている。
- チェコ共和国は、「AIオブザベートリ―&フォーラム(AIO&F)」を開始した。信頼あるAIの調査、発展及び利用のために好ましい社会的法的環境を創設するAIの法的側面に関する専門家のプラットフォームである。

出所)European Commission “AI Watch - National strategies on Artificial Intelligence: A European perspective, 2021 edition”
(https://publications.jrc.ec.europa.eu/repository/bitstream/JRC122684/ai_watch_report_national_ai_strategies.pdf)よりNRI作成

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

チェコのAI関連制度・政策　(v) インフラ

- AIの発展において、データインフラストラクチャーが正しく機能することは重要な前提条件である。したがってチェコ共和国は「調査情報へのオープンアクセスに関する国家戦略(National strategy on open access to research information)」を、2017年から2020年の間に立ち上げた。
- デジタル及び電気通信インフラストラクチャーの現代化は、高品質データの提供を促進させる。欧州高性能コンピューティング共同事業(EuroHPC JU)イニシアティヴの文脈においてチェコ政府は、ペタスケールHPCシステム「カロリーナ(Karolina)」を保有する、IT4イノベーションズの国家スーパーコンピューティングセンターを拡大し、前エクサスケールHPCシステムを構築するためのLUMIコンソーシアムに参加し、EuroHPC研究を支援することを計画している。
- 「デジタルチェコ共和国」戦略は、政府が今後数年以内にチェコにおいて５Gネットワークを配備するためのインターネットインフラストラクチャーについて、接続性の改善を優先とすることを強調している。そのため、チェコ共和国の産業貿易省とバイエルン国家首相府(State Chancellery)は、ミュンヘンとプラハの間に共通の5Gを通すことを目標としており、これは欧州委員会の「欧州設備接続(Connecting Europe Facility)」計画の一部でもある。

出所)European Commission “AI Watch - National strategies on Artificial Intelligence: A European perspective, 2021 edition”
(https://publications.jrc.ec.europa.eu/repository/bitstream/JRC122684/ai_watch_report_national_ai_strategies.pdf)よりNRI作成

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

チェコのAI関連制度・政策　(vi) 社会課題の解決：気候及び環境

- 二酸化炭素の排出によるグローバルな気温上昇は、気候変動のインパクトをよりよく管理し地球を守るための新たな道具を必要としている。PwCの最近の調査によると、気候変動に対処できる科学技術には、先進材料、クラウドテクノロジー、自動走行車、合成生物学、バーチャルリアリティ(VR)及び拡張現実(AR)、AI、ロボット、ブロックチェーン、３Dプリント、IoTがある。
- さらに、「デジタルチェコ共和国」戦略は、デジタル及びAI技術を用いて、顕在化する気候変動を適合化する新しく革新的な方法を探すための公的及び政治的議論の重要性を強調している。

出所)European Commission “AI Watch - National strategies on Artificial Intelligence: A European perspective, 2021 edition”
(https://publications.jrc.ec.europa.eu/repository/bitstream/JRC122684/ai_watch_report_national_ai_strategies.pdf)よりNRI作成

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

チェコのAI関連制度・政策　(vi) 社会課題の解決：COVID-19パンデミック

- COVID-19パンデミックの間、AIを用いたイニシアティヴやプロジェクトが発展してきた。チェコ共和国は、AI原則に基づいた「スマート検疫」の追跡システムを公表し、またCOVID-19関連の問題に答えるためのAIチャットボットを開発した。
- 「Hack the Crisis」もまた、AIによるアプリケーションの発展に貢献しているハッカソンである。
- チェコ政府はまた、デジタル改革ハブ、及び検査実験施設(Testing and Ecperimentation Facilities: TEFs)に注目しようとしている。TEFsについては、技術的能力を有する病院との協力構想が検討されている。

出所)European Commission “AI Watch - National strategies on Artificial Intelligence: A European perspective, 2021 edition”
(https://publications.jrc.ec.europa.eu/repository/bitstream/JRC122684/ai_watch_report_national_ai_strategies.pdf)よりNRI作成

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

チェコのAI関連制度・政策　(vii) モニタリングと今後のアップデート

■ チェコ共和国の国家AI戦略は産業防衛省がこれを調整するが、その実施はAI委員会によって監督される。AI委員会は「デジタルチェコ共和国」戦略の運営委員会の小委員会である。同戦略は７つの章から成り、それぞれ別の作業部会に割り当てられている。それぞれの作業部会はその戦略目的の達成の監視に対して責任を負う。1年に一度、運営委員会とチェコ政府は戦略の実施に関する進捗報告書を受け取る。

出所)European Commission “AI Watch - National strategies on Artificial Intelligence: A European perspective, 2021 edition”
(https://publications.jrc.ec.europa.eu/repository/bitstream/JRC122684/ai_watch_report_national_ai_strategies.pdf)よりNRI作成

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

オランダのAI関連制度・政策　(i) AI関連制度・政策の概要

■ 2019年10月、オランダ政府は「AI戦略的行動計画(Strategic action for artificial intelligence)」を公表した。同戦略は、グローバル市場のAI分野におけるオランダの競争力を強化するための様々な政策を提言している。オランダAI戦略のビジョンは三つの柱から成る。

- 社会的経済的機会を資本に変換すること：民間及び公的部門におけるAIの採用、利用、発展の奨励、社会問題への取組におけるAI利用の促進
- 最適状態を作り上げること：AIにおける教育や技能発展の支援、AIにおける研究やイノベーションの促進、質的データへのアクセスの容易化、デジタルインフラストラクチャーの向上
- 基盤を強化すること：信頼性、人権、消費者保護、市民保護など倫理的問題に関連する政策行動

■ AI戦略は、教育、R&Dとイノベーション、ネットワーキング、規制、インフラストラクチャーに関連する政策を通じて経済におけるAIを促進させることを目的とした、広範なイニシアティヴのリストを含んでいる。

■ オランダの戦略は付属書において、AIイノベーションと研究についての年間の政府予算は、1年あたり4500万ユーロ見積もられているとしている。2019年は6400万ユーロであった。2020年オランダは、官民パートナーシップオランダAI連合のために2350万ユーロ追加で資金と投下した。2021年4月、ドイツ経済及び社会のためのAIの可能性を最大化するために、今後最大2億7600万ユーロ追加して、投資計画が策定された。

出所)European Commission “AI Watch - National strategies on Artificial Intelligence: A European perspective, 2021 edition”
(https://publications.jrc.ec.europa.eu/repository/bitstream/JRC122684/ai_watch_report_national_ai_strategies.pdf)よりNRI作成

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

オランダのAI関連制度・政策　(ii) 人的資源

■ 公的教育及び訓練改革は、初等教育と中等教育でデジタルリテラシーを向上させ、高等教育でデジタルサイエンス技術とコンピテンシーを発展させる機会を提供する(国家データサイエンス訓練プログラム: National Data Science Trainee programme)とする政策を通じて行われることが予定されている。AIに関する国営のオンライン講座もまた、公務員は受講可能である。地域投資基金が資金提供する職業訓練イニシアティヴは、より密接に、労働市場における将来の(デジタル)需要にねらいを定めている。さらなる訓練と生涯学習は、デジタル技術に焦点をあてて、STAPスキームと生涯発展の向上のための多年プログラムを用いて行われている。

出所)European Commission “AI Watch - National strategies on Artificial Intelligence: A European perspective, 2021 edition”
(https://publications.jrc.ec.europa.eu/repository/bitstream/JRC122684/ai_watch_report_national_ai_strategies.pdf)よりNRI作成

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

オランダのAI関連制度・政策　(iii) 研究開発と社会実装

- AIの基本研究と応用研究を促進させるため、オランダ科学研究機構(Dutch Research Council)はAIに関する新しい研究計画を支援している。そのため、オランダAI連合はAIコンピテンスセンターの設立を提案している。企業がAIに投資するための適切な条件を備えるために、オランダ政府は、イノベーションクレジット(Innovation Credits)、シードキャピタルスキーム(Seed Capital Scheme)、オランダベンチャーイニシアティヴ(Dutch Venture Initiative)を通じて、イノベーション財政支援とベンチャーキャピタルへのアクセスを向上させている。さらに、商工会議所はAIに関する実践的な情報を提供している。提供される情報は企業のイノベーション努力を支援しうる。
- オランダ政府はまた、「知識・イノベーション誓約(Knowledge and innovation Covenant: KIC)」を発展させた。KIC2020-2023は、官民パートナーシップにおける基本的かつ実践的な研究を支援し、エネルギー転換、持続可能性、農業、水と食糧、ヘルスケア、安全などの重要な実現技術に焦点を当てている。AIはそれぞれの領域で重要な要素である。
- R&D&Iについては、AI、再生医療、ヘルスデータインフラストラクチャー、量子技術、水素/グリーン化学といった領域における５つのプロジェクトが国営成長基金(National Growth Fund)からの資金提供を受けていた。400以上の参加者からなる官民パートナーシップである「オランダAI連合(NL AIC)」は、AIに関するプロジェクト「AiNEdプログラム」の第一段階の資金調達のため、2億7600万ユーロの一部を受け取った。これはAIの発展と応用を加速させることを目的としている。注目されるのは、1)革新的なAIアプリケーシを促進する、2)基礎研究及び応用研究の知識ベースを強化する、3)AI教育及び訓練の可能性を増加させる、4)倫理的法的枠組みのある人間中心のAIを発展させる、5)AIのためにデータを利用可能にするような、大規模プロジェクトである。

出所)European Commission “AI Watch - National strategies on Artificial Intelligence: A European perspective, 2021 edition”
(https://publications.jrc.ec.europa.eu/repository/bitstream/JRC122684/ai_watch_report_national_ai_strategies.pdf)よりNRI作成

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

オランダのAI関連制度・政策　(iii) 研究開発と社会実装

- オランダ政府は、オランダAI連合などの、AIにおける協業や官民パートナーシップ(PPPs)を高く評価している。
- さらに法的環境でのAIアプリケーションの利用(AIに基づく文書自動作成やデューデリジェンスなど)やパブリックドメインでのAIアプリケーションの利用(チャットボットなど)における国内連携のいくつかの例を強調している。欧州AIコンソーシアや国際AI協力におけるオランダのパートナーシップを強化することで国際連携が奨励されている。
- さらにオランダは、AIグローバルパートナーシップ(GPAI)に参加している。

出所)European Commission “AI Watch - National strategies on Artificial Intelligence: A European perspective, 2021 edition”
(https://publications.jrc.ec.europa.eu/repository/bitstream/JRC122684/ai_watch_report_national_ai_strategies.pdf)よりNRI作成

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

オランダのAI関連制度・政策　(iv) 規制

■ 規制についてオランダ政府は、人権や消費者保護を尊重しており、よく発展した法的枠組みに基づいた、倫理的で信頼性のあるAI利用を主張している。オランダAI連合は例えば、人間中心のAIに関する研究、教育、諸機関の間の相乗効果を強化するため、ELSAラボ構想を作り出した。オランダ政府はまた、この問題に関するハイレベルエキスパートグループと欧州の指令へ積極的に参加していることを強調している。

■ 公共の価値の保護を支援し、信頼ある環境でのAIの利用を奨励するためにいくつかの立法改革が進行中である。

- アムステルダムAI登記(ヘルシンキとのパートナーシップ)：アムステルダムとヘル　シンキは、どのようにアルゴリズムが自治体に利用されているのかを追跡するAI登記を開始した。
- 自動運転に関する実験法(Experimental Law on self-driving vehicles)：運転手不在で実施する自動運転のテストが、特定の条件下で、公道で許されることとなった。2019年7月に発効した。
- AIの利用と発展におけるグッドガバナンスと消費者保護の原則が、自由情報法(Freedom of Information Act)、一般行政法(General Administrative Law)、一般データ保護規制(General Data Protection Regulation: GDPR)において改正された。オランダ政府は国内法において法執行指令(Law Enforcement Directive)を実施し、自動システムが利用された際の求人における差別を防止する法を決定した。
- オランダ政府は、アルゴリズムデータ分析適用のためのガイドラインを策定した。

出所)European Commission “AI Watch - National strategies on Artificial Intelligence: A European perspective, 2021 edition”
(https://publications.jrc.ec.europa.eu/repository/bitstream/JRC122684/ai_watch_report_national_ai_strategies.pdf)よりNRI作成

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

オランダのAI関連制度・政策　(v) インフラ

■ オランダの戦略は、データインフラストラクチャーを促進させ、データ利用とデータシェアリングの基盤を構築する政策を含んでいる。個人データ共有についてのFAIR原則の促進、「欧州共通データスペース(Common European Data Space)」への参加、データシェアリングソリューションのインベントリの設置がある。デジタル、電気通信インフラについては、オランダの戦略はとりわけ、デジタル接続性行動計画(高品質の接続性の実現を目的としている)やスーパーコンピューティングパワーへの政府投資(SURFにおけるスーパーコンピューターなど)に言及している。

出所)European Commission “AI Watch - National strategies on Artificial Intelligence: A European perspective, 2021 edition”
(https://publications.jrc.ec.europa.eu/repository/bitstream/JRC122684/ai_watch_report_national_ai_strategies.pdf)よりNRI作成

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

オランダのAI関連制度・政策　(vi) 社会課題の解決：気候及び環境

- NL AIC連合は、AIアプリケーションの重要な領域としてエネルギーと持続可能性を強調している。AIは、エネルギー消費を減らし、気候への好影響をもたらす革新的なプロジェクトを発展させるための核となる科学技術である。現在進行中の政策をまとめあげ、この領域における協力の前提条件を整えるための専用の作業部会が創設された。
- オランダ水パートナーシップ(NWP)は、協力して持続可能な水解決を発展させるために、水部門から集まった政府機関を含む諸機関のネットワークである。このパートナーシップは水部門の効率性や自由に解放された資源を向上させ、持続可能性と環境変動に積極的に貢献するような人間志向型のノウハウを強化するためにAIや機械の重要性を強調している。
- 2016年1月、オランダ王立気象研究所(the Royal Netherlands Meteorological Institute)は、KNMIデータラボを創設した。気候変動、天気予報、地震学におけるイノベーションを促進させ、調整することを目的としている。

出所)European Commission “AI Watch - National strategies on Artificial Intelligence: A European perspective, 2021 edition”
(https://publications.jrc.ec.europa.eu/repository/bitstream/JRC122684/ai_watch_report_national_ai_strategies.pdf)よりNRI作成

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

オランダのAI関連制度・政策　(vi) 社会課題の解決：COVID-19パンデミック

■ Holland投資ネットワークはCOVID-19に打ち勝つためにAIが利用できる様々な領域を特定している。

- 診断のための医用イメージングでのAIの利用
- リスク評価のためのAIの利用
- 曲線を平らにするためのAIの利用

■ 次のイニシアティヴとAIの革新的適用は近年オランダにおいて、COVID-19に対抗するために現れてきた。

- オランダ国立公衆衛生環境研究所(National Institute for Public Health and the Environment: RIVM)は、AIや機械学習を用いてウイルスの拡大を追跡しモデリングする新しいツールの利用において先頭に立っている。同研究所は感染症レーダーを使う。
- オランダがん研究所(NKI)からのチームが、CTスキャンにより数秒で正確にコロナウイルスを診断することのできる強力なアルゴリズムを開発するため、30以上のEUの病院に対し、後遺症患者のレントゲン写真の提出を促している。
- Maasstad病院はHolland AIと協力して、COVID-19陽性の可能性のある患者の、影響を受けた肺組織の割合を評価するために、AIに基づいたアルゴリズムを開発した。
- アムステルダムUMC病院とアムステルダム自由大学、マーストリヒトUMCは、コロナウイルスと闘うためのAIの利用を増加させるためのイニシアティヴを合意した。
- 欧州のAI専門家ネットワークであるCLAIREにおいて、ライデン大学は、集中治療部門から出てきた膨大な量のヘルスデータを活用するAIアプリケーションを開発している。
- オランダ水研究所(Dutch Water Research Institute: KWR)は、AI技術を使って、下水を監視し、感染した人間から生じることのあるウイルスのRNAトレースの出現を感知する測定方法を作り上げた。
- デルフト工科大学は、利用可能なデータを使って、将来のCOVID-19の発生を予想するアルゴリズムを実施している。
- アムステルダム大学メディカルセンターとマーストリヒト大学メディカルセンターからの研究者らは、コロナウイルスに罹った患者の治療方法を探すため、協力して、AIとビッグデータを使うプロジェクトに取りかかっている。

出所)European Commission “AI Watch - National strategies on Artificial Intelligence: A European perspective, 2021 edition” (https://publications.jrc.ec.europa.eu/repository/bitstream/JRC122684/ai_watch_report_national_ai_strategies.pdf)よりNRI作成

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

オランダのAI関連制度・政策　(vii) モニタリングと今後のアップデート

■ デジタル化(及びAI)のための国家戦略は2021年第2期に全体的な更新が行われる予定である。

出所)European Commission “AI Watch - National strategies on Artificial Intelligence: A European perspective, 2021 edition”
(https://publications.jrc.ec.europa.eu/repository/bitstream/JRC122684/ai_watch_report_national_ai_strategies.pdf)よりNRI作成

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

スイスのAI関連制度・政策　(i) AI関連制度・政策の概要

■ スイスは、国家AI戦略を公表しない予定であるが、スイス経済及び社会におけるAIの研究及び配備の条件となる枠組みを発展させる努力を現在行っている。2019年12月、スイス連邦参事会は、「AIに関する省庁間作業部会(Interdepartmental Working Group on Artificial Intelligence)」の報告書を承認した。この作業部会は2018年秋に、連邦参事会を代表して連邦経済教育研究省(EAER)によって設立された。この報告書は様々な政策領域において提言をしており、17のテーマ別に政策行動を挙げている。主に以下のものがある。

- AI関連技能とコンピテンシーを全ての教育レベルで向上させ、労働力のための生涯学習や技能再教育の機会を創設する
- AI研究とイノベーションを促進させ、アントレプレナー・エコシステムの競争力を強化する
- AIアプリケーションの幅広い採用と利用を通じて公共サービスを強化する
- (国際)ネットワークとパートナーシップを支援して、すべての経済と組織のプレイヤー間での情報及び知識の交換を確保する
- 持続可能かつ信頼のあるAIを保証するための規制及び倫理的枠組みを構築する
- AIの発展を促進させるためのデータインフラストラクチャーを発展させる
- 電気通信インフラストラクチャーを強化する、とりわけ、サイバーセキュリティに関する強化

■ 具体的な政治行動のためのこれらの課題に取り組むにあたって、AI作業部会は、「デジタルスイス戦略(Digital Switzerland Strategy)」に概括した諸政策の綿密な連携と統合を提言した。AIの適用のいくつかの側面、例えばデータ利用などは、2020年9月の「デジタルスイス戦略」が扱っている。

■ 更に、スイス政府はAIのための特別のガイドラインを2020年11月に採択した。同ガイドラインは、連邦政府の行政府や行政業務を任された諸機関のための一般的な指導枠組をおき、一貫したAI政策を確保することを意図している。ガイドラインの適用の定期的評価や更なる発展は今後行われる予定である。

出所)European Commission “AI Watch - National strategies on Artificial Intelligence: A European perspective, 2021 edition”
(https://publications.jrc.ec.europa.eu/repository/bitstream/JRC122684/ai_watch_report_national_ai_strategies.pdf)よりNRI作成

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

スイスのAI関連制度・政策　(ii) 人的資源

■ 教育研究イノベーション国家事務局(SERI)は、AIにおける人的能力を強化するための、教育における人工知能に関する報告書を公開した。この報告書は、教育におけるAIの採用のための政策を提言しており、また、AIが教育システムにもたらす機会や課題を強調している。特に、初等、中等、第三期教育における、AIの配備のために必要な技能を獲得する講座を発展させる必要があるとしている。以下の政策がある。

- すべての段階の教育システムにおいてAIの使用に必要な技能の移転を確保する。教育研究イノベーション国家事務局(SERI)は行政区画と綿密に連携してこれを確保する予定である
- 教育におけるAIの透明かつ信頼ある利用を保障する

■ 学生の教育に加えて、AI技能が全ての部門における労働力を支えることを確保することが必要である。社会人教育のための生涯学習プログラム、訓練、技能再教育、技能向上の機会がこれを可能にする。これらのタイプの訓練に莫大な可能性があり、その重要性は今後拡大し続けるだろう。

■ 作業部会は、かつての技術発展とは異なる方法でAIが労働市場を変えるだろうとしている。この意味で、労働人口の技能及びコンピテンシーは、労働市場の変わりゆく需要に素早く適応する必要がある。現在、労働市場で求められる技能を監視している。経済国家事務局(SECO)はAIにおける既存のコンピテンシーに関する課題を監視し新たな問題を扱っている。2017年11月、さらに連邦参事会はデジタルトランスフォーメーションが労働市場に与えるインパクトを監視することを決定した。モニタリングの結果は2022年末までに公開される。

出所)European Commission “AI Watch - National strategies on Artificial Intelligence: A European perspective, 2021 edition”
(https://publications.jrc.ec.europa.eu/repository/bitstream/JRC122684/ai_watch_report_national_ai_strategies.pdf)よりNRI作成

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

スイスのAI関連制度・政策　(iii) 研究開発と社会実装

- AI作業部会は、スイスには良質なAI研究及びイノベーションがあるが、課題も多いことを強調した。
- AIに関する科学研究については、SATWがSERIのために準備した、科学及び研究におけるAIに関する報告書で既存の活動と課題が指摘されている。スイスは、有名で設立から長い研究センターのダイナミックな研究環境に頼ることができる。更に、個人研究イニシアティヴと大学がこの研究環境を補完している。現在、AI作業部会の専門家は、既存の政策イニシアティヴが適切な支援を与え、連邦政府は更なる政策措置をとらなくて済むとしている。
- AIのイノベーションの強化のために、SATWがSERIのために準備した、産業及び行政におけるAIに関する報告書は、産業及び行政におけるAIについての包括的な課題の詳細な概観を示している。AI特許の量と質についてのスイスのパフォーマンスと、スイスのAIスタートアップの数から、スイスは強力で競争力のある位置づけにあることがわかる。したがって、作業部会は、産業界自体がAIの課題を非常によく扱っていると結論付ける。しかし産業界による自己規律のほかに、作業部会は、メディア、モビリティ、ヘルスケア、金融、農業、エネルギー及び気候などの重要分野における政策イニシアティヴをいくつも強調している。

出所)European Commission “AI Watch - National strategies on Artificial Intelligence: A European perspective, 2021 edition”
(https://publications.jrc.ec.europa.eu/repository/bitstream/JRC122684/ai_watch_report_national_ai_strategies.pdf)よりNRI作成

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

スイスのAI関連制度・政策　(iii) 研究開発と社会実装

- 【メディアと公共】作業部会は、メディアにおけるAI利用の増加、及びそれがもたらし得る課題(フェイクニュースなど)についての中間機関の役割を規律する必要性を強調している。具体的な政策行動を概括するガバナンス報告書が、2021年末までに連邦参事会に提出される予定である。
- 【自動運転モビリティ】2019年SERIのために準備された自動運転モビリティとAIに関する報告書が、自動運転モビリティに関する政府の努力を示している。連邦道路局(FEDRO)と連邦運輸局(FOT)は、データ交換を促進させるために自動化車両の発展をフォローアップし、データ保護を確保し、法的枠組を改正する。
- 【ヘルスケア】AIは、予防、予測、監視を改善することのできるデータドリブン医学を用いたヘルスシステムへの機会を多くもたらしつつある。データドリブン分析技術の発展やヘルスケア部門へのAIの導入は、データ及びプライバシー保護の必要性を拡大させている。このため、連邦公衆衛生局(FOPH)は、AIが医療やヘルスケアに与える影響を監視し、また既存法の改正の可能性を検討している。
- 【金融】金融産業においても、多大な労力を必要とする過程を、AIの利用が自動化し加速化させつつある。そのため、この部門におけるAI利用が拡大するに伴って適切なガバナンスの必要が現れている。連邦財務省(FDF)は、金融部門におけるAIの発展を監視し、適切な定期審査によって新たな問題を解決している。とくに、オペレーショナルリスクの規律と、金融部門におけるAIメソッドの利用における行動義務の概説を行う。
- 【農業】農業の文脈では、AIが、画像認識、収穫ロボット、とりわけコグニティブコンピューティング技術を通じて、精密農業を容易にしている。連邦農業局(FOAG)が農業における諸発展を監視し続けている。このため、フィールドデジタルデータと予測分析についての「ビジネスインテリジェンスコンピテンスセンター」が設立された。さらに、連邦経済教育研究省(EAER)とFOAGは、2018年、「スイス農業及び食糧産業のデジタイゼーション宣言(Charter on the digitisation of Swiss agriculture and the food industry)」を開始した。同宣言は、共通意識を育て、関連ステークホルダー間の協力を促進することを目的としている。

出所)European Commission “AI Watch - National strategies on Artificial Intelligence: A European perspective, 2021 edition”
(https://publications.jrc.ec.europa.eu/repository/bitstream/JRC122684/ai_watch_report_national_ai_strategies.pdf)よりNRI作成

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

スイスのAI関連制度・政策　(iii) 研究開発と社会実装

- 【エネルギー】AIの発展は、非常に効率的なエネルギー供給を可能にする。再生可能エネルギーの発展を支援し、省エネルギーを提供し、それによって気候保護に貢献する。全体的には、エネルギー供給の運用における現在の複雑性を単純化することが可能である。この点、スイス連邦エネルギー局(SFOE)はエネルギー産業におけるAIの課題に取り組んでいる((ⅳ)社会課題の解決を参照)。
- 【エネルギー】民間部門におけるイノベーションを促進させるため、サイバーセキュリティとエネルギー部門のためにテストベッドの創設が提言されている。サイバーセキュリティにおけるAI利用を増加させるため、国営サイバーセキュリティセンター(NCSC)と連邦国防国民保護スポーツ省(DDPS)は、連邦外務省(FDFA)とEAERと協力して、この分野におけるスイスAIテストセンターの可能性を評価する研究を始動している。エネルギー分野において連邦エネルギー局は、AI関連プロジェクトなど、新しい科学技術の発展と実験を促進させるため、「パイロット＆デモンストレーション計画(Pilot and Demonstration Programme)」を提供している。

出所)European Commission “AI Watch - National strategies on Artificial Intelligence: A European perspective, 2021 edition”
(https://publications.jrc.ec.europa.eu/repository/bitstream/JRC122684/ai_watch_report_national_ai_strategies.pdf)よりNRI作成

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

スイスのAI関連制度・政策　(iii) 研究開発と社会実装

■ さらにAIの利用は、行政サービスの質と効率を上げるための実効的な手段でもある。このため、連邦関税局(FCA)とスイス連邦統計局(FSO)、移民事務局(SEM)は以下のような様々なプロジェクトを支援している。

- 国境を超えるコストを減らすためのチャボットによるソリューションの発展、商品の密輸に関するリスク分析と管理を行うためのデータ分析プロジェクトの設立。いずれのプロジェクトも、連邦関税局を現代化しデジタル化することを目的とした「DaziTプログラム(DaziT Programme)」の一部である。
- 「Arealstatistikディープラーニング―ADELEプロジェクト」は、FSOが運用する、土地利用と土地被覆分類のためのディープラーニングアプリケーションである。
- 「NOGA codingの自動化(NOGauto)」に関するプロジェクトは、FSOで既に利用可能なデータを暗号化する機械学習メソッドを提案する。
- 「機械学習―Sosi」に関するFSOのプロジェクトは、社会保障制度に関するデータ分析を、機械学習的アプローチで行う。
- 「機械学習によるデータバリデーション」に関するプロジェクトは、機械学習アルゴリズムを用いると同時にデータの質を向上させながら、FSOでのデータバリデーションを拡大し加速させることを目指している。
- SEMの「庇護希望者のためのジョブアルゴリズム」プロジェクトは、労働市場を最適化しながら庇護希望者を国内の行政区画に割り当てる機械学習システムのパイロットテストである。

■ 類似のプロジェクトを促進させるため、AI作業部会は、連邦行政がデータ交換を奨励し、AI関連技術を用いて行政が利用可能な大規模データ収集を開発することを提言している。加えて、連邦行政におけるAIの適用について技術的側面に焦点を当てたAIコンピテンスネットワークの創設は、グッドプラクティスの共有を促進させることができる。

出所)European Commission “AI Watch - National strategies on Artificial Intelligence: A European perspective, 2021 edition”
(https://publications.jrc.ec.europa.eu/repository/bitstream/JRC122684/ai_watch_report_national_ai_strategies.pdf)よりNRI作成

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

スイスのAI関連制度・政策　(iii) 研究開発と社会実装

■ 以下の政策イニシアティヴが、AI関係アクターの間のよりよいネットワークと協力を促進するため、進行又は提言されている。

- 対話と、情報及び知識の交換を確保するためのプラットフォームを発展させる。作業部会は、連邦通信局(OFCOM)が創設したスイス「三者間プラットフォーム(Plateforme Tripartite)」が、AIに関する学際的な国営コンピテンスネットワークとなりうると提言している。
- ジュネーヴインターネットプラットフォーム(GIP)などの、デジタル政策データベースのためのハブを更に発展させることでAIプレイヤー間の協業を強化する。このプラットフォームは、OFCOMと連邦外務省(FDFA)によって始動され、AIを含むデジタルガバナンスのセンターとして機能してきた。ジュネーヴとジュネーヴインターネットプラットフォームの、グローバルデジタル及び技術政策のハブとしての重要性を強化することは、新しい外交政策戦略2020-2023の主たる目的でもある。
- 「ホライゾン欧州(Horizon Europe)」や「デジタル欧州計画」などの汎欧州イニシアティヴへの参加を支援し、特にスーパーコンピューティング、デジタルイノベーションハブ、応用デジタル技能に対する支援計画を通じて、グローバルデジタル経済における欧州の競争力を向上させることを目指す。
- サイバーセキュリティのための国際協力を強化する。FDFAは、サイバー外交及び安全政策特使室(Office of the Special Envoy for Cyber Foreign and Security Policy)を設立した。技術的なレベルでは、国際協力はインシデントマネジメントに関する情報交換に役立つと同時に、連邦インテリジェンス・サービスは、インフラストラクチャーがサイバー攻撃の影響を受けた国内の行政区画と集中的なコンタクトを維持している。

出所)European Commission “AI Watch - National strategies on Artificial Intelligence: A European perspective, 2021 edition” (https://publications.jrc.ec.europa.eu/repository/bitstream/JRC122684/ai_watch_report_national_ai_strategies.pdf)よりNRI作成

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

スイスのAI関連制度・政策　(iv) 規制

- 規則は、倫理及び包摂の原則に配慮しながら、AIイノベーションを促進させ、AIの採用及び適用の標準を作るための立法や勧告に関係する。
- AIの信頼ある、確かな、責任ある、公正な配備のための倫理的ガイドラインについて、スイス政府は国際的な議論に積極的に関わっており、AI利用における確立した価値と標準の尊重を確保することに貢献してきた。そのために、トレーサビリティ、透明性、包摂の原則を保障することが重要である。
- AI規制についてAI作業部会は、スイスにおけるAIの発展を可能にする一般的規制枠組を維持することを提案した。この枠組みには、メディア、モビリティ、ヘルスケア、金融、農業、エネルギー及び気候など特定のテーマ領域、政策領域におけるいくつかのクラリフィケーションとアダプテーションが含まれている。しかし実効的な規制は可能な限り多くの技術を対象とするべきであるから、連邦政府は「科学技術中立政策(technology-neutral policy)」に熱心に取り組み続けている。この政策は、特定の技術や技術特定型規制の促進を可能な限り避けるものである。FDFAはAIについての一般的な法的枠組を更に発展させるため特に以下の政策に注目している。
  - AI特定型国際法及びそのスイスへの影響を検討
  - 消費者との相互作用におけるAIシステムの可視性についての発展をフォローアップ
  - 司法制度におけるAIベースの決定に関する発展を監視(予測的司法)
- 法改正に従って、AI作業部会は、標準化の一般的向上と更なる相互運用性が、関連ステークホルダーの間のAI関連研究とイノベーションを奨励するだろうとしている。

出所)European Commission “AI Watch - National strategies on Artificial Intelligence: A European perspective, 2021 edition”
(https://publications.jrc.ec.europa.eu/repository/bitstream/JRC122684/ai_watch_report_national_ai_strategies.pdf)よりNRI作成

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

スイスのAI関連制度・政策　(v) インフラ

■ AI作業部会は、持続可能なインフラストラクチャーの実施も検討している。AI領域の能力を増加させるためのインフラストラクチャーに資金提供する可能性は技術的性格の課題である。強固なデータインフラストラクチャー(データ収集、データ共有プラクティスなど)と、ソリッドテレコムインフラストラクチャー(高速接続、適切なサイバーセキュリティなど)の両方に関係する。

■ データインフラストラクチャーについては以下の政策が言及されている。

- 刊行物へのオープンアクセス、オープンな研究データにおけるデータ交換インフラストラクチャーの支援。これらのイニシアディヴは、「オープンサイエンスのための欧州電子コンピューターインフラストラクチャー(BEAT platform)」と欧州オープンサイエンスクラウド(EOSC)との連携が可能である。
- 最近改正された「著作権及び関連する権利に関する連邦法(Federal Act on Copyright and Related Rights)」を通じてセキュリティとデータ保護を確保すること
- データ収集、データ共有、データ保護などに対し、部門特化型の措置を支援すること
- エネルギー戦略2050を公表すること。同戦略の目標には、エネルギー部門におけるAI配備のためのデータインフラストラクチャーを構築することが含まれている(気候及び環境を参照)。2027年末までに、スマートメータリングシステム(いわゆるスマートメーター)が電力部門に導入される予定である。電化製品/消費のデジタル及び高精度データ収集が可能になる。
- デジタルプラットフォーム(データハブ)クラウドの構築は、データ交換をより効率的にし、データをより容易に利用可能にすることが想定されている。標準化された機械可読インターフェイス(APIs)がこのプロセスにおいて重要な役割を果たす。

出所)European Commission “AI Watch - National strategies on Artificial Intelligence: A European perspective, 2021 edition”
(https://publications.jrc.ec.europa.eu/repository/bitstream/JRC122684/ai_watch_report_national_ai_strategies.pdf)よりNRI作成

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

スイスのAI関連制度・政策　(v) インフラ

■ テレコムインフラストラクチャーと関連するサイバーセキュリティ措置については、AI作業部会は、「サイバーセキュリティ及び安全保障政策におけるAI」に関する詳細な報告書に言及している。同報告書は以下のイニシアティヴを強調する。

- 「国家サイバーリスク保護戦略(NCS)」は、AIに関連するサイバーリスクに対する保護を強化するための、現在実行中及び計画された活動を示している。とりわけ、国家サイバーセキュリティセンター(NCSC)は、正式にはMELANIとして知られているが、政府コンピューター緊急対応チーム(GovCERT)と共に、AI関連の新たなサイバーリスクを分析することができる。
- 「重要インフラストラクチャー保護国家戦略(CIP)」には、重要インフラの保護と、それによる必需品と必要不可欠なサービスの利用可能性を確保する17の行動が挙げられている。同戦略は、必要不可欠なサービスを提供する新しいAIによる機会、全体的により良い保護を得ることを目的としている。
- 「サイバー国防行動計画(CDAP)」は、サイバー能力の強化を組織的に行うことを目指している。自己防衛に加え、主たる目的は、インテリジェンス法と軍事法のサイバー的側面を実施することで、サイバー攻撃にさらされる重要なインフラストラクチャーの運営者への支援を可能にすることである。2019年以来、「アルマスイス・サイバー国防キャンパス(Cyber Defence Campus of Armasuisse)」がAIの発展を含む新しい科学技術を予測し、探知し、監督するプラットフォームとなっている。同キャンパスは大学及び経済アクター両方と綿密な協力のもと運営されている。
- 「スイス・ドローン及びロボットセンター(SDRC)」は、国内及び二国間プロジェクトにおいてスイスの安全保障のためにロボットとAIを組み合わせることによる機会とリスクを、検証している。

出所)European Commission “AI Watch - National strategies on Artificial Intelligence: A European perspective, 2021 edition”
(https://publications.jrc.ec.europa.eu/repository/bitstream/JRC122684/ai_watch_report_national_ai_strategies.pdf)よりNRI作成

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

スイスのAI関連制度・政策　(vi) 社会課題の解決：気候及び環境

- 次の30年で温室効果ガスの排出を削減するという目標は、環境目標を達成するためにAIの可能性を完全に利用するスイスの強力なインセンティヴを構成している。
- AI作業部会は明確に、AIを、栄養、ハウジング、モビリティシステムの生態学的要請を満たす重要な科学技術と見なしている。このため、必要なデータを容易に利用可能にし、バリューチェーン及び市場の情報フローに統合する試みが行われている。連邦参事会は、「スイス・エネルギーデータのためのハブ」に関する報告書を公開した。この報告書は、エネルギー部門における国家データインフラストラクチャーは、再生可能エネルギーの発展と統合を可能にし、エネルギー効率を上げ、気候変動に対応し、新たなビジネスモデルを支える、デジタイゼーションとイノベーションに必要不可欠であると強調している。
- 連邦環境局は、環境に関する情報が、AIアプリケーションのために利用可能なデジタルデータセットの中で公開され、利用可能であることを確保する。また、循環型経済の課題に対してAI関連の環境問題にも取り組んでいる。
- AI技術はエネルギー、食糧、消費財需要を予測するのに役立ちうる。さらに、AIには、環境及び社会的側面を含む生産エコシステムに関する情報を統合するのと同じくらい、原材料に関する情報を管理することによって、生産計画における非効率性を減らす可能性がある。AIは、最も安いだけでなく最も環境に配慮した商品を特定し購入するために、消費者に情報を分け与えることができる。

出所)European Commission “AI Watch - National strategies on Artificial Intelligence: A European perspective, 2021 edition”
(https://publications.jrc.ec.europa.eu/repository/bitstream/JRC122684/ai_watch_report_national_ai_strategies.pdf)よりNRI作成

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

スイスのAI関連制度・政策　(vi) 社会課題の解決：COVID-19パンデミック

- COVID-19パンデミックについて連邦公衆衛生局は、「スイスCOVID アプリ及びコンタクトトレーシング」を開始した。
- さらに、スイス熱帯公衆衛生研究所(Swiss TPH)には、同研究所におけるCOVID-19関連のウェブページがあり、そこにはAI及び機械学習の利用も含まれている。同研究所は、バーゼル大学の関連機関であり、公的な機関として部分的にスイス連邦参事会とバーゼル＝シュタット準州からの支援を受けている。特に以下のイニシアティヴが示されている。
  - MistraL(Mitigation strategies for communities with COVID-19 transmission in Lesotho using AI on chest x-rays and novel rapid diagnostic tests)
  - CORESMA(COVID-19 Outbreak Response combining E-health, Serolomics, Modelling, Artificial Intelligence and Implementation Research)
  - MODCOVID(Using model-based evidence to optimise medical intervention profiles and disease management strategies for COVID-19 control)このアプローチは数理的モデルと機械学習を、製品開発決定プロセスと組み合わせる。
  - リスク評価及びリスク対応を向上させるため、リアルタイム臨床データを提供し、確立したmHealthである SORMAS(Surveillance Outbreak Response Management and Analysis System)を配備する。

出所)European Commission “AI Watch - National strategies on Artificial Intelligence: A European perspective, 2021 edition” (https://publications.jrc.ec.europa.eu/repository/bitstream/JRC122684/ai_watch_report_national_ai_strategies.pdf)よりNRI作成

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

スイスのAI関連制度・政策　(vii) モニタリングと今後のアップデート

■ スイスにおけるAIの発展と配備の過程は、監視され評価される予定である。

出所)European Commission “AI Watch - National strategies on Artificial Intelligence: A European perspective, 2021 edition”
(https://publications.jrc.ec.europa.eu/repository/bitstream/JRC122684/ai_watch_report_national_ai_strategies.pdf)よりNRI作成

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

2021年4月に公表されたEUのAI規則案では、新設される加盟国のAI規制当局が、学習等に用いられたデータセットやAIシステムのソースコードにアクセスする権限が定められている。

- EUは2021年4月、AIに関する規則案を公表した。同規則案はAIの持つリスクに応じて、禁止されるAIやハイリスクAI等複数のカテゴリを設定し、各リスクに応じた規制を導入するものであるが、実体的な規制の内容についてはすでに多数の分析が存在するため、ここでは詳述しない。
- 他方、同規則案第64条第1項は、新設される加盟国のAI規制当局である、market surveillance authoritiesがAIの学習や認証、テストに用いるデータセットについて完全なアクセスを持つことを定める。
- また、同条第2項は、特にハイリスクAIの規制への適合を確認するため、当局がAIシステムのソースコードに対してアクセス権限を持つことを定めている。

Article 64 Access to data and documentation

1. Access to data and documentation in the context of their activities, the market surveillance authorities shall be granted full access to the training, validation and testing datasets used by the provider, including through application programming interfaces ('API') or other appropriate technical means and tools enabling remote access.
2. Where necessary to assess the conformity of the high-risk AI system with the requirements set out in Title III, Chapter 2 and upon a reasoned request, the market surveillance authorities shall be granted access to the source code of the AI system.

出所)European Commission, "Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS"

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

前頁記載の当局によるアクセス権限については、欧州の領域外に所在するデータのうち、欧州から管理可能なものについても及ぼされる可能性がある。

- 前頁記載の通り規則案第64条1項はリモートアクセス権限について規定している。仮に外国において開発されたAIが欧州で利用され、当該AIに対してこの権限が行使される場合、外国に所在するデータへのアクセスが行われる可能性がある。
- 同様に、同条第2項のソースコードアクセスについても、当該AIが外国に所在するコンピュータ設備等において実施されている場合、当該設備上のソースコードに対してアクセスが行われる可能性が指摘できる。
- なお、上記のいずれのアクセスについても、命令の名宛人はEUに所在する現地法人等となる。当局は罰則付きの命令を発出し、当該現地法人等が域外の管理権を持つデータにアクセスを行ってそれを当局に提出することとなる。したがって、当局が直接海外のサーバーなどにアクセスするものではなく、そのようなアクセスを外国の主体に強制する権限を持つものではない。

- 上記権限の運用については各国の規制当局にゆだねられるが、規制当局として指定されるものにはかなり小規模なものもあり、特に外国に所在するデータの提出はデータの所在国との問題を生じさせる可能性もあるため、実際に権限が行使される可能性は高くない、との弁護士の見解も存在する。

出所)データ保護を専門とする弁護士へのヒアリングよりNRI作成

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

EU加盟国レベルではAIを対象にした法的規制は導入されておらず、ソースコードやアルゴリズム開示を義務づける規定はないが、ドイツの政策文書ではそれを支持するものも存在。

- 各国の(iv)規制の項で記載した通り、調査対象国では、AIを対象とした規制はいまだ導入されておらず、政府の委員会等が発表する透明性等に関する原則等が定められているに過ぎない。
  - ただしGDPRにおける自動化された意思決定に関する規制など一部パッチワーク的に実装されている規制は存在。
- したがって、加盟国レベルでソースコードやアルゴリズム開示を義務付けるAIを対象とした規制は未だ導入されていない。
- ただし、加盟国内でもAI規則案と同様の議論は存在している。ドイツでは、データ倫理委員会が2019年12月に公表した報告書において、先にEUのAI規則が述べたものと同様、AI規制当局がアルゴリズムシステムに対するアクセスや監査の権限を有するべきであると主張している；

5.1.2 Definition of oversight powers according to the tasks involved
The regulating body should, by law, clearly assign the relevant competent authorities the powers of intervention, including rights to information and rights of inspection and access, required for the supervision of algorithmic systems. Blueprints for such regulatory powers for content control can be found in various areas of the law. The competent supervisory authorities must, at all times, be able to examine algorithmic systems in sensitive areas of application or those with a high potential for harm. The audit and test procedures used in doing so must, in particular, cover systems where there is interaction with the user. This may, for example, take place via standardised interfaces. Such access can be used to carry out what are known as input-output tests, which check, for example, whether an algorithmic system systematically discriminates against groups. This is particularly useful in the case of learning systems which adapt their internal rules over time. Steps must be taken here to ensure that any testing of learning systems does not lead to a change in the system of rules whereby the system learns from the test data during the test.

出所) Data Ethics Commission, "Opinion of the Data Ethics Commission" (https://www.bmi.bund.de/SharedDocs/downloads/EN/themen/it-digital-policy/datenethikkommission-abschlussgutachten-lang.pdf?__blob=publicationFile&v=4), p. 199.

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

②データ・人工知能等に関する主要企業・業界団体等

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

以下調査項目に基づき、データ・人工知能等に関するEUの主要業界団体に係る分析を実施。

調査項目

1. ICT関連のEUレベルの業界団体であるDigital Europeの加盟団体を中心として、調査対象国における業界団体について調査を実施した。
2. 上記業界団体の加盟企業等も参考としつつ、データの収集・分析・活用に関連する、下記の新興技術の開発・実装動向毎の企業動向を調査した。
   - 人工知能、量子技術、ブロックチェーン、生体認証技術(顔認証技術等)等
3. 特に政策と関連の深い企業をリスト化の上、当該企業に係る深掘り調査を実施した。
4. 政策実現への関与については、各国レベルのほか、EUレベルの政策・事業に参画している企業(GAIA-Xの実現を図っているInternational Data Spaces Associationの加盟企業等)について調査した。
5. 調査対象国に進出している、データ流通や人工知能の活用に関わる主要日系企業の動向を調査した。

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

②データ・人工知能等に関するEUの主要業界団体(ドイツ)

Bitkom(ドイツ IT・通信・ニューメディア産業連合会)

団体概要

基本情報

- 経済、社会、行政のデジタル化を提唱。
- エネルギー、モビリティ、貿易、スマートホーム、都市・自治体に対してギガビットネットワークやデジタルインフラ展開を支援。
- **データ・ドリブン・ビジネス、データ保護・サイバーセキュリティ、プラットフォーム、破壊的技術、Work4.0、デジタル時代の生涯教育に係る政策を支持。**

拠点

- ドイツ(ベルリン)

成立年

- 1999年

業界

デジタルエコノミーに関連する分野

- ソフトウェア
- テレコム
- インターネットサービス
- ハードウェアや家電製品
- デジタルメディア　等

会員企業

- **2,000社**以上のデジタルエコノミーに関わる企業
  (中小企業:1,000社、スタートアップ：500以上含む)

取組内容

取組内容

- Bitkomイベント：hub.berlin等のイベントを開催。
- Bitkomアカデミー：ITやデジタルトレンドに係る専門家やエグゼクティブ向けのトレーニングを提供。
- Bitkomコンサル：デジタルエコノミー関連企業に対して、公共入札への参加やデータ保護に関するアドバイスを提供
- Bitkoリサーチ：市場調査に関するアドバイスやコンセプト策定、フィールド調査の実施、マーケティングの高度化等。
  具体的には、**2021年4月に、「ドイツ企業の人工知能(AI)の利用状況に関する調査結果」を実施し、同団体会長アヒム・ベルク氏は、AI投資も重要性を指摘している。**
- ウィー・フルサービス(Weee full-service)：Bitkomは電子機器のメーカー、輸入業者、販売業者に対して、電子機器、バッテリー、パッケージの販売と廃棄に関する欧州全域のコンプライアンスソリューションを提供。
  *Weeeとは、Waste Electrical and Electronic Equipmentを指す。

重点領域

- デジタルトランスフォーメーション
- 教育・仕事
- データプライバシーとセキュリティ
- ソフトウェア
- スタートアップ
- 政治・法律
- マネジメント＆中小企業

参考)bitkom
https://www.bitkom.org/EN/About-us/About-us.html

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

②データ・人工知能等に関するEUの主要業界団体(ドイツ)

ZVEI(ドイツ電気・電子工業連盟)

団体概要

基本情報	• 広範かつダイナミックな製品ポートフォリオを持つドイツのハイテク産業の利益を代表するロビー団体。 • 研究、技術、環境保護、教育、科学政策に関する提案を行い、ZVEIは技術進歩のペースメーカーとして機能している。 • 市場関連の国際標準化活動も支援。
拠点	• ドイツ
成立年	• 1918年
業界	• 電気・電子産業 • デジタル産業
会員企業	• 電気・電子産業(Electrical industry)に関わる**1,600社以上の企業** • 電気・電子産業ロビー団体として、ドイツで2番目に大きい

取組内容

取組内容	• 意見交換：電気産業分野における現在の技術、経済、法律、社会・政治的な話題に関して、経験や見解を会員内で交換 • リサーチ・レポート作成：「リファレンスアーキテクチャモデル　インダストリー4.0」等 • 団体立ち上げ：近時の具体的は以下の通り。 **①「プラットフォーム・インダストリー4.0」を設立。(2013年)** **②産業データの共同利用に関する公益団体「インダストリアル・データ・スペース協会(Industrial Data Space Association」を設立。(2016 年)** **③インダストリー4.0のプラットフォーム「インダストリアル・デジタルツイン協会(Industrial Digital Twin Association、IDTA)」を設立(2020年)**
重点領域	• インダストリー 4.0 • サステナビリティ • モビリティ • ヘルス • 建築・建築物 • エネルギー • サイバーセキュリティ • 社会と環境 • 教育とリサーチ • マーケットと法律

参考)ZVEI
https://www.zvei.org/en/association/about-us/tasks-and-objectives/general

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

②データ・人工知能等に関するEUの主要業界団体(オランダ)

NL digital(Nederland ICT)

団体概要

基本情報	• NLdigitalの有する専門知識と知識を活用することで、の会員企業に対して質の高いサービスと機会を提供し、会員企業がソリューション提供や成長・収益性の達成において正しい経営判断下すための支援を実施。 • DXの実現のため、NLdigitalは、デジタル経済の中核を担い、他の会員企業がデジタル化するために必要な製品・サービスを共同にて提供。
拠点	• オランダ
成立年	• 不明
業界	• 情報通信技術 • 電気通信
会員企業	• **ICT関連企業の625社以上。** • 多国籍企業から中小企業を含む。**オランダのデジタル関連の業界団体として、最大規模**である。

取組内容

取組内容	• 市場促進(Market Promotion)： ワークショップや懇親会等を含む年間100件以上のネットワークイベントの開催 • アドボカシー(advocacy)： 様々なテーマ毎のメンバーネットワークによる活動 • 個別サービス(individual services)： アドバイス、支援、質問対応等を年間約900件実施 (法的領域等)
重点領域	• デジタルトランスフォーメーション • 教育のデジタル化 • ICT労働市場の改善 • デジタルレジリエンス • デジタルガバメント • デジタルインフラ • カーボン・ニュートラルなデジタル部門 • 支援・復興 • インクルーシブなデジタル部門 • データの責任ある利用 • 現代の知的財産・著作権等

参考)NL digital
https://www.zvei.org/en/association/about-us/tasks-and-objectives/general

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

②データ・人工知能等に関するEUの主要業界団体(フランス)

AFNUM(Alliance Française des Industries du Numérique：フランスデジタル産業連盟)

団体概要

基本情報	• インフラ、インテリジェントシステム、デジタル消費財等の「デジタル社会の基盤」に係る企業を集め、フランスの経済成長と社会的課題において重要な役割を果たすデジタル部門における主要な専門組織が新設。 • テレビ、通信機器・端末、写真、コンピュータ、印刷を代表する歴史ある組合、GITEP TICS、SFIB、Simavelec、USPIIが合併により、AFNUMが組成。
拠点	• フランス
成立年	• 2015年
業界	• テレビ • 通信機器・端末 • 写真 • コンピュータ • 印刷　等
会員企業	• **上記業界の3,000以上の企業** (多国籍企業とフランスの中小企業) • AFNUMは、**フランスの主要な貿易連盟である FIEEC**(Fédération des Industries Électriques, Électroniques et de Communication)**の一部である。**

取組内容

取組内容	• ワーキンググループ組成：重点領域は以下の通り。
	  • 私的複製
	  • データ＆セキュリティ
	  • 環境・CSR
	  • 電波と健康関連規制
	  • 人工知能
	  • 法的事項
	  • 公共部門
	  • サービス＆テクノロジー
	• **政策提言：**
	  • **デジタルサービス法パッケージ(Digital Services Act package)に対する提言(2021年5月5日)**
	  →デジタル市場法案を歓迎
	  • **データフローに関するG7会議に対する提言(2021年5月20日)**
	  →他の業界団体と共に、G7に対して越境データフローをサミットの最優先事項とするよう要請
	  • **AI規則(Artificial Intelligence Act)に係るフィードバック(2021年7月28日)**
	  → AI規則を歓迎

参考)AFNUM
https://www.zvei.org/en/association/about-us/tasks-and-objectives/general

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

②データ・人工知能等に関するEUの主要業界団体(フランス)

Numeum

団体概要

基本情報

- Syntec NumériqueとTECH IN Franceの合併により誕生した、フランスにおけるデジタルエコシステムに係る専門業界団体。
- 本合併を機に会員企業、特に中小企業やスタートアップ企業を支援するサービスの提供することが可能となった。
- 行動方針は以下の通り。1)会員及び事業の促進、、2)自団体の利益保護、3)**デジタル・フランス**の欧州での具現化、4)デジタルエコシステムの活性化に基づくシナジーとイノベションの促進、5) デジタル企業向けサービスの強化

拠点

- フランス

成立年

- **2021年6月17日**

業界

- デジタルサービス
- ソフトウェア
- プラットフォーム
- エンジニアリング/テクノロジーコンサルティング　等

会員企業

- **2,300社以上の企業が参加。(フランスにおける当該領域の総売上高の85%に相当)**

取組内容

取組内容

- デジタル技術の経済的・社会的重要性の普及啓発
- デジタル専門職の魅力の向上/専門職の補助
- 企業のニーズの代弁
- デジタル専門職の保護
- エコシステムの活性化
- 研修と雇用促進

注力領域

- デジタルでの女性活躍
- デジタルに係る責任
- デジタル職の魅力向上
- インターナショナル
- スタートアップ
- イノベーションとテクノロジー
- サイバーセキュリティ
- 健康
- 都市・地域
- 新しい産業
- 経済/市場
- Covid-19
- 研究開発

デジタル共和国戦略

- 経済成長、雇用の伸長及び国際社会での地域強化の鍵は官民双方のデジタル・サービスの発展にあるという認識の下、2015 年 6 月に仏政府により公表された。
- 「デジタル・サービスの提供モデルとしての国家」等、4 つの主要方針の下で、14 の政策の行動計画を提示している。
- 仏政府は 2000 年代から数年ごとにデジタル社会化に対する一連の行動計画を提示してきた。
  - 「デジタル・フランス 2008」(サルコジ政権)
  - 「デジタル・フランス 2012-2020」(サルコジ政権)
  - 「デジタル化に関する政府活動ロードマップ」(オランド大統領)

参考)Numeum　https://numeum.fr/
総務省　平成28年版 情報通信白書
(https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h28/pdf/n6b00000.pdf)

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

②データ・人工知能等に関するEUの主要業界団体(フランス)

Numeum　Executive Directorに対するヒアリング

■ フランスと欧州のデジタル化の最優先課題は何か？(DIGITALEUROPE)

- **第一に、欧州での巨大IT企業を育成するために、好ましい規制環境を構築することである。**イノベーションに不必要な障壁を設けるのではなく、前述の目標をサポートするような政策的な取り組みが必要である。以下の法案が、重要な試金石となるため、その影響に細心の注意を払っていきたい。
  - **デジタルサービス法(DSA：Digital Services Act)**
  - **デジタル市場法(DMA：Digital Markets Act)**
  - **AI規則(Artificial Intelligence Act)**
  - **データ法(Data Act)等**
- **第二に、特にスキル不足の時代において都市と農村の格差の解消を含め、より良いデジタル教育、再教育、そしてすべての人のためのより良いキャリアを引き続き推進する必要がある。**この点については、次期フランス大統領任期中に、また任期中に、私たちNumeumは、より多くの提言等を行予定である。(Philippe Tavernier氏　Executive Director of Numeum)

■ EU理事会(閣僚理事会)の次期議長国がフランスであることは、欧州のデジタル移行において重要な役割を果たすと考えているか？どのような優先事項やマイルストーンが重要になるのか？(DIGITALEUROPE)

- EU理事会の議長国フランスは、欧州のデジタル・アジェンダを加速させる機会だと考えている。フランスの議長国としての優先課題は、今秋以降に発表されるが、**DMA、ネットワークと情報システムのセキュリティに関する指令の改訂(NIS 2：Directive on Security of Network and Information Systems)、データガバナンス法(Data Governance Act)等**、この6ヶ月で大きく進展する可能性がある事例となるだろう。また、フランスは、サイバーセキュリティ、AI、この夏に発表された気候変動対策パッケージに関する議論も進めることになる。
- 同時にフランスは、オーバーラップする議題に直面することになる。2022年4月上旬の大統領選挙により、議長国としての交渉に割く時間が短縮され、3月中には検討がスローダウンすることが予想されます。(Philippe Tavernier氏　Executive Director of Numeum)

参考)Digital Europe　"France has turned into a breeding ground for unicorns": meet Numeum's Executive Director Philippe Tavernier
(https://www.digitaleurope.org/news/france-has-turned-into-a-breeding-ground-for-unicorns-meet-numeums-executive-director-philippe-tavernier/)

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

②データ・人工知能等に関するEUの主要業界団体(フランス)

SECNAVI(Syndicat des Entreprises de Commerce International de Matériels Audio, Vidéo et Informatique)

団体概要

基本情報	• 輸入業者や海外企業のフランス支社による特定の要求に応えるために、設立された専門組織 • SCNAVIは、FICIME(the Federation of International Companies in Mechanics and Electronics：国際電機・電子事業者連盟)と提携
拠点	• フランス
成立年	• 1984年
業界	コンシューマーエレクトロニクスに関わる全ての業界 • テレビ、ビデオ、デコーダー、IT、電話機、プリンター、オーディオ、HiFi、コネクテッド機器、白物家電等
会員企業	• 30社以上の企業が参加。 (中小企業・大企業問わず)

参考)SECNAVI
(https://www.zvei.org/en/association/about-us/tasks-and-objectives/general)
(http://www.secimavi.org/uploads/9/6/8/3/9683840/secimavi_2018_-_en.pdf)

取組内容

取組内容

- ミーティング：Technical & Marketing Commission、After-Sales, Products and Regulatory Commission、Car Radio Club
- マーケット分析：コンシューマーエレクトロニクスの半期トレンド、製品群に係るターゲット分析、輸出入に係る四半期分析、月平均為替レート分析　等
- ワーキンググループ・委員会・ロビー活動参加：

① テクノロジー
- UHD / HDR / HFR
- DVB-T2 / HEVC
- HbbTV
- DAB+デジタルラジオ
- UHF帯放送

②周波数割当
- 国内外への国際ワーキンググループ傘下

③環境
- エネルギー効率ラベル
- 製品のエコデザイン
- EEAのライフサイクル
- 家庭用WEEE

④リーガル
- 私的録音録画補償金
- 低電圧、EMC、RED

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

②データ・人工知能等に関するEUの主要業界団体(スイス)

Swico(Swico Recycling)

団体概要

基本情報	• Swico Recyclingは、情報科学、家電、オフィス、通信、グラフィック産業、計測・医療技術などの分野で使用された廃棄電子・電気機器を引き取るための全国規模の非営利システム
拠点	• スイス
成立年	• 1994年

取組内容

取組内容	• Swico Recycling system： Swico Recyclingは、廃棄機器の引き取りを行う自主的な協同システム。1994年以来、スイスのIT、事務機器、家電、写真・フィルム分野のメーカーや輸入業者によって運営され、成功を収めている。

参考)Swico　(www.swico.ch)

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

新興技術の開発・実装動向に関係する企業動向(人工知能)

■ドイツでは、製造業大手を中心に進むAI導入が進む

名称	取組概要
ドイツ人工知能研究センター(DFKI)	1988年設立、ドイツのAI分野研究を主導する中核的な研究センター。官と民が出資する非営利有限会社。応用を念頭に置いた基礎研究を進めており、情報通信技術の分野で機能の開発、プロトタイプ開発および特許化など行う。研究開発プロジェクトは、19の研究部門と研究グループ、8つのコンピテンスセンター、8つのリビングラボで行われている。
Bosch	自動車部品大手。AIの技術開発に積極姿勢を打ち出す。2017年初めに、最先端のAIテクノロジーをボッシュの製品やサービスに展開してソリューションを生み出すために、ボッシュ人工知能センターをドイツ南部のレニンゲンに設立。
Amazon	2017年10月、チュービンゲンにAI研究施設の開設を発表。また、AI研究に取り組むシーメンスと提携と提携し、IoT(モノのインターネット)向け基本ソフトをアマゾン・ウェブ・サービスを通じて提供することで、工場デジタル化市場での地位強化を狙う。
IBM	米国IT大手。グローバルIoT本社を2015年にミュンヘンに設立しており、2017年2月には、2億ユーロを投じ、フランス金融大手のBNPパリバ、米国電子機器部品のアヴネット、フランスITコンサルティングのキャップジェミニ、インドのテック・マヒンドラといった企業も入居するIoT研究開発施設を開所。専門家1,000人が業務に当たり、IBMの顧客であるBMWなどの企業とのIoTや人工知能などによる協業を推進する。
Microsoft	米国IT大手。米国や中国に続く、欧州・中東・アフリカIoT＆AI拠点として、2017年4月にミュンヘンにIoT・AIインサイダー・ラボを設立。スタートアップ企業は同社の持つAI技術を活用し、また専門的アドバイスを受けることによって、製品やサービスの試作などを支援、成長を後押しする。

出所)JETRO 製造業大手を中心に進むAI導入(ドイツ)
(https://www.jetro.go.jp/biz/areareports/special/2019/0502/f30fadfcde4071cc.html?_previewDate_=null&revision=0&viewForce=1&_tmpCssPreview_=0%2F%2F)

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

新興技術の開発・実装動向に関係する企業動向(量子技術)

■ 2021年6月10日、量子コンピュータの自動車、化学・医薬品分野などでの活用を探るため、「量子技術活用コンソーシアム(QUTAC)」が設立された。

■ **QUTACに参加する企業12社；**

BASF	総合化学メーカー
BMW Group	自動車メーカー
Boehringer Ingelheim	製薬会社
Bosch	自動車部品メーカー
Deutsche Telekom AG	電気通信事業者
Infineon	半導体メーカー
Lufthansa Industry Solutions	IT企業
Merck	製薬会社
Munich Re	保険サービス企業
SAP	ソフトウェア企業
Siemens	製造・ソリューション企業
Volkswagen	自動車メーカー

参考)JETRO　ドイツ初の量子コンピュータが稼働、大手企業は産業利用を探るコンソーシアムを設立(ドイツ)
(https://www.jetro.go.jp/biznews/2021/06/9706afbba1332132.html)

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

新興技術の開発・実装動向に関係する企業動向(ブロックチェーン)

■ Forbesは、「Blockchain 50 2021」を発表。内、調査対象国に該当する企業と取組概要は以下の通り。

国	企業名	取組概要
フランス	Carrefour	Carrefourは、養殖卵、ノルウェー産サーモン、チーズ等の30以上の商品群に対してブロックチェーン技術で追跡をしています。これらの商品にはQRコードが付けられており、顧客はこれをスキャンし、食品の産地について詳しく知ることができる。Carrefourは、この機能によって売上を伸長させ、今後100の製品ラインに拡大することを目指している。
フランス	LVMH	LVMHは、ブロックチェーンを使用して製品を追跡し、ルイ・ヴィトンやブルガリなどのブランドの偽造品に対抗している。プラダやリシュモンのカルティエと共同で作ったこのプラットフォームには、1000万点近い高級品が登録されている。
ドイツ	Daimler	メルセデス・ベンツの高級車メーカーであるDaimlerは、生産から最近の資金調達まで、すべてをブロックチェーンで効率化している。
スイス	Credit Suisse	Credit Suisseはブローカーかつディーラーの野村インスティネットとの米国上場株取引の決済にパクソス・セトレッジ・サービス(Paxos Settlement Service)を利用している。ブロックチェーン技術により、参加者は従来の仲介業者を介さず、互いに直接取引を決済することができ、通常2日かかるところを即日決済が可能となる。
スイス	Novartis	Novartis は、自主回収の最大の理由である、処方箋の添付文書の誤記、古い情報の記載等を対象とするEUのブロックチェーンコンソーシアム、PharmaLedgerの主要メンバーである。ノバルティスは、メルク、マドリード工科大学とともに、医薬品のパッケージをスキャンしてメーカーに最新の情報をリアルタイムで要求し、患者がスキャンコードからアクセスできるアプリを構築しました。また、PharmaLedgerは、偽造医薬品や闇市場に対抗するために本技術を利用している。
スイス	Swisscom	Swisscomは、暗号株式発行のスタートアップDauraや、デジタル資産銀行Sygnumとの合弁会社である暗号カストディ会社Custodigitなど、様々な段階の11のブロックチェーン・アプリケーションを有しています。2020年11月には、金融機関のデジタル資産の作成、保管、取引を支援するFireblocksへの3000万ドルの投資を実施。
オランダ	ING Group	ING Groupは、ブロックチェーン技術をいち早く取り入れた銀行の一つであり、現在、暗号資産を認証し、国際的なマネーロンダリング防止基準に準拠させるために、他の金融機関のグループをリードしている。

出所)Forbes　Blockchain 50 2021(https://www.forbes.com/sites/michaeldelcastillo/2021/02/02/blockchain-50/?sh=343a9978231c)

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

②データ・人工知能等に関するEUの主要業界団体

新興技術の開発・実装動向に関係する企業動向(生体認証技術)

■ 生体認証(biometrics)技術に関連する企業一覧を作成。(肌色：売上高等の決済情報が開示されている企業)

■ ソフトウェアサービス、情報セキュリティに限らず多様な業種にて、生体認証が活用されている。

国	業種	企業名	企業概要
フランス	防衛	Safran Electronics & Defense SAS	Aviation navigation instruments manufacturer
フランス	種苗	RAGT Semences SAS	Corn production services, Seed production services, Sunflower production services, Wheat production services
フランス	ソフトウェアサービス	Another Brain	Another Brain is an artificial intelligence startup that develops AI in a way far beyond deep learning. (Source: Crunchbase)
フランス	バイオ・医薬品製造	Biologie et Industrie	Biologie et Industrie SAS, a biotechnology company, provides clinical research solutions in Europe and the United States. (Source: Crunchbase)
フランス	バイオ・医薬品製造	BIOTRIAL RENNES	Research and Development in the Physical, Engineering, and Life Sciences (except Biotechnology)
ドイツ	情報セキュリティ	Secunet Security Networks AG	Secunet Security Networks AG is an IT and telecommunications security provider.
ドイツ	電子部品・デバイス製造	IDEMIA Germany GmbH	Biometrics equipment manufacturer
ドイツ	バイオ・医薬品製造	MedPharmTec-Services	MedPharmTec-Services is a Pharmaceutical Contract Service Organisation providing expert assistance in drug development. (Source: Crunchbase)
チェコ	決済処理サービス	Worldcore	Worldcore is a Czech-based regulated payment institution offering wide range of payment solutions for everyone (Source: Crunchbase)
スイス	情報セキュリティ	BioID	BioID develops high-quality multimodal biometric authentication solutions (face and voice). (Source: Crunchbase)
スイス	情報セキュリティ	Eliametrix	Eliametrix is a biometrics access solutions, authentication, consulting, cyber protection / IT security services, and research company. (Source: Crunchbase)
スイス	防災・防犯機器	Keso	Keso is manufactures and distributes mechanical and electronic security cylinders for doors and industrial applications. (Source: Crunchbase)
スイス	ソフトウェアサービス	Spitch	Spitch is a global provider of B2B and B2C Conversational AI solutions (Source: Crunchbase)
スイス	ソフトウェアサービス	TECH5 SA	Biometrics-driven identity management software developer
オランダ	ソフトウェアサービス	Meltwater BV	Online media intelligence and social analytics Software-as-a-Service (SaaS) provider holding company
オランダ	ソフトウェアサービス	Neurolytics	SaaS Computer Vision (Source: Crunchbase)

参考)SPEEDA にて企業リストを作成。

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

②データ・人工知能等に関するEUの主要業界団体

新興技術の開発・実装動向に関係するスタートアップ動向(人工知能)

- マクロン大統領は2018年にAI国家戦略を公表し、AI研究開発に15億ユーロが投資。
- フランスの注目AI関連スタートアップ20社(20 French AI startups)の内、技術の観点で特徴のあるスタートアップを深掘りスタートアップとした。

社名	創業年	概要
anotherBrain	2017年	ディープラーニングを代替する「オーガニックAI」を開発中。同社は、人間の脳の構造からヒントを得て、データ処理・エネルギーをより節約し、プライバシーを保護する技術を構築。
Zelros	2016年	営業戦術に特化した保険業界専用のAI搭載ビジネスプラットフォームを構築中。
Owkin	2016年	創薬や精密医療分野の加速を目指し、医療研究に応用したAIを構築中。
Hyperlex	2017年	文書の重要な情報を特定し解釈することができる言語処理技術を開発し、リーガルテック向けAIを活用した契約書の作成・締結・分析プラットフォームを提供。
Hugging face	2016年	人工知能を搭載したバーチャルフレンドとチャットできるモバイルアプリを作ったことで注目された。言語処理に係るAIを開発。
Exotec	2014年	ロボットをベースにした受発注準備システムを構築中。
Synapse Medicine	2017年	医薬品に関する情報源に基づき、AIを使用し、患者毎にソリューションを提供する。
Shift Technology	2013年	保険業界向けに設計された不正検知技術を開発中。
Cardiologs	2014年	医療従事者が患者の心臓疾患をスクリーニングするのを支援。2020年1月に最新の資金調達ラウンドを実施。
Yseop	2008年	データをレポートや専門知識に変換するための自然言語生成ソリューションを、多言語かつリアルタイムで提供する。
Shippeo	2014年	道路輸送のためのAIを搭載した追跡システムを構築中。
Tinyclues	2010年	マーケターが顧客データベースからより多くの収益を上げるために構築された、AIを活用したターゲティングソリューションを提供。広告キャンペーンで適切なオーディエンスにリーチするためのマーケティングツール。
Prevision.io	2016年	エンタープライズAIプラットフォームを構築中。即座に使用可能なビジネスアプリケーションを通じて、あらゆる企業をAIファーストにするための自動機械学習ソフトウェアを提供。
Kayrros	2016年	データサイエンス、機械学習、コンピュータビジョン、大気モデリングにおける最先端の独自AI技術および、業界の深い専門知識を融合させたスタートアップ。
Prophesee	2014年	AIを使用して目や脳を模倣する技術を開発中。自律走行車、産業オートメーション、モノのインターネット、セキュリティ、監視、さらに、拡張現実やバーチャルリアリティ等の分野をターゲットにしている。初期の応用例としては、目の不自由な人の視力を回復させる医療機器への応用事例がある。
Cosmo Tech	2011年	産業界の企業が業務効率をシミュレーションし、最適化するための企業向けソフトウェアを開発中。
Craft AI	2015年	モバイル、ウェブ、モノのインターネットアプリケーションの開発者向けにAI-as-a-serviceを提供。
Deepomatic	2014年	企業が日常業務等の事務作業能力を補強することを可能にする。
Levia	2018年	会話型のAI技術を構築し、データベースを使用して、複雑な要求に人間のような自然な言葉で答えるためのメッセージングインターフェース(チャットボット型ソリューション)を構築。
Vekia	2008年	サプライチェーンの複雑な問題をモデル化し、最新の研究の進歩をベースとしたプランニング・ソフトウェアを開発中。

参考)sifted　20 French AI startups to watch(https://sifted.eu/articles/ai-startups-france/)

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

②データ・人工知能等に関するEUの主要業界団体

調査対象企業の選定

※赤字は、個票にて深掘りを行った企業/スタートアップ

技術	関連テーマ	深掘りの方向性	①の政策との関連	調査対象企業
ブロックチェーン	①クリプトバレー(スイス)	クリプトバレーにはブロックチェーン企業が800社以上集積。欧州委・スイス政府は**イノベーションを阻害しない金融規制や(規制の)サンドボックス制度**の検討を推進。	• 個人情報保護	• CreditSwiss(スイス) • Swisscom(スイス) • ING(オランダ)
	②デジタルプロダクトパスポート(欧州)	欧州委等は資源効率性プラットフォームを発足させ、**デジタルプロダクトパスポートによるサーキュラリティの可視化**を提案	• (非個人データに係る、公益目的の)GA	• Daimler (ドイツ) • Novartis(スイス)
クラウド基盤	③Gaia-Xサブプロジェクト GXFS(欧州)	**ユーザーのデジタル主権を強化する**サブプロジェクトGaia-X Federation Serviceを開始し、分散型IDの検討を、Vereign(スイス)・DAASI(ドイツ)主導で推進。	• 個人情報保護	• Vereign(スイス) • DAASI International(ドイツ)
	④Gaia-X(欧州)・Sovereign Cloud(ドイツ/フランス)	Scaleway(フランス)は、「**Gaia-Xは米系・中華系CSPの影響を強く受けており、本来のGaia-Xの目的を達成できていない**」として、Gaia-Xを脱退。 一方、各国レベルの取り組みとして**T-Systems(ドイツテレコム子会社)とOrange(フランス)は、Google Cloudに係るGoogleとのパートナーシップ締結を発表。また、Orangeは、Capgemini(フランス)及び、MicrosoftとのAzureに係るパートナーシップ締結を発表。**	• データローカライゼーション(仏国家クラウド戦略等)	• Scaleway(フランス) • T-Systems(ドイツ) • Orange(フランス) ※旧フランス・テレコム
量子技術	⑤QUTAC(ドイツ)・QuIC(欧州)	量子技術の先端技術、ユースケース、政策や法整備、標準化に係るコンソーシアムが欧州・ドイツで発足。	• AI関連制度・政策(処理を高速化)	• SAP(ドイツ) • Siemens (ドイツ)
人工知能	⑥AI国家戦略(フランス)	マクロン大統領は2018年にAI国家戦略を公表し、研究開発に15億ユーロが投資。国家の支援を受ける投資機関Bpifranceも積極投資。	• AI関連制度・政策	• anotherBrain、Owkin、Prophesee(フランス・スタートアップ)
生体認証	⑦顔認証等の禁止(欧州)	欧州委は、2021年AIに関する規制枠組みとなる規則案を発表。公共の場で顔認証技術を捜査に利用すること等が原則禁止とされた。	• 個人情報保護 • ガバメントアクセス	• N/A

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

②データ・人工知能等に関するEUの主要業界団体

調査対象企業と各国の政策の実行、抵触・変更の関係性

技術	#	企業名	国	概要	政策の実行	事業と政策の抵触・変更
ブロックチェーン	1	Credit Swiss	スイス	世界最大規模の金融コングロマリット	クリプトバレー政策下で、スイス経済相はUBSやクレディ・スイスなど民間金融大手を集め、3億フランの基金設立を呼びかけられている。	ブロックチェーン上のセキュリティメカニズムを通じたトラストの構築を一層強化していく可能性がある。
	2	ING Group	オランダ	オランダのアムステルダムに本社を置く、銀行業を中心とした世界的な金融グループ	INGグループは、分散型台帳技術(DLT：Distributed ledger technology) を用いたプラットフォームを開発。また、デジタル署名について、どのようなセキュリティメカニズムを追加すべきであるかに係る検討を行う。	ブロックチェーン上のセキュリティメカニズムを通じたトラストの構築を一層強化していく可能性がある。
	3	DAIMLER	ドイツ	1926年にベンツとダイムラー・モトーレン・ゲゼルシャフトが合併して設立した多国籍自動車企業	オーシャンプロトコルは、民間初の企業がデータを共有して収益化できる分散型データ交換プロトコル。本件との直接的な関連性は限定的であるが、欧州委員会は、B2B等のデータ共有を推進するイニシアティブCommon European Data Spaceを推進。	B2B、B2Gデータ共有等のスキームにより一層対応する可能性がある。
クラウド基盤	5	T-Systems	ドイツ	ドイツテレコム傘下のシステムインテグレータ	GAIA-Xやその前段となるSovereign Cloudをドイツ政府と連携して実施	ドイツ政府機関と難民申請の過程管理を行うブロックチェーン技術の実証を実施しGDPR整合性等を検討している。
	6	Orange	フランス	フランスの最大手通信事業者であるが、システムインテグレーション等の事業も展開	GAIA-Xやその前段となるSovereign Cloudをフランス政府と連携して実施	フランスの国家戦略実現に向け、Sovereign Cloud事業をマイクロソフト等と提携して提供予定である。
量子技術	7	SAP	ドイツ	ビジネスプロセス管理の分野で世界有数のソフトウェアメーカー	量子技術の先端技術、ユースケース、政策や法整備、標準化に係るコンソーシアムを発足。Trusted Cloud Principles(信頼できるクラウド原則)に意見提出。	量子技術に係る業界分野規制の検討を踏まえ、当該事業が変化していく可能性がある。クラウドに対するデータアクセスについても影響を受ける可能性がある。
	8	SIEMENS	ドイツ	多様な業界の製造及びシステムソリューション事業を幅広く展開。	量子技術の先端技術、ユースケース、政策や法整備、標準化に係るコンソーシアムを発足	量子技術に係る業界分野規制の検討を踏まえ、当該事業が変化していく可能性がある。

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

調査対象企業と各国の政策の実行、抵触・変更の関係性

技術	#	企業名	国	概要	政策の実行	事業と政策の抵触・変更
人工知能	8	Anotherbrain(スタートアップ)	フランス	ディープラーニングを代替する「オーガニックAI」を開発。同社は、人間の脳の構造からヒントを得て、データ処理・エネルギーをより節約し、プライバシーを保護する技術を構築。	プライバシーの保護に配慮し、GDPRに準拠し、AI技術を展開している。 クラウドプラットフォームへの接続を必要としないため、ガバメントアクセス等を回避することが可能である。また、説明可能なAI・アルゴリズムの透明性に配慮。	N/A （GDPR等のデータ保護規制には現状対応しているため、事業と政策の抵触・変更は確認できなかった。）
	9	Owkin(スタートアップ)	フランス	創薬や精密医療分野の加速を目指プラットフォームパートナー企業に提供し、探索・開発プロジェクトの加速を支援。	プライバシーの保護に配慮し、自社サービスを設計。「ローカルデータのサンプルを保持する複数の分散型エッジデバイスやサーバー間で、データ交換を行わず、アルゴリズム学習を行う機械学習技術」である連合学習(Federated Learning)の手法を活用したグローバル研究ネットワークと連携し、これまでにないプライバシー保護型の研究手法を推進。	N/A （データ保護規制には現状対応しているため、事業と政策の抵触・変更は確認できなかった。）
	10	Prophesee(スタートアップ)	フランス	神経工学の技術を応用し、マシンビジョンに革新を起こすセンサーの実用化に成功。	N/A	同社は、自動運転車、産業オートメーション、IoT、セキュリティと監視、AR(拡張現実)/VR(仮想現実)等にて、センシング技術を活用し、データを取得しているため、データ法案が定めるB2B、B2Cのデータ共有に対する対応を進めている/進めいていく可能性がある。

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

②データ・人工知能等に関するEUの主要業界団体

CREDIT SUISSE

基本情報

社内	CREDIT SUISSE
CEO	Thomas Gottstein (2020年2月14日-)
概要	クレディ・スイスはチューリッヒに本社を置くユニバーサル・バンクあるいは世界最大規模の金融コングロマリット。グローバルに大規模な事業展開をする欧州系投資銀行の一角を成す。
特筆すべき事項	• 2021年10月： クレディ・スイスは、イーサリアム(ETH)ブロックチェーンを利用し、スポーツリゾート企業の株式トークン化を支援することを発表 • 2021年4月： クレディ・スイスは、野村傘下インスティネットとの米株式取引の「同日決済(T+0)」に成功。本決済は、米パクソス・トラスト・カンパニーが提供するパクソス・セトルメント・サービス(ブロックチェーンを利用した同社決済サービスを利用)

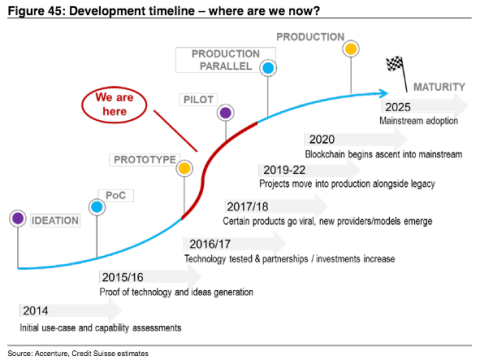
技術的な特徴

ブロックチェーン

強み

- 2015年には、クレディ・スイスは、グローバル大手銀行群と共同でのブロックチェーンの派生技術を用いたプロジェクトに参画している。本プロジェクトの狙いは、ブロックチェーンやその派生技術の業界標準規格を検討し、金融セクターへの新技術の採用を促進しネットワークを構築することである。

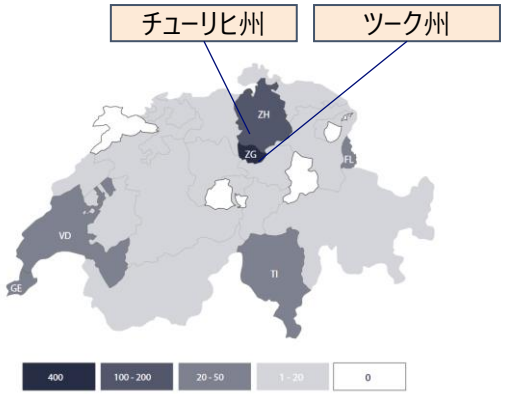
- 2018年時点で、クレディ・スイスは、ブロックチェーンの発展段階を予測しており、2025年にブロックチェーン技術が成熟期を迎えると見ている。



政策関連事項

1 クリプトバレー

- チューリヒ及び近郊ツーク州は、企業への税制優遇、工科大学や応用科学大学の存在により、フィンテック企業の集積が進む。
- 特にツーク州は、ブロックチェーン「イーサリアム」を運営する財団(イーサリアム財団)や、350以上の仮想通貨関連事業者が本籍を置いており、世界屈指の仮想通貨関連企業の集積地として「クリプトバレー」と呼ばれている。ツーク州政府もブロックチェーン技術を用いた起業を支援しており、住民の電子番号導入や、2018年7月には住民投票にブロックチェーン技術を用いたシステムの実証試験を実施。
- スタートアップ企業の成長局面を支援するために、**シュナイダー・アマン経済相はUBSやクレディ・スイスなど民間金融大手を集め、3億フランの基金設立を呼びかけている。**



(参考)CVVC Insights　The Cypto Valley's Top 50 H1 2019

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

②データ・人工知能等に関するEUの主要業界団体

ING Group

基本情報

社内	ING Group 
CEO	Steven van Rijswijk (2020年7月1日–)
概要	INGグループは、オランダのアムステルダムに本社を置く、銀行業を中心とした世界的な金融グループ。1991年から2016年までは、保険業と銀行業が融合された世界的な金融コングロマリットであったが、2000年代後半の世界金融危機により、INGが経営危機に陥り、その再建策として、全ての保険部門（資産運用業務を含む）と米国部門(ING U.S.)の売却が行われた
特筆すべき事項	• 2020年12月： イーサリアムブロックチェーンでトークン発行、デジタル資産のテストを実施 • 2019年12月： INGブロックチェーンチームの支援により、証券貸付プラットフォームが商業的にライブ化され、コメルツ銀行、クレディ・スイス、UBSとの初の商業的ライブ取引を実行。 • 2018年： INGとHQLAxは、クレディ・スイスとともに、R3 Cordaブロックチェーン・プラットフォーム上のHQLAx証券貸付アプリを利用し、初のライブ取引を実行。

技術的な特徴

ブロックチェーン

強み

- INGグループは、多数のブロックチェーンプロジェクトに投資。例えば、イーサリアムを拡張したパーミッション型ブロックチェーン「GoQuorum」を活用した貿易取引プラットフォームを提供するKomGo SAと連携し、2019年7月に、初の商品取引を実行。
- INGは、ABN AMRO、BNPパリバ、Citiバンク、Société Générale、UBS等と共同でデジタル資産ポストトレード市場インフラストラクチャであるPyctorを開発。
- Pyctorが提供するインフラは、顧客が規制に準拠した方法でデジタル資産を安全に発行、アクセス、管理することが可能となる。

政策関連事項

1 ブロックチェーンによる鍵管理・デジタル署名

- INGグループは、分散型台帳技術(DLT：Distributed ledger technology) を用いたプラットフォームを開発しており、マルチパーティ計算(MPC ：Multiparty computation)と呼ばれる暗号化技術に注力。DLTプラットフォームにおける鍵の管理を容易にすることを目指す。
- また、デジタル署名について、どのようなセキュリティメカニズムを追加すべきであるかに係る検討を行う。

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

②データ・人工知能等に関するEUの主要業界団体

DAIMLER

基本情報

社内	DAIMLER 
CEO	Ola Källenius (2019年5月22日–)
概要	DAIMLER(メルセデス・ベンツ・グループAG)はドイツ シュトゥットガルトに本拠を置く多国籍自動車企業。1926年にベンツとダイムラー・モトーレン・ゲゼルシャフトが合併してダイムラー=ベンツが設立された。
特筆すべき事項	• 2021年 5 月：Daimlerの金融・イノベーション部門子会社Daimler Mobility AGが自社ブロックチェーンプラットフォームMobility Blockchain Platformのライセンスをモビリティ関連のスタートアップであるbloXmoveに付与 • 2020年 9 月：Daimlerは、ブロックチェーンを活用したモビリティ・プラットフォームMoveXを発表。普段車とは異なる車両でも、オーディオやシート、ライトなどの設定の引継ぎが可能。 • 2018年 3 月：Daimlerは、安全で環境にやさしい運転に対して報酬を与えるために、MobiCoin(仮想通貨)を発行

技術的な特徴

ブロックチェーン

強み

- **ブロックチェーンによるサプライチェーン管理**
  カーボンニュートラル：Mercedes-BenzとCirculorは、ブロックチェーンを用いたCO2排出量に透明性を担保するパイロットプロジェクトに取り組む。具体的には自動車のバッテリーなどで使用する"コバルト"のサプライチェーンをブロックチェーンで管理することによって、リサイクル材料やガス排出量を追跡。
  児童労働問題対応：
  労働条件・人権・環境保護・安全性・企業論理・コンプライアンス等に関する情報を確認するために、ブロックチェーンは活用される。

弱み

- Daimlerのブロックチェーン技術自体に係る優位性は限定的である。また、自動車業界では、ブロックチェーン技術でコバルトのサプライチェーン管理を行う企業が増加傾向にあり、Volkswagen、Ford、VOLVO等も同様のプロジェクトを発表済み

政策関連事項

1 **Ocean Protocol (ブロックチェーンデータ共有)**

- オーシャンプロトコルは、企業がデータを共有して収益化できる分散型データ交換プロトコル。
- 本取り組みは、データ駆動型企業化を進めるDaimler社のパイロット・プロジェクトであり、オーシャンプロトコルとのこのコラボレーションにより、安全なエンタープライズB2Bデータマーケットプレイスを構築して、データを収益化して機能させることを目的としている。
- 本件との直接的な関連性は限定的であるが、欧州委員会は、B2B等のデータ共有を推進するイニシアティブCommon European Data Spaceを推進。

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

②データ・人工知能等に関するEUの主要業界団体

T-Systems

基本情報

社内	T-Systems 
CEO	Adel Al-Saleh(2021年1月1日-)
概要	ドイツテレコムの子会社であり、2021年時点で従業員28000名、年間売上約40億ユーロ。ドイツのほかEU域内外に拠点を有し、幅広いシステムインテグレーションやクラウドサービスを提供する。
特筆すべき事項	• 2021年11月には、コロナの影響による同社の受注減に伴い、親会社ドイツテレコムが分社化又は売却を検討しているとの報道がある。 • 2021年9月、Google Cloudと協力のもと、Sovereign Cloudに関する新サービスを提供すると発表した。

技術的な特徴

クラウド

強み
- 通常のクラウドサービスのほか、オンプレミスなど幅広い設置方法に対応している。Sovereign Cloudについて、同社は①データ主権、②ソフトウェア主権、③オペレーション主権、から構成されるとして、Google Cloudの多様な機能を、完全なデータのコントロール権を確保して利用できるとする。2022年の半ばに商用サービスを開始予定。

弱み
- Google Cloudと提携の無い自社単独のサービスについては、機能性に弱点を抱えることが指摘される。

ブロックチェーン

強み
- 政府や製造業等の大規模なプロジェクトにおけるブロックチェーン技術の実装に強みを有していると目される。
- 実際、右記載の政府系案件等を受託している。

政策関連事項

1 Sovereign Cloud
- ドイツがフランス等と進めるGAIA-X計画の一環であり、まずは現行のクラウドサービスの管理権の確保を主眼にしている。
- 同社及びドイツテレコムはGAIA-Xの創設メンバーであり、同社CTOのAhrens氏が2021年にGAIA-X議長に就任している。

2 ブロックチェーン
- ドイツ連邦移民難民局(BAMF)が進める難民申請の申請過程をブロックチェーンを用いて効率的に管理するプロジェクトに参画している。
- 上記プロジェクトは、初期のフィージビリティスタディと概念実証(PoC)を経て、パイロットプロジェクトを実施する段階であり、T-Systemがそのシステム開発等を受託している。

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

②データ・人工知能等に関するEUの主要業界団体

Orange

基本情報

社内	Orange 
CEO	Stéphane Richard (2011年3月1日-)
概要	フランステレコムのブランド名がOrangeである。通信部門以外にソフトウェア開発部門(IT部門)を有し、フランスのほかEU域内外(日本含)に拠点を有し、幅広いシステムインテグレーションやクラウドサービスを提供する。
特筆すべき事項	• 2019年5月、Orangeは日本NTTとAIや5G等に関する技術協力協定を締結した。期限は2022年までとなっている。 • 2021年5月SecNumCloudに準拠したクラウドサービス(Cloud de Confiance)を提供する合弁会社Bleuの設立を発表した。同社は米Microsoft社の提供するクラウド基盤Azureを活用してサービスを提供する。

技術的な特徴

クラウド

強み
- フランス政府のクラウド戦略に沿って、SecNumCloudの基準に準拠するサービスが提供できる点が強みである。これにより、政府や自治体といった公的機関、医療機関等の重要インフラ運営者に対してクラウドサービスを提供できる。

フィンテック

強み
- 子会社としてOrange Bankを2017年に設立し、モバイル専業の銀行サービスを提供している。
- 2021年にはフランスのベンチャー企業Younitedと提携して、キャリアショップを含むクロスチャネルでの顧客管理やローンなどの金融サービス提供を効率化する計画を発表している。

政策関連事項

1 Sovereign Cloud

- 左記の通り、フランス政府が推進するクラウド計画と歩調を合わせてサービス展開を開始している。
- 同サービスはまた、フランスがドイツ等と進めるGAIA-X計画の一環であり、同社はGAIA-Xの創設メンバー22社のうちの1社である。

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

②データ・人工知能等に関するEUの主要業界団体

SAP

基本情報

社内	SAP 
CEO	Christian Klein (2019年10月10日-)
概要	ドイツヴァルドルフに本社を置く欧州最大級のソフトウェア会社。ビジネスプロセス管理の分野で世界有数のソフトウェアメーカーとして、データを効果的に処理し、組織全体に情報がスムーズに行き渡るようにするソリューションを開発。
特筆すべき事項	• 2022年３月： SAPはロシアでの事業停止を発表。ウクライナ政府がOracleとSAPに対し、ロシアとつながりのある事業体との取引関係を直ちに打ち切るように要請したことに起因。 • 2021年２月： SAP・IBM、クラウド移行支援で連携強化。「SAP」ワークロードのクラウドへの移行を支援する「RISE with SAP」プログラムをサブスクリプションで提供開始。 • 2021年７月： Google Cloud、顧客のクラウド移行を支援するSAPサービス「RISE with SAP」の戦略的パートナー連携を発表。

技術的な特徴

クラウド

強み
- アプリケーション間の統合の容易性。顧客の特性や要望に応じてパーソナライズされた製品を提供するビジネスモデルへと転換を進める企業が増えており、このような企業は、規模や業種に関わらず、ビジネスプロセス全体を統合し、バリューチェーン全体でデータモデルを共有する仕組みづくりが必要になっており、業務アプリケーションにも統合のための仕組みが重要である。
- ソリューションから価値実現までのスピード。急速に変化するビジネス環境に鑑みると、企業は、価値実現までの時間短縮化を求めている。SAPは、このような要望に応えるため、クラウドを活用した製品、ソリューションのリリース速度を高速化している。SAPは、スタックのモジュール化によりSAP C/4HANA Publicを平均4カ月未満で導入可能としている。

弱み
- 開発言語の縛りによる開発者不足・高いコスト。業務システムの多くは、java、C、C+等が構築されている。他方、SAPは、SAPシステム上でのみ動作するABAPを採用している。

政策関連事項

1 量子技術に係るコンソーシアム(QUTAC)
- 2021年6月10日、SAPは、BASF・BMW・Bosch等のグローバル企業とともに、量子コンピューティングの実用化に向けた開発を進めるために、新たに量子技術・応用コンソーシアム(QUTAC)に参加。
- SAPは、QUTACの中で**物流、生産、調達における量子コンピューティング技術の活用を推進する。輸送ルート、サプライチェーン、生産計画を最適化**の為のソフトウェア・アプリケーションの開発に重点を置く。この取り組みにより、企業がコストを削減し、配送の信頼性を向上させ、空輸を回避することが可能となる。

2 Trusted Cloud Principles (信頼できるクラウド原則)
- 2021年10月1日、Microsoft、Amazon、Google等は「Trusted Cloud Principles」という新たな業界イニシアチブを発表。
- 顧客の権利を保護する共同のコミットメントを定義し、クラウドでデータを保存、処理する企業のために基本的な保護を確立、保証することを目指すとしている。また、イノベーション、セキュリティ、プライバシーを妨げる国際的な法の抵触などを解決する狙いがある。
- このイニシアティブには、SAP、Atlassian、Cisco、IBM、Salesforce、Slackも賛同している。

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

②データ・人工知能等に関するEUの主要業界団体

SIEMENS

基本情報

社内	SIEMENS 
CEO	Roland Busch(2021年2月3日-)
概要	ドイツのバイエルン州ミュンヘンの企業。もともと電信、電車、電子機器の製造会社から発展し、現在では情報通信、交通、防衛、生産設備、家電製品等の分野で製造、およびシステム・ソリューション事業を幅広く手がける会社。
特筆すべき事項	• 2021年2月：クラウドビジネスを本格拡大する方針(デジタルツインの積極化)と、脱炭素化に向けた新たな情報基盤を展開 • 2021年４月：Google Cloud、製造業におけるAIベースのソリューションで協力 • 2020年3月：NECと連携し、プラントの稼働を監視するAIソリューションを提供

技術的な特徴

クラウド

強み
- MindSphere(SIEMENSのIoT基盤)は導入のしやすさと、使いやすさに重点が置かれている。顧客側で使用しているレガシーアプリケーションが分解されて置き換わる形で、MindSphereのSaaSやアプリが導入される。
- MindSphereはCloud Foundry(オープンソースのPaaSソフトウェア)をベースにしたアプリ開発プラットフォームを提供しており、Alibaba、AWS、Azureが提供するアプリとの連携が可能である。

弱み
- MindSphereは、エッジやオンプレでは使いにくく、クラウドで使用するのと比べて機能や性能が劣る。

量子技術

強み
- Siemens Digital Industries Softwareは、Xcelerator製品ポートフォリオとして、3D CADソフトウェア「NX」の最新版を発表した。AI(人工知能)や高度なシミュレーションなどの先進技術を強みとする。
- 「AI-Rad Companion Brain MR」*1 ,「AI-Rad Companion Prostate for Biopsy」*1,「AI-Rad Companion Organs RT」の医療機器認証を取得しており、医療分野でのAIを活用した画像解析サポートを大幅に強化

政策関連事項

1 **量子技術に係るコンソーシアム(QUTAC)**
- 量子技術の先端技術、ユースケース、政策や法整備、標準化に係るコンソーシアムが欧州・ドイツで発足。

2 **AIに係るイニシアティブ**
- 医療分野でのAI活用に強みを持っており、複数のフレームワーク・プロジェクトや政府のイニシアチブ(例：疫病予防のためのAI)に関与。

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

②データ・人工知能等に関するEUの主要業界団体

anotherbrain(フランス・スタートアップ)

基本情報

社内	anotherbrain	
CEO	Bruno Maisonnier	2017年創業
概要	ディープラーニングを代替する「オーガニックAI」を開発。同社は、人間の脳の構造からヒントを得て、データ処理・エネルギーをより節約し、プライバシーを保護する技術を構築。	
特筆すべき事項	• 2019年10月： シリーズAラウンドにて、1,900万ユーロを調達。①AI特化グローバルファンドAlpha Intelligence Capital②フランスベンチャーキャピタルDaphni③SEB Alliance④Robinson Technologiesが投資を実施。 (以降の出資は確認できていない。)	

技術的な特徴

AI

- **Bio inspired**
  ①大脳皮質と同等の効率性：ディープラーニングのように人間の脳をミクロ・ニューロンレベルではなく、よりマクロなスケールで大きなニューロン集団が運動や曲面の知覚のような専用機能を持つような脳の振る舞いを再現している。
  ②センシングモダリティに汎用的に対応：同社の技術は、あらゆる感覚に対応可能で、視覚だけでなく、嗅覚や聴覚等、大脳皮質と同じように扱うことが可能。
- **Self-learning**
  ①教師なし学習：同社テクノロジーは環境から基本的な法則やパターンを抽出し、それを使って高度なタスクを実行することが可能。
  ②インクリメンタルな学習：新しいタスクのたびに、ゼロから始めるのではなく、オーガニックAIは以前の学習に基づき、知識を常に増やし、学習させることが可能。
- **Frugal by design**
  ①超低データ量：同社の技術は、大規模なデータベースまでスケールアップすることも可能である一方、そのタスクを実行するために必要なデータはごくわずかである。
  ②超低エネルギー：限られたデータサンプルで効率的に学習させることで、計算能力を2倍に向上させている。また、同社アルゴリズムは、ディープラーニング技術に比べて計算負荷が非常に低い。
  ③超低コスト：1チップに集積された当社の技術は、あらゆるデバイスに容易に搭載することが可能であり、超低コストのAIソリューションを構築することが可能。

政策関連事項

1 プライバシーの保護に配慮した設計	• GDPRに準拠した当社のAI技術は、ローカルでリアルタイムに実行・更新が可能。 • クラウドプラットフォームへの接続を必要としない。これにより、インターネット接続を介した「ビッグブラザー」ソリューションやハッキングの可能性を防ぐことが可能。
2 説明可能なデザイン	• ディープラーニングの「ブラックボックス」的なAIソリューションが、追跡や説明が不可能な決定を下すのとは異なり、私たちのテクノロジーは、そのプロセスを監査し、どのように、なぜそうなったかを知る可能性や、透明性のあるアルゴリズムを提供する。

参考)AnotherBrain https://anotherbrain.ai/

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

②データ・人工知能等に関するEUの主要業界団体

Owkin(フランス・スタートアップ)

基本情報

社内	Owkin	
CEO	Thomas Clozel, MD	2016年創業
概要	創薬や精密医療分野の加速を目指プラットフォームパートナー企業に提供し、探索・開発プロジェクトの加速を支援。 Owkinプラットフォームの特徴は、１)データアクセス・フェデレートラーニング、２)生物学と医学の専門知見に基づくマルチモーダルな情報、３)理解可能なAIにある。	
特筆すべき事項	• 2021年11月：仏サノフィ(製薬・バイオテクノロジー企業)がフランスの医療研究プラットフォームOwkinに1.8億ドルの投資。現在までにOwkinは合計3.2億ドルを調達し、企業価値評価額が10億ドルを超えた。 • 2021年9月：スイスActelion Pharmaceuticals(製薬企業)との協業を発表。臨床試験の設計や結果の分析方法の改善に係る機械学習技術の開発を目指す。	

技術的な特徴

AI

- **マルチモーダルなデータアクセス：**
  マルチモーダルなデータアクセスを活用し、最先端の説明可能なAIを導入することで、疾患に対する理解を深め、バイオマーカーの開発や新薬ターゲットの特定を実施。
  また、過去の研究と新たな研究をマッチングさせるAIツールを構築し、新薬の組み合わせや薬剤再利用の機会を特定する。

- **精密医療分野での治療の個別化：**
  精密医療(Precision medicine)は、患者の腫瘍の実際の特徴に基づいて治療方法を個別化(Personalize)する。これまでの精密医療のアプローチは、主にがん遺伝子の活性化等の単一のバイオマーカーに基づいて。しかし現在、Owkinは、免疫療法などの革新的な治療法の設定に必要とされる、より包括的でマルチモーダルな特徴の特定へと移行している。

政策関連事項

1 プライバシーの保護に配慮した設計

- 「ローカルデータのサンプルを保持する複数の分散型エッジデバイスやサーバー間で、データ交換を行わず、アルゴリズム学習を行う機械学習技術」である連合学習(Federated Learning)の手法を活用したグローバル研究ネットワークと連携し、これまでにないプライバシー保護型の研究手法を推進。

参考) Owkin https://owkin.com/

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

②データ・人工知能等に関するEUの主要業界団体

Prophesee(フランス・スタートアップ)

基本情報

社内	Prophesee	
CEO	Bruno Maisonnier	2014年創業
概要	事象変化部分のみを捉える次世代のセンシングデバイスを提供。これまでのイメージセンサとは大きく異なり、「見る」のためのデータではなく、「処理」のためのデータを出力する。 これにより後段処理の負荷が飛躍的に減らすことが可能。	
特筆すべき事項	• 2021年12月：SynSenseと共同にて、Propheseeのイメージセンサー「Metavision」とSynsenseのニューロモーフィックプロセッサ「DYNAP-CNN」を統合したイベントベースの単一チップイメージセンサーを共同開発中であることを発表。	

技術的な特徴

AI・センサ

- 神経工学の技術を応用し、マシンビジョン(マシンビジョン：画像の取り込みと処理に基づいて機器を動作させるシステムであり、自動検査、プロセス制御、ロボットのガイドなどに使用される。)に革新を起こすセンサーの実用化に成功。
- 当技術は、動き(差分)情報をセンシングする際に、静止部分ではなく、変化を検出する視神経や脳神経の原理に画像処理のヒントを得たイベント駆動型のセンサー。
- **同社のセンサーとカメラシステムは、自動運転車、産業オートメーション、IoT、セキュリティと監視、AR(拡張現実)/VR(仮想現実)等の分野で応用することが可能。**
- 幅広い使用モデルにおいて、マシンビジョンのスピード、信頼性、効率を大幅に向上させ、新たな可能性を広げている。

政策関連事項

1 センシングに係るデータ共有（B2B/B2G）

- 同社は、自動運転車、産業オートメーション、IoT、セキュリティと監視、AR(拡張現実)/VR(仮想現実)等にて、センシング技術を活用し、データを取得しているため、データ法案が定めるB2B、B2Cのデータ共有に対する対応を進めている/進めいていく可能性がある。

参考) Prophesee https://www.prophesee.ai/stories/
JETRO フランスのベンチャー企業PROPHESEEが東京に合同会社を設立(https://www.jetro.go.jp/invest/newsroom/2019/ab110ee9cf320f7c.html)

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

②データ・人工知能等に関するEUの主要業界団体

International Data Spaces Association

団体概要

基本情報

- デジタル社会において、組織間のデータの共有を進める上では「データ主権」が重要となっており、Industrial Data Space Association は、「データ主権」を担保しつつ、セキュアにデータを共有する仕組み作りを推進。

拠点

- ドイツ

成立年

- 2014年

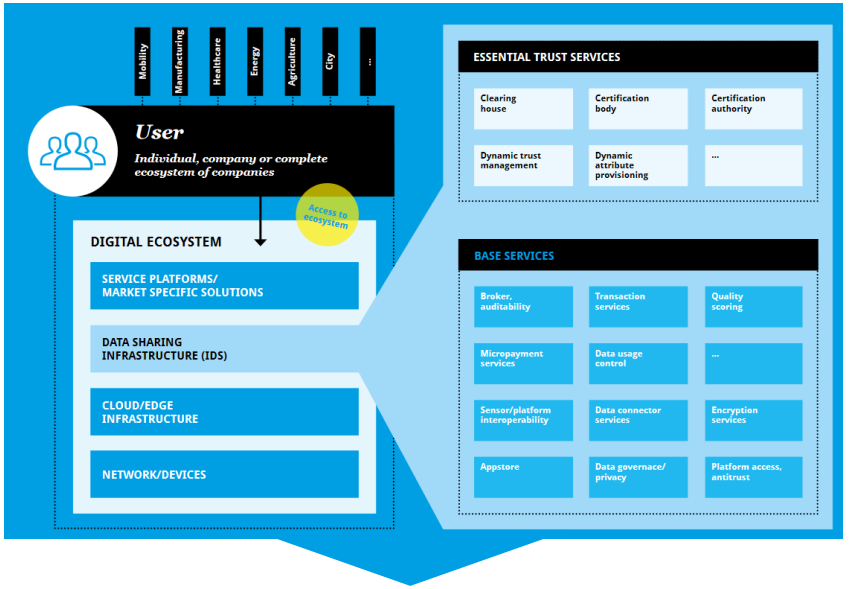
会員企業

- 主体：　フランホーファー研究機構
- 初期会員：Volkswagen社等の企業16社。
- **133会員企業**(現在：22か国)

取組内容

取組内容

IDSアーキテクチャを用いた、信頼・自己決定に基づくデータ共有基盤の標準化を構築を目指す。(a standard for data sovereignty – for the trustworthy, self-determined exchange of data)



企業・異業種間データを共通利用し、Industry4.0に基づく競争力のあるサービス・アプリケーションの創出を狙う。

参考) International Data Spaces　Enabling Data Economy(https://internationaldataspaces.org/wp-content/uploads/dlm_uploads/IDSA-brochure-International-Data-Spaces-Enabling-Data-Economy.pdf)

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

②データ・人工知能等に関するEUの主要業界団体

International Data Spaces Association(会員企業-調査対象国)

INTERNATIONAL DATA SPACES ASSOCIATION

対象	企業/団体等
ドイツ	ADVANEO
ドイツ	AGMADATA
ドイツ	Allianz
フランス	AtoS
ドイツ	Audi
ドイツ	bill-X
ドイツ	Bitergo
ドイツ	Boehringer Ingelheim
ドイツ	Brainport Industries
ドイツ	BDR.(Bundesdruckerei)
ドイツ	CDQ　Sharing Data Excellence
フランス	Cea
ドイツ	Cybus
チェコ	CTU (CZECH TECHNICAL UNIVERSITY IN PRAGUE)
ドイツ	DAIMLER
ドイツ	Data Ahead
ドイツ	DATATRONIQ
ドイツ	Deutsche Bank
ドイツ	Deutsche Telekom
ドイツ	DGZFP (Deutsche Gesellschaft für Zerstörungsfreie Prüfung e.V.)
ドイツ	DHBW
ドイツ	Eccenca
ドイツ	Engie Deutschland
オランダ	EAISI (Eindhoven University of Technology)
ドイツ	exceet (Utimaco)
ドイツ	Fir RWTH Aachen
ドイツ	FIWARE Foundation
ドイツ	Fraunhofer
ドイツ	GeoNet.MRN
ドイツ	German Edge Cloud
ドイツ	GESIS(Gesellschaft für Informationssysteme mbH)
ドイツ	Iav automotive engineering
フランス	IMT (Institut Mines-Telecom)
スイス	Industrie 2025
オランダ	Innopay
ドイツ	Ionos
ドイツ	KNORR-BREMSE
ドイツ	Komsa
ドイツ	L3S research center
ドイツ	Logata Digital Solutions
ドイツ	Minnosphere
ドイツ	.msg
フランス	Nexedi
ドイツ	Nicos AG
ドイツ	olmogo
ドイツ	PI-lar
ドイツ	QuinScape
オランダ	Orealworld
ドイツ	REWE　Group
ドイツ	Rittal GmbH
ドイツ	Salzgitter AG
ドイツ	SAP
ドイツ	Schaeffler AG
ドイツ	SETLOG
ドイツ	SICK　Sensor Intelligence
ドイツ	SIEMENS
ドイツ	SMEV AG　smart mobility evolution
ドイツ	STS
ドイツ	MY EGO
ドイツ	Thyssenkrupp
オランダ	TNO
ドイツ	T systems
ドイツ	TÜV NORD GROUP
ドイツ	Uniklinik RWTH Aachen
ドイツ	Uniscon
ドイツ	Unity Consulting & Innovation
ドイツ	Witten/Herdecke University
オランダ	University of Amsterdam
オランダ	University of Twente
ドイツ	The VDMA
ドイツ	Volkswagen
ドイツ	wetransform
ドイツ	ZVEI

出所)International Data Space Association　Members(https://internationaldataspaces.org/we/members/)

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

②データ・人工知能等に関するEUの主要業界団体

Common European Data Space

Common European Data Space	■ 背景として、**GDPRの対象外である非個人データについては、域内における自由流通を促進**するための規則が18年11月に公布され、データローカライゼーションの原則禁止やデータポータビリティに関する行動規範の作成について規定が為されていた。 ■ 改めて、欧州データ戦略の中で、**公共、民間、市民から生成されるデータが、社会善の為に安全かつ公正に利用されるデータの単一市場**の構築及び、環境、エネルギー、農業等の９つの領域にて、ルール策定のイニシアティブの立ち上げを明記。
Common European **Industrial** Space	データの生成と活用を通じて、製造業での効率性と競争力確保を目指す。
Common European **Green Deal** Space	サーキュラーエコノミー、バイオダイバーシティ、森林伐採、コンプライアンス保証等、とりわけ、気候変動に対応するためのデータ活用を目指す。
Common European **mobility data** Space	コネクテッドカー及びその他交通のデータに基づき、ロジスティックスと交通機関利用のクロスモーダルデータエコシステムの構築を目指す。
Common European **health data** Space	ヘルスデータの利用と再利用を強化・拡大し、ヘルスケアセクターのイノベーション・治療のエビデンスベース化を通じて、ヘルスケアシステムの効率化・持続可能化を目指す。
Common European **financial data** Space	金融機関に対する、商品、決算情報、決済に関わる情報開示に加え、消費者及び事業者が、銀行口座データにアクセスできるオープンバンキングの構築を目指す。
Common European **energy data** Space	エネルギー分野において、透明性のある方法でのデータポータビリティ獲得を目指す。エネルギーデータ特有の問題であるデータのリアルタイム性、カスケード効果、既存技術と最先端技術の混合等にも取り組む。
Common European **agricultural data** Space	農業分野でのサステナビリティと競争性確保の為、サプライチェーン、気候等の環境データを生産データと組み合わせることで、生産アプローチの緻密化・テイラーメイド化を目指す。
Common European **data** Space for **public administration**	政治における腐敗の撲滅また、公共の支出の質の向上の為に、公共調達に関わるデータの透明性及びアカウンタビリティの確保を目指す。
Common European **skills data** Space	欧州の人材スキル(資格、学習機会、仕事スキルセットに関わるデータ)を新たな、移り行くスキルニーズに対応を目指す。

参考)Data Economy　EU DATA STRATEGY 2020(http://www.dataeconomy.eu/eu-data-strategy-2020/#page-content)
島村智子「【EU】非個人データの域内自由流通枠組みに関する規則」

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

②データ・人工知能等に関するEUの主要業界団体

データ流通や人工知能の活用に関わる主要日系企業の動向調査について、調査の対象とする業種は、以下の基準に基づいて選定した。

- 調査対象国に進出している、特にデータ流通や人工知能の活用に関わる主要日系企業の動向を調査した。
- **データ流通や人工知能の活用に関わる主要日系企業業種の基準：**

１．サイバー領域における重要インフラと指定されている：
IT/ICT(情報通信)、化学、金融、物流、海運航空、インフラ、医療は、サイバー領域における重要インフラと指定されているため、調査対象業種とした。
加えて、
２．データ関連政策に対する当該業界分野の関連度が高い：
製造業は、サイバー領域における重要インフラと指定されていないが、データ関連政策に対する関連度が高く、進出日本企業も多いため、リストに追加した。

対象業種	１．サイバー領域における重要インフラと指定されている	（１．に加えて） ２．データ関連政策に対する当該業界分野の関連度が高い
①製造	×	○
②IT/ICT(情報通信)	○	○
③化学	○	○
④金融	○	○
⑤物流	○	○
⑥海運/航空	○	○
⑦インフラ	○	○
⑧医療	○	○
食品	×	×
卸	×	×
旅行	×	×
（その他業種）	×	×

参考)内閣サイバーセキュリティセンター　重要インフラの情報セキュリティ対策に係る第４次行動計画(https://www.nisc.go.jp/active/infra/outline.html)

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

②データ・人工知能等に関するEUの主要業界団体

①製造②IT/ICT(情報通信)③化学④金融⑤物流⑥海運/航空⑦インフラ⑧医療を対象業種とし、海外進出企業に係るデータベースを作成した。

企業リスト

調査対象国
進出企業
(N=2,138)

分析対象企業リスト

調査対象国
進出企業
(N=783)

#	対象業種	企業数
①	製造	381
②	IT/ICT（情報通信）	65
③	化学	110
④	金融	107
⑤	物流	72
⑥	海運/航空　等	9
⑦	ガス/電力/水道等のインフラ	14
⑧	医療	25
	合計	783

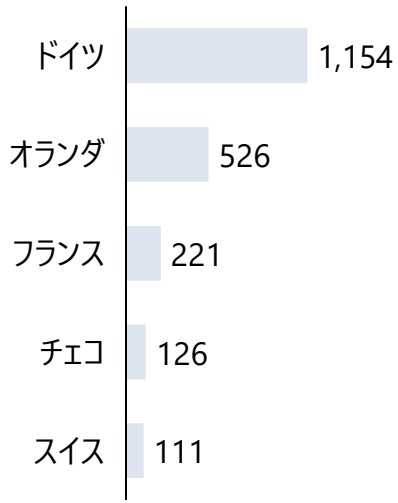
条件

■ 調査対象国：

〇フランス
〇ドイツ
〇オランダ
〇チェコ
〇スイス

■ 全業種を抽出：

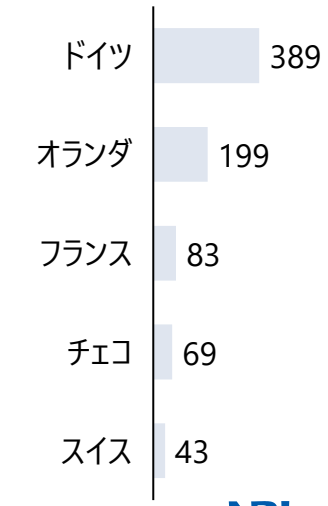
構成



条件

■ 以下に関連する業種名を抽出：
①製造
②IT/ICT(情報通信)③化学
④金融
⑤物流
⑥海運/航空
⑦インフラ
⑧医療

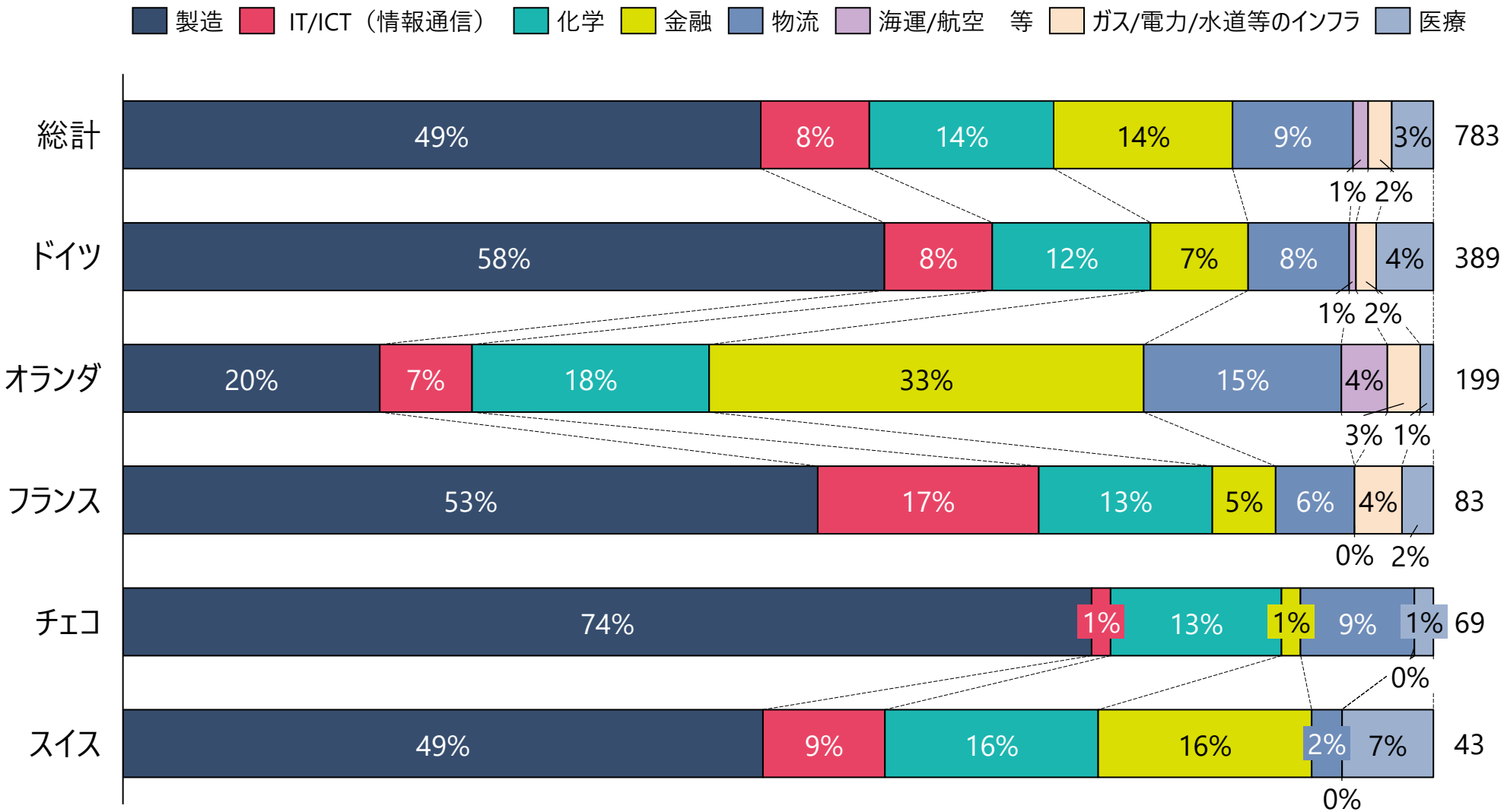
構成



参考) 東洋経済　海外進出企業総覧[国別編]2021年版よりNRI作成

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

調査対象国に、進出企業の業種割合は異なる。
一方、オランダを除く調査対象国では、製造業が進出企業の半数以上を占めている。



参考) 東洋経済　海外進出企業総覧[国別編]2021年版よりNRI作成

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

②データ・人工知能等に関するEUの主要業界団体

本調査対象国の特徴は以下の通り。

調査対象国	調査対象国の特徴
ドイツ	● 進出企業の内、最も多い業種は、製造業で、調査対象業種の58％を占める。 ● 製造業の中でも、いすゞモーターズ・パナソニック等の自動車関連部品(カーエレクトロニクスや、カーエアコン)メーカーの進出が顕著である。
オランダ	● 進出企業の内、最も多い業種は、金融業で、調査対象業種の33％を占める。 ● みずほ銀行や三菱UFJフィナンシャル・グループの証券部門等の大手金融機関は欧州拠点をオランダに構えている。 ● パナソニックやトヨタ等の大企業のファイナンス関連業務を扱う拠点もオランダに多く見れらる。
フランス	● 進出企業の内、最も多い業種は、製造業で、調査対象業種の53％を占める。 ● 製造業の中で、他国と比較すると精密機器・電気機器等の自動車関連以外の進出企業割合が高い。 ● また、IT/ICT(情報通信)においては、ソフトウエア開発企業が大半を占める。
チェコ	● 進出企業の内、最も多い業種は、製造業で、調査対象業種の74％を占める。 ● 当該業種の中でも、トヨタ・プジョー・シトロエン・オートモービル・チェコ、アイシン・ヨーロッパ・マニュファクチャリング・チェコ等も進出しており、自動車関連事業にて重要な拠点であるといえる。
スイス	● 進出企業の内、最も多い業種は、製造業で、調査対象業種の49％を占める。 ● しかし、製造業の中で自動車関連企業の割合は低く、精密機器や機械の割合が高い。

参考) 東洋経済　海外進出企業総覧[国別編]2021年版よりNRI作成

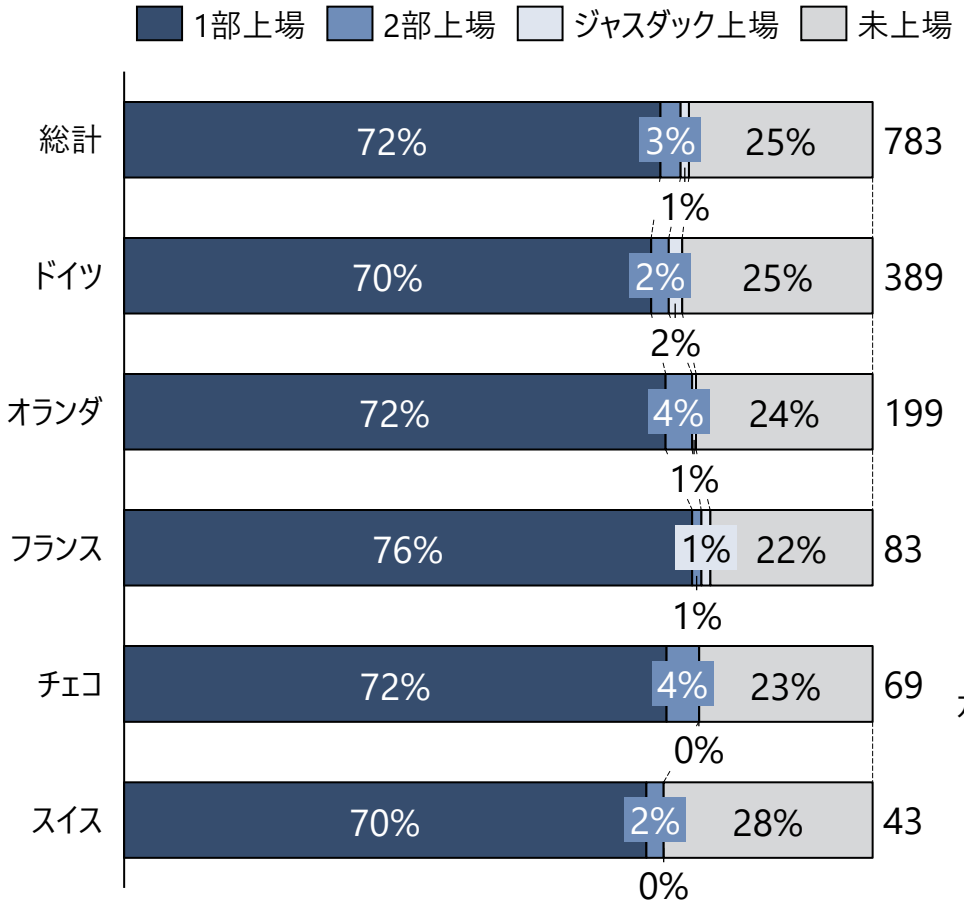
Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

(参考)海外企業進出分析(上場区分)

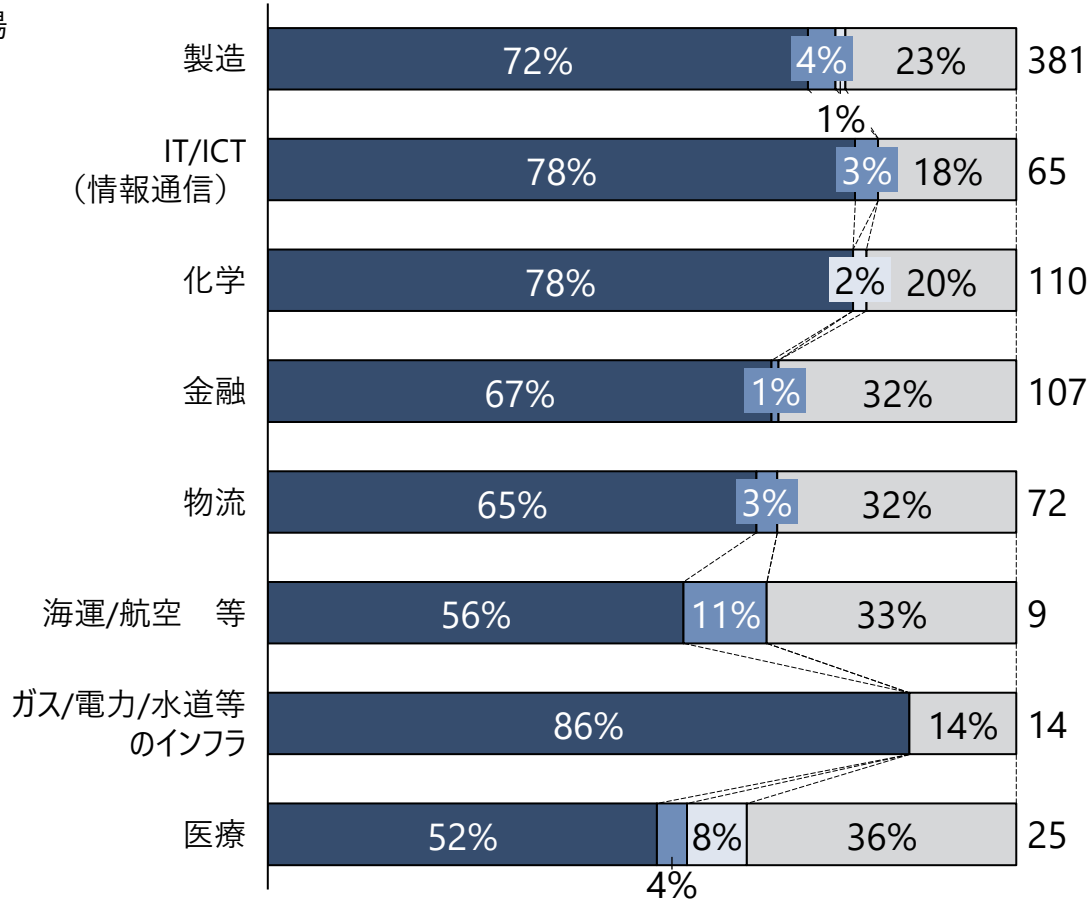
■ 調査対象国への進出企業の70%程度が東証一部上場企業。

■ 調査対象国・業種別の上場比率の差異は限定的。

調査対象国別



業種別



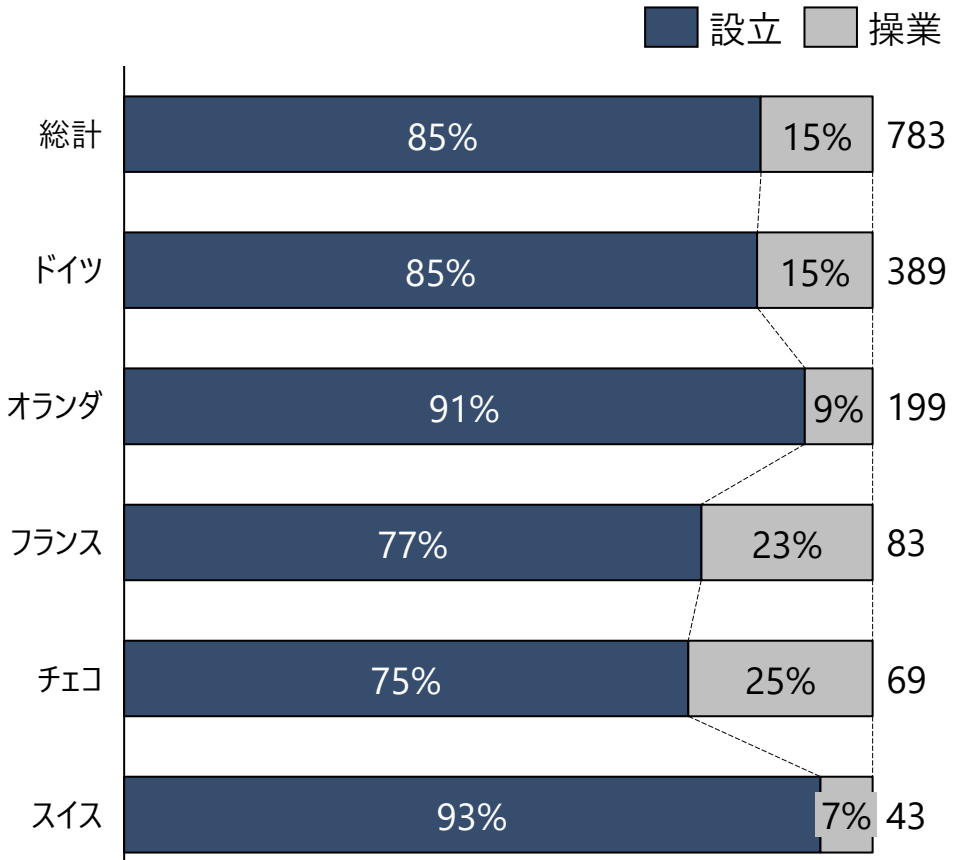
参考) 東洋経済　海外進出企業総覧[国別編]2021年版よりNRI作成

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

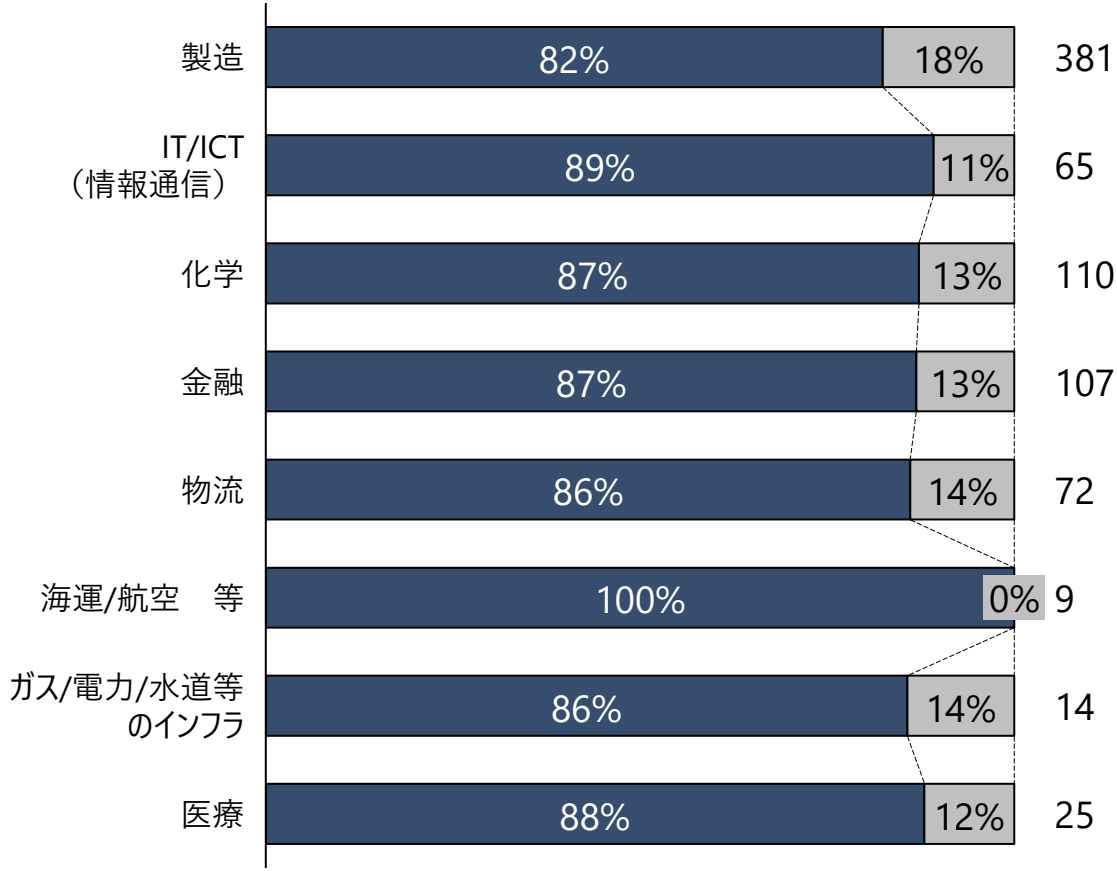
(参考)海外企業進出分析(設立・操業)

- 調査対象国への進出企業の85％が現地法人を設立している。
- フランス・チェコは、他の調査対象国と比較して、操業率が高い。
- 海運/航空等を除く、業種別の設立・操業比率の差分は限定的。

調査対象国別



業種別



参考) 東洋経済　海外進出企業総覧[国別編]2021年版よりNRI作成

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

③各種政策が企業活動に与え得る影響

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

フランスにおいて各種政策が企業活動に与え得る影響

- フランスにおいては、個人データについて、GDPRに基づくEU域外への移転制限が存在する。例えば、フランスにおいて個人データを取り扱う日本企業は当該データを一定の例外の元でだけEU域外に移転できる。
  - EUから域外に移転したデータについては、引き続きEUの水準でのデータ保護が求められる。
- 業種別のローカライゼーション義務も規定されており、金融と通信において問題となる。
  - 決済データの国内保管を義務付ける政策が政府機関が主催した有識者検討会で提案されており、これが実施された場合には日系の金融機関(銀行やクレジットカード会社)に影響を与える可能性がある。
  - 次に通信記録の保管義務があるが、日系事業者のうち通信を営むものは限られるため、影響は限定的と考えられる。

- さらに、日系企業に大きく影響を与えうる措置が、ローカライゼーションに近い義務を負わせるクラウド認証の導入やAI規則案におけるソースコード等の開示である。
  - 日系企業のうち、SecNumCloudの認証を求められる業種は、例えば金融(上述)や医療関連のIT等があり、これらの業種では認証を受けたフランス企業のサービスを使わざるを得なくなる可能性が生じる。結果、グローバルなデータ共有が困難となり、追加的な設備投資や運用費用が必要となる可能性がある。
  - また、AI規則案においても、ハイリスクAIの内容によってはソースコードやデータセットの開示が求められる可能性がある。これについては、AIが外国で開発された場合、外国にあるデータに関しても提供が求められるか否かが問題となるが現時点では明らかではない。
- フランスは法執行や諜報を目的としたガバメントアクセスを規定しており、保管データに対するアクセスが実施される可能性がある。
  - また、国外のデータに対する諜報目的でのガバメントアクセスも規定されており、このような可能性も存在する。
  - 2015年の国内安全法(Internal Security Code)の大幅改正以来、監視体制は強化される傾向にある。

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

フランスにおいて各種政策が企業活動に与え得る影響

■ フランスにおけるデータの移転や保管に係る義務、ガバメントアクセス、ソースコード等の開示要求の概要

データの種類		個人データ	非個人データ
データの移転制限	国内⇒国内	• GDPRにおける取扱いの制限	• (知的財産権や営業秘密の保護等、既存法令で規律)
	国外⇒国内	• (該当なし)	• (該当なし)
	国内⇒国外	• GDPRにおける移転制限	• データ法案にて越境移転制限あり
データの保管	国内	• 決済データローカライゼーション提案 • クラウド認証基準(SecNumCloud) • 通信記録保存(通信事業者)	• クラウド認証(SecNumCloud)
	国外	• EUからの移転データの場合、GDPR水準の保護を継続	• (該当なし)
ガバメントアクセス	国内	• 国内法上、法執行・諜報の双方でGA権限あり	• 国内法上、法執行・諜報の双方でGA権限あり
	国外	• 国際的なデータに対する諜報活動の可能性あり	• 国際的なデータに対する諜報活動の可能性あり
ソースコード等の開示要求	国内	• AI規則案ではソースコード等の開示義務あり	• AI規則案ではソースコード等の開示義務あり
	国外	• AI規則案ではソースコード等の開示が義務付けられる可能性あり	• AI規則案ではソースコード等の開示が義務付けられる可能性あり

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

ドイツにおいて各種政策が企業活動に与え得る影響

- ドイツにおいては、個人データについて、GDPRに基づくEU域外への移転制限が存在する。例えば、ドイツにおいて個人データを取り扱う日本企業は当該データを一定の例外の元でだけEU域外に移転できる。
  - EUから域外に移転したデータについては、引き続きEUの水準でのデータ保護が求められる。
- 業種横断的な税務関連、業種別のローカライゼーション義務(通信)も規定されている。
  - 付加価値税のインボイスの国内保存義務があるため、全世界的な経理システムの統合等について問題を生じさせる可能性がある。
  - 通信記録の保管義務があるが、日系事業者のうち通信を営むものは限られるため、影響は限定的と考えられる。
- さらに、日系企業に大きく影響を与えうる措置が、ローカライゼーションに近い義務を負わせるクラウド関連政策やAI規則案におけるソースコード等の開示である。
  - フランスと並んで、主権クラウドに関する政策が進行中であり、政府関連の事業についてはこのクラウドシステムへの格納を求められる可能性がある。この場合、グローバルに米系企業のクラウドPF上で構築されているシステムについては、主権クラウドへの移管が求められ、コスト増となる可能性が指摘できる。
  - また、AI規則案においても、ハイリスクAIの内容によってはソースコードやデータセットの開示が求められる可能性がある。これについては、AIが外国で開発された場合、外国にあるデータに関しても提供が求められるか否かが問題となるが現時点では明らかではない。
- ドイツでは諜報や法執行を目的としたガバメントアクセスを規定しており、日本企業の保管データに対するアクセスが実施される可能性がある。
  - また、国外のデータに対する諜報目的でのガバメントアクセスも規定されており、このような可能性も存在する。一方、2020年には、ドイツ連邦憲法裁判所は、連邦情報庁(BND)は海外で大規模な監視を行うことはできず、外国人市民や国境を越えた通信に関連してもドイツ憲法(基本法)に拘束されることを明らかにしている。
  - 自動車分野において、デジタル化・自動化に関する研究、交通事故の分析等の公共の利益のために、政府機関がデータの提出を要請できるケースがある。

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

ドイツにおいて各種政策が企業活動に与え得る影響

■ ドイツにおけるデータの移転や保管に係る義務、ガバメントアクセス、ソースコード等の開示要求の概要

データの種類		個人データ	非個人データ
データの移転制限	国内⇒国内	• GDPRにおける取扱いの制限	• (知的財産権や営業秘密の保護等、既存法令で規律)
	国外⇒国内	• (該当なし)	• (該当なし)
	国内⇒国外	• GDPRにおける移転制限 • ヘルスケアデータの移転制限	• データ法案にて越境移転制限あり
データの保管	国内	• 通信記録保存(通信事業者) • 付加価値税のインボイスの国内保存義務 • 主権クラウドに関する政策が進行中	• 付加価値税のインボイスの国内保存義務あり • 主権クラウドに関する政策が進行中
	国外	• EUからの移転データの場合、GDPR水準の保護を継続	• (該当なし)
ガバメントアクセス	国内	• 国内法上、法執行・諜報の双方でGA権限あり	• 国内法上、法執行・諜報の双方でGA権限あり • 自動車分野にて法執行・諜報以外の公益目的に基づく、非個人データを中心とした提供要請あり。
	国外	• 国際的なデータに対する諜報活動の可能性あり	• 国際的なデータに対する諜報活動の可能性あり
ソースコード等の開示要求	国内	• AI規則案ではソースコード等の開示義務あり	• AI規則案ではソースコード等の開示義務あり
	国外	• AI規則案ではソースコード等の開示が義務付けられる可能性あり	• AI規則案ではソースコード等の開示が義務付けられる可能性あり

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

オランダにおいて各種政策が企業活動に与え得る影響

■ オランダにおいては、個人データについて、GDPRに基づくEU域外への移転制限が存在する。例えば、オランダにおいて個人データを取り扱う日本企業は当該データを一定の例外の元でだけEU域外に移転できる。

- EUから域外に移転したデータについては、引き続きEUの水準でのデータ保護が求められる。

■ ローカライゼーションについては、公文書の国内保存義務があるものの、事業上の価値があるものは限られると推測され、また日系企業の公文書管理への関与も確認できなかったため、日系企業への影響は限定的と考えられる。

■ さらに、日系企業に大きく影響を与えうる措置が、AI規則案におけるソースコード等の開示である。

- また、AI規則案においても、ハイリスクAIの内容によってはソースコードやデータセットの開示が求められる可能性がある。これについては、AIが外国で開発された場合、外国にあるデータに関しても提供が求められるか否かが問題となるが現時点では明らかではない。

■ オランダでは諜報や法執行を目的としたガバメントアクセスを規定しており、日本企業の保管データに対するアクセスが実施される可能性がある。

- また、国外のデータに対する諜報目的でのガバメントアクセスも規定されており、このような可能性も存在する。

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

オランダにおいて各種政策が企業活動に与え得る影響

■ オランダにおけるデータの移転や保管に係る義務、ガバメントアクセス、ソースコード等の開示要求の概要

データの種類		個人データ	非個人データ
データの移転制限	国内⇒国内	• GDPRにおける取扱いの制限	• (知的財産権や営業秘密の保護等、既存法令で規律)
	国外⇒国内	• (該当なし)	• (該当なし)
	国内⇒国外	• GDPRにおける移転制限	• データ法案にて越境移転制限あり
データの保管	国内	• 公文書の国内保存義務あり	• 公文書の国内保存義務あり
	国外	• EUからの移転データの場合、GDPR水準の保護を継続	• (該当なし)
ガバメントアクセス	国内	• 国内法上、法執行・諜報の双方でGA権限あり	• 国内法上、法執行・諜報の双方でGA権限あり
	国外	• 国際的なデータに対する諜報活動の可能性あり	• 国際的なデータに対する諜報活動の可能性あり
ソースコード等の開示要求	国内	• AI規則案ではソースコード等の開示義務あり	• AI規則案ではソースコード等の開示義務あり
	国外	• AI規則案ではソースコード等の開示が義務付けられる可能性あり	• AI規則案ではソースコード等の開示が義務付けられる可能性あり

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

チェコにおいて各種政策が企業活動に与え得る影響

■ チェコについては、越境移転規制、ローカライゼーション、ガバメントアクセスについては、EUレベルの規制・政策のみが関連していることが確認できた。

■ チェコにおいては、個人データについて、GDPRに基づくEU域外への移転制限が存在する。例えば、チェコにおいて個人データを取り扱う日本企業は当該データを一定の例外の元でだけEU域外に移転できる。

- EUから域外に移転したデータについては、引き続きEUの水準でのデータ保護が求められる。

■ ガバメントアクセスとして日系企業に大きく影響を与えうる措置が、AI規則案におけるソースコード等の開示である。

- また、AI規則案においても、ハイリスクAIの内容によってはソースコードやデータセットの開示が求められる可能性がある。これについては、AIが外国で開発された場合、外国にあるデータに関しても提供が求められるか否かが問題となるが現時点では明らかではない。

■ また、チェコでは諜報や法執行を目的としたガバメントアクセスを規定しており、日本企業の保管データに対するアクセスが実施される可能性がある。

- また、国外のデータに対する諜報目的でのガバメントアクセスも規定されており、このような可能性も存在する。

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

チェコにおいて各種政策が企業活動に与え得る影響

■ チェコにおけるデータの移転や保管に係る義務、ガバメントアクセス、ソースコード等の開示要求の概要

データの種類		個人データ	非個人データ
データの移転制限	国内⇒国内	• GDPRにおける取扱いの制限	• (知的財産権や営業秘密の保護等、既存法令で規律)
	国外⇒国内	• (該当なし)	• (該当なし)
	国内⇒国外	• GDPRにおける移転制限	• データ法案にて越境移転制限あり
データの保管	国内	• (該当なし)	• (該当なし)
	国外	• EUからの移転データの場合、GDPR水準の保護を継続	• (該当なし)
ガバメントアクセス	国内	• 国内法上、法執行・諜報の双方でGA権限あり	• 国内法上、法執行・諜報の双方でGA権限あり
	国外	• 国際的なデータに対する諜報活動の可能性あり	• 国際的なデータに対する諜報活動の可能性あり
ソースコード等の開示要求	国内	• AI規則案ではソースコード等の開示義務あり	• AI規則案ではソースコード等の開示義務あり
	国外	• AI規則案ではソースコード等の開示が義務付けられる可能性あり	• AI規則案ではソースコード等の開示が義務付けられる可能性あり

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

スイスにおいて各種政策が企業活動に与え得る影響

■ スイスについては、越境移転規制、ローカライゼーション、ガバメントアクセスについていずれも国内法に関連する規定・政策が存在することが確認された。

■ スイスにおいては、個人データについて、連邦データ保護法に基づく国外への移転制限が存在する。例えば、スイスにおいて個人データを取り扱う日本企業は当該データを一定の例外の元でだけEU域外に移転できる。

- スイスから域外に移転したデータについては、引き続きスイスの水準でのデータ保護が求められる。
- EUとは十分性を相互に確認しているが、日本への十分性認定はない。

■ ローカライゼーションについては、マネーロンダリング対策から、金融取引情報等のコピーがスイス国内に保管されるべきことが求められている。

■ スイスでは諜報や法執行を目的としたガバメントアクセスを規定しており、日本企業の保管データに対するアクセスが実施される可能性がある。

- また、国外のデータに対する諜報目的でのガバメントアクセスも規定されており、このような可能性も存在する。一方、外国の自然人についても、DPAに救済措置を求めることができる。

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

スイスにおいて各種政策が企業活動に与え得る影響

■ スイスにおけるデータの移転や保管に係る義務、ガバメントアクセス、ソースコード等の開示要求の概要

データの種類		個人データ	非個人データ
データの移転制限	国内⇒国内	• 連邦データ保護法における取り扱いの制限	• (該当なし)
	国外⇒国内	• (該当なし)	• (該当なし)
	国内⇒国外	• 連邦データ保護法における越境移転制限(GDPR類似)	• (該当なし)
データの保管	国内	• マネーロンダリング対策のため関連書類を国外保存する場合、国内にハード又は電子コピーの保管義務あり	• (該当なし)
	国外	• スイスからの移転データの場合、スイス連邦法水準の保護を継続	• (該当なし)
ガバメントアクセス	国内	• 国内法上、法執行・諜報の双方でGA権限あり	• 国内法上、法執行・諜報の双方でGA権限あり
	国外	• 国際的なデータに対する諜報活動の可能性あり	• 国際的なデータに対する諜報活動の可能性あり
ソースコード等の開示要求	国内	• (該当なし)	• (該当なし)
	国外	• (該当なし)	• (該当なし)

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

(参考)EUにおいて各種政策が企業活動に与え得る影響

■ EUにおけるデータの移転や保管に係る義務、ガバメントアクセス、ソースコード等の開示要求の概要

データの種類		個人データ	非個人データ
データの移転制限	域内⇒域内	• GDPRにおける取扱いの制限	• 原則なし(非個人データ域内自由流通枠組みに関する規則において原則自由流通を規定)
	域外⇒域内	• (該当なし)	• (該当なし)
	域内⇒域外	• GDPRにおける移転制限(十分性を担保された国・組織 • 、同意などに基づく一時的な除外など)	• データ法案にて越境移転制限あり(データ処理サービスが対象)
データの保管	域内	• (該当なし。ただし仏独中心に主権クラウドに係る基準をEUワイドに拡大する動きあり)	• (該当なし。ただし仏独中心に主権クラウドに係る基準をEUワイドに拡大する動きあり)
	域外	• EUからの移転データの場合、GDPR水準の保護を継続	• (該当なし)
ガバメントアクセス	域内	• デジタルサービス法案、デジタルマーケット法案、データ法案等により、公益等に資するガバメントアクセスによるデータ提供義務あり。	• デジタルサービス法案、デジタルマーケット法案、データ法案等により、公益等に資するガバメントアクセスによるデータ提供義務があり。
	域外	• デジタルサービス法案、デジタルマーケット法案、データ法案等により、公益等に資するガバメントアクセスによるデータ提供が義務付けられる可能性あり。	• デジタルサービス法案、デジタルマーケット法案、データ法案等により、公益等に資するガバメントアクセスによるデータ提供が義務付けられる可能性あり。
ソースコード等の開示要求	国内	• AI規則案ではソースコード等の開示義務あり	• AI規則案ではソースコード等の開示義務あり
	国外	• AI規則案ではソースコード等の開示が義務付けられる可能性あり	• AI規則案ではソースコード等の開示が義務付けられる可能性あり

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

④データ政策に関する主要マスコミ・有識者の論調

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

データ政策に関する主要マスコミ・有識者の論調　概要

■ データ越境移転に関連し得る制度に関連して、具体的な規制・施策に対する主要マスコミ・有識者等の論調を整理し、各制度の今後の見通しを提示した。

#	国・地域	データ越境移転に関連し得る制度（類型）	規制・政策名	主要マスコミ・有識者の論調	今後の見通し(NRI分析)
1	フランス	データローカライゼーション	決済データのローカライゼーション	CNILは、経済・財務省の委員会がまとめた決済データのローカライゼーションを求める報告書について、これを支持する報告書を公表した。	個人データの取り扱いに関して包括的な権限を持つCNILの支持を得たことで政府内での本政策の推進が加速する可能性がある。
2	フランス	データローカライゼーション	SecNumCloud改正	Cross Border Data Forumは、本規則は実質的に米系事業者にEU企業との合弁によるサービス提供のみを認めるものであるとして、内外差別的との批判がある。	左記批判はあるものの、既述の通りフランス政府全体のクラウド戦略にも規定されるため、変更される可能性は低い。
3	フランス	ガバメントアクセス	コンセイユ・デタによる大規模な通信監視に関する判決	仏コンセイユ・デタは、通信監視に係る国内判決が欧州司法裁判所の判例に沿わない方向で実施されたとして、市民団体より批判を受けている。	2015年のシャルリー・エブド襲撃事件を契機に安全保障を優先する法令が継続して採択・可決されており、個人の権利保障が強化される見込みは限定的。
4	フランス	ガバメントアクセス	電子通信のデータ保持に関する2006年3月24日付けフランス政令2006-358号	仏コンセイユ・デタは、EUデータ保存指令の国内化法の取り消しを却下した。この判断は、EU司法裁判所の判決に沿っていない。	2015年のシャルリー・エブド襲撃事件を契機に安全保障を優先する法令が継続して採択・可決されており、個人の権利保障が強化される見込みは限定的。
5	ドイツ	ガバメントアクセス	通信データ保持法	独連邦憲法裁判所は、EUデータ保存指令の国内化法である通信データ保持法に違憲判断を下し、データ削除と管理ルールの厳格化命じている。	ガバメントアクセス等に係るデータのアクセス主体の義務や手続き面の強化が検討される。
6	EU	ガバメントアクセス 越境移転制限	データ法案	欧州産業連盟は、データ法案に規定されている公共機関等へのデータ提供義務については、従前から協力を行っていると主張している。また、EU・米国間の越境移転枠組みの早期設計を主張。	本意見書による法案への影響は限定的か。
7	EU	ガバメントアクセス 越境移転制限	データ法案	デジタルヨーロッパは、ガバメントアクセスに係るルール設定について一定評価を示している一方、データ法により、さらなる越境移転制限が課される可能性に懸念を示している。	本意見書による法案への影響は限定的か。
8	EU	ソースコード開示	AI規則案	日本経団連は、ソースコード開示権限を当局に認める規定が、ビジネスを阻害するともに、日EUEPAの関連規定に反するとの指摘を行っている。	AI規則案の左記規定については、主要加盟国であるドイツの有識者報告書でも類似の権限を規定すべきことを定めており、変更される可能性は低い。

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

CNILは、決済データのローカライゼーションを求める経済・財務省報告書を支持

■ フランスのデータ保護監督機関CNILは、決済データのローカライゼーションに関する経済・財務省委員会報告書を引用しつつ、次のように述べ、前述の委員会見解を外国からのアクセスからのデータ保護に関する一つの解決策として肯定的に評価している；

■ GDPRはデータ保護とデータの自由流通の双方を定めるものであり、それゆえEU市民のデータを取り扱う第三国の主体は、EUのルールと価値に基づいて当該データを取り扱う必要がある。

■ 外国の立法によって上記の取り扱いができないのであれば、EUへのローカライゼーションを求めるべきとの見解が、左記の委員会の見解である。CNILも医療データについて同様の理由付けを行っている(後述)。

■ また、GDPRに加え、金融機関は特に重要なセクタとしてサイバーセキュリティ上の義務を負っており、例えば適切な安全管理措置をとることや、サイバーインシデントについてANSSIへの報告義務等が定められている。

■ データローカライゼーションは、データ主権とセキュリティを担保しつつ、EU市民のコントロール権を確保し、規制当局にも適切な対処を可能にするものである。ただし、(データローカライゼーションは)データ保護に関して必要条件でも十分条件でもない。

出所)CNIL, “QUAND LA CONFIANCE PAIE Les moyens de paiement d’aujourd’hui et de demain au défi de la protection des données”, p. 76.

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

SecNumCloud改正

米産業団体は原則として外国企業の認証取得が不可能であるため、同改正は外国企業に対する差別であり、特に米国企業の排除を狙ったものであるとして批判している。

- 本改正の狙いは、重要サービスを運用する企業と政府機関へのサービス提供において、外国のクラウド企業を不利にし、実質的に排除するためである。このプログラムが実行されれば、外国クラウド企業または外国クラウド企業を利用する企業が「信頼ある」とみなされるのは原則不可能となる。
- 実質的に認証は現地企業のみが取得を許されており、外国企業は「信頼ある」との認証を受けるために現地の合弁事業を設立する必要がある。
- フランスの政策決定者はSecNumCloudの保護主義的規制を、米国によるクラウド法の域外適用の危険性に基づいて正当化する。このような保護主義的措置はデータのプライバシー又はセキュリティに貢献しないし、実際にはサイバーセキュリティ上のベストプラクティスを害する。
- これらの規制を進めるなかで、フランスは協力や建設的な代替手段を無視している。米国企業の狙いうちは、欧州技術及びデジタル主権に関するフランス及びドイツのビジョンの明確な一部である。より懸念されるのは、フランスが欧州規模のSecNumCloud「主権要件」を主張していることである。
- 最新の改正案では、国外のクラウドサービスプロバイダーに対する明確な保護主義となった。フランスはこれまで国外の企業に認証を与えておらず、こうした事実上の差別的障壁としての現在の利用に加えて、新しい露骨な保護主義的規定が導入されることになる。したがってEUの貿易コミットメントに反すると思われる。
- こうした規制は、中国が差別的なライセンス要件を通じた国内のクラウドサービス市場の厳格な管理のために用いている規制と似ている。中国は現地合弁事業の設立を少数ではあるが外国企業に認めているのに対して、フランスは未だ認めていないことを考えると、フランスの方がより厳格でさえある。
- こうした規制はインターネットやクラウドサービスの分散的性質を害し、フランス及びEUを拠点とする企業が、米国その他の外国クラウドサービスプロバイダーのセキュリティ上の技術を活用することを妨げることになる。

出所) NIGEL CORY, ""SOVEREIGNTY REQUIREMENTS" IN FRANCE—AND POTENTIALLY EU—CYBERSECURITY REGULATIONS: THE LATEST BARRIER TO DATA FLOWS, DIGITAL TRADE, AND DIGITAL COOPERATION AMONG LIKEMINDED PARTNERS" (https://www.crossborderdataforum.org/sovereignty-requirements-in-france-and-potentially-eu-cybersecurity-regulations-the-latest-barrier-to-data-flows-digital-trade-and-digital-cooperation-among-likemi)よりNRI作成

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

SecNumCloud改正

データローカライゼーションや現地で閉じたオペレーションを要求されることで、効率的なクラウド運用ができなくなる旨を指摘している。

- データローカライゼーションはサイバーセキュリティを侵食する。ITシステムの脆弱性を特定し、企業がサイバー攻撃を予見しそれに対処するためのデータ共有を妨げる。
- またビジネスの慣習をも変えられる。サービス部門を問わず企業は、市場や規制遵守目的で現地子会社を持つが、現地でのオペレーションを支援するために外国の施設やスタッフを用いることができた。しかしこのプロポーザルにより、クラウドプロバイダーは重要なタスクには現地の人材をあてなければならない。データの評価や遠隔メンテナンスを行う際にユーザーが直面する問題を診断し、解決するのに必要な技術的支援を行う職員はEU内の人材でなければならない。いずれの場合においても、企業は「アクセス権限が認められる人物がEU内にいるということを確認」しなければならない。
- 改正案では、クラウド企業には一般的な監視及び報告要件が課せられる。リスク評価要件の一部として、企業は「関与する第三者による、委任主体データの守秘義務違反リスク」を考慮に入れることなどが求められる。これはEDPBのポストSchrems II の報告及び監視要件に似ている。この要件は、データ移転がリスクを生じさせるか判断する際に、移転先各国の法律及び慣行をレビューすることを企業に求めている。
- ここにはいくつかの理由で問題がある。運用上、クラウド企業は、顧客がそのクラウドで保存しているデータに自由にアクセスできず、どのようなタイプのデータなのか、特別のリスクはなんであるのかを知り得ない。外国で保存されている関連データについては、クラウド企業がどこの国に移転又は保存されているのか、また関連リスクを正確に知ることは困難となる。しかし、そのインパクトと報告要件はサーベイランスよりも非常に広くなる。データ及びメタデータ収集は、競争、反資金洗浄および詐欺、刑事捜査の一部として、フランスと他のEU加盟国、世界中の他国に共通する法的要件である。

出所) NIGEL CORY, ""SOVEREIGNTY REQUIREMENTS" IN FRANCE—AND POTENTIALLY EU—CYBERSECURITY REGULATIONS: THE LATEST BARRIER TO DATA FLOWS, DIGITAL TRADE, AND DIGITAL COOPERATION AMONG LIKEMINDED PARTNERS" (https://www.crossborderdataforum.org/sovereignty-requirements-in-france-and-potentially-eu-cybersecurity-regulations-the-latest-barrier-to-data-flows-digital-trade-and-digital-cooperation-among-likemi)よりNRI作成

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

SecNumCloud改正

EUがWTO協定など国際通商協定において負っている内国民待遇義務に違反する可能性があり、安全保障やプライバシーを理由とする例外に当たるかも不明確であると指摘。

- EUの国際通商コミットメントには、無差別原則と内国民待遇が含まれる。これらは基本的な通商法原則で、EU-英国通商協定、WTO政府調達協定など多くの主要貿易協定に含まれている。SecNumCloudの更新版は、WTO政府調達協定の内国民待遇規定の明らかな違反に思われる。中心的な問いは、フランス(及びEU)は、これらの主権要件を、国家安全保障、プライバシー及びその他の公共政策上の利益によって例外を通じて正当化するか否かという問いである。諸国がこれらの例外を偽装された貿易障壁を実施するために濫用することを妨げる規定はあるが、法的先例を提供する国家安全保障関連の紛争はまだほとんどないため、非常に不明確のままになっている。

- こうしたデジタル貿易及び協力に対する新しい欧州による障壁に対しては、未だバイデン政権から明確な反応がなされていない。バイデン政権と他のEU貿易パートナーは、熱心に抵抗すべきである。
- フランスは、EUのサイバーセキュリティ機関である「欧州ネットワーク・情報セキュリティ機関(ENISA)」がSecNumCloudと同等の「主権要件」を、EUクラウドセキュリティスキーム(EUCS)の発展のための作業に組み込むことを主張している。そのようなEU規模の規制は、多くの企業と政府機関に対し、ごくわずかのサービスプロバイダーだけが認証を受けられるEUCS認証サービスのみの利用が義務付けられることになる。SecNumCloudと同様の規制が実現してしまえば、外国のプロバイダーにとっては深刻な問題となる。

出所) NIGEL CORY, ""SOVEREIGNTY REQUIREMENTS" IN FRANCE—AND POTENTIALLY EU—CYBERSECURITY REGULATIONS: THE LATEST BARRIER TO DATA FLOWS, DIGITAL TRADE, AND DIGITAL COOPERATION AMONG LIKEMINDED PARTNERS" (https://www.crossborderdataforum.org/sovereignty-requirements-in-france-and-potentially-eu-cybersecurity-regulations-the-latest-barrier-to-data-flows-digital-trade-and-digital-cooperation-among-likemi)よりNRI作成

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

仏コンセイユ・デタは、通信監視に係る国内判決が欧州司法裁判所の判例に沿わない方向で実施されたとして、市民団体より批判を受けている。

- **EDRi は、Conseil d'Etat(コンセイユ・デタ)による大規模な通信監視に関する判決(2021年 4 月21日)を批判。**
  - 本判決により、Conseil d'Etatは仏諜報機関から法の支配の原則を取り払うことになった。
- EDRi によると、本判決は、欧州司法裁判所(CJEU)の多くの判決の根本を無視していると言う。
  - 2020年10月 ：CJEUは情報機関のデータへのアクセスを規律するフランスの法律(2021年7月30日付 テロ行為防止・諜報活動に関する法律)および通信事業者にすべての通信メタデータ(IPアドレス、位置情報など)を一般化・未分別に保持することを義務付ける法律の両方が基本的権利に反すると判断している。
- EDRi(European Digital Rights)とは、2002年6月10日に設立した、ヨーロッパのデジタルな市民運動の自由を求める団体である。

出所)EDRi　France's highest court validates mass surveillance in the long term
(https://edri.org/our-work/frances-highest-court-validates-mass-surveillance-in-the-long-term/)

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

電子通信のデータ保持に関する2006年3月24日付けフランス政令2006-358号

仏コンセイユ・デタは、EUデータ保存指令の国内化法の取り消しを却下した。この判断は、EU司法裁判所の判決に沿っていない。

- フランスにおいて、データ保持指令は、電子通信のデータ保持に関する2006年3月24日付けフランス政令2006-358号により実施され、フランス郵便・電子通信法典の第R.10-11項以降が制定された。当該規定は、関連データの作成・処理日から1年間のデータ保持期間を定めている。
- **2007年、電子通信サービス事業者の複数の団体が、特にプライバシーの権利の侵害を理由に、フランス政令2006-358号の取り消しを求めて提訴した。**
- **フランスのコンセイユ・デタはこのような請求を却下。判事は、フランス政令2006-358号が追求する公安上の利益に照らせば、データ保持による私生活への干渉は十分に不釣り合いなものではないと判断した。**
  - フランスのConseil d'Etatが依拠した法的根拠(欧州人権条約第8条)は、EU司法裁判所が提示した法的根拠(EU基本権憲章第7条、8条、11条)と異なることから、EU司法裁判所の決定は議論を再燃させる可能性が高い。また、フランス政令2006-358号の根拠となる法的根拠の(少なくとも一部の)取り消しにより、フランス政府は当該政令の廃止を余儀なくされる可能性がある。

- また、2014年にEU司法裁判所がEUのデータ保持指令を破棄して以来、EU諸国は執拗にこれを復活させようとしている。フランスの裁判では、政府がデジタル著作権NGOであるLa Quadrature du NetとPrivacy Internationalに対抗している。EU司法裁判所の判決後、フランスの国家評議会に戻り、同評議会がこの問題を決定することになります。公聴会の日程はまだ決まっていないと、同機関の関係者は述べている。**フランスは現在、この判決が自国の「憲法上のアイデンティティー」に反すると主張することで、事実上EUの裁判所を回避しようとしていると、この件に詳しい関係者は、公にこの件を話すことは許可されていないため匿名を条件に語った。**
  - 2006年に初めて導入され、それ以来ほとんど使われていない「憲法上の同一性」の概念は、国レベルでのEU法の適用を避けるために発動されることがある。フランスはまた、EU司法裁判所が安全保障に関連する事柄について判決を下すべきではないとも述べている(安全保障は依然として国の権限である)。

出所)JONES DAY　EU Data Retention Directive Declared Null and Void: What is Next and How The Ruling Has Been Received in the Member States (https://www.jonesday.com/en/insights/2014/04/eu-data-retention-directive-declared-null-and-void--what-is-next-and-how-the-ruling-has-been-received-in-the-member-states)

POLITICO　France seeks to bypass EU top court on data retention (https://www.politico.eu/article/france-data-retention-bypass-eu-top-court/)

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

通信データ保持法

独連邦憲法裁判所は、EUデータ保存指令の国内化法である通信データ保持法に違憲判断を下し、データ削除と管理ルールの厳格化命じている。

■ **ドイツ連邦憲法裁判所は、2010年3月2日、通信事業者に対し、すべての通信記録を6カ月間保持することを義務付けた法律(通信データ保持法)を違憲とする判決を下した。**

- 現時点で保存されているデータを速やかに削除し、データ保持の条件を厳格化するまで法律の執行を停止するよう命じている。

■ ドイツでは2006年のEU指令に基づき、2007年11月に通信データ保持法が制定され、2008年1月1日付で施行された。

- 捜査機関がテロや組織犯罪への関与が疑われる人物の通信記録を入手しやすくすることを最大の目的としたもので、通信事業者に携帯電話を含む通話記録(日時や相手の電話番号)、IPアドレス、電子メールのアドレスやメールヘッダなどを6カ月間保持するよう義務付ける内容である。
- これに対し、ドイツ国内では同ルールの導入に反対する声が高まり、プライバシー保護団体AK Vorratの主導で市民3万5,000人が法律の無効化を求める訴訟を提起。
- 裁判所は判決で、現行法ではデータ保持のセキュリティが十分とはいえず保存されたデータがどのように利用されているかも不明確で、一般市民は当局の監視下で基本的人権が制限されていると感じる可能性があると指摘。現行ルールの下でのデータ保持は「市民の重大なプライバシー侵害」につながると結論づけた。

■ しかし、原告側はデータ保持法の完全な無効化を求めていたが、裁判所は通信データの保存と利用に関するルールを厳格化したうえで法律を運用すべきだとの判断を示した。具体的には、以下対策を講じるよう求めている。

- 通信データを暗号化してセキュリティを強化する
- データ管理の透明性を高めてデータの利用目的などが明確にわかるようにする
- 連邦データ保護監察官が通信データの管理プロセスに関与する体制を整える

ＥＵデータ保存指令　概要(２００６年２月３日採択)※2014年４月、EU司法裁判所判決により無効とされた

■ データ保存に関する加盟国の義務：

- 指令に規定するデータ(通信履歴等)が保存されることの確保(不完了呼を含む)
- 保存されたデータが、特定の場合に、国内法に従って、適切な国家機関にのみ開示されることの確保
- データへのアクセスに関する手続・条件の国内法による規定
- 通信が行われた日から最低６ヶ月、最大２年間データが保存されることの確保

■ 対象となるデータの範囲：いずれも個別の通信にかかるデータ

出所) LAIT ドイツの通信データ保持法に違憲判断、データ削除と管理ルールの厳格化命じる判決 (https://www.lait.jp/copyright/copyright_world570.html)
総務省 参考資料：通信履歴の保存の在り方関係資料 (https://www.soumu.go.jp/main_content/000340246.pdf)

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

欧州産業連盟は、データ法案に規定されている公共機関等へのデータ提供義務については、従前から協力を行っていると主張している。また、EU・米国間の越境移転枠組みの早期設計を主張。

【データ法案に対するコメント】

- 欧州産業連盟は、欧州企業はグローバルなデータ競争に直面しており、賢明かつ競争力のある法的枠組みが必要だとした上で、市場メカニズムが機能しているとの前提の下、データ法が規定するデータ共有によってEU企業が投資、成長する際の障壁となってはならない主張した。上記の他、データ法案に係るコメントは以下の通り。
  - (1)顧客情報や新製品情報などの企業秘密の機密性が損なわれないこと。
  - (2)EUの一般データ保護規則(GDPR)や知的財産権との一貫性を持たせること。
  - (3)安全で互換性、ポータビリティーがあり、公開性の原則に基づいたクラウドインフラを通じてデータ共有枠組みを設計することが重要であること

【公共機関等へのデータ提供の要請に対するコメント】

- ガバメントアクセスについては、公的部門へのデータの提供については、「新型コロナ危機」を例に挙げて、緊急事態に対処するため、企業側はこれまでも協力してきたと指摘している。

【越境移転規制に対するコメント】

- 声明ではまた、EU・米国間にデータ移転枠組みがないことから、欧州企業が法的な不確実性やコスト増加に直面しているとして、強固な仕組みの設計と速やかな採択を支持する。

出所) JETRO　欧州委のデータ法案、欧州産業界からは懸念の声も上がる
(https://www.jetro.go.jp/biznews/2022/02/49313ab2539508fd.html?_previewDate_=null&revision=0&viewForce=1)

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

データ法案

デジタルヨーロッパは、ガバメントアクセスに係るルール設定について一定評価を示している一方、データ法により、さらなる越境移転制限が課される可能性に懸念を示している。

【データ法案に対するコメント】

- データ法案がコネクテッドデバイスに蓄積されるデータの利用について明確化し、公的部門へのデータ提供についてルールを設定することを評価した。
- 一方で、法案には懸念すべき点もあるとして、例えば、データ共有に関する企業間契約は引き続き任意で商業的に実行可能なものとすべきで、競争法に抵触しない限り、企業間の緊密な連携を可能とする仕組みといった企業間のデータ共有への支援やインセンティブが必要だとした。また、データへのアクセスや共有について、企業間と企業・消費者間それぞれ個別に的を絞った方法が求められると指摘した。

【公共機関等へのデータ提供の要請に対するコメント】

- **政府がデータにアクセスするためのルールを設定することは、規制の分断を避けるための良いステップである。**
- **しかし、そのようなアクセスの理由は厳密に定義されるべきであり、濫用の余地はなく、加盟国はこの要件を回避してはならない。**

【越境移転規制に対するコメント】

- データ法案はGDPRよりもさらに(beyond)データの越境移転を制限しているという懸念も示した。

出所) JETRO　欧州委のデータ法案、欧州産業界からは懸念の声も上がる
(https://www.jetro.go.jp/biznews/2022/02/49313ab2539508fd.html?_previewDate_=null&revision=0&viewForce=1)

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

日本経団連はソースコードの開示権限を規定することに反対し、日EUEPAのソースコード開示要求禁止義務との整合性を明確にすべきと意見表明している。

■ 経団連の表明した意見；

(意見)
ソースコードは企業にとって競争力の源泉となる重要な資産であり、契約・安全保障などの理由により開示できない場合がある。また、ユーザーがデータを当局に開示することを懸念し、AIの導入が進まない可能性もあるため、当局によるアクセスが行われるべきではない。仮に調査が必要となる疑義が生じた際には、まずは企業に対して説明責任を求めるなど、ソースコードの開示に依らない適切な対処法を検討すべき。
日EUEPAの第八章73条においては、日EU間におけるソースコードのアクセス要求が明確に禁止されており、同条との整合性を明確に示すべき。

出所)日本経済団体連合会「欧州AI規制法案に対する意見」(https://www.keidanren.or.jp/policy/2021/069.html)

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

参考資料　データ法案　概要

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

参考資料

EUデータ法案　基本事項　概要

データ法概要：

■ EUのルールや価値観に沿って、**より多くのデータを利用可能にする**重要な施策。

■ データガバナンス法(2020年11月提案)を補完する位置づけ。

- データガバナンス法：
  データ流通を促進するためのプロセスと構造を構築
- **データ法：**
  誰がどのような条件の下でデータから価値を創造できるかを明確化

■ IoT機器から生成されるデータの使用に関するルールを設定することで、公平性を確保。

- 一般的に、モノやデバイスのユーザーは、自らが生成するデータについて完全な権利を持つべきだと考えている。
- しかし、これらの権利はしばしば不明確であり、メーカーは専門家と消費者の両方のユーザーがIoT機器を使用する際に作成したデジタルデータを十分に活用できるように製品を設計しているとは限らない。
- そのような重要なデジタルデータを基にした能力の公正な分配が行われず、デジタル化と価値創造を阻害する事態を招いている。

■ 規則や条件が異なる、特定の状況に応じて検討されたデータアクセスに係る権利間の一貫性を確保を目的とする。

- データ法は既存のデータアクセス義務を損なうものではないが、将来の規則はデータ法と整合性を取るべきである。
- 既存の規則を評価し、関連する場合はその見直しの際にデータ法案と整合させる必要がある。

出所)European Commission　Data Act(https://digital-strategy.ec.europa.eu/en/policies/data-act)

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

参考資料

EUデータ法案　基本事項　機能・目的

データ法が規定する措置内容等：

■企業、市民、行政の利益の為、より多くのデータを利用可能とするために、以下のような一連の措置等を規定。

- **データを生成する企業や消費者に対し、誰がどのような条件でそのようなデータを利用できるのかという法的確実性を高め、メーカーが高品質のデータ生成への投資を継続するためのインセンティブを与えるための措置：**
  これらの措置により、サービスプロバイダー間のデータ移転が容易になり、規模の大小にかかわらず、より多くの主体がデータエコノミーに参加することができるようになる。
- **公正なデータ共有を妨げる契約上の不均衡の濫用を防止するための措置：**
  中小企業は、市場で著しく優位な立場にある当事者が課す不公正な契約条件から保護される。また、欧州委員会は、そのような市場参加者が公正なデータ共有契約を作成し交渉できるように、モデル契約条項を作成する。
- **公共部門が特定の公益目的のために必要な民間部門が保有するデータにアクセスし利用するための手段：**
  例えば企業の負担を最小限に抑えながら、公共の緊急事態に迅速かつ安全に対応するための洞察力を導くことが挙げられる。
- **欧州連合のクラウド市場を開放するために、顧客がデータ処理サービスの異なるプロバイダー間で効果的に乗り換えるための正しい枠組み条件を設定する新しい規則：**
  これらは、効率的なデータ相互運用性のための全体的な枠組みにも貢献する。
- **データベース指令のデータ保護に係る側面を見直しに係る規定：**
  特に、sui generisデータベース権(特定のデータベースの内容を保護する権利)の役割と、IoT機器によって生成又は取得されたデータから生じるデータベースへの適用の明確化に係る規定が存在する。これによりデータ保有者と利用者の利益のバランスが、欧州連合のデータ政策の広範な目的に沿うようになる。

出所)European Commission　Data Act(https://digital-strategy.ec.europa.eu/en/policies/data-act)

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

参考資料

EUデータ法案　基本事項　欧州連合に対する効果・影響

欧州連合に対する効果・影響：

■ データ法は、イノベーションと新たな雇用のための強力なエンジンとなり、データに基づくイノベーションの第二の波の最前線に、欧州連合が確実に立つことができる。

- **B2C/B2Bデータ共有：**
  ユーザーが自分のデータをより簡単に転送「ポート」できるようにすることで、個人と企業に、スマートオブジェクト、機械、デバイスの使用により生成されるデータの管理を強化し、それによって、製品のデジタル化の利点を享受できるようにするものである。
- **B2Bデータ共有(アフターサービス事業者に係る事例)：**
  関連データにアクセスできるようになることで、アフターサービス事業者はサービスの改善・革新を図り、メーカーが提供する同等のサービスと対等に競争できるようになる。したがって、コネクテッド製品のユーザーは、より安価な修理・メンテナンス業者を選び、あるいは、自身で保守・修理をすることが可能となる。そうすれば、その市場において価格低下と言った恩恵を受けることができるとされる。これはコネクテッドプロダクトの寿命を延ばし、グリーンディールの目標に貢献する可能性もある。
- **B2Bデータ共有(産業内での事業者に係る事例)**
  産業機器の機能に関するデータが利用可能になれば、工場の現場での最適化が可能になる。工場や、農場、建設会社は、機械学習に基づくものも含めて、操業サイクル、生産ライン、サプライチェーン管理を最適化できるようになる。
  精密農業では、コネクテッド機器から得られたデータのIoT分析により、農家が天候や、温度、水分、価格に関する洞察を提供することができる。また、GPS信号等のリアルタイムデータを分析し、最適化および収量の増加方法に関する洞察を提供することもできる。これにより、農場計画が改善され、農家が必要な資源のレベルについて意思決定できるようになる。
- **B2Bデータ共有(零細・中小事業者に係る事例)**
  欧州連合の企業、特に零細・中小事業者は、データアクセスとポータビリティの権利により、自らが生成するデータに基づいて競争し、イノベーションを起こす可能性がより高まる。サービス提供者間でデータを転送することが容易になり、その結果、規模に関係なく、より多くの関係者がデータ経済に参加するようになる。

出所)European Commission　Data Act(https://digital-strategy.ec.europa.eu/en/policies/data-act)

注)データ法に係る開パブリックコンサルテーションは、2021年6月3日から9月3日まで実施された。サマリレポートは以下。https://digital-strategy.ec.europa.eu/en/public-consultation-data-act-summary-report

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

参考資料

EUデータ法案　各章の概要

各章の概要	概要
第Ⅰ章 総則	■ 本規則の主題と範囲を定義し、本手段を通じて使用される定義を定めている。
第Ⅱ章 B2C及び B2Bデータ共有	■ 消費者および企業が所有、レンタル、リースする製品や関連サービスにより生成されるデータにアクセスするための法的確実性を高める。 ■ 製造業者や設計者は、デフォルトでデータに容易にアクセスできるように製品を設計しなければならず、どのデータに対してどのようにアクセスできるのかについて透明性を確保しなければならない。 ■ 本章の規定は、ユーザーと合意の下でメーカーが、提供する製品又は関連サービスからデータにアクセスし使用する可能性に影響を与えるものではない。 ■ データ保有者は、ユーザの要求に応じて当該データを第三者に提供する義務がある。ユーザーは、データ保有者に対してアフターマーケットサービスの提供者等の第三者のサービス提供者へのデータアクセスを提供する権限が付与されている。零細企業はこれらの義務から免除される。
第Ⅲ章 データを利用可能にすることを法的に規定されたデータ保持者の義務	■ データを利用可能にする義務に適用される一般的な規則を定めている。 ■ データ保有者が第 II 章又は他の欧州連合法、加盟国の法令により、データ受領者に対して データを利用可能にする義務を負っている場合に、一般的な枠組みは、データが利用可能になる条件および、データを利用可能にすることに対する補償を扱っている。いかなる条件も公正かつ非差別的でなければならず、いかなる補償も合理的でなければならない。ただし、欧州連合法又は、欧州連合法を導入する加盟国国内法が、データ利用可能にすることに対する補償を除外したり、より低い補償を規定したりすることを妨げるものではない。 ■ 零細・中小企業に対して規定される補償は、部門別法令に別段の定めがない限り、データを利用可能にするために発生したコストを超えることはできない。加盟国が認定する紛争解決機関は、補償金または条件について意見の異なる当事者が合意に至るのを支援することが可能である。

出所)European Commission Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on harmonised rules on fair access to and use of data (Data Act)　(https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=COM:2022:68:FIN)

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

参考資料

EUデータ法案　各章の概要

各章の概要	概要
第Ⅳ章 企業間のデータのアクセスおよび使用に係る不公正な取引条件	■ 企業間のデータ共有に係る契約において、契約条件が一方の当事者から零細・中小企業に対して一方的に押し付けられる場合の不公正な契約条件を取り上げている。本章では、データアクセスと使用に関する契約上の合意が、契約当事者間の交渉力の不均衡を利用しないことを保証している。 ■ 不公正性テストの手段には、データ共有関連の契約条項の不公正を定義する一般条項と、常に不公正である又は不公正であると推定される条項のリストがある。不平等な交渉力の状況下では、このテストは不公正な契約を避けるために、より弱い契約当事者を保護する。このような不公正な契約は、契約当事者双方によるデータの使用を阻害する。 ■ 不公正性テストによって、本規定は、データ経済における価値の公正な配分を保証するものである。欧州委員会が推奨するモデル契約条件は、商業当事者が公正な条件に基づいて契約を締結することを支援するものである。
第Ⅴ章 例外的な必要性に基づく、公共部門機関、連合機関、政府機関に対するデータ提供	■ 提出を要請されたデータが例外的に必要な場合に、公共部門機関、連合機関、政府機関が、企業が保有するデータを利用するための調和された枠組みを作成している。 ■ 本枠組みは、データを使用可能にする義務に基づいており、公共部門機関が特定のデータを使用する例外的な必要性があるにもかかわらず、新しい法律の制定又は既存の報告義務によって適時にそのようなデータを市場で取得できない場合にのみ、適用される。 ■ 公衆衛生上の緊急事態、大規模な自然災害や人為的災害等の公共の緊急事態に対応するための例外的な必要性がある場合、**データは無料で使用可能である。** ■ その他の例外的な必要性(公的緊急事態の予防、緊急事態からの回復支援等)の場合、データを使用可能にするデータ保有者は、関連**データを使用可能にするための費用に合理的なマージンを加えた補償を受ける権利**を有する。 ■ データを要求する権利が乱用されないため、又は、公共部門がそのデータの使用について説明責任任を果たす為に、**データの要求は比例的である必要があり、達成すべき目的を明確に示し、データを利用可能にする企業の利益を尊重する**必要がある。 ■ **管轄当局は、すべての要請に係る透明性と一般への公開を保証する。**また、その結果として生じるあらゆる苦情にも対応する。

出所)European Commission Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on harmonised rules on fair access to and use of data (Data Act)　(https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=COM:2022:68:FIN)

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

参考資料

EUデータ法案　各章の概要

各章の概要	概要
第VI章 データ処理サービスの乗り換え	■ クラウド、エッジ、その他のデータ処理サービスの提供者に課される、契約及び、商業、技術上の最低規制要件を紹介し、このようなサービス間の乗り換えを可能にする。特に、顧客が他のサービス提供者に乗り換えた後も、サービスに係る機能的同等性(最低レベルの機能)を維持することを保証するものである。 ■ 本提案は、技術的に実現不可能な場合の例外を含むが、この点についてはサービス提供者に立証責任がある。 ■ 本提案は、特定の技術標準やインターフェースを義務付けてはいない。しかし、欧州標準やオープンなインターオペラビリティに係る技術仕様が存在する場合は、それらと互換性のあるサービスであることを要求する。
第VII章 国際的なコンテクストにおける非個人データの保護措置	■ 欧州連合域内で保有される非個人データへの違法な第三者アクセスに、欧州連合市場で提供されるデータ処理サービスによって対処するものである。 ■ 本提案は、欧州連合市民や企業が保有するデータへのアクセス要求の法的根拠には影響を与えず、欧州連合のデータ保護とプライバシーの枠組みを損なうものではない。この提案は、プロバイダーが技術的、法的、組織的なあらゆる合理的な手段を講じて、厳しい条件が満たされない場合に限り、欧州連合法の下で当該データを保護に係る競合義務に抵触するようなアクセスを防止しなければならないという方法等の特定のセーフガードを提供する。 ■ 同規則は、WTOおよび二国間貿易協定におけるEUの国際公約を遵守している。
第VIII章 インターオペラビリティ	■ データスペースの運営者オヨにデータ処理サービス提供者がインターオペラビリティ関して遵守すべき必須要件とスマートコントラクトに関する必須要件が規定されている。 ■ シームレスなマルチベンダークラウド環境を促進するため、データ処理サービスのインターオペラビリティに関するオープンな相互運用性仕様と欧州標準を実現する。

出所)European Commission Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on harmonised rules on fair access to and use of data (Data Act)　(https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=COM:2022:68:FIN)

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

参考資料

EUデータ法案　規律内容・適用対象

概要

規律内容

■ 本法案は、以下に係る調和のとれた規則を規定するものである。(第1条1 項)

- ①その利用又は環境に関係するデータを取得、生成及び収集し、公的に利用可能な電気通信サービスを介してデータ通信することが可能である製品や、そのような製品に組み込まれ、その作動に不可欠なデジタルサービスの利用から生成されたデータをその利用者(個人のみならず、法人も含む)に利用可能なものとすること。
- ②データ保持者(data holders)がデータ受領者(data recipients)にデータを利用可能にすること。
- ③公共の利益のもとに実施される業務の遂行のためにデータに関して例外的な必要性がある場合に、データ保持者が公的セクター等にデータを利用可能にすること。

適用対象

■ データ法案は、以下の主体に適用される。(第1条2項)

- (a)EU 域内に上市された「製品」の製造者及び「関連サービス」の供給者並びに当該製品又はサービスの利用者
- (b)EU 域内のデータ受領者にデータを利用可能なものとしている「データ保持者」
- (c)データを利用可能なものとされている EU 域内のデータ受領者
- (d)(i)公共の利益のもとに実施される業務の遂行のためにデータに関して例外的な必要性がある場合に、データ保持者に当該データを利用可能にすることを要求する公的セクターの機関、及び EU の施設・機関・団体、並びに(ii)そのような求めに応じて当該データを提供するデータ保持者
- (e)EU 域内の消費者に対して「データ処理サービス」を提供している当該サービスのプロバイダー

■ ただし、零細・中小企業は一定の義務について免除されている。(例：第7条1項、第14 条2項)

参考)西村あさひ法律事務所　EUデータ法案の公表と日本企業への影響(ヨーロッパニューズレター)、長島・大野・常松法律事務所　欧州データ法(Data Act)の法案の公表(テクノロジー法ニュースレター)よりNRI作成

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

参考資料

EUデータ法案　適用範囲に関する規定・管轄当局

概要

適用範囲に関する規定

- 「データ」とは、行為、事実または情報のデジタル表現およびそれらの収集物を指し、音声、映像または音響映像記録の形式を含む。(2条1号)
  →データ法案は、一般データ保護規則(GDPR)とは異なり、個人データだけでなく、非個人データ(産業データ)を含むデータを対象とする。
- 「製品」とは、その利用又は環境に関係するデータを取得、生成及び収集し、公的に利用可能な電気通信サービスを介してデータ通信することが可能であり、その主な機能がデータの保存や処理にはない有形の動産を指す。(2条2号)
  →IoT 製品等が該当。ただし、パソコンやサーバー、スマートフォン等、コンテンツを生成するのに人のインプットが必要となる機器については本法案の対象外とされている。(前文15項)。
- 「関連サービスについても、「製品」に組み込まれ、その作動に不可欠なデジタルサービスを指す。(2条3号)
  →IoT 関連サービス等が該当。
- 「データ処理サービス」とは、原則として、スケーラブルで弾力性のある共有可能なコンピューティング資源について、消費者がオンデマンドで管理することや、広範なリモートアクセスを可能にするデジタルサービスを意味する。(2条12号)
  →クラウドサービス等が該当。

管轄当局

- 各加盟国は、本規則の適用および執行の責任者として、1つまたは複数の管轄当局を指定するものとします。加盟国は、1つ以上の新たな当局を設立することも、既存の当局に依存することも可能である。(31条1項)
- 本条第1項に影響を与えることなく、以下のとおりとする。(31条2項)
  - (a) 規則(EU)2016/679(GDPR)の適用を監視する責任を負う独立監督当局は、個人データの保護に関する限り、本規則の適用を監視する責任を負うものとする。規則(EU)2016/679の第VI章(独立監督機関)及び第VII章(協力と一貫性)が準用されるものとする。監督当局の任務と権限は、個人データの処理に関して行使されるものとする。
  - (b) 本規則の実施に関連する特定の分野別データ交換の問題については、分野別当局の権限を尊重するものとする。
  - (c) 本則の第VI章の適用及び執行を担当する国の権限ある当局は、データ及び電子通信サービスの分野での経験を有すること。

出所)西村あさひ法律事務所　EUデータ法案の公表と日本企業への影響(ヨーロッパニューズレター)、
長島・大野・常松法律事務所　欧州データ法(Data Act)の法案の公表(テクノロジー法ニュースレター)にNRI作成

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

参考資料

EUデータ法案　条文構成

条文構成(１/２)

第Ⅰ章　総則 (GENERAL PROVISIONS)

第１条　対象および範囲
(Subject matter and scope)
第２条　定義
(Definitions)

第Ⅱ章　B2CおよびB2Bデータ共有 (BUSINESS TO CONSUMER AND BUSINESS TO BUSINESS DATA SHARING)

第３条　製品又は関連サービスの使用によって生成されたデータをアクセス可能ににする義務
(Obligation to make data generated by the use of products or related services accessible)
第４条　製品または関連サービスの使用によって生成されたデータにアクセスし、それを利用するユーザーの権利
(The right of users to access and use data generated by the use of products or related services)
第５条　データを第三者と共有する権利
(Right to share data with third parties)
第６条　ユーザーの要求によってデータを受領する第三者の義務
(Obligations of third parties receiving data at the request of the user)
第７条　B2CおよびB2Bデータ共有義務の範囲
(Scope of business to consumer and business to business data sharing obligations)

第Ⅲ章　データを利用可能にすることを法的に規定されたデータ保持者の義務 (OBLIGATIONS FOR DATA HOLDERS LEGALLY OBLIGED TO MAKE DATA AVAILABLE)

第８条　データ保有者がデータ受信者にデータを提供する条件
(Conditions under which data holders make data available to data recipients)
第９条　データを利用可能にすることに対する補償
(Compensation for making data available)
第10条　紛争解決
(Dispute settlement)
第11条　技術保護手段およびデータの不正使用又は開示に関する規定
(Technical protection measures and provisions on unauthorised use or disclosure of data)
第12条　データを利用可能にすることを法的に規定されたデータ保有者の義務の範囲
(Scope of obligations for data holders legally obliged to make data available)

第Ⅳ章　企業間のデータのアクセスおよび使用に係る不公正な取引条件 (UNFAIR TERMS RELATED TO DATA ACCESS AND USE BETWEEN ENTERPRISES)

第13条　零細企業、中小企業に一方的に押し付けられた不当な契約条件
(Unfair contractual terms unilaterally imposed on a micro, small or medium-sized enterprise)

第Ⅴ章　例外的な必要性に基づく、公共部門機関、連合機関、政府機関に対するデータ提供 (MAKING DATA AVAILABLE TO PUBLIC SECTOR BODIES AND UNION INSTITUTIONS, AGENCIES OR BODIES BASED ON EXCEPTIONAL NEED)

第14条　例外的な必要性に基づいてデータを利用可能にする義務
(Obligation to make data available based on exceptional need)
第15条　データの使用に係る例外的な必要性
(Exceptional need to use data)
第16条　公共部門機関、連合機関、政府機関がデータを利用可能にする他の義務との関係性
(Relationship with other obligations to make data available to public sector bodies and Union institutions, agencies and bodies)
第17条　データ提供の要請
(Requests for data to be made available)
第18条　データ提供要請への遵守
(Compliance with requests for data)
第19条　公共部門機関、連合機関、政府機関の義務
(Obligations of public sector bodies and Union institutions, agencies and bodies)
第20条　例外的な必要性がある場合の補償
(Compensation in cases of exceptional need)
第21条　例外的な必要性の下での研究機関や統計機関の貢献
(Contribution of research organisations or statistical bodies in the context of exceptional needs)
第22条　相互扶助および国境を越えた協力
(Mutual assistance and cross-border cooperation)

出所)European Commission Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on harmonised rules on fair access to and use of data (Data Act)　(https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=COM:2022:68:FIN)

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

参考資料

EUデータ法案　条文構成

条文構成(２/２)

第Ⅵ章　データ処理サービスの乗り換え (SWITCHING BETWEEN DATA PROCESSING SERVICES)

第23条　データ処理サービスの提供者間の効果的な乗り換えに対する障害の除去
(Removing obstacles to effective switching between providers of data processing services)
第24条　データ処理サービスの提供者間の乗り換えに係る契約条件
(Contractual terms concerning switching between providers of data processing services)
第25条　乗り換えに係る料金の段階的な撤廃
(Gradual withdrawal of switching charges)
第26条　乗り換えに係る技術的側面
(Technical aspects of switching)

第Ⅶ章　国際的なコンテクストにおける非個人データの保護措置 (INTERNATIONAL CONTEXTS NON-PERSONAL DATA SAFEGUARDS)

第27条　国際的なアクセスおよび移転
(International access and transfer)

第Ⅷ章　インターオペラビリティ (INTEROPERABILITY)

第28条　インターオペラビリティに係る必須要件
(Essential requirements regarding interoperability)
第29条　データ処理サービスにおけるインターオペラビリティ
(Interoperability for data processing services)
第30条　データ共有を目的としたスマートコントラクトに関する必須要件
(Essential requirements regarding smart contracts for data sharing)

第Ⅸ章　実施および執行 (IMPLEMENTATION AND ENFORCEMENT)

第31条　管轄当局
(Competent authorities)
第32条　管轄当局に対する苦情申し立てに係る権利
(Right to lodge a complaint with a competent authority)
第33条　制裁金
(Penalties)
第34条　モデル契約条項
(Model contractual terms)

第Ⅹ章　指令1996/9/ECに基づくsui generis権利 (SUI GENERIS RIGHT UNDER DIRECTIVE 1996/9/EC)

第35条　特定のデータを含むデータベース
(Databases containing certain data)

第Ⅺ章　最終規定 (FINAL PROVISIONS)

第36条　規則(EU) No 2017/2394の改正について
(Amendment to Regulation (EU) No 2017/2394)
第37条　指令(EU)2020/1828の改正について
(Amendment to Directive (EU) 2020/1828)
第38条　委任の行使
(Exercise of the delegation)
第39条　委員会の手続き
(Committee procedure)
第40条　データへのアクセス及び使用に関する権利及び義務を規定する他の欧州連合の法的行為
(Other Union legal acts governing rights and obligations on data access and use)
第41条　評価およびレビュー
(Evaluation and review)
第42条　発効と適用
(Entry into force and application)

出所)European Commission Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on harmonised rules on fair access to and use of data (Data Act)　(https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=COM:2022:68:FIN)

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

参考資料　デジタルの十年におけるデジタル権利及び原則に関する宣言

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

参考資料　European Declaration on Digital Rights and Principles for the Digital Decade　概要

基本的には基本権憲章を中心とした権利がデジタル時代にも継続適用されることを定める。ただし、加盟国で先駆的な動きのあるデジタル課税やワークライフバランス等が加わり、偽情報等についてのPFの責任がやや後退した表現となっている点が特徴的。

該当章・権利	宣言の内容（赤字は特にデータ流通に関連する記載）	関連するEU・加盟国の政策	既存EU/加盟国政策との関係
加盟国の義務(第II章)	アクセス可能で、安全かつ信頼のできるデジタルアイデンティティがすべての業績官で利用されることを定めるとともに、安価かつ高速なデジタル接続手段へのユニバーサルアクセス、およびネットワーク中立性が規定される。	デジタルアイデンティティについてはeIDAS規則において、ユニバーサルサービスやネットワーク中立性については、European Electronic Communications Codeや Net Neutrality Regulationにおいて規定されている。	類似の内容を定める。
デジタル課税(第II章)	デジタル課税については明言していないものの、「デジタルトランスフォーメーションから利益を得る市場の全てのアクターが、自らの社会的責任を引き受け、全ての欧州の人々の利益のために、公共財、公共サービス、インフラのコストに公正で均衡な貢献をするための、十分な枠組みを発展させること」がそれを規定しているとの分析がある。	デジタル課税についてはフランス政府が特に積極的に推進しており、フランスのほか、イタリアやスペインが導入済である。	類似の内容を定めるが、加盟国レベルの立法がEUレベルに拡大される可能性がある。
ワークライフバランスの権利(第II章)	全ての人が接続を切ることができ、デジタル環境でのライフワークバランスのためのセーフガードから利益を得ることができるよう確保すること。	フランス政府が近時導入した「労働者が接続を切る権利（“right to disconnect”）に近い内容を定めている。	類似の内容を定めるが、加盟国レベルの立法がEUレベルに拡大される可能性がある。
アルゴリズムやAIの透明性(第III章)	宣言では、AIやアルゴリズムの透明性を高めるとともに、差別を防ぐためこれらが適切なデータセットに基づいて構築されていることを規定する。また、アルゴリズムや人工知能などの技術が、健康、教育、雇用及び私生活に関するものなど、人々の選択を予断するために使われないことを確保することを規定する。	左記の内容についてはすでにAI規則案において一定程度規定されている。	類似する
表現・言論の自由と偽情報・フェイクニュース規制のバランス(第IV章)	宣言は、一方で表現の自由、公開の民主主義的議論、意見の多様性と、他方で偽情報、違法コンテンツの削除や有害コンテンツの事前抑制のバランスを規定している。 上記の実現について一般的な監視義務を設置するは否定されている。	デジタルサービス法案でも同様の立場が取られている	類似するが発展あり 将来の可能性も含めてより一般的な監視義務の否定に踏み込んだ表現となっている。
プラットフォーム規制(第II章、第IV章)	市場での公正競争の観点から特に大規模なプラットフォーマーやゲートキーパーの義務を定めている。また、特にSNSを念頭に置いていると考えられる、「人民を分断するのではなく団結させることを目指した技術にアクセスできるべきである」との規定もある。	デジタルサービス法案やデジタル市場法におけるゲートキーパー規制に類似するものである。	類似する
デジタル遺産(第V章)	「自らのデジタル遺産を決定でき、死後自らに関する公に利用可能な情報に何が起きるかを決定することができるべき」とされ、「異なるデジタルサービス間で個人データを容易に移動する可能性を確保すること」が規定される。 ただし、コミットメントとして具体的な動きは規定されていない。	議論はあるものの、具体的な政策や規制とはなっていない。	新規追加 具体的な権利として規定された点が新しい追加事項である。

出所) Dominik Arncken and Christoph Nüßing, “A Digital Magna Carta? The European Declaration of Digital Rights”
(https://www.jdsupra.com/legalnews/a-digital-magna-carta-the-european-4946481/)よりNRI作成

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

参考資料

デジタルの十年におけるデジタル権利及び原則に関する宣言(NRI仮訳)

■ European Declaration on Digital Rights and Principles for the Digital Decade

- 我々は、人間を中心とした、デジタルトランジションに関する欧州の方法を促進させることを目指す。それは欧州の価値に基づき、全ての個人とビジネスに利益をもたらすものでなければならない。
  したがって我々は以下の通り宣言する。

■ Chapter Ⅰ：デジタルトランスフォーメーションにおいて人間を中心とすること

- 人間は欧州のデジタルトランスフォーメーションの中心にある。技術は、完全に安全に、全ての欧州の人々の基本的権利を尊重して、全ての欧州の人々に仕え、益し、及び全ての欧州の人々に願望を追及する力を与えるべきである。
- 我々は以下にコミットする。
  - ―全ての人々を益し、全ての欧州の人々の生活を向上させるデジタルトランスフォーメーションのための民主的枠組を強化すること。
  - ―EUの価値及びEU法が認めた個人の諸権利が、オフラインと同様にオンラインで尊重されることを確保するために必要な措置をとること。
  - ―安全で安心なデジタル環境のため、公私問わず全てのデジタルアクターによる、責任ある誠実な行動を促進させること。
  - ―我々の国際関係においても、デジタルトランスフォーメーションについてのこのビジョンを積極的に促進させること。

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

参考資料

デジタルの十年におけるデジタル権利及び原則に関する宣言(NRI仮訳)

■ Chapter II ：連帯と包摂

- 全ての人々は、人民を分断するのではなく団結させることを目指した技術にアクセスできるべきである。デジタルトランスフォーメーションは、EUにおける公正な社会経済に貢献すべきである。
- 我々は以下にコミットする。
  - ―技術的ソリューションが人民の権利を尊重し、その行使を可能にし、包摂を促進させることを確保すること。
  - ―誰一人取り残さないデジタルトランスフォーメーション。これはとくに、高齢者、障がいを持つ又は周縁におかれた人、弱い立場にいる又は市民権をはく奪された人、及びそれらを代表して行動する人を含む。
  - ―デジタルトランスフォーメーションから利益を得る市場の全てのアクターが、自らの社会的責任を引き受け、全ての欧州の人々の利益のために、公共財、公共サービス、インフラのコストに公正で均衡な貢献をするための、十分な枠組みを発展させること。

- コネクティビティ
- 全ての人は、EUのどこでも、手頃な価格で高速なデジタルコネクティビティにアクセスできるべきである。
  我々は以下にコミットする。
  - ―全ての人のため、居所や収入に関係なく、優れたコネクティビティへのアクセスを確保すること。
  - ―内容、サービス、及びアプリケーションが不正にブロック又は劣化されない、中立でオープンなインターネットを保護すること。

- デジタル教育及び技能
- 全ての人は教育、訓練、生涯学習に対する権利を有し、全ての基本的及び応用のデジタル技能を獲得することができるべきである。
  我々は以下にコミットする。
  - ―全ての教育及び訓練機関にデジタルコネクティビティ、インフラ及びツールを備える努力を促進させ、支援すること。
  - ―学習者及び教育者が、経済、社会及び民主的プロセスに積極的に参加する、全ての必要なデジタル技能及びコンピテンスを獲得し共有することを可能にする努力を支援すること。
  - ―全ての人に、スキルアップ及びリスキリングを通じて、職業のデジタル化によってもたらされた変化に適応する可能性を与えること。

デジタルの十年におけるデジタル権利及び原則に関する宣言(NRI仮訳)

■ Chapter Ⅱ ：連帯と包摂(続き)

- 労働条件
- 全ての人は、雇用形態、モダリティ又は期間に関わらず、現実の職場におけると同様に、デジタル環境において、公正、正義、健康で安全な労働条件、及び適切な保護に対する権利を有する。
  我々は以下にコミットする。
  - ―全ての人が接続を切ることができ、デジタル環境でのライフワークバランスのためのセーフガードから利益を得ることができるよう確保すること。

- オンラインでのデジタル公共サービス
- 全ての人は、EU全体の重要なオンラインでの公共サービスにアクセスできるべきである。誰も、デジタル公共サービスのアクセス及び利用の際に、必要以上にデータを提示することを求められない。
  我々は以下にコミットする。
  - ―全ての欧州の人々が、幅広いオンラインサービスへのアクセスを提供する、アクセス可能で安全で信頼できるデジタルアイデンティティを与えられるよう確保すること。
  - ―政府情報の広範なアクセス可能性と再利用を確保すること。
  - ―EUじゅうの途切れない安全で相互利用可能な、医療関連記録を含む、人々の需要に合うよう設計されたデジタルヘルス及びケアサービスへのアクセスを促進させ支援すること。

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

参考資料

デジタルの十年におけるデジタル権利及び原則に関する宣言(NRI仮訳)

■ Chapter III ：選択の自由

- アルゴリズムと人工知能システムの相互作用
- 全ての人は、デジタル環境での選択肢を知らされ、自ら人工知能のアドバンテージから利益をえる権利を与えられるべきであると同時に、自らの健康、安全、基本的権利に対するリスク及び損害から保護されるべきである。
  我々は以下にコミットする。
  - ―アルゴリズム及び人工知能の利用についての透明性を確保し、人々がそれらと関わるとき権利を与えられ知らされることを確保すること。
  - ―アルゴリズムのシステムが、違法な差別を避けるための適切なデータセットに基づいており、人民に影響を与える結果についての人間による監視が可能であるよう確保すること。
  - ―アルゴリズムや人工知能などの技術が、健康、教育、雇用及び私的生活に関するものなど、人々の選択を予断するために使われないことを確保すること。
  - ―人工知能及びデジタルシステムが、安全で、完全に人民の基本的権利を尊重して、利用されることを確保するためのセーフガードを提供すること。

- 公正なオンライン環境
- 全ての人は、いずれのオンラインサービスを利用するかを、客観的、透明で信頼ある情報に基づいて実効的に選択することができるべきである。
- 全ての人は、デジタル環境において公正に競い、イノベートする可能性をもつべきである。
  我々は以下にコミットする。
  - ―基本的権利が保護され、並びに、プラットフォームの責任が、とくに大規模なプレイヤー及びゲートキーパーが、よく規定される、安全、安心で公正なオンライン環境を確保すること。

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

デジタルの十年におけるデジタル権利及び原則に関する宣言(NRI仮訳)

■ Chapter IV：デジタル公共空間への参加

- 全ての人は、信頼できる、多様で多言語のオンライン環境にアクセスできるべきである。多様な内容へのアクセスは多元的な公的議論に貢献し、全ての人が民主主義に参加することを可能にするべきである。
- 全ての人は、検閲され又は脅される恐れなく、オンライン環境において表現の自由に対する権利を有する。
- 全ての人は、自らが利用するメディアサービスを誰が所有し管理するのかを知る手段を有するべきである。
- 非常に大規模なオンラインプラットフォームは、世論及び公の議論(public discourse)の形成におけるそのサービスの役割を考慮して、オンラインでの自由な民主的議論を支援すべきである。彼らはサービスの機能及び利用から生じる、偽情報キャンペーンを含む、リスクを最小限にし、表現の自由を保護するべきである。
  我々は以下にコミットする。
  - ―市民的関与及び民主的参加を促すための技術の発展及び最大利用を支援すること。
  - ―オンラインにおける基本的権利、とりわけ表現及び情報の自由のセーフガードを継続すること。
  - ―いかなる一般的な監視義務を設置することなく、表現及び情報の自由に対する権利を完全に尊重して、それがもたらす不利益と比例させて、あらゆる形態の違法な内容に取り組むための措置を執ること。
  - ―人民が差別及びその他の形態の有害な内容から保護される、オンライン環境を創設すること。

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

参考資料

デジタルの十年におけるデジタル権利及び原則に関する宣言(NRI仮訳)

■ Chapter Ⅴ：安全、安心及び権利付与

- 保護された、安全で安心なオンライン環境
- 全ての人は、安全、安心で、設計上プライバシーが守られた、デジタル技術、プロダクツ、サービスにアクセスできるべきである。
  我々は以下にコミットする。
  - ―データ侵害及びサイバー攻撃を含むサイバー犯罪から、人民、ビジネス、公的機関の利益を保護すること。これには、アイデンティティセフト又はマニピュレーションからデジタルアイデンティティを保護することが含まれる。
  - ―オンライン上の安全と欧州のオンライン環境の統合を弱体化させようとする者、又はデジタルを用いて暴力及び憎悪を促進させる者に対抗し、責任を負わせること。

- プライバシーと、データに対する個人のコントロール
- 全ての人は、オンラインにおいて自らの個人データの保護に対する権利を有する。その権利は、データがどのように使われ、だれに共有されるのかについてのコントロールを含む。
- 全ての人は、電子機器を用いた自らの通信及び情報の機密性に対する権利を有する。誰も違法なオンラインサーベイランス又はインターセプション措置に晒されてはならない。
- 全ての人は自らのデジタル遺産を決定でき、自らの死後それに関連する公に利用可能な情報に何が起きるかを決定することができるべきである。
  我々は以下にコミットする。
  - ―異なるデジタルサービス間で個人データを容易に移動する可能性を確保すること。

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.

参考資料

デジタルの十年におけるデジタル権利及び原則に関する宣言(NRI仮訳)

■ Chapter Ⅴ：安全、安心及び権利付与(続き)

- 子供と若者はオンライン上で保護され能力が与えられるべき
- 子供と若者は、安全で情報に基づいた選択を行い、オンライン環境における自らのクリエイティビティを表現する能力を与えられるべきである。
- 年齢に応じた素材が、子供の経験、幸福及びデジタル環境への参加を向上させるべきである。
- 子供は、デジタル技術を通じて実行される又は促進される全ての犯罪から保護される権利を有する。
  我々は以下にコミットする。
  - ―子供及び若者のための、ポジティブで年齢に応じた、安全なデジタル環境を促進させること。
  - ―全ての子供に、オンライン環境を活動的かつ安全に渡り、オンラインでの選択を情報に基づいて行うのに必要な技能及びコンピテンスを獲得する機会を提供すること。
  - ―全ての子供を、オンラインでの有害で違法な内容、搾取、マニピュレーション及び虐待から保護し、デジタル空間が犯罪の実行又は促進に利用されることを防止すること。

■ Chapter Ⅵ：持続可能性

- 環境への深刻な損害を避けるため、及び循環型経済を促進させるため、デジタル製品及びサービスは、環境及び社会への悪影響を最小限に抑える方法で設計され、生産され、使用され、処理され、リサイクルされるべきである。
- すべての人は、責任ある選択ができるように、デジタル製品及びサービスの環境への影響及びエネルギー消費に関する、正確で理解しやすい情報にアクセスできるべきである。
  我々は以下にコミットする。
  - ―環境及び社会への影響が最小の、持続可能なデジタル技術の発展及び利用を支援すること。
  - ―環境及び気候への好影響あるデジタルソリューションを発展させ配備すること。

Copyright(C) Nomura Research Institute, Ltd. All rights reserved.