

平成29年度産業経済研究委託事業

# 海外におけるデータ保護制度に関する 調査研究

## 調査報告書

平成29年11月

 **MUFG** 三菱UFJリサーチ&コンサルティング

## 目次

はじめに：本調査の目的.....	4
サマリー .....	7
第1章 アメリカ.....	9
1．概要.....	9
(1) 法制度.....	9
(2) 政策動向.....	10
2．営業秘密 .....	11
(1) 概説 .....	11
(2) 州法 .....	11
(3) 連邦法.....	13
(4) 営業秘密によるデータ保護.....	15
3．不正アクセス行為の規制.....	16
(1) 概説 .....	16
(2) コンピュータ犯罪取締法.....	17
(3) 不正アクセス行為の規制によるデータ保護 .....	17
4．契約.....	18
5．知的財産法.....	19
(1) 著作権法によるデータ保護の沿革.....	19
(2) DMCA.....	20
(3) DMCA の評価・運用 .....	20
6．プライバシーデータに係る取扱い.....	21
7．データの保護可能性 .....	21
第2章 欧州（欧州委員会）.....	24
1．概要.....	24
2．データベース保護指令.....	25
(1) 指令の特徴.....	25
(2) 具体的な規定の内容.....	25
(3) 現在における評価.....	26
3．営業秘密保護指令.....	27
(1) 指令の特徴.....	27
(2) 具体的な規定の内容.....	28
(3) 現在における評価.....	28
4．単一デジタル市場戦略とデータ保護.....	29
(1) 欧州単一デジタル市場戦略.....	29
(2) 欧州委員会コミュニケーションペーパー .....	29

(3) 現在における評価とさらなる取組み .....	30
(4) 非パーソナルデータの域内における自由な流通のための枠組みに関する規則草案 .....	31
5. 契約上の取扱い .....	32
第3章 ドイツ .....	33
1. 概説 .....	33
(1) ドイツにおける関連法制の概要 .....	33
(2) 政策動向 .....	33
(1) 概要 .....	33
(2) UWG .....	34
(3) 新法(営業秘密法) .....	36
3. 契約 .....	36
4. 不正行為 .....	37
5. データの保護可能性 .....	37
(1) 自動車業界によるガイドライン策定の動き .....	37
(2) データベース保護指令及び同国内法 .....	38
(3) 産業界、研究所等のデータの保護・利活用をめぐる新たな動き .....	39
第4章 フランス .....	40
1. 概説 .....	40
(1) フランスにおける関連法制の概要 .....	40
(2) 政策動向 .....	41
2. 営業秘密 .....	41
(1) 概要 .....	41
(2) 「製造秘密」及び「営業秘密」に係る知的財産法典、労働法典及び刑事罰 .....	42
3. 雇用における忠誠義務 .....	42
4. 契約 .....	43
5. データの保護可能性 .....	43
第5章 イギリス .....	44
1. 概説 .....	44
(1) イギリスにおける関連法の概要 .....	44
(2) 政策動向 .....	44
2. 営業秘密 .....	45
(1) 概要 .....	45
(2) 保護の対象及び問題となる行為 .....	46
(3) 救済 .....	46
3. 競争法 .....	47

4 . 不正アクセス .....	48
5 . 契約 .....	49
6 . プライバシーデータ .....	49
第 6 章 中国 .....	51
1 . 概説 .....	51
( 1 ) 中国における関連法制の概要 .....	51
( 2 ) 政策動向 .....	51
2 . 反不正競争法 .....	51
3 . サービス業革新発展大綱 ( 2017 ~ 2025 年 ) .....	53
4 . データの保護可能性 .....	53
第 7 章 世界知的所有権機関 ( World Intellectual Property Organization : WIPO ) ....	55
1 . 概説 .....	55
( 1 ) WIPO における関連法制の概要 .....	55
( 2 ) 政策動向 .....	55
2 . WIPO 著作権条約におけるデータベース保護 .....	55
( 1 ) 規定の特徴 .....	55
( 2 ) 検討の経緯 .....	56
第 8 章 経済協力開発機構 ( Organization for Economic Co-operation and Development : OECD ) .....	57
1 . 概説 .....	57
( 1 ) OECD における関連法制の概要 .....	57
( 2 ) OECD プライバシーガイドライン ( 1980 年策定、2013 年改訂 ) .....	57
( 3 ) OECD における関連委員会活動等の概要 .....	58
( 4 ) 科学・技術・革新総局 ( Directorate for Science, Technology and Innovation : DSTI ) の取組み .....	60
( 5 ) 医療ガバナンスに関する理事会勧告 .....	61
( 参考 ) 各国・国際機関比較表 .....	62
アメリカ .....	63
欧州委員会 .....	64
ドイツ .....	65
フランス .....	66
イギリス .....	67
中国 .....	68

## はじめに：本調査の目的

AI、IoTが実装される第四次産業革命においては、データの収集・活用や関連技術の開発は企業の競争力の源泉となることから、その利活用を進めることが我が国産業のさらなる発展のために極めて重要な課題となっている。

データ利活用を円滑に進めるためには、その利活用と保護のバランスの取れた柔軟な知的財産制度を構築することが必要であり、保護制度としていかにあるべきかについて活発に議論されているところである。

こうした議論を進めるにあたって、諸外国におけるデータの保護制度について把握し、我が国の保護制度検討の参考にしつつ検討を進めることは極めて重要であるところ、海外におけるデータの保護に関する制度については、十分な調査が行われておらず、制度の運用状況やユーザーからの評価、新たな制度の検討状況のような周辺状況については、断片的にしか把握できていないのが実情である。

越境的なデータ流通が加速する第四次産業革命においては、国際調和を図ることも一層重要となる中、このように、諸外国の制度やその検討状況に関する情報の不足は、我が国におけるデータの保護制度の検討を進めるにあたり、大きな障害となることが予想され、また、諸外国における情報の不足により、民間企業からは、海外でのデータの収集・活用をおこなうビジネスの展開を躊躇してしまうといった意見を聞くことも多く、制度面以外での施策においても重要となる情報であるといえる。

そのために、本調査においては、諸外国におけるデータ保護に関する制度等について実態調査を行い、我が国における制度との比較をおこなった。その際、単に条文等の違いを比較するのみでは、各国におけるデータ保護の実態や我が国における議論への示唆を得ることは難しいことから、各国におけるデータ保護の在り方に関する議論についても可能な限り調査をおこなった。本調査結果が、我が国における議論に有益な示唆を提供できれば幸いである。

なお、本調査は文献調査に加えて、各国現地における関係者等へのヒアリングを実施している。イギリス、中国の現地関係者へのヒアリングについてはオリック・ヘリントン&サトクリフ LLP の協力を得た他、当社研究員がアメリカ及びフランスの現地調査を実施した際には同事務所の弁護士にも法律専門家としてヒアリングにご協力を頂いた。また同事務所の矢倉信介パートナー弁護士には同事務所海外拠点との調整と法律専門家としての助言を頂いた。

<調査対象国・国際機関>

アメリカ、欧州（欧州委員会）、ドイツ、フランス、イギリス、中国、世界知的  
所有権機関（WIPO）、経済協力開発機構（OECD）

<現地調査期間>

アメリカ、欧州（欧州委員会）、ドイツ、フランス、WIPO、OECD：平成 29  
年 6 月

イギリス、中国：平成 29 年 8 月

## < 本調査における「データ」の定義 >

本調査では、データ利活用に係わるデータの種類を、「個人情報」「パーソナルデータ」「価値あるデータ（事業活動において有用であり、企業が投資しているデータ）」「目的のもと取得・編集・加工されているデータ」の4つに大別し、特に「価値あるデータ」に着目し、その他のデータは「価値あるデータ」との対比として調査した。

データの種類	データイメージ	企業におけるデータ利活用例
その他データ		
目的のもと取得・編集・加工されているデータ (経済価値の有無は不明)	自然現象・社会現象について公的な目的等で取得・公開しているデータ。 ・気象情報、交通情報、人口動態データ等 ・公的機関による取得・公表に加えて、民間企業による取得・有償提供(例:気象情報サービス)や、公的機関によるローデータの有償提供もある。	「価値のあるデータ(事業活動において有用であり、企業が投資しているデータ)」「パーソナルデータ」「個人情報」との組み合わせによるビッグデータ化。 当該データ(目的のもと取得・編集・加工されているデータ)の有償提供。等
価値あるデータ (事業活動において有用であり、企業が投資しているデータ)	事業活動において発生するデータ。 ・工場・プラントの生産設備の稼働データ、産業用移動体機械(建機、車両、航空機等)の位置情報データ、設備(空調、昇降機、OA機器等)の稼働データ、研究データ(実験・計測データ等)、法人顧客情報等、個人と切り離されたデータ。	稼働データと製品耐用年数に基づく、機器のメンテナンス・修繕、予防保全サービス。 生産現場・建設現場等の工程改善コンサルティング。 交通車両・航空機の運航コンサルティング。 R&Dの精度向上・効率化。等
パーソナルデータ 「個人情報の利活用と保護に関するハンドブック」を参照	「個人情報」に限定されない、個人の行動・状態に関するデータ。 ・Web閲覧・遷移・購買データ、店舗内行動データ、自動車走行データ、移动通信端末等から発信される個人の位置情報、体温・血圧等のバイタルデータ等。	SNS、Webポータルサービス、EC等のインターネットサービスにおけるパーソナルレコメンデーション、商品開発。 小売、飲食、その他リテールサービスにおける顧客行動分析に基づく店舗内マーケティング、商品開発。 自動走行、自動車の商品開発。 個人向け健康管理サービス、法人向けバイタルデータ販売。等
個人情報 「改正個人情報保護法」第2条を参照	生存する特定の個人を識別できる情報であり、氏名、生年月日、その他の記述等、及び個人識別符号。 ・DNA、顔、虹彩、声紋、歩行の態様、手指の静脈、指紋・掌紋、旅券番号、基礎年金番号、免許証番号、住民票コード、マイナンバー、各種保険証等。	SNS、Webポータルサービス、EC等における会員向けサービス、銀行、証券、クレジットカード等の金融サービスにおける個人認証。 小売、飲食、その他リテールサービスにおける会員向けサービス。等

## サマリー

データ保護については、アメリカ・欧州委員会・ドイツ・フランス・イギリス・中国でおおよそ営業秘密や契約による保護が基本となるという考え方は共通であった（ただし営業秘密に関する法体系は各国で異なる）。

アメリカでは、価値あるデータについては、営業秘密に該当する場合には営業秘密によって保護することが基本であり、連邦法によりサポートされるという意見である。アメリカの現行法において各法令がパッチワークのような状態であり、重複性もあるが、ロバスト性の高い保護を実現している。一方で、営業秘密に該当しないデータにつき、契約関係のない第三者による不正取得に対する保護は十分でないとの指摘もある。今般日本で検討している行為規制のアプローチがベストプラクティスとなり、各国に普及させていくことを期待している。なお、権利付与型の保護はデータの流通を阻害するため、適していないとの意見である。

欧州委員会では、価値あるデータは、契約による保護を基本としている。契約外の第三者による不正取得に対しては、営業秘密、競争法、サイバーセキュリティ法、内部告発者保護法等の各国現行法の範囲内で保護されるものがあると認識されている。

ドイツでは、価値あるデータは、契約による保護を基本としており、第三者による不正取得については、当該データが営業秘密に該当する場合には営業秘密で規制するという考えである。また、自動車業界による自主的ガイドラインを策定する動きがあり、産業界から注目されている。

フランスでは、価値あるデータは、契約及び営業秘密で対応可能なものについては、それぞれに基づいて保護されるという考えである。フランス国内法において営業秘密は製造秘密としての刑事的保護と民法による一般不法行為の規制により保護される。

イギリスでは、価値あるデータは、営業秘密（機密情報の保持）、競争法、コンピュータ不正使用法で対応可能な範囲内で保護されるという考えである。営業秘密はコモン・ローに基づいている。

中国では、価値あるデータは、営業秘密に該当する場合には営業秘密で保護されるという考えである。サービス業革新発展大綱による知的財産権保護制度の整備については、本報告書作成時点では具体的な法制度の検討・立案は確認されていない。



国・国際機関	データ保護に関する考え	法制度によるデータ保護				契約によるデータ保護における特徴	権利付与によるデータ保護における特徴	その他動向
		営業秘密		不正アクセス				
		制度名称	民事：刑事	制度名称	民事：刑事			
アメリカ	<ul style="list-style-type: none"> <li>価値あるデータは、営業秘密関連法、その他現行法、契約等によってロバスト性の高い保護を実現している。一方で、契約関係にない第三者による不正取得等に対する懸念もある。</li> </ul>	不法行為法リステイトメント 連邦経済スパイ法 (EEA) 統一営業秘密法 (UTSA) 連邦営業秘密保護法 (DTSA)	-	コンピュータ犯罪取締法 (刑法第1030条)	-	懲罰的損害賠償	連邦著作権法 (インターネット上のコンテンツを対象としたデジタルミレニアム著作権法)	-
欧州委員会	<ul style="list-style-type: none"> <li>価値あるデータは、契約による保護を基本としている。契約外の第三者による不正取得に対しては、営業秘密、競争法、サイバーセキュリティ法、内部告発者保護法等の各国現行法の範囲内で保護されるものがあるという考え。</li> </ul>	営業秘密保護指令	-	-	-	モデル契約開発中	データベース保護指令 (著作権と sui generis による保護)	単一デジタル市場戦略
ドイツ	<ul style="list-style-type: none"> <li>価値あるデータは、契約による保護を基本としており、第三者による不正取得は営業秘密に該当する場合には営業秘密で規制するという考え。</li> </ul>	不正競争防止法 (UWG) 民法 (823条, 1004条)	-	刑法202a,b条	-	-	データベース保護指令に基づく国内法	自動車業界による自主的ガイドライン
フランス	<ul style="list-style-type: none"> <li>価値あるデータは、契約及び営業秘密で対応可能なものについてはそれぞれについて保護。</li> </ul>	知的財産法典 (621-1条) 民法典 (1382, 1383条) 労働法典 (1227-1条) 刑法典 (311 2, 313 1条)	-	刑法典 (323 1, 323 3条)	-	-	知的財産法典 (341-1条) (著作権)	-
イギリス	<ul style="list-style-type: none"> <li>価値あるデータは、営業秘密 (機密情報の保持)、競争法、コンピュータ不正使用法等対応可能な範囲内で保護。</li> </ul>	コモン・ロー	-	コンピュータ不正使用法 (1条, 3条)	-	-	データベース保護指令に基づく国内法	-
中国	<ul style="list-style-type: none"> <li>価値あるデータは、営業秘密に該当する場合には営業秘密で保護</li> </ul>	反不正当竞争法 民法通則 (118条) 刑法 (219条)	-	サイバーセキュリティ関連法	-	-	-	サービス業革新発展大綱

なお、法律専門家によればイギリスでは「商業上センシティブな情報」に該当する場合は、当該データは競争法が適用されるとの見解。

## 第1章 アメリカ

### 1. 概要

#### (1) 法制度

連邦国家であるアメリカにおける法は、基本的に州法と連邦法によって構成されている。営業秘密は、州法におけるコモン・ローにより保護されてきたが、連邦刑事法において営業秘密の保護を強化するため、1996年に連邦経済スパイ法（Economic Espionage Act：EEA）が制定され、20年以上運用されてきた。近年まで連邦法としては、刑事的救済のみが取扱われ、民事的救済はもっぱら州法によっていたが、2016年に連邦営業秘密保護法（Defend Trade Secrets Act：DTSA）が制定されたことで連邦レベルでも民事的救済を求めることが可能となった点が注目されている。

不正アクセス行為の禁止についても州法及び連邦法が刑事的救済を規定している。コンピュータ・ネットワークにおける不正アクセスの規制は、州間・国際間でも起こりうることから、連邦法における規制が重要であるとされ、連邦刑法第1030条を改正する形で法整備が行われている。中でもコンピュータ犯罪取締法では、コンピュータに対する不正なアクセス行為と、コンピュータ及びデータへ損害を与える行為を規制している。

知的財産法の領域においては、伝統的に連邦著作権法が「額に汗（sweat of the brow）の理論」を用いて編集著作物や事実・データを集積した編集物を保護してきた。1990年代にはデータベース保護について、連邦著作権法による保護のアプローチが検討されていたが、司法において創作性を求める傾向が強まる中、データベース自体のオリジナリティが否定されたことや、権利取得がデータベースの流通を阻害し、市場形成に寄与していないという意見が産業界から上がったことから、データ保護における保護手段として著作権は適切ではないとみられている。このような考え方は、インターネット上でデジタルコンテンツが数多く取扱われるようになる中、1998年に制定されたデジタルミレニアム著作権法（Digital Millennium Copyright Act：DMCA）による連邦著作権法改正以降も維持されている。

「価値あるデータ」の保護については、今回実施した現地調査においても、特に産業界から契約による保護を尊重すべきであるとの声も聞かれたところである。アメリカにおける民事救済は、コモン・ロー上、金銭賠償が原則であり、差止請求が認められるのは金銭賠償では救済が不十分である場合に限られるというのが一般的な理解であるが、実務上は契約書の中に、あらかじめ秘密保持義務違反による損害は金銭賠償だけでは救済が不十分であることから、差止請求権を発生させることを明記するといった運用も広く行われている<sup>1</sup>。もっとも契約関係のない第三者が秘密情報を侵害した場合には、契約違反に基づく民事

<sup>1</sup> この点、アメリカの実務に詳しい法律専門家によれば、契約書上、差止請求が可能であることが明記されている場合であっても、金銭賠償の原則によらないで差止を求める必要性については裁判所において判断されることになるとの指摘があった。

的救済を受けることはできず、不法行為による民事救済を受けることとなる。不法行為の場合にも差止請求は認められる可能性があるが、上記金銭賠償の原則の適用を受けることは契約違反の場合と同様である<sup>2</sup>。民事的救済を受けることができる点においては、我が国とアメリカの制度は類似しているものの、損害賠償においてアメリカには懲罰的損害賠償制度が存在する点も留意すべき点としてあげられる。

以上のようにアメリカにおける関連法制度を概観すると、現行法によるデータ保護は、各法令（営業秘密の保護、不正アクセスの規制、契約、著作権による権利付与）によって保護対象や規制行為がパッチワークのように構成されており、重複する部分もあるが、堅牢性の高い保護を実現していると認識されている<sup>3</sup>。

## （２）政策動向

データは現行法によって一定程度保護されうると考えられており、2016年のDTSA 制定後、新たな制度制定の動きはない。DTSA 制定に際しては連邦議会においても様々な議論が行われているが、議会資料によれば、アメリカにおける産業界にとって営業秘密保護が以前にも増して重要となっているという現状認識が示されている。具体的には、アメリカ企業が保有する資産の約 8 割が無形資産（intangible）であり、その大多数が営業秘密であるとの現状認識<sup>4</sup>や、アメリカにおける公開企業（Publically Traded Companies）が 5 兆ドルの価値を有する営業秘密を保有しているといった現状認識<sup>5</sup>が示されている。その中で、今日の企業は、データないし事業上重要な情報をクラウド上で保管することが多くなり、企業は当該営業秘密にアクセスし、活用・蓄積することが必要な製造事業者やサービス提供者とのネットワークに依存していることから、秘密情報を共有する能力は、アメリカ経済の成長に極めて重要であるといった指摘もなされている<sup>6</sup>。その意味で、今回調査対象としている「価値あるデータ」についても一定程度が営業秘密に該当し、DTSA によって一応の手当てがなされているとの理解がある程度存在している。

現地調査においても法律専門家からは、営業秘密によって「価値あるデータ」の保護も一定程度対応しうる問題であるとの指摘<sup>7</sup>があった一方で、政府関係者からは、技術革新の進展を見守りつつ、利害対立を調整する意味でも政府主導でトップダウンの制度を検討する必要があるとの指摘もあった<sup>8</sup>。ただし、デー

<sup>2</sup> この点について法律専門家によれば、不法行為の方が、契約違反の場合や明確に営業秘密侵害に該当する場合に比べると、差止請求が認められるためのハードルは高くなるというのが、一般的な実務感覚であるとの指摘があった。

<sup>3</sup> 現地調査（法律専門家）より。

<sup>4</sup> 162 CONG.REC S1626.

<sup>5</sup> 162 CONG.REC H2033.

<sup>6</sup> 162 CONG.REC S1626.

<sup>7</sup> 現地調査（法律専門家）より。

<sup>8</sup> 現地調査（政府関係者ヒアリング）より。

タによって利活用の方法が異なり、保護手段もデータの利活用の実態を捉え、業種別に検討する必要があると考えられている。現在は業種別のワークショップを開催し、産業界や有識者の意見を聞く等の動きがみられる<sup>9</sup>。

## 2．営業秘密

### (1) 概説

アメリカにおける営業秘密は従来、トレード・シークレットとして各州法におけるコモン・ローによって保護されてきた経緯があり、基本的な営業秘密の保護対象や行為規制の原型は古くから判例によって形作られてきた。後述するように、統一的な理解は、不法行為法リステイメント( Restatement of Torts ) や統一営業秘密法( Uniform Trade Secrets Act : UTSA ) によって整理されているが、リステイメントにおいて不法行為法の一部として整理されていることから分かるように、営業秘密は不法行為に基づく民事的救済によって保護するというのが州法の元来的な保護の考え方であった。

刑事的保護については各州法が営業秘密の窃盗を処罰する特別規定を置く等して保護してきたが、1996年に初めて連邦レベルで営業秘密を保護する EEA が成立し、刑事的保護を定めた。その後も民事的保護は長らく州法に委ねられてきたが、2016年に DTSA により連邦レベルでの民事的救済が制定されたことで、営業秘密について運用の柔軟性と秘密情報の保護性が高まっている。

なお、民事的保護における損害賠償については、前掲のとおり、アメリカは懲罰的損害賠償により、実際に生じた損害の金額を超える賠償額が認められる場合がある。

### (2) 州法

#### 州法における沿革

各州のコモン・ローによって発展したトレード・シークレットについて統一的な理解が示された初期のモデル法として、1939年に米国法律協会( American Law Institute : ALI ) が発表した不法行為法リステイメントを指摘することができる。不法行為法リステイメントによれば、「営業秘密は、事業において利用され、当該情報について知らないか利用していない競合業者よりも優位に立つ機会を与える製法、パターン、装置、又は、情報の編集物である。化学化合物の製法、製造・物質の取扱いや保護の過程、機械その他の装置のパターン、顧客リスト等が考えられる」と定められている<sup>10</sup>。また、規制する行為については、不正な手段による情報の入手や開示に係る不法行為責任を認めるという形

<sup>9</sup> 現地調査(政府関係者ヒアリング)より。

<sup>10</sup> Restatement (First) of Torts (1939) § 757. 訳語は、経済産業省(委託先:三菱総合研究所)「諸外国における営業秘密保護制度に関する調査研究報告書」(2014年)27頁参照。

で規定している<sup>11</sup>。

不法行為法リステイメントが策定された後も、各州法における営業秘密に係るコモン・ローの発展度合いに差異があったことや、営業秘密保護の要件や救済等のあり方について異なる点が存在していたため<sup>12</sup>、これを克服する目的で1979年に統一州法委員全国会議において、UTSAが採択され、各州に本法をモデルとした州法を制定するよう勧告された<sup>13</sup>。

## UTSA

UTSAは、営業秘密の不正取得（misappropriation）に対する民事的救済を規定しており、不正取得や営業秘密に係る定義（1条）を定め、差止請求（2条）、損害賠償請求、不当利得返還請求、懲罰的損害賠償等（3条）を定めている。不正取得自体の理論も不正競争行為に係る州法におけるコモン・ローとして発展してきたものであるが、いわゆるINS判決<sup>14</sup>が不正競争（unfair competition）行為の一類型として不正取得を位置づけて以来、第三者にただ乗りするという多様な行為について救済の根拠となってきた経緯がある。

UTSAでは営業秘密の不正取得について、不正な手段（窃盗、贈収賄、不実表示、秘密保持義務違反もしくはその教唆、又は電子的もしくはその他の手段によるスパイ行為）による取得、開示、使用であるとしている<sup>15</sup>。営業秘密自体の定義については、「（ ）一般的に知られておらず、かつ、その開示又は利用により経済的価値を得ることができる他の者が適切な手段により解明することは容易ではないものから、独立した現実の又は潜在的な経済価値を引き出し、かつ、（ ）秘密性を維持するのに状況に鑑みて合理的な努力が必要な、情報、製法、パターン、編集物、プログラム、装置、方法、技術、又は、プロセス」であるとしている<sup>16</sup>。

## 統一営業秘密法の運用・評価

UTSAは、ニューヨーク州、マサチューセッツ州、ノースカロライナ州を除く、47州とコロンビア特別区等において採用されており<sup>17</sup>、各州法に大きな影響を与えている。州内における営業秘密侵害に関する民事的救済は州法で対応されていることから、後述するDTSAにおいて連邦法における営業秘密の民事的救済規定が整備された後も、UTSAに準拠した各州法が運用されている。そ

<sup>11</sup> Restatement (First) of Torts (1939) § 758-759.

<sup>12</sup> 千野直邦『営業秘密保護法』（中央経済社、2007年）106頁。

<sup>13</sup> Richard F. Dole, Jr., Identifying the Trade Secrets at Issue in Litigation under the Uniform Trade Secrets Act and the Federal Defend Trade Secrets Ant, 33 Santa Clara High Tech. L.J.470 (2017).によれば、第二次不法行為法リステイメントから営業秘密に係る記述が削除されることとなったこともUTSAの策定に繋がったと指摘されている。

<sup>14</sup> International News Service v. Associated Press, 248 U.S.215 (1918).

<sup>15</sup> UTSA § 1(1)(2).

<sup>16</sup> UTSA § 1(4). 訳語については、経済産業省（2014年）・前掲注を参照。

<sup>17</sup> Brian T. Yeh, Protection of Trade Secrets: Overview of Current Law and Legislation, CRS Report (2016) p.6.

のため、UTSA は今なお、アメリカ国内の営業秘密保護において活用されている法制度といえる<sup>18</sup>。

UTSA が、州間のハーモナイゼーションをもたらしているかどうかという点については見解が分かれており、肯定的な意見もある一方で、各州は UTSA を独自に解釈し、州裁判所も UTSA をそれぞれに解釈していることから否定的に捉えている見解も少なくない<sup>19</sup>。

### (3) 連邦法

#### 連邦法における沿革

前掲のようにアメリカの営業秘密はリストイメントや UTSA によって州法の領域で取扱われてきたが、UTSA の制定以降、産業におけるデジタル化の急速な展開と、物理的な侵害行為を伴わない営業秘密の不正取得が容易になってきた状況への対応が要請されていた<sup>20</sup>。また、州をまたぐ営業秘密の不正取得回避について、連邦刑事法<sup>21</sup>が盗難財産の州際取引等の規制に係わる制定法として存在していたが、直接的に営業秘密を保護するものではなかった。係る背景を踏まえて、連邦刑事法として直接的に営業秘密の保護を強化するため、1996 年に EEA が制定され、営業秘密の侵害を処罰するよう規定された。また、民事における営業秘密侵害訴訟について連邦裁判所で扱うことができるよう、2016 年に DTSA が制定され、これにより、連邦法での刑事・民事の双方での救済のための法制度が整備された。

#### EEA

EEA は、外国政府・機関・職員による営業秘密の不正取得<sup>22</sup>、及び民間の個人・企業による営業秘密の不正取得<sup>23</sup>の 2 つを規定している。

営業秘密の定義に係る特徴として、有形物だけでなく無形物を明示的に含めている点、電子的記録等の保管方法を問わない点、財務的、事業的、科学的、技術的、経済的又は工学的情報に関する図案、計画、編集物、プログラム機器、製法、設計、試作品、方法、技術、過程、手続、プログラム又はコードを含む規定となっている点等を指摘することができる<sup>24</sup>。また秘密保持のために合理的な措置を講じていること、当該情報が公衆に一般的に知られていないか、適切な方法で解明することができないということから、現実又は潜在的な独立した経済価値を有することも明記されている<sup>25</sup>。

<sup>18</sup> 現地調査（政府関係者ヒアリング）より。

<sup>19</sup> Kaylee Beauchamp, *The Failure of Federalizing Trade Secrets: Why the Defend Trade Secrets Act of 2016 Should Preempt State Law*, 86 *Miss. L.J.* 1031.

<sup>20</sup> 千野・前掲注、125 頁。

<sup>21</sup> 窃盗罪の規定を中心に対処する州法及び盗品運搬、詐欺等の規定で処理する連邦法が存在。

<sup>22</sup> 18USC § 1831.

<sup>23</sup> 18USC § 1832.

<sup>24</sup> 18USC § 1839(3). UTSA の定義よりも具体例が多く列挙されている。

<sup>25</sup> 18USC § 1839(3)(A)(B).

禁止行為については、営業秘密の窃取（窃取、不正流用、漏えい・隠匿、詐欺・偽計による取得）、複製（許諾ない複製、複製、スケッチ、描画、撮影、ダウンロード、アップロード、改変、写真複製、再製、送信、送付、郵送、コミュニケーション又は伝達）、営業秘密侵害があることを知りながら当該営業秘密を受領、購入、所有することと定めている<sup>26</sup>。また EEA は当該禁止行為について、未遂や共謀行為についても禁止している。

EEA は、その後の判例を受けて、対象の明確化や罰則を強化する形で改正され、2012 年には営業秘密不正取得明確化法によって機密性のあるコンピュータ・プログラムが営業秘密の保護対象になるよう営業秘密の定義を改めている。また、2013 年には外国及び経済活動スパイ罰則強化法によって、罰金金額が引き上げられている。

EEA に係る事案の捜査は FBI の Economic Espionage Unit が一義的には担当するが、司法省も企業や州が管理する営業秘密窃盗についての訴追権限を有している。司法長官も EEA 違反の事案に対して差止請求等の民事救済を連邦裁判所求める権限を EEA によって与えられている。しかしながら、EEA は 1996 年以降必ずしも十分に営業秘密を保護してきたとは理解されておらず、EEA に基づいて訴追された事案は、起訴されたものが 125 件、有罪判決に至ったものが 10 件と「わずか」ととどまっているとの指摘もある<sup>27</sup>。

#### DTSA

DTSA によって州法レベルでは進展が見られたものの、当然、州毎に民事手続や証拠の基準が統一的でなかったことから、EEA を改正する形で 2016 年に DTSA が制定された。DTSA では、営業秘密の定義については、上記 EEA で整理したとおりだが、連邦法上、営業秘密の不正取得（misappropriation）に対し、当該営業秘密のさらなる開示・使用その他拡散を防止するために、相手方に対して事前通告なしの差押（Ex parte Seizure）請求<sup>28</sup>、不正取得及びその恐れがある場合の差止請求<sup>29</sup>、損害賠償の請求<sup>30</sup>、懲罰的損害賠償の請求<sup>31</sup>等を認める内容となっている。DTSA が連邦法であることから当然ではあるが、連邦地方裁判所にこれら申立・請求に関する民事訴訟管轄権があることも明記されている<sup>32</sup>。差押は、DTSA において創設された特徴的な制度であり、民事的救済の為の訴訟提起前であっても申立をおこなうことができるものであるが、相手側に対する事前通告なしで裁判所が差押命令を発することができる強力なものであり、あくまでも例外的な自体に対して非常の手段として採用される救済措置であると定められている<sup>33</sup>。差止請求についても、一般的には金銭賠償の

<sup>26</sup> 18USC § 1832(a).

<sup>27</sup> Brian T. Yeh, *supra* note, p.18.

<sup>28</sup> 18USC § 1836(b)(2).

<sup>29</sup> 18USC § 1836(b)(3)(A).

<sup>30</sup> 18USC § 1836(b)(3)(B).

<sup>31</sup> 18USC § 1836(b)(3)(C).

<sup>32</sup> 18USC § 1836(c).

<sup>33</sup> 18USC § 1836(b)(2)(A)( ).

原則から、金銭賠償による救済では不十分とされる場合にのみ差止が認められるのに対して、DTSA は差止が認められないのは例外的であるとの認識を前提として、差止が認められない場合に営業秘密の使用を侵害者が継続する場合に合理的なロイヤルティの支払いを命じることができることも明記されている<sup>34</sup>。

このように連邦法における営業秘密の保護は、州法での規定をベースとしてつ産業の変容に沿う形で対象を改定し、刑事から民事へと救済を拡大している。また、連邦法制定により、具体的な訴訟における手続、証拠基準が統一化され、運用に資する制度となっている。

#### DTSA の運用・評価

DTSA 制定から間もないため、判例は限定的であるものの、差止を請求するケースもみられる。2016 年の Dazzle Software II, LLC v. Kinney 事件は事前通告なしの差押 (Ex parte Seizure) が最初に問題となった営業秘密侵害申立て事案であったが、事前通告なしの差押は認められなかった。また、今回の裁判期日において裁判所への提出が必要となるデータ及びデバイスの保全について、保全命令で十分であるとして、事前通告なしの差押を認めなかったケースもある<sup>35</sup>。初めて事前通告なしの差押が認められたのは、Mission Capital Advisors LLC v. Romaka 事件においてであった。この事案は、不動産金融会社が顧客リスト関連文書等の機密文書を従業員が侵害したとして訴えられたもので、侵害が発覚した際、従業員が隠ぺいする恐れがあったものの、裁判所は当該従業員のプライバシーや本事案で問題とされていない文書等への影響にも配慮を示していた。しかし当該企業が、差止を必要とするファイルとその所在、差止を実施する合理的手段について示すことが決め手となり、差止が認められている。

現状としては、企業へのガイドライン提示による周知及び判例の蓄積による実際の法執行の内容の明確化を待つ段階であるとの指摘が現地調査においては聞かれた<sup>36</sup>。

#### (4) 営業秘密によるデータ保護

アメリカにおける営業秘密は、コモン・ローの時代から産業変化に対応する形で対象や救済措置を改訂した経緯があり、いつの時代も柔軟である。原則となる要件が明確で、第三者による不正取得にも対応できるため、企業のニーズを満たしており、価値あるデータ保護の手段として適していると、行政<sup>37</sup>、法律

<sup>34</sup> 18USC § 1836(b)(3)(A)( )。

<sup>35</sup> OOO Brunswick Rail Mgmt v. Sultanov, (N.D.Cal.Jan.6, 2017)。

<sup>36</sup> 現地調査 (政府関係者ヒアリング) より。

<sup>37</sup> アメリカ商務省が 2017 年 1 月に公表した「Fostering The Advancement of The Internet of Things」と題するグリーンペーパーにおいても、「営業秘密として保護できる情報の種類は事実上無限である」と指摘している。また IoT の普及により、ビジネス環境として、機密情報の偶発的な公開から保護するための適切な管理なしでのデータ共有により、営業秘密が公開されるリスクがさらに高まることや、営業秘密の保護は、IoT 分野におけるイノベーションの促進にとって重要な要素の 1 つと考えられるといった指摘もなされている。



専門家、産業界のそれぞれが認識している<sup>38</sup>。例えば産業界においては、データ保護については営業秘密による保護が基本であるとしながら、営業秘密の保護要件が満たされない場合に契約を用いた保護によるとの認識が示されている<sup>39</sup>。

現地の法律専門家によれば、企業内においてシステム等で管理されるデータであれば（容易にリバースエンジニアリング可能なものでなければ）、非公知性を満たし、企業内のシステムで管理されているため秘密管理性を満たし、データの不正取得は事業に影響を与えることから有用性を満たすため、基本的には営業秘密性を有するとの指摘があった。またこのような考え方は IoT 関連機器から自動集積されるデータについても同様であるとの認識も示された<sup>40</sup>。

また、DTSA により、刑事・民事の双方における保護が可能となったことを受け、各国と営業秘密保護の国際的協調の推進を期待する意見もあがっている<sup>41</sup>。

### 3．不正アクセス行為の規制

#### (1) 概説

アメリカでは、コンピュータ及びネットワークへの不正アクセス行為は、コンピュータ犯罪として州・連邦レベルでそれぞれ刑法により規制している。不正アクセス行為はコンピュータ・ネットワークの技術進展、普及に応じて州間・国際間で起こることから、連邦法での規制が重要となる。

連邦法では、1984年に総合犯罪規制法(Comprehensive Crime Control Act)にコンピュータ及びネットワークに対する不正アクセス・不正使用に対処する規定を導入した。これは、単一の新しい制定法として、刑法 1030 条を制定し、コンピュータに関連する詐欺及び関連行為を規制している。その後、1986年にコンピュータ犯罪取締法(Computer Fraud and Abuse Act)<sup>42</sup>でコンピュータ関連の刑事犯罪その他の不正行為に関する予防、訴追及び救済を規定し、電子コミュニケーション・プライバシー法(Electronic Communications Privacy Act)<sup>43</sup>でコンピュータ・ネットワークにおける交信の傍受を規制している。いずれも刑法 1030 条の改正法であり、以降もアメリカにおけるコンピュータ・ネットワークの不正アクセス行為は、基本的には刑法 1030 条を改正する形で整備されている<sup>44</sup>。

<sup>38</sup> 現地調査（政府関係者、法律専門家、産業界ヒアリング）より。

<sup>39</sup> 現地調査（産業界ヒアリング）より。

<sup>40</sup> 現地調査（法律専門家ヒアリング）より。

<sup>41</sup> 現地調査（政府関係者ヒアリング）より。

<sup>42</sup> 18USC § 1030

<sup>43</sup> 18USC § 2511

<sup>44</sup> 刑法 1030 条以外では、刑法 1028 条（身分証明書類、認証機能、及び情報に関する詐欺及び関連行為）、刑法 1029 条（アクセス装置に関する詐欺及び関連行為）、刑法典（1362 条 通信回線、通信局、又は通信システム）、刑法（2511 条 有線通信、口頭の会話又は電子的通信の傍受及び開示の禁止）、刑法 2518 条（有線通信、口頭の会話又は電子的通信の傍受のための手続）、刑法 2703 条（顧客の通信又は記録の要求された開示）が関連

データ保護については、コンピュータ犯罪取締法において、保護対象としてデータが規定されており、本法は不正アクセス行為規制によるデータ保護において重要な法制度であるという意見があった<sup>45</sup>。

## (2) コンピュータ犯罪取締法

コンピュータ犯罪取締法は、故意に無権限にコンピュータにアクセスし、州間・国際間の通信をおこなう保護されたコンピュータ、又は金融機関やクレジットカード発行人のファイナンスレコードから情報を取得すること、保護されたコンピュータに損害を与えること又は威嚇し金銭を要求すること、アクセスに必要な情報・パスワードの無権限取引を規制している。

コンピュータ犯罪取締法は、コンピュータそのもの、及びコンピュータ上のデータ、プログラム、システムを保護の対象としている。これらの保護対象に対して、故意による不正アクセス、不正アクセスによる情報の取得、不正アクセスにより損害を与える行為<sup>46</sup>、アクセスに必要な情報・パスワードの無権限取引を規定している。

コンピュータ犯罪取締法では、規制行為に違反した場合は、罰則として罰金又は拘禁刑を科している<sup>47</sup>。

## (3) 不正アクセス行為の規制によるデータ保護

不正アクセス行為は、刑法において、コンピュータ及びコンピュータ上のデータを保護対象とし、第三者の故意による不正アクセス、不正取得、損害を与える行為について罰則を科すことで規制している。一方で、第三者が不正に取得したデータをさらに流通した場合における差止を規定しておらず、民事的な救済措置の効果はない<sup>48</sup>。

価値あるデータについての保護について、現地調査では不正アクセス行為の規制による保護を第一義的に考える法律専門家もいたが、営業秘密がもっとも適しており、営業秘密によって保護されない場合に不正アクセス行為に対する規制によって対応することになるのではないかとの指摘もあった<sup>49</sup>。

なお、アメリカにおいてはオバマ政権下の2013年2月に、Executive Orderとしてサイバーセキュリティフレームワークの策定が要請され<sup>50</sup>、アメリカ国立

---

する。

<sup>45</sup> 現地調査（法律専門家ヒアリング）より。

<sup>46</sup> 損害を与える行為については、意図的にプログラムを送信して保護されたコンピュータに権限なく損害を与えること、無権限で保護されたコンピュータにアクセスし損害を与えることを行為類型として規定。

<sup>47</sup> 刑法 1030 条 (a) (5)

<sup>48</sup> 現地調査（法律専門家ヒアリング）より。

<sup>49</sup> 現地調査（政府関係者ヒアリング）より。

<sup>50</sup> Strengthening the NIST Cyber Framework Against Advanced Threats (5<sup>th</sup> Dec 2013)

標準技術研究所（National Institute of Standards and Technology：NIST）が企業や有識者とのワークショップを実施して取りまとめたフレームワークが、2014年2月に公表されている<sup>51</sup>。

ただし、政府関係者によれば、コンピュータ、データに関連する技術が進展する中、データの保護についてはサイバーセキュリティの側面だけでは十分とはいえず、知的財産（営業秘密を含む）の観点も含めて幅広い側面から保護手段を検討する必要があるという指摘もあった<sup>52</sup>。

#### 4．契約

アメリカでは契約において約因を明記することが求められており、秘密保持契約においても契約違反に該当する行為等が明確に記載されて締結される。また契約違反に基づく損害賠償請求や差止請求についても契約書上、違反の効果として詳細に定めておくことが広く行われている。差止請求については、コモン・ロー上、金銭賠償の原則があることから、一般論としては損害賠償によって十分な救済が受けられないことを証明しなければならないが、契約上、秘密情報の漏えいについては金銭賠償では十分な救済とならないことから差止請求を認める旨を明記することも実務上は多い。

この点、現地調査においては、データ保護においても、データの所有権を明確にする点、秘密保持契約を締結する点から、企業間のデータ保護において一般的な手段と見られているとの指摘があった<sup>53</sup>。また、実際にデータ利活用したコンサルテーションやソリューションを提供している企業は、自社のデータ利活用に適する契約内容にできるため、契約による保護を前提としていると考えているようである<sup>54</sup>。

その場合、実務上は契約書の中に、あらかじめ秘密保持義務違反による損害は金銭賠償だけでは救済が不十分であることから、差止請求権を発生させることを明記するといった運用が広く行われている<sup>55</sup>。

ただし、現地の法律専門家によれば、契約によるデータ保護は、あくまで個別企業間においてその効果が発揮され、第三者による不正取得に対しては十分ではない点や、契約内容の厳密性については各国の契約法・契約慣習による点から、その保護性は十分ではないと考えられているとの指摘があった<sup>56</sup>。またコンソーシアムを形成してデータを共有する際、2～3社ならしっかりと契約を結べるが、多くの企業（例：100社）が参画すると各社ごとに、契約を取り交わす

<sup>51</sup> NIST, Launch of the Cybersecurity Framework (12<sup>th</sup> Feb 2014).

<sup>52</sup> 現地調査（政府関係者ヒアリング）より。

<sup>53</sup> 現地調査（法律専門家ヒアリング）より。

<sup>54</sup> 現地調査（産業団体ヒアリング）より。

<sup>55</sup> この点、アメリカの実務に詳しい法律専門家によれば、契約書上、差止請求が可能であることが明記されている場合であっても、金銭賠償の原則によらないで差止を求める必要性については裁判所において判断されることになるとの指摘があった。

<sup>56</sup> 現地調査（法律専門家ヒアリング）より。

のは難しく、その場合は、一般不法行為としての損害賠償として扱うしかないとの懸念も示された<sup>57</sup>。不法行為の場合にも差止請求は認められる可能性があるが、上記金銭賠償の原則の適用を受けることは契約違反の場合と同様である<sup>58</sup>。

また、契約違反に係る損害賠償については、前掲のとおり、アメリカは懲罰的損害賠償により、実際に生じた損害の金額を超える賠償額が認められる場合がある。

## 5. 知的財産法

特許法については、権利保有者が安心してデータを公開し、データの自由な流通が促進されることを企図して、2014年に§ 101 guidelineによりビッグデータの構造について特許性を認める方針を示した。また、ビッグデータ生成過程におけるインフラシステムについても特許性が認められる可能性があるが、データ収集技術は進展のスピードが速く、特許取得する必要性は決して高くはないという声があがっている<sup>59</sup>。そのため、特許法によるデータ保護については部分的であり、その評価も今後見定められる状況にあるといえる。

一方、伝統的に連邦著作権法が編集著作物や事実・データを集積した編集物を保護してきた経緯があり、過去にはデータベース保護についても著作権法の領域で検討された経緯もあることから、以降では著作権法について記載する。

### (1) 著作権法によるデータ保護の沿革

アメリカにおいては古くから編集著作物や事実・データを集積した編集物に関する判例の蓄積がある。例えば1909年連邦著作権法制定前の判例の中には、著作者が労力をかけて創作した場合にその作品に対して著作物性を認めるものが多数あるといわれている<sup>60</sup>。1909年連邦著作権法が制定されて以降の裁判例においても、著作者が労力をかけて創作している場合にはその作品に対して著作物性を認めるもの（額に汗の理論）もあったが、一方で、素材の選択や創作性を重視する判例もあった<sup>61</sup>。この点、「裁判所は、基本的に編集物にも創作者の個性という意味でのオリジナリティを要求し、それを認めることができないような編集物で、かつ、その創作に多くの投資が必要とされたものについて、額に汗の理論により、競争関係にある者の利用に限って規律してきた」<sup>62</sup>と指摘

<sup>57</sup> 現地調査（政府関係者ヒアリング）より。

<sup>58</sup> この点について法律専門家によれば、不法行為の方が、契約違反の場合や明確に営業秘密侵害に該当する場合に比べると、差止請求が認められるためのハードルは高くなるというのが、一般的な実務感覚であるとの指摘があった。

<sup>59</sup> 現地調査（政府関係者ヒアリング）より。

<sup>60</sup> 蘆立順美『データベース保護制度論』（信山社、2004年）10頁。蘆立教授は、具体例として、Howell v. Miller, 91 F. 129 (6th cir. 1898). Mead v. West Pub. Co., 80 F. 380 (D. Minn. 1896)を指摘する。

<sup>61</sup> 蘆立・前掲注、18頁以下。

<sup>62</sup> 蘆立・前掲注、25頁。

されている。

その後、1991年のFeist判決<sup>63</sup>では、著作物であるために要求されるオリジナリティには、独立の創作の他に最小限のクリエイティビティが必要であり、これは憲法上要請される要件であるという解釈を示し、額に汗の理論を否定し、創作性を保護要件としている<sup>64</sup>。

Feist判決以降、各裁判所が保護要件として要求しているオリジナリティの基準は高いものでなく、ありふれたもの、表現方法が制限されているもの、その著作物の性質上そのような表現とならざるをえないもののみオリジナリティが否定されているといわれている<sup>65</sup>。なおFeist判決の中で裁判所は、労力の部分について不正競争の理論(theory of unfair competition)によって保護される可能性を指摘しており、従来、連邦著作権法によって額に汗の理論で保護されてきた労力については、各州のコモン・ローにおける不正競争行為として救済されるという考え方を後押しした可能性がある。係る経緯もあり、アメリカにおいては著作権を付与する形でのデータベースの保護については、産業発展への寄与が高くないという意見があがり、産業界から今なおそのような評価を受けている<sup>66</sup>。

## (2) DMCA

DMCAは、インターネットサービスの普及に伴い、主としてインターネット上におけるデジタル著作物を保護するため、1998年に制定された。DMCAでは、アクセス・コントロールを回避する装置等の製造、輸入、公衆提供その他の取引とともに、回避行為自体が禁止されている。またコピー・コントロール等著作物の権利を効果的に保護する技術的手段を回避する装置等の製造、輸入、公衆提供、供給その他の取引が禁止されている他、オンラインにおける著作権侵害行為が発生した際、プロバイダーへの当該コンテンツの削除要請を規定している。

## (3) DMCAの評価・運用

このようにDMCAは、デジタルコンテンツの保護を強く意識した内容となっているものの、紙媒体のデータベース及び著作物性を有さないデータベースに対する保護を与えるものではなく、Feist判決で示されているように、データの収集・集積について経済的コストや労力を割いていたとしても、創作性がないデータないしデータベースについてはやはり連邦著作権法によっては保護されない。

また、実務上も1991年Feist判決を契機に、著作権によるデータベース保護

<sup>63</sup> Feist Publications, Inc. v. Rural Telephone Service, 499 U.S.340 (1991).

<sup>64</sup> 蘆立・前掲注、26頁。

<sup>65</sup> 蘆立・前掲注、44頁。

<sup>66</sup> 現地調査(政府関係者ヒアリング)より。

が検討された<sup>67</sup>。しかし、当時検討されていたデータベースはある一時点で完成した著作物が単一ファイルとして独立する形で存在していたことに対して、昨今のデータ利活用におけるデータは、工場での生産データ等、編集著作物性のない事実の情報をリアルタイムで複数のステークホルダーが更新するため、その性質が異なると考えられている。特に、著作権によるデータ保護は権利保護が強すぎるため、データ流通に適しておらず、産業発展への寄与も小さいと認識されている。なお、2013年にアメリカ商務省タスクフォース(Internet Policy Task Force)よりDMCAの改正に関するグリーンペーパー<sup>68</sup>が公開されたが、あくまで保護対象は電子化された著作物であり、本調査の対象であるデータ保護に関する検討を行っておらず<sup>69</sup>、現地調査においても連邦著作権法による保護の可能性を指摘する声は聞かれなかった。

## 6. プライバシーデータに係る取扱い

プライバシーデータについては、各種文献、現地ヒアリングにおいても、現状では本調査で対象としている価値あるデータとは区別として捉えられている。

具体的にはプライバシーデータは、連邦取引委員会(Federal Trade Commission: FTC)による消費者保護施策において保護されており、産業界としてもプライバシーデータはFTCによる取締りにより保護・規制されていると認識している<sup>70</sup>。

ただし、FTCは、技術の進展に応じてプライバシーデータの範囲は変わると捉えており、現在も分野別(例:自動運転等)のワークショップを開催し、有識者、産業界から意見を収集している。プライバシーデータの範囲の拡大については、価値あるデータの保護を検討する中でも着目すべき動きといえる。

## 7. データの保護可能性

現地調査においては、政府関係者、産業界、法律専門家に共通して、「データは21世紀の石油」であり保護対象となりえるもの」と認識していた<sup>71</sup>。特に政府関係者において、このような認識が定着していることから、通商政策や産業政策においてデータ利活用を進めていく上で、競争上、必要となる環境整備の必要性は強く意識されている様子が見えられた。

<sup>67</sup> 当時行われたデータベース保護の議論について、現地調査(産業界ヒアリング)では、政府主導で検討が行われたものの、企業の運用に即した検討となっていなかったとの指摘もあった。

<sup>68</sup> The Department of Commerce Internet Policy Task Force, Copyright Policy, Creativity, and Innovation in The Digital Economy, July, 2013.  
<https://www.uspto.gov/sites/default/files/news/publications/copyrightgreenpaper.pdf>

<sup>69</sup> 現地調査(政府関係者ヒアリング)より。

<sup>70</sup> 現地調査(産業界ヒアリング)より。

<sup>71</sup> 現地調査(政府関係者、産業界、法律専門家ヒアリング)より。

2017年1月にアメリカ商務省が公表したグリーンペーパーでは、IoTの進展・普及による、産業・事業の拡大や、連結するデバイスの規模・数量の大幅に増加に触れた上で、その広範な接続性による影響について、民間セクター、大学、政府、市民社会からの多くの利害関係者のコメントをもとに、現在の技術的・政策的状況をまとめている<sup>72</sup>。

当該グリーンペーパーの中でもIoTにおける知的財産として、著作権、特許、営業秘密、商標についてまとめている。著作権、特許、営業秘密、商標のそれぞれについてIoTにおける関わりを示唆しているが、営業秘密について特にその重要性を指摘している点は意味深い。

具体的には、著作権については「事実」としてのデータは著作権としての保護対象と考えづらいと示しており、特許に関して、IoT技術は産業を前進させる影響力を有しているものの、IoTに固有のものではないと捉えられている。また、商標は、複数のデバイスがつながることで1つのサービスを提供する際に、サービスを一種のブランドとして標章する際に利用されることに言及しているものの、サービスのブランドを商標で標章すること自体はIoTに固有のことではないと指摘している。営業秘密については、保護対象となる情報が幅広く、IoTを構成するデバイスや接続性が急増することで、営業秘密の脆弱性が生じることを指摘しており、機密情報を漏えいから保護するため、営業秘密管理の重要性を示している<sup>73</sup>。

「価値あるデータ」の保護について、産業界の見解としてはデータの流通を促進すべきであるが、第三者からの不正取得に対する対応とのバランスが必要であるとの考え方については共通しており、日本におけるデータ利活用とデータ保護の双方を考慮した検討について賛同する意見も聞かれた<sup>74</sup>。「価値あるデータ」は各社間の契約によって保護されるべきであり、第三者からの不正侵害については、不正アクセス行為の規制によって保護されるべきであるとの指摘もあったが、「価値あるデータ」の保護については、営業秘密によって保護されると理解しており、営業秘密の保護要件を満たさない場合には契約違反による救済を求めていくことになるとの意見もあった<sup>75</sup>。

政府関係者や法律専門家の中には、例えばコンソーシアムのように多数の企業が「価値あるデータ」を共有する場合を念頭に、秘密管理性の要件を満たさない場合等、営業秘密によって保護されない場合もあることから、不正アクセス行為の規制による保護が一義的には重要であると指摘する者もいた。しかし、

---

<sup>72</sup> The Department of Commerce Internet Policy Task Force & Digital Economy Leadership Team, *Fostering The Advancement of The Internet of Things*, January 2017, Executive Summary.

[https://www.ntia.doc.gov/files/ntia/publications/iot\\_green\\_paper\\_01122017.pdf](https://www.ntia.doc.gov/files/ntia/publications/iot_green_paper_01122017.pdf)

<sup>73</sup> The Department of Commerce Internet Policy Task Force & Digital Economy Leadership Team, *Fostering The Advancement of The Internet of Things*, January 2017, Executive Summary. P.34-39.

<sup>74</sup> 現地調査（産業団体ヒアリング）より。

<sup>75</sup> 現地調査（産業団体ヒアリング）より。各企業においては、むしろデータ流通の促進によるイノベーションに対する関心が高く、データ保護の必要性についての意識はまだ十分とはいえないとの指摘もあった。

知的財産を取扱う関係省庁の関係者はいずれも当該データにつき秘密管理可能なものについては営業秘密による保護がもっとも適しているとの認識を示した他、法律専門家もデータ保護により高い専門性を有する者からは営業秘密による保護を一義的には検討すべきであるとの認識も示された<sup>76</sup>。また国際的なハーモナイゼーションの観点からも営業秘密による保護を検討すべきであるとの指摘も複数聞かれ、このような指摘は営業秘密よりも不正アクセス行為の規制による保護の重要性を指摘した産業団体からも聞かれた<sup>77</sup>。

---

<sup>76</sup> 現地調査（政府関係者、法律専門家ヒアリング）より。

<sup>77</sup> 現地調査（政府関係者、産業団体ヒアリング）より。



## 第2章 欧州（欧州委員会）

### 1. 概要

欧州委員会において、データ保護に係る議論は以前から様々な形で議論され、関連する制度が整備されてきた経緯がある。近年、我が国においても特に注目されているのは、2016年5月に発効した一般データ保護規則（General Data Protection Regulation：GDPR）<sup>78</sup>についてであり、EUを含む、欧州経済領域（EEA）内で取得した個人情報等を、EEA外に移転することを原則として禁止するものである。2018年5月には罰則を伴う適用開始が予定されており、日本企業にも大きな影響が指摘されていることから、関係機関や各企業では対応が進められている。

もっともGDPRが対象としているのは個人情報等であり、本調査で注目している「価値あるデータ」の大半が対象外となる。欧州委員会における関連制度としては、データベース保護指令（96/9/EC）及び営業秘密保護指令（2016/943/EU）があり、これらと「価値あるデータ」の関係について整理をおこなうことが必要となる。

また欧州委員会は2015年に「欧州単一デジタル市場戦略」<sup>79</sup>を公表し、データ保護のあり方についても議論が盛んとなっている。この「欧州単一デジタル市場戦略」にも示されている欧州単一デジタル市場政策（Digital Single Market）を上位政策とし、2017年1月には「欧州データ経済の構築」<sup>80</sup>と題する政策文書を公表している。さらに、パーソナルデータの第三国移転についてのモデル契約<sup>81</sup>は既に示されているところであるが、これ以外に、欧州域内の企業間のデータの取扱いに係るモデル契約が欧州委員会によって開発されているところである<sup>82</sup>。

欧州委員会においては、司法・消費者総局（Justice and Consumer：DG JUSTICE）、通信ネットワーク・コンテンツ・技術総局（Communications

---

<sup>78</sup> Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation),  
<http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN>

<sup>79</sup> Digital Single Market Strategy, Brussels, 06 May 2015, Statement by Vice-President Andrus Ansip, [http://europa.eu/rapid/press-release\\_SPEECH-15-4926\\_en.htm](http://europa.eu/rapid/press-release_SPEECH-15-4926_en.htm)

<sup>80</sup> Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions “Building a European Data Economy,” Brussels, 10. 1. 2017, COM(2017) 9 final  
<https://ec.europa.eu/digital-single-market/en/news/communication-building-european-data-economy>

<sup>81</sup> DG JUSTICE ウェブサイト “Model Contracts for the transfer of personal data to third countries,”  
[http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index\\_en.htm](http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index_en.htm)

<sup>82</sup> 現地調査（有識者ヒアリング）より

Networks, Content and Technology : DG CONNECT )、域内市場・産業・起業・中小企業総局 ( Internal Market, Industry, Entrepreneurship and SMEs : DG GROWTH ) が、それぞれの立場からデータ保護や利活用に係る制度・政策を所管している。概ね連携は図られているものの、各総局の政策目的の相違から、異なる観点での調査や提言がなされているとの見方がある<sup>83</sup>。

## 2 . データベース保護指令

### ( 1 ) 指令の特徴

データベース保護指令は、著作権による保護と、独自の権利 ( sui generis ) による保護の両方を定めている点が特徴である<sup>84</sup>。欧州委員会がデータベース保護の必要性を指摘したのは 1988 年であった<sup>85</sup>が、当時は著作権法のオリジナリティの基準に基づく保護がもっとも適切なアプローチであるとされていた<sup>86</sup>。その後、1992 年に欧州委員会から sui generis による保護を含む案<sup>87</sup>が示され、1996 年に最終案が採択されるに至っている。同指令は冒頭、データベースが各国の現行法によって十分に保護されておらず、このことがデータベースやデータベースを提供することに対して負の影響を与えているという認識を示している<sup>88</sup>。

### ( 2 ) 具体的な規定の内容

具体的には、コンテンツの選択又は配列によって知的創作物を構成するデータベースを著作権の保護対象として明記し ( 同指令 3 条 )、加えてコンテンツの入手、検証、表示について「相当の投資」がなされているデータベース ( 非電子的なものも含まれる ) の作成者に対してデータベースの「実質的な部分」の抽出行為及び ( 又は ) 再利用を妨げることができる sui generis を付与している ( 同指令 7 条 )。著作権による保護については、あくまで創作性を要求しており、著作権による保護のアプローチに際しては額に汗の理論を採用しないことを示

<sup>83</sup> 現地調査 ( 有識者ヒアリング ) より。

<sup>84</sup> データベース保護指令については、長塚隆「EU のデータベース保護政策」情報の科学と技術 49 巻 7 号 ( 1999 年 ) 340 頁以下、蘆立順美『データベース保護制度論』( 信山社、2004 年 ) 199 頁以下等が比較的詳しく紹介を行っている。

<sup>85</sup> Green Paper on Copyright and the Challenge of Technology - Copyright Issues Requiring Immediate Action. COM (88) 172 final, 7 June 1988.

<sup>86</sup> Working programme of the Commission in the field of copyright and neighbouring rights. Follow-up to the Green Paper. COM (90) 584 final, 17 January 1991. 同レポートによれば、1990 年に実施されたヒアリングにおいて sui generis のアプローチを支持する見解はなく、全ての発言者がデータベースは著作権によって保護されるべきであると指摘し、この考え方は WIPO の代表とも共有されたと指摘されている ( 6.2 )。

<sup>87</sup> Proposal for a Council Directive on the legal protection of databases. COM (92) 24 final, 13 May 1992.

<sup>88</sup> 96/9/EC (1)(2).

している。これに対して、sui generis による保護については経済的資源、時間、努力や労力等を含む「投資」を保護することを明確にしている<sup>89</sup>。

ここでデータベースとは、「体系的又は方法論に基づいて配列され、かつ、電子的その他の手段で個別にアクセスが可能な、独立した作品、データ又はその他の独立した素材の収集物」(同指令 1 条)と定義されており、比較的広く保護範囲を捉えているが。しかしながら、体系的又は方法論に基づく配列が必要であることから、「無造作に素材を集めただけのものはデータベースに該当しない」と指摘されている<sup>90</sup>。

### (3) 現在における評価

同指令について、特に sui generis による保護については早い時期から批判も多かったことが指摘されている<sup>91</sup>。また同指令が採択された後の判例によって、多くのデータベースが sui generis によって保護されないことが示され、データベースの構造(データの保管や処理システム)に対する投資しか保護されないという理解が定着したともいわれている<sup>92</sup>。2005 年には欧州委員会から同指令のレビューをおこなったワーキングペーパーが発表されたが、欧州委員会自ら起草した同指令に対して批判的な内容であった<sup>93</sup>。

今回実施した現地調査においても、同指令について当初から産業界は好意的ではなく、10 年ほど前に見直しの機運が高まった際にも評価はネガティブであったとの指摘があった<sup>94</sup>。この見直しは、後ろ向きの限定的なものであったため、経済のデジタル化という市場の変化への対応を念頭においた抜本的なものとはならなかった。また同指令は支持されてこなかったこともあり、欧州裁判所の判例において制限的な解釈がなされてきた経緯があるとの指摘も聞かれた<sup>95</sup>。

なお欧州委員会は、データベース保護指令に係るパブリック・コンサルテーションを 2017 年 5 月 24 日から 8 月 30 日まで実施中であり、見直しの必要性が指摘されている。この点ドイツで実施した現地調査によれば、データベース保護指令によってはビッグデータを十分に保護できず、同指令はサブスタンスを

---

<sup>89</sup> 96/9/EC (40)。

<sup>90</sup> 蘆立・前掲注、203 頁。

<sup>91</sup> 蘆立・前掲注、206-216 頁。

<sup>92</sup> フランク・ゴツェン「データベースの製作者に対する産業財産権保護 - 欧州及び日本の保護制度の今後に関する考察」知財研紀要(2007 年)3 - 4 頁。

<sup>93</sup> DG Internal Market and Services Working Paper. First evaluation of Directive 96/9/EC on the legal protection of databases, 12 December 2005. フランク・前掲注、5 頁は同ディスカッションペーパーが、自ら起草した同指令に対する評価として驚くほど批判的であったと評している。

<sup>94</sup> 現地調査(有識者ヒアリング)より。欧州委員会ウェブサイト“The EU Single Market – Protection of Database, stakeholder consultation”によれば、2005 年 12 月に域内市場サービス総局(DG Internal Market and Services)が評価レポートを提出のうえ利害関係者コンサルテーションを実施している。

[http://ec.europa.eu/internal\\_market/copyright/prot-databases/index\\_en.htm#maincontentSec3](http://ec.europa.eu/internal_market/copyright/prot-databases/index_en.htm#maincontentSec3)

<sup>95</sup> 現地調査(有識者ヒアリング)より。

失うのではないかと、また自動車、健康等突出した分野が既に出てきていることから、新たな制度整備をおこなう場合セクター別のアプローチとなるのではないかと、といった指摘があった<sup>96</sup>。また欧州、ドイツ及びフランスの産業界、有識者等のいずれからでも、新たな法制度導入については否定的で、企業間の契約や既存の法体系によって対応すべきであるとの意見があった<sup>97</sup>。

### 3．営業秘密保護指令

#### (1) 指令の特徴

営業秘密保護指令は 2013 年に指令案<sup>98</sup>が提示された。同指令案においては、イノベティブな事業活動のために必要な環境整備をおこなうことが必要であり、営業秘密は非技術的なものを含めたイノベーションや競争力のために重要であるにもかかわらず、現状において欧州域内における不統一な保護状況が国を超えた研究開発や知識の流通を阻害しているとの認識が示されている。同指令案の公表に先だって欧州委員会は 2 つの委託調査を実施しているが、最初に実施された調査報告書<sup>99</sup>によれば、欧州域内において統一的な保護制度や営業秘密の定義が存在していないことや、差止や損害賠償による救済を受けることができるものの各国において保護対象や保護要件、善意取得者に対する対応等について不統一であり、刑事罰規定が大半の加盟国において整備されながら訴追がなされておらず、十分な保護がなされているかについては疑問であると指摘されている。次に実施された調査報告書<sup>100</sup>によれば、欧州域内による営業秘密に係るルールが不統一であることから、営業秘密管理や権利行使についての透明性が確保されず、コストも高いものになっていると指摘されている。加えて訴訟における立証負担が大きく、訴訟手続における情報漏えい防止措置が不十分である等、現行制度には不備があることから、営業秘密を有する者は司法救済を求めない傾向があると指摘している。また欧州企業を対象とした調査結果等も踏まえ、同報告書は、営業秘密について統一的な保護をすべきであると結論を述べている。

2016 年に採択された営業秘密保護指令 (2016/943/EU) は、欧州において統一的な制度となっていなかった営業秘密保護について、共通の定義を提供し (同指令 2 条)、営業秘密侵害に該当する行為としない行為を明確にしている (同指

<sup>96</sup> 現地調査 (政府関係者ヒアリング) より。

<sup>97</sup> 現地調査 (産業界及び有識者ヒアリング) より。

<sup>98</sup> Proposal for a Directive of The European Parliament and of The Council on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure. COM(2013)0813 final. 同指令案を紹介する文献として、鈴木薫「営業秘密の保護に関する EU 指令案」パテント 68 巻 8 号 (2015 年) がある。

<sup>99</sup> Horgan Lovells International, Report on Trade Secrets for the European Commission, 2010.

<sup>100</sup> Baker&Mckenzie, Study on Trade Secrets and Confidential Business Information in the Internal Market, April 2013.

令3条、4条)点が特徴的である。現在、域内国は2018年の期限に向けてそれぞれ国内法整備を実施中である。

## (2) 具体的な規定の内容

同指令は、営業秘密がノウハウ、営業情報、技術情報を含む概念であることを明確にした上で、営業秘密の定義について、「当該情報と類似する情報を通常扱う関係者(circles)に属する者にとって、当該情報が集合として又は構成する正確な配列や構造が、一般的に知られておらず又は容易に知ることができないという意味において秘密であること」、「秘密であることによって商業的価値があること」、「当該情報を合法的に管理するものによって、当該情報を秘密とするために合理的な措置を講じていること」の全てを満たすことが必要であることを明記している(同指令2条)。

営業秘密侵害に該当しない行為として、「独自の発見又は創作」、「リバースエンジニアリングに相当する行為」、「誠実な商慣習に従った行為」等を明記している(同指令3条)。これに対して、「誠実な商慣習に反する不正アクセスや不正使用」、「不正取得や秘密保持契約等の契約上の義務に違反した不正使用や不正開示」、「営業秘密が第三者によって不正取得されたことについて知りうべき場合の営業秘密取得、使用、開示」、「悪意又は過失による侵害品の生産、提供」は営業秘密侵害に該当する行為として明記されている(同指令4条)。

## (3) 現在における評価

営業秘密保護指令の導入が急がれた背景として、現地調査では「ルークスリークス(ルクセンブルクの銀行員が罰せられた事件)」<sup>101</sup>の影響があるとの指摘が複数なされた。また、フランスにおいては国内で営業秘密に関する法案策定の動きが、新聞社や業界団体等の反対を受け不成立となった背景があった。営業秘密保護指令は採択されてから比較的日子が浅いものの、今回実施した現地調査においては、有識者から懐疑的な意見も聞かれた。指令策定のためのプロセスが長引き過ぎて、結局、妥協の産物となっているとの指摘や、指令の実施形態が不透明であるといった見解もあった。また同じく有識者からは、新たなデジタル経済に対応する意図で策定されたものではなく、自動生成されるデータ・リアルタイムのデータに適用するにはかい離があり、必ずしも後述するデジタル市場戦略に沿った内容になっている訳ではないとの指摘もあった<sup>102</sup>。

欧州最大の経済大国であるドイツにおいても同指令の対応について遅れを指摘する声もあったが、ドイツにおける現地調査においては、「インターネット上での市場のつながりが益々進む中、欧州域内でハーモナイズが図られることは望ましい」という好意的な声も聞かれた<sup>103</sup>。

<sup>101</sup> Luxembourg Leaks. 民間サイト(ジャーナリストのグループ)の紹介記事の一例として、The International Consortium of Investigative Journalists, November 5, 2014,

<sup>102</sup> 現地調査(有識者ヒアリング)より。

<sup>103</sup> 現地調査(政府関係者ヒアリング)より。

## 4 . 単一デジタル市場戦略とデータ保護

### ( 1 ) 欧州単一デジタル市場戦略

欧州委員会は、デジタルデータの潜在的な価値を最大限活用するためのイニシアチブとして、単一デジタル市場戦略を推進している。2015年に欧州委員会が文書として「A Digital Single Market Strategy for Europe」<sup>104</sup>を公表しているが、消費者及び事業者に対するオンラインでの商品やサービスへのよりよいアクセスの確保、デジタルネットワークとサービスが盛んになるための環境整備、欧州デジタル経済のポテンシャル最大化を目指すとしている。その中で、データ・オーナーシップという観点でビッグデータの取扱いについて論点の提示がなされている<sup>105</sup>こともあって、欧州においても比較的関心が高まっている。

なお、欧州委員会においてデータ経済に関連する総局の所管は、DG JUSTICEが契約法（ただし、消費者契約に係る）、DG CONNECTがデジタル経済の著作権法、特許法、デジタルコンテンツに関するモデル法（提案段階）等、DG GROWTHが産業育成の観点からの検討、をそれぞれ担当している<sup>106</sup>。各DGによる取組みは、委員会の提案やコミュニケーションのために欧州委員全ての了承が必要となる、そこで横断的な調整が図られる。

### ( 2 ) 欧州委員会コミュニケーションペーパー

欧州委員会は2017年1月に「欧州データ経済の構築( Building a European Data Economy )」<sup>107</sup>と題するコミュニケーションペーパーを公表している。特に自動集積されるデータへのアクセス及びデータ移転に関する議論において、「自動集積される生データ ( Raw machine-generated data )」の保護について比較的詳細に論じている。すなわち、データベース保護指令( 96/9/EC )による保護の可能性については、当該自動集積される生データを扱うデータベースの構築について相当の投資がなされている場合にのみ適用されうるとし、営業秘密保護指令( 2016/943/EU )は2018年6月までに国内法化が進んだとしてもデータが企業にとって知的資本として秘密にされ、「営業秘密」の要件を満たしていなければ保護がされないことからEUレベルでは既存のルールで直接的に「自動集積される生データ」に適用されるものはないと指摘している<sup>108</sup>。

コミュニケーションでは、現状としてデータを精製する機械がユーザーに所有されている場合においても、製造者又はサービスプロバイダーが事実上の所有者になっており、ユーザーが第三者によるデータの利用を許可できないこと

<sup>104</sup> A Digital Single Market Strategy for Europe - COM(2015) 192 final.

<sup>105</sup> COM(2015) 192, p.15.

<sup>106</sup> 現地調査（政府関係者ヒアリング）より。

<sup>107</sup> Building a European Data Economy, COM/2017/09 final.

<sup>108</sup> COM/2017/09 final, p.10.

は問題になりえるとしている。というのも、このような制度のギャップにおいてデータをコントロールする力をもつプレイヤーが不公平な契約基準を用いて有利になりえるからである。いくつかの加盟国では、不公正条項契約指令（Directive on Unfair Contract Terms）を B to B ビジネスに準用する国もあるが、全ての加盟国ではないため、データの搾取が起こり得、契約をおこなう双方に力の差がある場合には問題となると指摘される。

将来的な「自動集積される生データ」の活用に向けて、当該データへの匿名アクセスの促進、当該データの共有促進、投資や資産の保護、秘密情報が開示されることの回避、データのロックイン効果の最小化といった点について議論が必要であると指摘した上で、今後関係者との議論の中で、データの共有促進のためのガイダンス、データ特定や交換に係る技術革新、標準的な契約ルール、公共目的や特定目的でのデータアクセス、データ作成者の権利、対価の獲得といった点について検討が必要であるとしている<sup>109</sup>。

### （3）現在における評価とさらなる取組み

2017年1月のコミュニケーションペーパー発表とともに、データの取扱いに関しては様々な見解が示されている。その中には、データが日常的な取引の副産物であり、データの囲い込み等のリスクを考えれば原則的にはデータ自体の経済的価値を認めるべきではなく、経済的価値等がある場合には各事業者がデータを管理・コントロールすればよいのではないかといった見解がある<sup>110</sup>。このような考え方のもと、データの保護が不法行為の種類によって為されるべきであると考えられる一方、域内での統一的な保護を営業秘密保護指令がなしえるのかという点については現時点において明確な見解は示されていないようである<sup>111</sup>。

これらの議論が進む中で発表された本件コミュニケーションペーパーは、現地調査においても複数の機関において関心を示す声が聞かれた。有識者からは、こうした欧州委員会の問題提起に対して、多様な利害関係者から意見が出されているとの指摘があった<sup>112</sup>。これらの意見は、パブリック・コンサルテーション<sup>113</sup>において収集され、データの流通を促進する仕組みの在り方に関する議論が活発に進められている。また、これに加えたさらなる対話の場として複数回

<sup>109</sup> COM/2017/09 final, p.11-13.

<sup>110</sup> Max Planck Institute for Innovation and Competition, Data Ownership and Access to Data –Position Statement of the Max Planck Institute for Innovation and Competition of 16 August 2016 on the Current European Debate

<sup>111</sup> Max Planck Institute for Innovation and Competition, Data Ownership and Access to Data –Position Statement of the Max Planck Institute for Innovation and Competition of 16 August 2016 on the Current European Debate

<sup>112</sup> 現地調査（有識者ヒアリング）より。

<sup>113</sup> European Commission, Summary report of the public consultation on Building A European Data Economy  
<https://ec.europa.eu/digital-single-market/en/news/summary-report-public-consultation-building-european-data-economy>

ワークショップが開催され、データの共有・移転・アクセス・再利用といったテーマや、公的な利用、SMEs への影響、また自動システムやロボット・IoT 等最新テクノロジーにおける責任等、様々な観点から議論が行われ、理解が深められている<sup>114</sup>。

#### (4) 非パーソナルデータの域内における自由な流通のための枠組みに関する規則草案

これらの取組みの結果として、2017年9月13日に欧州委員会は「非パーソナルデータの域内における自由な流通の枠組みに関する規則草案 (Proposal for a Regulation of the European Parliament and of the Council on a framework for the free flow of non-personal data in the European Union)」<sup>115</sup> を公開した。この規則草案は、非パーソナルデータの自由な流通を実現するための実行的な規定であり、今後の欧州域内における非パーソナルデータの流通に関する主要な指針となることが予想される。ここでは、本規則草案の概要を以下にあげる。

非パーソナルデータの域内における自由な流通の枠組みに関する規則草案<sup>116</sup>  
(Proposal for a Regulation of the European Parliament and of the Council on a framework for the free flow of non-personal data in the European Union)

本規則草案は第1条においてその目的を、データローカライゼーション規制、対象機関のデータの利用可能性、そして専門的なユーザー (professional users) へのデータの移植 (porting) に関するルールを定めることにより、パーソナルデータを除くデータの域内における自由な流通を確実にするためのものとしている。

そして、データローカライゼーションの原則禁止を定める第4条では、安全保障の目的で正当と見なされる場合を除き、EU域内におけるデータのストレージその他のプロセッシングを特定の加盟国の領土内に制限すること、及び他の加盟国におけるストレージその他のプロセッシングを禁止・制限することを認

<sup>114</sup> European Commission, Stakeholder Dialogue on Building a European data economy  
<https://ec.europa.eu/digital-single-market/en/news/stakeholder-dialogue-building-european-data-economy>

<sup>115</sup> European Commission, Proposal for a Regulation of the European Parliament and of the Council on a framework for the free flow of non-personal data in the European Union (COM(2017)495)  
<https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-european-parliament-and-council-framework-free-flow-non-personal-data>

<sup>116</sup> European Commission, Proposal for a Regulation of the European Parliament and of the Council on a framework for the free flow of non-personal data in the European Union (COM(2017)495)  
<https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-european-parliament-and-council-framework-free-flow-non-personal-data>



めないとしている。

さらに、第 5 条は本規則が所轄官庁によるデータへのアクセスを妨げないとし、データが他の加盟国において蓄積・プロセッシングされたとしても、当局のデータへのアクセスが必ずしも拒否されないとしている。

また、第 6 条では、欧州委員会が EU レベルでの自主規制の行動規範の作成を促進すると述べられており、これによりプロバイダーの切り替えの際のベストプラクティスに関するガイドラインが明確化され、さらにプロバイダーデータのストレージとプロセッシングの契約がなされる前に、専門的なユーザーに十分に詳細で明確で透明性のある情報が提供されるとしている。

これに加えて、第 7 条では、各加盟国がこの規則をワンストップで実行する任務をおこなう機関を設置し、委員会及び他の加盟国との連携が円滑に行われるように定めている<sup>117</sup>。

## 5 . 契約上の取扱い

前述のとおり、価値あるデータの取扱いについて既存の制度がないため、この取扱いについては契約の当事者自治の原則に基づき、企業間の契約に委ねることが適当であるとの見解が太宗であった<sup>118</sup>。これに関連し、欧州委員会 DG JUSTICE によるデータに関するモデル契約開発については、一定程度有用であろうが、どの程度活用が広がるかは不明であるとの認識が持たれている。また、DG JUSTICE はパーソナルデータの第三国移送に関するモデル契約<sup>119</sup>を既に策定しているが、産業データに関するモデル契約を開発中といわれている<sup>120</sup>。

<sup>117</sup> Regulation of the European Parliament and of the Council, 2017/0228(COD), Article 1,(24) ~ (27)

<sup>118</sup> 現地調査（産業団体及び有識者ヒアリング）より。

<sup>119</sup> DG JUSTICE ウェブサイト “Model Contracts for the transfer of personal data to third countries,”

[http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index\\_en.htm](http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index_en.htm)

<sup>120</sup> 現地調査（産業団体及び有識者ヒアリング）より

## 第3章 ドイツ

### 1. 概説

#### (1) ドイツにおける関連法制の概要

欧州連合の加盟国であるドイツにおいては、データの保護に関連する法制についても、基本的に欧州指令や欧州規制に基づき国内法制が整備されている。また、国内の運用に際しては、ドイツ民法や刑法といった独自の法体系にも関わることから、これらに着目する必要がある。

具体的には、営業秘密に関する規定を有する既存の不正競争防止法及び営業秘密保護指令を受けての同規定改正の動き、この執行に係る刑法や民法、さらには、「価値あるデータ」に一部関わる個人情報保護法等であり、以下に概観する。

#### (2) 政策動向

ドイツ産業界は、「デジタルに行け (go digital)」を標榜しており、新たに大量のデータを扱うこととなっている分野、企業は巨大な投資を行い、ブームとなっているとの見方がある<sup>121</sup>。ドイツ産業連盟 (Bundesverband der Deutschen Industrie : BDI) は欧州委員会のパブリック・コンサルテーションに対して意見書を提出、プラットフォーム Industrie 4.0 の法的枠組作業部会 (legal framework working group) がデータの取扱いに関する検討を進めている等、データに対する産業界を中心とする関係者の関心は高い。

ドイツは現在、政権間のバランスをとった政策運営となっているため、政治的なリーダーシップが発揮しにくい状況であり、産業界の関心が高いデータ保護分野を含め、本年 (2017 年) 9 月に連邦議会選挙後の動きとなるものと認識されている<sup>122</sup>。

ドイツ連邦政府内の所轄省庁は、産業データ保護に関しては連邦内務省 (Ministry of Interior)、欧州指令を受けた法改正 (営業秘密法) は連邦司法消費者省 (Ministry of Justice and Consumer)、産業政策の観点からの調整を連邦エネルギー省 (Ministry of Economy and Energy) が所管している。

### 2. 営業秘密

#### (1) 概要

ドイツにおける営業秘密に係る制度的保護<sup>123</sup>は、不正競争防止法 (Gesetz

<sup>121</sup> 現地調査 (有識者ヒアリング) より。

<sup>122</sup> 現地調査 (産業団体及び有識者ヒアリング) より。

<sup>123</sup> ドイツにおける営業秘密について紹介する文献として、経済産業省 (委託先: 三菱総合

gegen den unlauteren Wettbewerb : UWG ) 17 条が営業秘密漏えいについて刑事罰を設けることによって図られている。UWG は禁止される不正競争行為の類型として営業秘密を明確には定めていないことから、UWG が禁止するいずれかの不正競争行為に該当しない限り、営業秘密は UWG8 条以下に定められている除去請求権、不作為請求権（差止及び予防的差止請求権）損害賠償請求権、利益剥奪請求権の規定によっては保護されない。民事的保護については、UWG17 条に該当する行為について、不法行為に基づく損害賠償責任を定める民法 823 条 2 項に基づく損害賠償、不正な侵害の排除請求権を定める民法 1004 条に基づいた差止請求の対象となる。もっともドイツにおいては、刑事的エンフォースメントを通じて得た証拠を用いて民事責任を追及するといったことが頻繁に行われており、UWG に基づく刑事的エンフォースメントも民事上の証拠収集のために利用されることが多いとの指摘されている<sup>124</sup>。

## ( 2 ) UWG

### 法の特徴

現行の UWG は、2004 年に成立・施行したものである。この際、旧法は廃止されており、旧法を中心として自由競争を前提とした市場ルールとしての競争法としての側面を残しつつ、国内及び EU において強まっていた消費者保護強化の流れを汲んだものとなっている<sup>125</sup>。その後、企業対消費者の商業慣行に関する欧州指令（2005/29/EC）の発効等を受け、2010 年、2016 年に累次改訂がなされているが、UWG は営業秘密に関しては欧州委員会の動きに先駆けた法制度となっており、17 条に対する改正はない<sup>126</sup>。

旧法は 1896 年に成立した法律であり、当初から従業員等による営業秘密漏えい行為を禁止し、これに刑事罰を科するという営業秘密保護規定が設けられていた。19 世紀後半におけるドイツでは営業の自由が確立していく中、1851 年プロイセン諸国刑法典やその後のドイツ帝国刑法典においても経済発展のために

---

研究所)「諸外国における営業秘密保護制度に関する調査研究報告書」(2014 年)、特許庁(委託先:三菱 UFJ リサーチ & コンサルティング)「人材の移動による技術流出に係る知的財産の在り方に関する調査研究報告書」(2011 年)、経済産業省(委託先:TMI 総合法律事務所)「諸外国の訴訟手続における営業秘密保護の在り方等に関する調査研究報告」(2010 年)等がある。

<sup>124</sup> 経済産業省(委託先:TMI 総合法律事務所)「諸外国の訴訟手続における営業秘密保護の在り方等に関する調査研究報告」216 頁。

<sup>125</sup> 現行 UWG 制定の背景等については、中田邦博「ドイツ不正競争防止法の新たな展開 - 新 UWG について」立命館法学 298 号(2004 年)が詳しい。中田教授は、「ドイツにおいては、不正競争防止法の改革によって、一方で、自由化の要請、すなわちヨーロッパ共同体が基本条約に規定する人・物・サービス、資本の自由の展開に対応するとともに、他方で(将来的な)EU 消費者保護の展開を受け止めたということができよう」(同 279 頁)と指摘している。

<sup>126</sup> 連邦司法消費者省ウェブサイトでは、ドイツ語・英語にて現行法条文、ドイツ語にて改訂毎の全文を公開している。Act Against Unfair Competition (現行法の英文)  
[http://www.gesetze-im-internet.de/englisch\\_uwg/englisch\\_uwg.html#p0169](http://www.gesetze-im-internet.de/englisch_uwg/englisch_uwg.html#p0169)

は技術の自由な交流が必要であるとの考えから、営業秘密保護規定が設けられなかったが、1880年頃には工業上の秘密窃取が蔓延しはじめたこともあり、同法の制定に繋がったといわれている<sup>127</sup>。その意味で UWG は立法当初から自由競争を前提としつつ、これを阻害する不正競争行為に係るルールを定めることに主眼が置かれていた法律であったといえる。

そもそも旧法が刑事的保護のみを規定することとなった背景としては、当時の判例も1874年商標保護法等の反対解釈によって、特別規定による以外は競業上いかなる行為も許されると判断したものもあり、特別法による保護が無ければ不法行為に基づく民事上の責任追及が難しかったが指摘されている<sup>128</sup>。ドイツ民法典は1900年に施行され、不法行為に基づく損害賠償請求権や権利侵害に係る差止請求権が明記されたが、1896年に成立した旧 UWG が明文で禁止する行為類型以外の不正競争行為については十分な対応ができなかったことから、1909年の旧 UWG 改正に際して、いわゆる概括条項(旧 UWG1 条、現行 UWG3 条)が設けられた。これによって営業秘密漏えいのように個別に刑事罰規定がない不正競争行為についても、不正競争行為自体の立証により不法行為に係る主観的要件の立証責任を軽減し、また損害が発生していることまで立証せずとも不正競争行為自体の存在を立証することによって差止請求をなしえるという点において、民事的保護の強化を意図したものであったといわれている<sup>129</sup>。

#### 具体的な規定の内容

刑事罰規定を定めている UWG17 条 1 項は、従業員による雇用期間中の営業秘密の漏えいを禁止している。また同 17 条 2 項は従業員に限らず、不当な目的で、技術的手段の利用、複製物の作成、媒体の取得といった手段を用いて営業秘密を取得することを禁止している。加えて同 19 条によりこれらの教唆・幫助行為についても刑事罰の対象とされている。なお 2004 年以前の旧法には営業秘密漏えいについて損害賠償請求権を定める規定があったが、現行の UWG には承継されていない。

しかし、UWG は営業秘密について明確な定義規定を置いていない。この点、判例においては、非公知であること、企業の営業に関わること、当該企業の意思に基づいて秘密とされていること、経済的な利益があること、が要件であるといわれており<sup>130</sup>、諸外国のそれと特段異なる点はない。

もっとも UWG 自体について、保護対象があいまいであるとの指摘があり、「価値のあるデータ」を保護すべきであることは否定されないが、どのような行為が禁止されるのか、例えば当該データのローデータの中には価値が見いだせないものも含まれていることが想定されることから営業秘密として保護対象とな

<sup>127</sup> 千野直邦『営業秘密保護法』(中央経済社、2007年)72-73頁。

<sup>128</sup> 千野・前掲書、73頁。

<sup>129</sup> 千野・前掲書、77頁。

<sup>130</sup> AIPPI, Protection of trade secrets through IPR and unfair competition law (Q215)(Germany), 2010. p.1-3. 同報告書は判例として、BGH, GRUR 1955, 424, 425 – Möbelpaste; GRUR 1961, 40, 43 – Wurftaubenpressen; GRUR 2003, 356, 358 – Präzisionsmessgeräte を指摘している。

りえるのかといった点について疑問であるとの声も聞かれた<sup>131</sup>。

### (3) 新法(営業秘密法)

既に触れた EU における営業秘密保護指令を国内法において実施すべく、ドイツ連邦政府は現地調査実施時である 2017 年 6 月の段階で法改正の準備が行われており、9 月の連邦議会選挙の後、10 月か 11 月に発布の予定で調整が図られているところであった<sup>132</sup>。ただし、欧州委員会が同指令を策定する過程にドイツ連邦政府担当者は関与してきたことから、同指令と整合的な国内法の策定に大きな支障はないとの認識が連邦政府部内<sup>133</sup>においてなされている。

営業秘密法に関しては、UWG17 条の規定を新法に移管した上で、新法の規定で営業秘密保護指令との整合性を確保する方向性で検討が行われているとの指摘があった。また営業秘密について何をどこまで保護するかという点について、明確な定義がある訳ではなく、新法が成立した後においても運用に委ねられる部分が残ることも想定されているようである<sup>134</sup>。

現地有識者が産業界と議論をしている中で、製造業(機械、自動車)、情報産業、ロジスティクス業界、通信業界といった主要な産業界においては新たな法整備は不要であるとの意見が太宗を占めているとの指摘もあった<sup>135</sup>。有識者からは「ドイツにおける営業秘密保護指令の国内法化対応が済む前に同指令自体が見直される可能性すらある」<sup>136</sup>という意見も聞かれたが、政府関係者からは「同指令に対して必ずしも賛意ばかりではないことも承知してはいるが、昨年(2016 年)発出されたばかりでもあり、にわかに見直しをおこなうという地合いではない」<sup>137</sup>として冷静なコメントが聞かれた。

## 3. 契約

ドイツ産業界においては既に指摘したように、製造業(機械、自動車)、情報産業、ロジスティクス業界、通信業界といった主要な産業界においてはデータ保護について、企業間の契約によって図られるべきであるとの声は多い。商業活動や商用実験において、大量の産業データが作られた場合、ビジネス・アイデアを持つ人によって活用が図られ、新たなビジネス・モデルが台頭する動きを促進することが望ましく、そのために最善の方法は契約による利用範囲の

<sup>131</sup> 現地調査(政府関係者ヒアリング)より。

<sup>132</sup> 2017 年 10 月時点では、ドイツ連邦司法消費者保護省の HP 等で新法は未公表である。

<sup>133</sup> ドイツ連邦政府部内では、司法消費者保護省、内務省及び経済エネルギー省が連携し、同法を含むデータ関連の法制度をめぐる協議や整備を取り進めている。

<sup>134</sup> 現地調査(政府関係者ヒアリング)より。

<sup>135</sup> 現地調査(有識者ヒアリング)より。

<sup>136</sup> 現地調査(有識者ヒアリング)より。

<sup>137</sup> 現地調査(有識者ヒアリング)より。

確定と保護であるとの見方が共有されているためである<sup>138</sup>。

特に大企業においては契約により多くを委ねるべきであるとの声もあるが、中小企業の場合には、大企業との力関係から自社の望む内容での契約締結が難しいことに一定の懸念があることから、必ずしも同意見でない可能性が指摘されている<sup>139</sup>。自動車業界等では、独自にデータの種類による分類を行い、それぞれについてガイドラインを定める動きを見せており注目されている<sup>140</sup>。

#### 4．不正行為

ドイツにおいては刑法が不正行為について重要な役割を果たしている。特にデータ保護との関係で重要な法令として、秘密に管理されているデータに権限なくアクセスし、これを取得する行為を禁止する刑法 202a 条及び 202b 条を指摘することができる。また同法 203 条は他者から当該秘密の開示を受けた者がこれを第三者に開示する行為、同法 204 条が他者から当該秘密の開示を受けた者がこれを使用する行為をそれぞれ禁止している。

刑法 202a 条によって秘密に管理されているデータへの不正アクセスが刑法によって禁止されることになったのは、1986 年に成立した第 2 次経済犯罪防止法によってであり、当時東側諸国からの産業スパイから技術等を守ることに主眼がおかれていた。

なお、不正行為を防止することを内部から牽制することの有用性が認識されており、内部告発者保護に関するドイツ国内の取組み及びこれに影響を与える欧州委員会の動きも関連づけて指摘されている<sup>141</sup>。

#### 5．データの保護可能性

##### (1) 自動車業界によるガイドライン策定の動き

産業データ（本報告書における「価値のあるデータ」と概ね一致した概念）に係る法制度については新たな保護規制を望む声は少なく、分野横断的な法制度とは一線を画し、分野毎に検討を進めることの有用性が指摘されているところである。その先端的な例として、既述のとおりドイツの自動車産業のガイドライン策定に向けた取組みが注目に値するとのことが、複数の関係者から聞かれた<sup>142</sup>。すなわち、ドイツ自動車産業連盟（Verband der Automobilindustries：VDA）は、2016 年 9 月に「自動車（及び自動車が生成するデータ）へのアクセ

<sup>138</sup> 現地調査（政府関係者、産業団体ヒアリング）より。

<sup>139</sup> 現地調査（政府関係者、産業団体ヒアリング）より。

<sup>140</sup> 現地調査（産業団体ヒアリング）より。

<sup>141</sup> 現地調査（政府関係者、産業団体ヒアリング）より。

<sup>142</sup> 現地調査（政府関係者、産業団体ヒアリング）より。

スに関する意見」と題する意見書<sup>143</sup>を公表した。同意見書では、デジタル化により自動車同士が継続的に通信することが可能となり、自動車や道路等に係るデジタル情報により、事故の予防、燃料効率性、環境影響の低減等多様な可能性が開かれる、「自動車はデータ生成の主体となりつつある」との現状認識を示しつつ、自動車の安全性( vehicle safety )、運転の安全性( automotive security ) 及びデータプライバシーを 3 つのリスクとして、これに対応するポジションを明らかにすることで、差別のないイノベーションを可能にすることが意図されている。同ペーパーではまず、OEM メーカーは生成されたデータの安全な移送を確保する責任を持ち、B to B のインターフェースを標準化・保持することが求められる、第三者は OEM の B to B インターフェース又は中立的なサーバーを介して OEM のサーバーからデータにアクセスできる、との 2 段階の構造を示しつつ、「B to B OEM インターフェースのアクセスは B to B の契約に基づくものである」とし、契約による合意に基づくデータへのアクセスを基本とすることを明言している。さらに、データ利用のカテゴリーの考え方( Concept for data usage category ) を天候や道路状況等の公共データから個人情報まで 5 つの段階に分けて示した上で、異なる保護が必要であるとしている。

なお、現地調査によれば、VDA は同意見書をさらに発展される協議を行っており、より詳細なガイドラインの作成を企図しているとのことである<sup>144</sup>。

VDA は、同意見書に先駆けて、ネットワークに常時接続する「コネクテッド・ビーグル」におけるデータ保護に関する指針<sup>145</sup>を提示し、接続性やこれに伴う新たなサービスを促進させるために、透明性の向上、顧客自身によるデータ共有範囲の選択( self-determination )、データの安全性の 3 点の確保を会員企業に求めている。

## ( 2 ) データベース保護指令及び同国内法

ドイツは 1996 年のデータベース保護指令に基づき 1998 年 1 月の期限までに国内法整備を間に合わせた数少ない EU 加盟国のひとつであった<sup>146</sup>。しかしながら、ドイツにおいても同指令ならびに同法の活用について前向きな評価は聞かれるところではなかった。また、現在、欧州委員会がパブリック・コンサルテーションを実施中の欧州データベース指令の見直しに関連し、既存の指令や

<sup>143</sup> VDA, Position on Access to the vehicle (and vehicle generated data), 19 September 2016  
<https://www.vda.de/en/topics/innovation-and-technology/network/access-to-the-vehicle.html>

<sup>144</sup> 現地調査(政府関係者、産業団体ヒアリング)より。

<sup>145</sup> VDA, Data Protection Principles for Connected Vehicles, 3 November 2014,  
<https://www.vda.de/en/topics/innovation-and-technology/network/data-protection-principles-for-connected-vehicles.html>

<sup>146</sup> DG INTERNAL MARKET AND SERVICES WORKING PAPER  
First evaluation of Directive 96/9/EC on the legal protection of databases, Brussels, 12 December 2005,  
[http://ec.europa.eu/internal\\_market/copyright/docs/databases/evaluation\\_report\\_en.pdf](http://ec.europa.eu/internal_market/copyright/docs/databases/evaluation_report_en.pdf)

これによる各国法は対象を構造化されたデータベースに限定しているため、今日のビッグデータとは異なり、サブスタンスを失うのではないかといった懐疑的な意見が呈されている<sup>147</sup>。

### (3) 産業界、研究所等のデータの保護・利活用をめぐる新たな動き

標準と共通のガバナンスモデルを持つバーチャルのスペースにおいて、ビジネスのエコシステムのデータを安全に交換し、リンクさせる「産業データスペース (industrial data space)」と称するイニシアチブが2014年末にドイツの産官学により実施されている。フラウンフォーファー研究所が中心となり、研究及び実証実験を実施、報告書で法的側面についても言及している<sup>148</sup>。

プラットフォーム Industrie 4.0 は、連邦経済エネルギー省及び産業界や有識者の代表による協議体であるが、その法的枠組作業部会 (legal framework working group) は、Industrie 4.0 の法的な機会とリスクを評価し、新たなビジネス・モデルの開発や発展に資することを目的としている<sup>149</sup>。同作業部会ではデータの取扱いに関する検討がおこなわれており、ドイツ連邦政府が力を注ぐ産業政策である Industrie 4.0 の文脈の中でデータに係る法制度についての見解や方向性が示されていくかどうかが注目される。

ドイツの産業界は、パーソナルデータの活用に関して「アメリカ企業に水をあけられ、グーグルのようなアメリカ企業にビジネスの上で優位を取られて久しい」と認識しているが、2年ほど前から非パーソナルデータ (non-personal data) の重要性が高まってきているとしている。産業界は総じて政府に対して規制や法の導入を求めないが、データに関連してもまさに同様の立場であり、新法の導入には反対する立場であること、企業間の契約で対応することが望ましいと考えていることは上述のとおりである。しかし、2017年半ば頃から「異なる意見も出はじめている」との見方もある。「自動車業界のように、自主的にソリューションを見いだせるところばかりではなく、5年後の姿がわからない業界も多い」中、「基本的には現在、契約によるソリューションを企業に委ね、第三者による不正行為は不正競争防止法で救うという方向ではあるものの、救いきれる場合ばかりではないことも承知している」との意見があり<sup>150</sup>、一定の法制度の導入への期待もみられるところが現状である。

<sup>147</sup> 現地調査 (政府関係者、有識者ヒアリング) より。

<sup>148</sup> Fraunhofer, Whitepaper on Industrial Data Space – Sovereignty over data, <https://www.fraunhofer.de/content/dam/zv/en/fields-of-research/industrial-data-space/whitepaper-industrial-data-space-eng.pdf>

<sup>149</sup> Plattform Industrie 4.0, Between data protection and supporting innovation: the Legal Framework for Industrie 4.0 <http://www.plattform-i40.de/I40/Navigation/EN/Industrie40/AreasOfAction/LegalFramework/legal-framework.html>

<sup>150</sup> 現地調査 (産業界ヒアリング) より。



## 第4章 フランス

### 1. 概説

#### (1) フランスにおける関連法制の概要

フランスにおける営業秘密に係る制度的保護<sup>151</sup>に関しては、法案が出された経緯はあるものの、未だ一般の制定法は存在しない。営業秘密に係る事項は、一般法であるフランス民法に定める民事上の責任の原則及び不法行為の適用に準拠<sup>152153</sup>することとなる。フランス法において、競争相手の営業秘密を不正に開示する行為は不正競争行為とみなされ、法的責任を問われる<sup>154</sup>。さらに、特定の場合においては、フランス労働法における「製造上の秘密の開示」にあたり、違反があった場合には刑事的な制裁手段の対象となるが、違反行為の成文法による定義はない。ただし、全体的には営業秘密の保護は、主として不法行為法又は契約法に基づいた決定による判例法に準拠している<sup>155</sup>。なお、判例数は10年以上にわたり、余り多いとはいえない。

また、フランス知的財産法典には、従来は「製造秘密」、その後「営業秘密」を保護する規定があるが、その定義は成文化されていない。また、データベースを保護する規定が設けられており、複数の判例があるが、データベース性の判断はケースバイケースであることが判示されている。

なお、個人情報保護に関しては、1978年に情報処理及び自由に関する国家委員会（Commission nationale de l'informatique et des libertés : CNIL）が設立されて以来、厳格な制裁が志向されているが、裁判所が異なる判断をすることもあるとの指摘がある<sup>156</sup>。

---

<sup>151</sup> フランスにおける営業秘密について紹介する文献として、経済産業省（委託先：TMI 総合法律事務所）「知的財産の適切な保護に関する調査研究 東アジア大における不正競争及び営業秘密に関する法制度の調査研究報告 欧米の法制度との比較において」（2007年）特許庁（委託先：三菱UFJリサーチ&コンサルティング）「人材の移動による技術流出に係る知的財産の在り方に関する調査研究報告書」（2011年）経済産業省（委託先：TMI 総合法律事務所）「諸外国の訴訟手続における営業秘密保護の在り方等に関する調査研究報告」（2010年）等がある。

<sup>152</sup> 経済産業省（委託先：TMI 総合法律事務所）「知的財産の適切な保護に関する調査研究 東アジア大における不正競争及び営業秘密に関する法制度の調査研究報告 欧米の法制度との比較において」（2007年）第II編 P. -100

<sup>153</sup> Report by AIPPI, Protection of Trade Secrets through IPR and Unfair Competition Law, 17 March 2010.

<sup>154</sup> 経済産業省（委託先：TMI 総合法律事務所）「知的財産の適切な保護に関する調査研究 東アジア大における不正競争及び営業秘密に関する法制度の調査研究報告 欧米の法制度との比較において」（2007年）第II編 P. -100

<sup>155</sup> 経済産業省（委託先：TMI 総合法律事務所）「知的財産の適切な保護に関する調査研究 東アジア大における不正競争及び営業秘密に関する法制度の調査研究報告 欧米の法制度との比較において」（2007年）第II編 P. -100

<sup>156</sup> 現地調査（有識者ヒアリング）より。

## (2) 政策動向

フランスにおいては、デジタルトランスフォーメーション政策がとられ、デジタル共和国法 (Digital Republic Act) が 2015 年 12 月に承認、2016 年 10 月に施行された。これは、個人情報に関わるものであり、1978 年フランスデータ保護法等を、一般データ保護規則 (GDPR) の発効に先駆けて改正するものであった。

また、「価値あるデータ」の関連では、フランスにおいてもドイツの Industrie 4.0 と同様に、国家戦略として「産業の未来 (Industry of the Future)」が打ち出され、プラットフォームが形成されているが、ここでもデータの取扱いが関心事項とされている。

いずれにせよ、フランスにおいて産業データの保護を明示的に対象とする法制度は存在せず、データに関する法令については、新大統領の下、より正確なものとなることが期待され、複数の EU 指令を受けた法改正を含め、今後 5 年間は注目していくことが必要であるとの意見が聞かれた<sup>157</sup>。

## 2. 営業秘密

### (1) 概要

本章冒頭で述べたとおり、フランスにおいて営業秘密に係る固有の制定法は存在しない。営業秘密の保護に関連した事項は、フランス民法典第 1382 条及び第 1383 条に定める民事上の責任の原則の適用に準拠する。民法典が編纂された時代にまでさかのぼる基本的な条文であり、損害に対する補償を定めたものである。競争相手の営業秘密を不正に開示する行為はこの条項に照らし合わせて法的責任を問われる<sup>158</sup>。

フランスでは、略式裁判 (summary judgement) が制度上存在しないことから、判決前のエンフォースメントは難しいとされるが、主張自体に疑義が無ければ仮処分を申し立てることはできる。仮処分の命令が出せるのは、本件が緊急で、相手方が真摯な対応をしない場合、切迫した損失や明白な違法状態を回避するために当該命令が不可欠である場合、申立人が履行を求めようとしている相手方の義務について致命的な争いがない場合であるといわれている<sup>159</sup>。また理論上は、不法行為に対して差止請求を提起することができるものの、営業秘密侵害に際しての差止請求は、ほとんど認められていないといわれている。

なお、フランス国内では近年 2 度にわたり営業秘密に特化した国内法制定の動きがあった。1 度目は 2014 年であり、司法省主体の政府提案であった。この法案では保護の対象となる営業秘密として扱われるデータの範囲を「公知でな

<sup>157</sup> 現地調査 (有識者ヒアリング) より。

<sup>158</sup> 現地調査 (有識者ヒアリング) より。

<sup>159</sup> Elizabeth Oger-Gross, Anastasia Pitchouguina, Elodie Valette and Anaïs Harlé, Litigation and enforcement in France: overview, Global Guide 2016/17.

い情報であって、商業上の価値を有し、秘密として保持するために合理的な措置が取られたもの」と定義していた。しかし、新聞社からの強い反対をはじめ、業界団体からも反対があって成立しなかった。この法案は内部告発者に関する情報源の秘匿性の問題を含むものであった。

2度目は2015年であり、厳密には法案ではなく「プロジェクトの提案」というかたちをとった。先の法案等の際に議論の焦点となった内部告発者については例外扱いとされていたものの、報道機関からも反対があり、法案につながることはなかった<sup>160</sup>。

こうした国内法案の不成立の後、2016年に営業秘密保護指令が出され、2018年までに国内法を整備する必要がある。欧州指令で営業秘密の定義や例外が明確になるが、現在はケースバイケースの対応であることから、どの程度実質的に情報を守る措置となるかは未だわからないという指摘がある<sup>161</sup>。

## (2) 「製造秘密」及び「営業秘密」に係る知的財産法典、労働法典及び刑事罰

フランスにおいては「製造秘密 ( manufacturing secret )」についての保護は知的財産法典に規定( L621-1 )にされ、労働法典でも参照されている( L1227-1 )。労働法典では、企業のいかなる経営者・従業員も、企業の製造秘密を公開し、又は公開を企図した場合には刑事罰を科せられることが規定されている。2008年5月の法改正では、「製造秘密」は「営業秘密」に置き換えられた。しかしながら、既述のとおり、成文法では製造秘密、営業秘密とも定義規定はない。さらに、フランスの裁判所において定義を緻密化するような判例の蓄積はない<sup>162</sup>。

なお、フランス労働法典 ( Code du travail ) 第 L.152-7 条は、「製造上の秘密の開示」の場合における刑事的制裁手段を定めている。従業員が営業秘密を外部に漏れいした場合、フランス法に基づき2年間の服役又は30万ユーロの罰金を科せられる。

### 3. 雇用における忠誠義務

フランスにおいては、民法典第 L.1134 条3項及び第 L.1135 条、ならびに労働法典第 L. 120-4 条に基づき、役員や従業員等の被雇用者は、契約期間を通じて雇用主に対して忠誠義務 ( obligation of employee loyalty ) を負い、機密情報の保護の義務もこれに含まれるものと解されている。被雇用者が創造した情報を、対象となる情報が含んでいたとしても、情報の当初の管理は雇用者側に属する。ただし、情報の管理主体は当該情報が特許情報を含むかどうかで扱いは変わる。特許を取得しうる情報である場合には、知的財産法典第 L. 611-7 条に基づき、その発明が雇用契約、公的セクター、又は研究契約のいずれの下に行

<sup>160</sup> 現地調査 ( 有識者ヒアリング ) より。

<sup>161</sup> 現地調査 ( 有識者ヒアリング ) より。

<sup>162</sup> 現地調査 ( 有識者ヒアリング ) より。

われたかをまず特定した上で対応が図られる。他方、特許を取得しうる情報を含まない場合（発明を含まない「被技術的秘密」であった場合）にはこの条項の対象外となる。

なお、フランス法は雇用契約終了後にはかつての被雇用者に義務を課すことはないが、雇用主は、かつての被雇用者との間において、雇用契約終了後における競業禁止契約を特に締結していない場合でも、かつての被雇用者の不正行為が雇用主に対して特定の損失を生じた旨の証拠を提示することを条件として、損害賠償を取得することができる。このような事件において、雇用主は、不正競争に関する判例法に基づき損害賠償請求訴訟を提起することとなる<sup>163</sup>。

#### 4．契約

フランスにおいても、価値あるデータの企業間における法的枠組みは契約により定められるのが通常であるとの認識が持たれていた<sup>164</sup>。

現状において、契約は、従業員との間の労働契約と、第三者である顧客、サービス提供者等に営業秘密等のデータを開示又は移送するにあたっての、非開示合意（NDAs）や移送契約（transfer agreement）等が含まれる。営業秘密に関する法制度が不在であることから、営業秘密や製造秘密は、知的財産法典の判例によって進展してきたことと並行して、営業秘密を阻害する契約又は不正競争に関わる申し立てによっても進展してきた。

#### 5．データの保護可能性

フランスの産業界は、デジタルデータに個人情報が含まれていることにより自由移動が妨げられることはビジネスへの制約だと考えており、的確な匿名化が図られ、営業秘密として企業に属することとなることが必要だと考えている<sup>165</sup>。

フランスにおいては、ドイツの自動車業界のように、突出した動きを見せている業界はないが、総合経済団体が、データの扱いに関して欧州委員会との協議や情報収集・提供や周知に努めている。

---

<sup>163</sup> 経済産業省(委託先:TMI 総合法律事務所)「知的財産の適切な保護に関する調査研究 東アジア大における不正競争及び営業秘密に関する法制度の調査研究報告 欧米の法制度との比較において」(2007年)第II編 P. -105.

<sup>164</sup> 現地調査(産業団体、有識者ヒアリング)より。

<sup>165</sup> 現地調査(産業団体ヒアリング)より。

## 第5章 イギリス

### 1. 概説

#### (1) イギリスにおける関連法の概要

イギリスにおける経済的に価値のあるデータの保護は、第一義的にコモン・ローにより「機密情報 (confidential information)」が保護され、これが侵害された場合には差止等民事的な救済措置を請求することができるという意味において図られている。機密情報の保護については、刑事的救済措置はないものの、窃盗や著作権侵害にあたとされる場合には刑事的措置を施すことが可能である。これに加えて、1989年競争法によって「商業的にセンシティブな情報 (commercially sensitive information)」が保護され、救済手段として制裁金の支払い等に加え、刑事的訴えをおこなうことが可能な場合もある。さらに、データへの不正なアクセスが為された場合には、1990年コンピュータ不正使用法により刑事罰が執行される。なお、2016年に採択された営業秘密保護指令については、イギリスがEU離脱に先立ち本指令に基づく新たな制度を導入する可能性は低いという見方もある。

また、イギリスにおいてパーソナルデータはデータベース保護指令を受けて設置された1989年データ保護法により保護されている。2016年の一般データ保護規則 (GDPR) の成立により、規則が有効となる2018年までにGDPRに則したパーソナルデータの保護制度の策定が求められている。さらに、現在新たなパーソナルデータの保護のための新法策定が計画されているが、この新法とGDPRの整合性についてはイギリスのEU離脱の先行きを踏まえ、様々な意見がある。データ保護制度全般におけるイギリスのEU離脱の影響は、未だ明らかになっていない。

#### (2) 政策動向

近年のイギリス国内におけるデータ保護に関する動向として、イギリス政府は2017年3月に、イギリスデジタル戦略の一部として、政策ペーパー「イギリス経済におけるデータの力の解放と、その利用に対する国民の信頼向上 (unlocking the power of data in the UK economy and improving public confidence in its use)」<sup>166</sup>を公表した。この政策ペーパーの中では、データ経済の支援、市民の信頼構築、政府データの効率的な利用が主要な柱としてあげられている。

特に「データ経済の支援」においては、産業界におけるデータのさらなる利活用に向けて、インフラ構築等の取組みの支援の必要性が示されている。また、

---

<sup>166</sup> Department for Digital, Culture, Media & Sport, “Policy paper 7. Data-unlocking the power of data in the UK economy and improving public confidence in its use,” <https://www.gov.uk/government/publications/uk-digital-strategy/7-data-unlocking-the-power-of-data-in-the-uk-economy-and-improving-public-confidence-in-its-use>

データの越境移動については、EUの方針に沿ったデータ保護法及びセーフガードの維持に加え、イギリスのEU離脱プロセスに関連し、データ移動を阻害しないような法的透明性の維持が明言されている。

「市民の信頼構築」においては、政府及び事業者がデータを提供した者の信頼を維持することが重要であるとし、イギリスの個人情報保護の監督機関であるインフォメーション・コミッション（Information Commission : ICO）を中心として、パーソナルデータを保護する法的枠組みの構築及びそのプロセスへの人々の参加を支援していくことが宣言されている。

このような政策ペーパーが発表される一方で、イギリス政府においてデータの保護を担うイギリス文化・メディア・スポーツ省は、イギリスのデジタルエコノミーに向けたアプローチは、現在停滞しているという見解を示している<sup>167</sup>。

## 2. 営業秘密

### (1) 概要

イギリスにおいて、営業秘密を含む技術的、商業的、その他の情報はコモン・ロー上の信頼関係の法理（the law of confidence）の下で保護される<sup>168</sup>。信頼関係の法理において、秘密情報（confidential information）を取得した者は、一定の要件を満たした場合には衡平法上の秘密保持義務（equitable duty of confidence）を負い、秘密保持義務違反（breach of confidence）の行為があった場合には、民事訴訟を提起することができる<sup>169</sup>。

なお、2016年に欧州委員会において採択された営業秘密保護指令について、イギリスでは現行制度でTRIPS協定の定める義務が果たされているという見解が一般的であり、EU離脱交渉の完了時期を問わず、本指令を施行するための制度は導入されないのではないかという見解がある<sup>170</sup>。

---

<sup>167</sup> 現地調査（法律専門家インタビュー）より。

<sup>168</sup> 一般論としては、イギリスにおける営業秘密保護は、複数の不法行為類型からコモン・ローによって発展したものであるといわれている。またイギリスにおける救済は、裁判所において訴権が認められる場合には何らかの救済が裁判所によって認められる可能性がある訳であるが、営業秘密についても侵害態様等によって、様々な根拠に基づいて救済がなされる。そのため、信頼関係の法理もその一態様であるという理解ができる。この点、例えば小野昌延『営業秘密の保護【増補】』（信山社、2013年）191-192頁等も参照。

<sup>169</sup> 現地調査（法律専門家インタビュー）より。

<sup>170</sup> Mewburn Ellis LLP「イギリスのEU脱退（「イギリスのEU離脱」）が知的財産権に及ぼす影響」

<http://mewburn.com/wp-content/uploads/2017/07/Withdrawal-of-the-UK-from-the-EU-Japanese-.pdf>

## (2) 保護の対象及び問題となる行為

Coco v A.H. Clark (Engineering) Ltd 判決<sup>171</sup>以降、秘密保持義務違反行為について民事訴訟を提起する場合の要件として、営業秘密の保持者は(i)情報がその質や本来の性質において機密であること、(ii)情報が秘密保持義務を有すると分かるように授受されたこと、そして(iii)不正な利用があり、それが被害をもたらしたことを証明しなければならない。また、特に(i)の秘密性の要件については、Thomas Marshall (Exports) Ltd v Guinle 事件<sup>172</sup>以降、以下の基準が用いられている<sup>173</sup>。

- (a) 当該情報の開示が、情報の保有者を害するか又は競合者等にとって有利になると保有者が確信していること。
- (b) 当該情報が依然として秘密である（公知になっていない）と保有者が確信していること。
- (c) 上記2点に関する保有者の確信が合理的であること。
- (d) 関連する特定の産業又は取引の慣行に照らして、当該情報が秘密情報として保護されるべきものであると判断されること。

イギリスの裁判所において機密として取扱われた情報の例として、化学式のような技術に関する秘密、工業プロセスのような機械に関する秘密、製品やプロセスの改善、財務・統計情報、見積額、仕入れ値、事業戦略等の商業的情報、顧客や供給元の商業的記録、ソフトウェアのソースコード等がある<sup>174</sup>。

## (3) 救済

秘密保持義務違反に対してのもっとも有用な救済方法は差止である。差止は、(i)営業秘密の第三者への伝達等の行為を防ぎ、(ii)機密情報を所有者に返還することを求めたり、当該情報のさらなる開示を防ぐことを求めたりする目的で行使されうる。イギリスの裁判所においては、緊急に差止命令を取得することができるため、差止による救済は営業秘密のさらなる伝達を防ぎ秘密性と法的保護を維持するのに有用である<sup>175</sup>。また、対象となる営業秘密が既に伝達されている場合には、将来の利用に対しての差止命令を取得することが可能である。

営業秘密の所有者は、秘密保持義務違反によって生じた損失について、差止請求に加えて、若しくは差止請求に代わって、損害賠償請求をおこなうことができる。ただし、損害賠償ではさらなる情報の伝達や機密情報の利用を防ぐことはできず、また損害賠償が有用となるのは被告が賠償をするのに十分な資金

<sup>171</sup> Coco v A.H. Clark (Engineering) Ltd. [1969] R.P.C.41, Judge Megarry, J. para 11

<sup>172</sup> Thomas Marshall (Exports) Ltd v Guinle [1979] Ch 227, [1978]IRLR 174, [1978]ICR 905

<sup>173</sup> 経済産業省（委託先：TMI 総合法律事務所）「諸外国の訴訟手続における営業秘密保護の在り方等に関する調査研究報告」（2010年）

<http://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/H21shogaikoku.pdf>

<sup>174</sup> 現地調査（法律専門家インタビュー）より。

<sup>175</sup> 現地調査（法律専門家インタビュー）より。

を保持している場合のみというのが実情である。損害は、通常は不法行為の原則に基づいて評価され、法的には請求者を義務違反が生じていない状態へと回復させることを目的とする。損害は、使用料 (royalty) に基づく評価、又は被告が義務を違反していなければ原告が得たであろう利益に基づいた評価によって算定される。

また、原告は損害賠償の代わりに利得の精算 (account of profit) を選択し、被告が義務違反によって得た利益の計算にもとづいた賠償を請求することもできる。原告は、損害賠償又は利益の精算のどちらかしか選べず、実際には利益の精算を選択することはまれである<sup>176</sup>。これに加えて、裁判所はさらなる不正利用を防ぐために、機密情報が含まれた物の引き渡しを命令することができる。

イギリスにおいては、営業秘密の不正利用に特化した刑事規定はない。ただし、現地の法律家によれば場合には刑事的措置を講ずることが可能であり、保護対象が営業秘密と重複する可能性が指摘されている<sup>177</sup>。

- (i) 書類や媒体等の営業秘密を含む財産が不正に盗まれた場合 (1968 年窃盗法第 1 条)
- (ii) 著作権を侵害した物を作成又は取扱った場合 (1968 年著作権・デザイン・特許に関する法律 107 条)

### 3. 競争法

イギリス及び EU においては、企業は独立して製品やサービスを供給又は購入するべきという原則があり、その原則の下で競争法は経済活動においてどのような情報が共有されることができ、どのように共有すべきかを規制する。EU の機能に関する条約 (Treaty on the Functioning of European Union) は第 101 条において競争制限的協定・協調的行為を規制し、第 102 条で市場支配的地位の濫用行為を規制している。これに倣い、イギリスでは 1998 年競争法によって、イギリス国内における取引に影響を与える反競争的協定 (第 1 章) 及び支配的地位の濫用 (第 2 章) に対する規定が定められている<sup>178</sup>。1998 年競争法によって、商業的にセンシティブな情報 (commercially sensitive information) の伝達は、競争法違反とされている。「商業的にセンシティブな情報」は競争法において定義されていないが、実務においては公的なドメインではない分野における再販売価格や、製造能力又はコスト等の情報が、商業的にセンシティブであり競争法の範疇となる可能性が高いとされている。法律専門家からも本調査の対象である「価値あるデータ」も「商業的にセンシティブな情報」として捉えられる可能性があるという指摘があった。<sup>179</sup>

<sup>176</sup> 現地調査 (法律専門家インタビュー) によれば、実際には被告が義務違反によって得た利益の計算を原告側がおこなうことは困難であるという指摘があった。

<sup>177</sup> 現地調査 (法律専門家インタビュー) より。

<sup>178</sup> 公正取引委員会ウェブサイト

<http://www.jftc.go.jp/kokusai/worldcom/kakkoku/abc/allabc/u/uk.html>

<sup>179</sup> 現地調査 (法律専門家インタビュー) より。



また、競争市場庁（Competition & Markets Authority：CMA）のガイドライン<sup>180</sup>によれば、競合企業への情報開示について以下のような行為が競争法違反にあたるとされる。

- (i) リポートや割引を含む価格に関する意向や、誰に何をどのような条件で販売しようとしているかといった事業戦略等、事業の将来について競合企業と議論をおこなうこと。
- (ii) 自社の顧客の将来の価格設定の計画を別の顧客に開示すること。
- (iii) 専門的な場であるか社交的な場であるかを問わず、競合企業が将来の価格設定の計画やその他の競争の観点からセンシティブな情報について議論をおこなう場に滞在すること。

商業的にセンシティブな情報を伝達したと認められた企業は、最大で全世界での売上の10%の制裁金（financial penalties）を支払わなければならない。また、違反行為に参加した企業内の個人は、15年間イギリス企業において取締役（Director）を務める資格をはく奪され、刑事上有罪となる可能性もある<sup>181</sup>。

#### 4．不正アクセス

1990年コンピュータ不正使用法（Computer Misuse Act 1990）は、アクセスを許可されていないプログラムやデータへ不正にアクセスをおこなう意図でコンピュータを機能させること（同法第1条）及びさらなる違反行為をおこなう意図をもって違反行為をおこなうこと（同法第2条）を禁止している。成立背景として、同法成立以前にはサイバー犯罪に対処するための実質的な法律が存在せず、ハッキング等の事犯において対処ができていない現状があったことや、欧州法務委員会の1989年のコンピュータ犯罪に関する勧告が出されたことが同法の導入の一因であるとされている<sup>182</sup>。

不正アクセス罪の法定刑は正式起訴の場合には2年以下の禁固刑又は罰金刑（併科可）であり、略式起訴の場合には12か月以下の禁固刑又は法廷上限以下の罰金刑（現在は、5,000ポンド、併科可）となっている<sup>183</sup>。

---

<sup>180</sup> Competition & Markets Authority, “Competitors’ information: how to limit your competition law risks,”  
[https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/358298/Competitors\\_information.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/358298/Competitors_information.pdf)

<sup>181</sup> Company directors and competition law (OFT Guidance June 2011)  
[https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/284410/oft1340.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/284410/oft1340.pdf)

<sup>182</sup> Council of Europe Committees of Ministers, Recommendation No. R(89)9 of the Committee of Ministers to Member States on Computer-Related Crime,  
<https://wcd.coe.int/com.instranet.InstraServlet?command=com.instranet.CmdBlobGet&InstranetImage=610660&SecMode=1&DocId=702280&Usage=2>

<sup>183</sup> 経済産業省（委託先：TMI 総合法律事務所）「諸外国の訴訟手続における営業秘密保護の在り方等に関する調査研究報告」（2010年）  
<http://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/H21shogaikoku.pdf>

## 5 . 契約

イギリスにおいても、契約自由の原則のもと当事者はお互いの望む契約を自由に結ぶことができる。情報を共有する際に機密性を保持するための方法として、イギリス知的財産庁は秘密保持契約（non-disclosure agreements）に関するガイダンスを公表している<sup>184</sup>。ガイダンスにおいて、秘密保持契約は原則として、記録されておりかつ「機密」であることが記された情報のみを保護し、また会合やプレゼンテーションで共有された情報も保護するとされている。また、秘密保持契約においては、情報の利用目的を限定することが求められるが、それは同時に、事業活動に即した現実的なものである必要がある。さらに、秘密保持契約においては機密として保持する期間についても考慮することが求められる。通常は3~5年であることが多いが、特許を取得していないノウハウや、顧客リスト、プロジェクト参加者の個人的な情報等は永久的に機密とされうる。

データの保護可能性として、単一制度でのデータ保護は困難であり、複数の制度の組み合わせによる保護となる旨が指摘され、具体的には、セキュリティにおける保護、データ管理、契約による秘密保持等、複数手段によってデータが不正取得・公開されることを防ぐべきという意見が述べられている<sup>185</sup>。

## 6 . プライバシーデータ

イギリスでは、データベース保護指令を受けて1998年に制定されたデータ保護法（Data Protection Act 1998 : DPA）が制定されている。実務において、DPA及びICOは、一般に事業活動に即した立場をとり、現実的なアプローチを適用していると認識されている<sup>186</sup>。

また、今後のパーソナルデータ保護法制の動向として、2018年5月に有効となるGDPRは、有効となる時期には未だイギリスのEU離脱プロセス交渉は完了していないと予想されるため、イギリス政府及びICOはGDPRがイギリスにおいても適用されることを明言している。

さらに、2017年6月に発表された新たな立法議案は、パーソナルデータ保護の世界的な枠組みに合致する新法及び、デジタル憲章（digital charter）の提案に言及している<sup>187</sup>。このうち新法は、個人が自己のパーソナルデータに対してさらにコントロールを持つことを可能にし、DPAに代わりデジタル時代に合った新たなデータ保護の枠組みを実現するものになっているとしている。ICOは新法に

<sup>184</sup> Intellectual Property Office, 'Guidance: Non-disclosure agreements'

<https://www.gov.uk/government/publications/non-disclosure-agreements/non-disclosure-agreements>

<sup>185</sup> 現地調査（法律専門家インタビュー）より。

<sup>186</sup> 現地調査（法律専門家インタビュー）より。

<sup>187</sup> Queen's Speech, 21 June 2017 Volume 783.

<https://hansard.parliament.uk/lords/2017-06-21/debates/359B47E0-E2CB-41F8-908C-4294844C1518/Queen%E2%80%99Speech>

ついて、成立予定ではあるが具体的時期は未定としており、新法の内容は GDPR を踏まえたものになることが予想されるとしている<sup>188</sup>。一方で、ICO 及びイギリス政府は、EU 離脱後のイギリス法が EU によって適切であると見なされるかについては不透明であるとし、EU 加盟国とイギリスの間でのパーソナルデータの移動を妨げる可能性が懸念されている<sup>189</sup>。

また、新たなデジタル憲章は、イギリスを、デジタル事業をおこなうにあたり最適であり、かつもっとも安全にオンラインでいることができる国にすることを目的としており、この憲章の下で、利用者及び事業者の自由と安全性の適切なバランスを実現する法体系が整備されていくとしている。

しかしながら、イギリスにおけるデータ保護政策を管轄し、ICO の出資をおこなう文化・メディア・スポーツ省は、新たなデータ保護法及び、デジタルエコノミーに対するイギリスの取組みは、「停滞している」と述べている<sup>190</sup>。

---

<sup>188</sup> 現地調査（法律専門家インタビュー）より。

<sup>189</sup> 現地調査（法律専門家インタビュー）より。

<sup>190</sup> 現地調査（法律専門家インタビュー）より。

## 第6章 中国

### 1. 概説

#### (1) 中国における関連法制の概要

中国では、China Food and Drug Administration による薬事法規則 (The Implementing Regulations for the Drug Administration Law) において、非公開の治験データの保護を定める<sup>191</sup>他は、データ保護に係わる特別法は存在しない。

現地の法律専門家によれば、本調査の対象となるデータ保護については、反不正当竞争法 (Anti-Unfair Competition Law) による保護が適用されるという意見があがっている<sup>192</sup>。

反不正当竞争法では、営業秘密の対象と規制行為を規定し、救済措置は刑法で懲役・罰金、民法で差止、損害賠償を規定する構成となっている。

なお、個人情報保護については、2012年に公布・施行された「ネットワークにおける情報保護強化に関する全国人民代表大会常務委員会決定」で、ネットワークサービス提供者、及びその他の事業者による個人情報電子データの取扱いの原則として、情報の収集と利用の目的・方式及び範囲に関する明示・同意取得の規定と、法令ならびに両当事者の合意に違反する情報収集・利用が禁止された<sup>193</sup>。

#### (2) 政策動向

本調査で対象とする価値あるデータの保護について、2017年7月21日に国家発展改革委員会より「サービス業革新発展大綱(2017~2025年)」が発表され、インターネット、ビッグデータ、電子商取引等の分野の知的財産権保護規定の整備について示された<sup>194</sup>。

上記は制度整備の方針が示されているにとどまっており、本報告書作成時点では具体的な法制度の検討・立案は確認されていないが、今後の動向が注目される。

### 2. 反不正当竞争法

中国における知的財産保護は1978年の改革開放政策をきっかけに、1982年の商標法、1984年特許法、1987年民法通則における契約責任又は不法行為の

---

<sup>191</sup> Regulations for Implementation of the Drug Administration Law of the People's Republic of China, Article 35.

<sup>192</sup> 現地調査(法律専門家インタビュー)より。

<sup>193</sup> 全人代委員会「ネットワークにおける情報保護強化に関する全国人民代表大会常務委員会決定」(2012年)

<sup>194</sup> 国家発展改革委員会「サービス業革新発展大綱(2017~2025年)」(2017年)

規定、1990年著作権法の成立を経て、1993年に反不正競争法が成立して、法制度が整備されている<sup>195</sup>。

反不正競争法は、1992年に調印された「知的財産権の保護に関する中国政府と米国政府間の合意覚書」において、中国政府は1993年7月1日までに営業秘密の保護を図るための特別法案を提出しなければならない旨が述べられていることに基づくと思われる<sup>196</sup>。

反不正競争法では、営業秘密の対象として非公知性・有用性・秘密管理性を満たす技術情報及び経営情報と定め、規制される行為については不正取得、不正使用、約定・秘密保持契約に反する公開・使用・他者への使用許諾、違反行為を明らかに知った又は知りうる第三者による不正取得、不正使用、暴露について、営業秘密侵害行為として定義している。救済措置としては、民法・刑法のそれぞれで民事的措置、刑事的措置を定めている。

民事的措置については、民法通則において、技術情報の侵害への保護として、著作権、特許権、商標権等と併せて、発明又はその他の技術成果の剽窃・改ざん・冒用等の侵害に対する、差止（侵害の停止、影響の除去）損害賠償を規定しており<sup>197</sup>、また、顧客情報等の発明又は技術成果に該当しない営業秘密の保護については、故意又は過失による財産の侵害への民事責任において侵害の停止、妨害の排除、危険の除去を規定している<sup>198</sup>。

刑事的措置については、刑法において営業秘密侵害罪を規定しており、反不正競争法で定める営業秘密に対する、不正取得・不正使用に対して懲役又は罰金を規定している<sup>199</sup>。

データの不正取得・不正使用に関する判例としては、インターネットを通じて競合他社のデータを不正取得し、事業において利用することで、反不正競争法に抵触したものが指摘された<sup>200</sup>。

なお、反不正競争法については、改正案が2017年2月の第12期全国人民代表大会常務委員会第26回会議審議に付託、同年11月に可決され、2018年1月1日に施行される予定である。改正法では、インターネット分野における不正競争に係る条項の追加等がなされている<sup>201</sup>。ただしその内容としては、事業者がネットワークにおける技術的手段を利用して、他の事業者が合法的に提供するネットワーク製品又はサービスの正常な運用の妨害や、破壊する行為を

---

<sup>195</sup> 金春陽「営業秘密の法的保護」P.3

<sup>196</sup> 金春陽「営業秘密の法的保護」P.6

<sup>197</sup> 民法通則第118条

<sup>198</sup> 民法通則第106条2項、134条1項

<sup>199</sup> 刑法 第219条

<sup>200</sup> 現地調査（法律専門家インタビュー）より。

<sup>201</sup> 改正反不正競争法では、その他にも商業賄賂関連規定の整備（贈賄対象者の明確化）、秘密侵害関連規定の調整（従業員、元従業員又はその他組織、個人による営業秘密の秘密保持侵害事由の規定）、独占禁止法との整理（ダンピング等に関する規定の反不正競争法からの削除）、民事賠償優先原則の確定（経営者が民事賠償責任及び行政処罰を同時に負う場合、財産が同時支払いに不足する際に、民事賠償責任を優先させることを規定）が含まれる。

規制するものであり、本調査における価値あるデータの保護と直接的に関連するものではない<sup>202</sup>。

### 3．サービス業革新発展大綱（2017～2025年）

本調査の対象である価値あるデータの保護に関する政策動向として、2017年7月21日に国家発展改革委員会より「サービス業革新発展大綱（2017～2025年）」が発表された。

サービス業革新発展大綱（2017～2025年）では、知的財産権保護制度について、専利権、商標権、著作権、営業秘密保護等の法律・法規の整備、ビジネス・モデル特許保護制度の研究、知的財産権審査、登録手続の改善、簡素化、知的財産権の情報資源の共有推進、知的財産権侵害に関する懲罰的賠償制度の整備、企業の海外における権利保護支援メカニズムの整備について言及されている他、インターネット、ビッグデータ、電子商取引等分野の知的財産権保護規定の整備が示されている。

上記で示されている規定整備について本調査報告書作成時点では方針にとどまっており、本報告書作成時点では具体的な法制度の検討・立案は確認されていないが、今後の動向が注目される。

ただし、中国では過去にも全国人民代表大会（National People Congress）において、電子商取引に関する規制が検討されたが、2017年9月末時点において未だ2013年に提出した法案が通過していないことも踏まえると、サービス業革新発展大綱はスローガンを示しているものの、具体化には時間を要するという指摘もある<sup>203</sup>。

### 4．データの保護可能性

中国では、反不正競争法、及び刑法、民法通則に基づいて、秘密として管理されているデータについては、営業秘密の保護によって当該データ保護がなされると、法律専門家は考えており、実際の判例においてもデータの不正取得・不正利用に関しては、反不正競争法が適用されている。

法律専門家の見解として、保護対象の広さ、国際ハーモナイゼーションの観点で、他の制度と比較し、営業秘密の要件に該当する「価値あるデータ」は営業秘密による保護が適しているという意見が聞かれた。

具体的には、著作権との比較において「価値あるデータ」は必ずしも著作物性を有するとは限らない点を指摘している。また、契約はあくまで当事者間の営業秘密の保護を高めることはできるが、第三者による不正取得を回避できるものではない点を指摘している。またサイバーセキュリティ関連法においては、

<sup>202</sup> 中華人民共和国反不正競争法（2017年11月改正）第12条  
[http://www.npc.gov.cn/npc/xinwen/2017-11/04/content\\_2031432.htm](http://www.npc.gov.cn/npc/xinwen/2017-11/04/content_2031432.htm)

<sup>203</sup> 現地調査（法律専門家インタビュー）より。

中国では個人情報に関する文脈で注目されており、今般の調査における「価値あるデータ」を主眼とした内容には必ずしもなっていない点を指摘している。したがって、他制度との比較において反不正競争法による営業秘密の保護が「価値あるデータ」の保護にもっとも適しているという見解であった<sup>204</sup>。

一方で、サービス業革新発展大綱（2017～2025年）に示されるよう、今後、当該分野における知的財産保護の動きが起こりうることから、現行法の見直しや新法立案等、注目する必要がある。

---

<sup>204</sup> 現地調査（法律専門家インタビュー）より。

## 第7章 世界知的所有権機関( World Intellectual Property Organization :WIPO )

### 1 . 概説

#### ( 1 ) WIPO における関連法制の概要

知的財産に関する国連専門機関である WIPO においては、WIPO 著作権条約 ( 2002 年発効 ) においてデータベースに関する規定が設けられており、著作権による保護対象とされている。また、同規定の対象とならない創造性を持たないデータベース ( non-original database ) に関する検討が 1998 年から 2004 年に行われたが、これが条約や機関決定等を生み出すこととはならなかった。

本調査の対象となるデータ保護に係る他の法制である営業秘密に係る制度的保護、不正競争防止法、契約法といった分野については、WIPO において関連する検討等は特段行われていない。

#### ( 2 ) 政策動向

創造性を持たないデータベースの保護をめぐることは、上述のとおり 1998 年から 2004 年まで年に 2 回開催される WIPO 内の著作権等常設委員会 ( Standing Committee on Copyright and Related Rights :SCCR ) において検討されたが、何らかの決議に至ることなく、2004 年 6 月の同会合において WIPO における議論継続を求める意見は少数派となり<sup>205</sup>、以降の著作権等常設委員会において取上げられることはなかった。

また、その後も関連する議論が提起された経緯はない。

### 2 . WIPO 著作権条約におけるデータベース保護

#### ( 1 ) 規定の特徴

1996 年に採択された WIPO 著作権条約「第五条 データの編集物 ( データベース )」は、次のとおり知的創造物であるデータその他の素材の編集物を保護する規定がなされている。

##### 第五条 データの編集物 ( データベース )

素材の選択又は配列によって知的創作物を形成するデータその他の素材の編集物は、その形式のいかんを問わず、知的創作物として保護される。その保護は、当該データその他の素材自体に及ぶものではなく、また、当該編集物に含まれるデータその他の素材について存在する著作権を害するものでもない<sup>206</sup>。

<sup>205</sup> WIPO, Standing Committee on Copyright and Related Rights, Eleventh Session, Geneva, June 7 to 9, 2004, Report Adopted by the Committee, SCCR/11/4, September 16, 2004.

<sup>206</sup> 公益社団法人著作権情報センター  
[http://www.cric.or.jp/db/treaty/wch\\_index.html#05](http://www.cric.or.jp/db/treaty/wch_index.html#05)



これは、創造著作権による保護と独自の権利 (sui generis) による保護の両方を定めているデータベース保護指令とは異なり、後者の保護対象となる創造性のないデータベースは、対象外とされている<sup>207</sup>。

## (2) 検討の経緯

欧州委員会は 1998 年にデータベース保護の必要性を指摘し<sup>208</sup>、その後、1992 年に欧州委員会から sui generis による保護を含む案<sup>209</sup>が示され、1996 年に最終案が採択された。また、アメリカにおいても同様の法案が検討されていたことを受け、同じ 1996 年に欧米から WIPO に対して sui generis による保護を含む条約草案が提出された。しかし、アメリカ国内の法案をめぐる議会審議が停滞したことを受け、WIPO において著作権条約の採択と同時に予定されていたデータベース保護条約の採択は見送られることとなった<sup>210</sup>。

著作権等常設委員会において、1998 年から、データベースの保護(1998~1999 年)、途上国におけるデータベースの保護の経済的影響(2002 年)、創作性のないデータベースの保護(2002~2003 年)といったテーマを中心に検討がなされた。このうち、特に「創作性のないデータベースの保護」については、投資がなされたとしても創作性が認められない場合にデータベースは著作権を帯びないという問題につき、sui generis による保護、不正使用 (misappropriation) や不正競争に対する保護等の可能性について議論がなされたものの、コンセンサスに至るような議論の進捗は見られなかった。2004 年 6 月の会合において、以降は各国の代表による要求があった場合にのみ議論がなされることとされたものの、以降、今日までいずれの加盟国からも提起がなされなかったことは前述のとおりである。

---

<sup>207</sup> データベース保護に関する WIPO、EU、アメリカ等における相違等については、長塚隆「EU のデータベース保護政策」情報の科学と技術 49 巻 7 号(1999 年)340 頁以下、蘆立順美『データベース保護制度論』(信山社、2004 年)199 頁以下等が比較的詳しく紹介を行っている。

<sup>208</sup> Green Paper on Copyright and the Challenge of Technology - Copyright Issues Requiring Immediate Action. COM (88) 172 final, 7 June 1988.

<sup>209</sup> Proposal for a Council Directive on the legal protection of databases. COM (92) 24 final, 13 May 1992.

<sup>210</sup> 武田貞生、奥住啓介、横溝一陽、天野辰美「データベースの法的保護に関する動向調査」(平成 16 年)一般財団法人日本情報経済社会推進協会  
<https://www.jipdec.or.jp/archives/publications/J0004834>

## 第 8 章 経済協力開発機構 ( Organization for Economic Co-operation and Development : OECD )

### 1 . 概説

#### ( 1 ) OECD における関連法制の概要

OECD は先進国間の意見や情報の交換を通じ、経済成長、貿易自由化及び途上国支援に貢献することを目的とし、約 30 の委員会において多岐にわたる活動を行っている。

OECD は分野によって拘束力を有する条約や一定の指針を示すガイドライン等を策定することもあり、データに関連するものとして「OECD プライバシーガイドライン」が策定されている。しかしながら、本調査の中心的な調査対象のひとつである経済的価値を有するデータの保護に関しては、ガイドライン等の策定が行われる方向にはなく<sup>211</sup>、「データ主導型の成長と福祉」といったテーマ等に関して調査研究や検討が行われているのが現状である。

#### ( 2 ) OECD プライバシーガイドライン ( 1980 年策定、2013 年改訂 )

OECD プライバシーガイドラインは、1980 年に策定され、2013 年に改訂されている。1980 年制定の背景には、1960 年代以降のコンピュータを利用した情報処理が急速に発展したこと、欧米諸国を中心とする各国において個人情報保護を目的とする法律が制定されたこと等があった。また、2013 年の改訂の背景には、30 年以上前となった起草時から個人情報保護をめぐる状況が進展し、インターネット・クラウドコンピューティングの発展、収集・利用・保存されるパーソナルデータ量の増大、社会的経済的利益の価値とプライバシーに対する脅威、パーソナルデータのグローバルな利用可能性といった状況が出現したことがあげられる<sup>212</sup>。

同ガイドラインの目的は、加盟国間の情報の自由な流通を促進すること、及び、加盟国間の経済的社会的関係の発展に対する不当な障害の創設を回避すること ( 同ガイドライン前文より )<sup>213</sup>である。

制度が対象とするデータは「パーソナルデータ」、すなわち識別された又は識別されうる個人 ( データ主体 ) に関するすべての情報 ( 1 条 b ) のうち、公的又は私的部門において、取得方法又は性質若しくは利用状況からみて、プライバシーと個人の自由に対する危険を含んでいるもののすべて ( 2 条 ) である。

<sup>211</sup> 現地調査 ( 国際機関職員インタビュー ) より。

<sup>212</sup> 総務省スマートフォンを経由した利用者情報の取扱いに関する WG ( 第 2 回 ) ( 2013 年 ) 資料 7 「諸外国における現状」 p.12  
[http://www.soumu.go.jp/main\\_content/000150899.pdf](http://www.soumu.go.jp/main_content/000150899.pdf)

<sup>213</sup> 個人情報保護委員会「諸外国等における個人情報保護制度の運用実態に関する検討委員会・報告書」( 2007 年 ) P.105  
[https://www.ppc.go.jp/files/pdf/personal\\_report\\_1901caa.pdf](https://www.ppc.go.jp/files/pdf/personal_report_1901caa.pdf)

1980年の策定当初より、次の「OECD 8原則」が規定されている。すなわち、  
 収集制限の原則（適法かつ公正な手段によって本人への通知又は同意に基づ  
 く収集をおこなうこと）、データ内容の原則（データ内容の正確性、完全性、  
 最新性を確保すること）、目的明確化の原則（利用目的を明確にすること）、  
 利用制限の原則（利用目的以外の目的での利用は行わないこと）、安全保護  
 の原則（個人情報の安全管理をおこなうこと）、公開の原則（パーソナルデー  
 タの収集事実、所在、利用目的や管理者等に関する情報を公開すること）、個  
 人参加の原則（本人が関与できる機会を提供すること）、責任の原則（個人情  
 報の管理にあたっての責任の所在を明確にすること）。また、2013年の改訂時の  
 新たな追加事項<sup>214</sup>は、「プライバシーを保護する法律の制定」「プライバシー執  
 行機関の設置」「表現の自由との関係」「プライバシー・マネジメント・プログ  
 ラム」「セキュリティ侵害通知」「国家的なプライバシー保護方針」「教育・普及  
 啓発、プライバシー保護技術の向上」「国際的な相互運用・評価指標の開発」「保  
 護手段の原則・指針の提示」である。

2015年の欧州司法裁判所によるセーフハーバー協定無効判決、2016年のEU  
 一般データ保護規則の制定を踏まえ、今後OECDにおいては欧州とアメリカの  
 間のパーソナルデータの取扱いが主要な議論の1つとなりえる<sup>215</sup>。

なお、OECDにおける1980年から2013年までのプライバシーをめぐる議論  
 の経緯は以下のとおりである。

（参考）1980年から2013年までの議論の発展経緯

1978	OECD 科学技術政策委員会において検討開始
1980	OECD プライバシーガイドライン採択
1998	グローバルネットワークにおけるプライバシー保護に関する閣僚宣言
2003	プライバシー・オンライン：政策及び実際のガイダンス
2007	プライバシーを保護する法の執行における越境協力に関する理事会勧告 <sup>216</sup>
2011	情報セキュリティ・プライバシー作業部会(WRISP)改正の検討開始
2013	OECD プライバシーガイドライン改正の採択

（3）OECDにおける関連委員会活動等の概要

OECDの約30の委員会のうち、経済的価値のあるデータに関連する活動をお  
 こなう委員会として、デジタル経済政策委員会、競争委員会、科学技術政策委  
 員会、消費者委員会等があげられる。これらの委員会の構造は以下のとおりで  
 ある。

<sup>214</sup> 内閣官房「パーソナルデータに関する検討会」（第3回）（2013年）新保委員提出資料  
 p.9 <http://www.kantei.go.jp/jp/singi/it2/pd/dai3/siryoku1.pdf>

<sup>215</sup> 現地調査（有識者インタビュー）より。

<sup>216</sup> 個人情報保護委員会「諸外国等における個人情報保護制度の実態調査に関する報告書」  
 （2008年）P.223  
[https://www.ppc.go.jp/files/pdf/personal\\_report\\_2003caa\\_5.pdf](https://www.ppc.go.jp/files/pdf/personal_report_2003caa_5.pdf)

デジタル経済政策委員会（Committee on Digital Economy Policy：CDEP）<sup>217</sup>

ICTの発展のため、またICTの発展により生じた課題に対して必要な政策及び規制環境の促進について議論をおこなう目的で1982年に設立された。プライバシーガイドラインの改正(2013年)(後述)は本委員会による活動である。CDEPの下部には、通信インフラ・サービス政策作業部会（Working Party on Communication Infrastructures and Services Policy：WPCISP）、デジタル経済セキュリティ・プライバシー作業部会（Working Party for Security, Privacy for Digital Economy：WPSPDE）、デジタル経済計測分析作業部会（Working Party on Measurement and Analysis of the Digital Economy：WPMAD）がある。

競争委員会（Competition Committee）<sup>218</sup>

加盟国における競争法及び競争政策の進展について検討し、またその整備及び施行に関する加盟国の協力を促進するため、1961年に設置されている。下部組織として第二作業部会（競争と規制）、第三作業部会（執行と協力）がある。

2016年11月のOECD競争委員会本会合においては「ビッグデータに関するヒアリング」<sup>219</sup>が行われた。デジタルエコノミーの発展に伴うビッグデータの重要性を鑑み、「競争法はビッグデータの利用によって生じる問題に対応するための有効な手段を有しているか」「競争法の執行において、ビッグデータはどのように評価すべきか」といった点について取上げ、ビッグデータが事業者に競争上の優位性をもたらすことを踏まえ、次のような競争法執行上の問題が生じる可能性があるとして結論された。一定の取引分野の画定、企業結合規制（事前届出基準）、市場支配力の測定（市場支配的地位の認定）、市場支配的地位の濫用規制、カルテル規制及び競争法の執行におけるプライバシーの考慮。

科学技術政策委員会(Committee for Scientific and Technological Policy：CSTP)

<sup>220</sup>

科学技術に関する議論、科学技術・イノベーションが経済成長に果たす役割、研究体制の整備強化や政府と民間の役割、国際的な研究開発協力の在り方等について検討をおこなうことを目的として1963年に設置されている。下部組織には、科学技術指標専門家作業部会(Working Party of National Experts on Science and Technology Indicators：NESTI)、イノベーション技術政策作業部会(Working Group on Innovation and Technology Policy：TIP)、グローバル・サイエンス・フォーラム(Global Science Forum：GSF)、バイオ・ナノ・コンバージングテクノロジー作業部会(Working Party on Biotechnology, Nanotechnology and Converging

<sup>217</sup> OECD 日本政府代表部（OECD の概要）

<http://www.oecd.emb-japan.go.jp/about/6-2.html>

<sup>218</sup> OECD 日本政府代表部（OECD の概要）

<http://www.oecd.emb-japan.go.jp/about/4-7.html>

<sup>219</sup> OECD Big data: Bringing competition policy to the digital era

<http://www.oecd.org/competition/big-data-bringing-competition-policy-to-the-digital-era.htm>

<sup>220</sup> OECD 日本政府代表部（OECD の概要）

<http://www.oecd.emb-japan.go.jp/about/6-1.html>

Technologies : BNCT ) がある。1980 年プライバシーガイドラインに関する検討をおこなった。

消費者政策委員会 ( Committee on Consumer Policy : CCP ) <sup>221</sup>

消費者政策分野における加盟国の協力の推進・強化に貢献することを目的として 1969 年に設置されている。近年では特にデジタル経済化に伴う消費者問題や製品安全分野に重点的に取り組む。

同委員会においては「電子商取引に関する消費者保護ガイドライン」が 1999 年に策定され、2016 年に改訂されている。これは、インターネットの普及に伴う電子商取引の発展を背景に、これに対応した適切な消費者保護政策を構築することの必要性が高まったことから、貿易障壁とならない、電子商取引をおこなう消費者の保護制度の構築を目指すものである。同ガイドラインの中で、プライバシー及びセキュリティに関しては以下のとおり規定されている<sup>222</sup>。

「電子商取引に関する消費者保護ガイドライン」のプライバシー及びセキュリティに係る規定

- ・ 事業者は、消費者データの収集と利用に関連した行為が、合法、透明、公平であり、消費者の参加及び選択を可能にし、合理的なセキュリティ保護措置を提供することを確保することにより、消費者のプライバシーを保護すべきである ( 48 条 )。
- ・ 事業者は、消費者が電子商取引に参加する際の悪影響を減少させ、又は緩和するために、デジタルセキュリティリスクを管理し、セキュリティ対策を実施すべきである ( 49 条 )。

( 4 ) 科学・技術・革新総局 ( Directorate for Science, Technology and Innovation : DSTI ) の取組み

上記 ( 3 ) 科学技術政策委員会の運営を担当する科学・技術・革新総局では、2015 年 10 月に報告書「成長と福祉のためのデータ主導型イノベーション：ガバナンスとビジネスへの示唆は何か？」<sup>223</sup>をとりまとめて公表した。同報告書では、データ及びデータ分析はもっとも重要なイノベーション促進材料となっており、政府はブロードバンドネットワークのみならず、データそれ自体を含む 21 世紀型のインフラを再定義する必要があることを述べている。データ主導型イノベーションからの利益を拡大するために、政府には、データに対する

<sup>221</sup> OECD 日本政府代表部 ( OECD の概要 )

<http://www.oecd.emb-japan.go.jp/about/4-9.html>

<sup>222</sup> 消費者庁「電子商取引における消費者保護 OECD 勧告」( 2016 年 )

[http://www.caa.go.jp/adjustments/pdf/160617adjustments\\_1.pdf](http://www.caa.go.jp/adjustments/pdf/160617adjustments_1.pdf)

<sup>223</sup> OECD, Directorate for Science, Technology and Innovation, Data-driven Innovation for Growth and Well-being; What implications for Government and Business? October 2015.

現地調査への協力を得た OECD 職員によれば、同報告書が本調査の対象である「経済的価値を持つデータ」というテーマにもっとも近い取組み成果である。

投資や、データ共有・再利用を促進するとともに、グローバルバリューチェーンを阻害するような、国境を越えたデータの移送に対する障壁の低減を図ることが求められる。さらに政府は、データ主導型イノベーションから中小企業が恩恵を受けることに注力すべきであるとしている。

#### ( 5 ) 医療ガバナンスに関する理事会勧告<sup>224</sup>

2017年1月、OECD理事会は医療データガバナンスに関する理事会勧告を採択した。同勧告は、特定されている、或いは特定可能な個人の健康に関する情報を指し、その他の関連するパーソナルデータを含む「個人医療データ」を対象とするものである。各国の医療データガバナンスのフレームワークの構築と、各国間のフレームワークの調和を目的としており、勧告内容には、「個人医療データの利用の承認」「効果的な同意と選択メカニズム」「プライバシーとセキュリティに関するトレーニングと能力開発」等が含まれている。

---

<sup>224</sup> OECD, OECD Recommendation on Health Data Governance  
<http://www.oecd.org/els/health-systems/health-data-governance.htm>

和訳(厚生労働省ウェブサイト):

<http://www.mhlw.go.jp/file/06-Seisakujouhou-10500000-Daijinkanboukokuusaika/0000150343.pdf>

(参考) 各国・国際機関比較表

データ保護については、アメリカ・欧州委員会・ドイツ・フランス・イギリス・中国でおおよそ営業秘密及び契約による保護という考えは共通。(ただし営業秘密に関する法体系は各国で異なる)

		データ保護に関する考え	データ保護に係わる制度(概要)
各国各機関概要	アメリカ	<ul style="list-style-type: none"> <li>価値あるデータは、営業秘密に該当する場合には営業秘密による保護が基本であり、連邦法によりサポートされる考え。</li> <li>アメリカの現行法において各法令がパッチワークのような状態であり、今後日本で検討している行為規制のアプローチがベストプラクティスとなり、各国に普及させていくことを期待している。</li> </ul>	<ul style="list-style-type: none"> <li>営業秘密: 民事的救済について州法(UTSA)、連邦法(DTSA)</li> <li>不正アクセス: 刑法第1030条(コンピュータ犯罪取締法)</li> <li>権利付与: 連邦著作権法</li> </ul>
	欧州委員会	<ul style="list-style-type: none"> <li>価値あるデータは、契約による保護を基本としている。契約外の第三者による不正取得に対しては、営業秘密、競争法、サイバーセキュリティ法、内部告発者保護法等の各国現行法の範囲内で保護されるものがあるという考え。</li> </ul>	<ul style="list-style-type: none"> <li>データベース保護: データベース保護指令(著作権、sui generisによる保護)</li> <li>営業秘密: 営業秘密保護指令(欧州域内での営業秘密の定義、規制行為、救済措置の統一を図る)</li> <li>単一デジタル市場戦略: 2015年「A Digital Single Market Strategy for Europe」、2017年「欧州データ経済の構築」(コンサルテーションペーパー)</li> </ul>
	ドイツ	<ul style="list-style-type: none"> <li>価値あるデータは、契約による保護を基本としており、第三者による不正取得は営業秘密に該当する場合には営業秘密として保護する考え。</li> <li>また、自動車業界による自主的ガイドラインを策定する動きがあり、産業界から注目されている。</li> </ul>	<ul style="list-style-type: none"> <li>営業秘密: 不正競争防止法(UWG)17条による刑事罰と、刑事的に違法とされる行為についての不法行為に基づく民事救済</li> <li>不正アクセス: 刑法典202a,b条</li> <li>権利付与: 欧州データベース保護指令に基づく国内法</li> </ul>
	フランス	<ul style="list-style-type: none"> <li>価値あるデータは、契約及び営業秘密で対応可能なものについてはそれぞれ保護されるとの考え。フランス国内法において営業秘密は製造秘密としての刑事的保護と民法による一般不法行為の規制により保護される。</li> </ul>	<ul style="list-style-type: none"> <li>営業秘密: 民法1382条及び1383条、知的財産法典621-1条、労働法典1227-1条(「製造秘密」及び「営業秘密」の規定)、労働法152-7条(「製造秘密」及び「営業秘密」に係わる刑事罰を規定)、刑法311-2条(窃盗)、313-1条(詐欺)</li> <li>データベース保護: 知的財産法典341-1条~343-7条</li> <li>不正アクセス: 刑法323-1条(不正アクセス)、323-3条(不法なデータ入力・消去・改変)</li> </ul>
	イギリス	<ul style="list-style-type: none"> <li>価値あるデータは、営業秘密(機密情報の保持)、競争法、コンピュータ不正使用法で対応可能な範囲内で保護されるという考え。</li> </ul>	<ul style="list-style-type: none"> <li>営業秘密: コモン・ローに基づく差止、損害賠償</li> <li>競争法: 競争法第1章(イギリス国内における取引に影響を与える反競争的協定)及び、第2章(支配的地位の濫用)</li> <li>コンピュータ不正使用法: 第1条(不正アクセス)、第2条(意図的な違反行為)</li> </ul>
	中国	<ul style="list-style-type: none"> <li>価値あるデータは、営業秘密に該当する場合には営業秘密で保護するという考え。</li> </ul>	<ul style="list-style-type: none"> <li>営業秘密: 反不正当竞争法(規制行為、対象)、民法通則第118条(差止、損害賠償に基づく民事救済)、刑法219条(懲役、罰金)</li> <li>サービス業革新発展大綱が2017年7月に公表され、知的財産権保護制度の整備が記載されているも、本報告書作成時点では具体的な法制度の検討・立案は確認されていない。</li> </ul>

## アメリカ

価値あるデータについては、営業秘密に該当する場合には、営業秘密によって保護することが基本であり、連邦法によりサポートされるという意見。アメリカの現行法において各法令がパッチワークのような状態であり、重複性もあるが、ロバスト性の高い保護を実現している。一方で、営業秘密に該当しないデータについて、契約関係のない第三者による不正取得に対する保護に対し懸念もあり、今般日本で検討している行為規制のアプローチがベストプラクティスとなり、各国に普及させていくことを期待している。なお、権利付与型の保護はデータの流通を阻害するため、適していないとの意見。

データ保護に関する認識	データ保護に関する法制度	制度運用・評価
<ul style="list-style-type: none"> <li>データは「21世紀の石油」であり、保護対象となりえるものと認識している。</li> <li>データ保護は営業秘密が基本であり、営業秘密として保護の可能性が低い場合は契約による保護、第三者からの不正取得に対しては不正アクセスの規制に対する規制で保護する考え。</li> <li>現行法による保護は、各法令（著作権、営業秘密、不正アクセス、FTCによる取締り、民法、刑法等）による保護範囲（対象や禁止行為）がパッチワークのように構成されている。重複する部分もあるが、堅牢性の高い保護を実現している。</li> <li>一方で、営業秘密に該当しないデータにつき、契約関係のない第三者による不正取得に対する保護は十分でないとの指摘もある。</li> <li>今般日本で検討している行為規制のアプローチがベストプラクティスとなり、各国に普及させていくことを期待している。</li> </ul>	<p style="text-align: center;"><b>営業秘密</b></p>	<ul style="list-style-type: none"> <li>UTSAは今なお州内での営業秘密保護において機能している。</li> <li>DTSAは制定後間もないが、差止を請求する判例が複数あり、今後の判例蓄積により運用が明確化する見込み。</li> <li>営業秘密は、原則となる要件が明確であり、第三者による不正取得にも対応できるため、価値あるデータ保護の手段として適していると、行政、法律専門家、産業界は認識。</li> </ul>
	<p style="text-align: center;"><b>契約</b></p>	<ul style="list-style-type: none"> <li>企業間のデータ保護において一般的な手段。</li> <li>ただし、第三者による不正取得に対して保護性が十分ではないと考えられている。</li> </ul>
	<p style="text-align: center;"><b>不正アクセスの規制</b></p>	<ul style="list-style-type: none"> <li>第三者の故意による不正アクセス、不正取得、損害を与える行為を規制しており、コンピュータ・ネットワークにおける不法行為の規制として一般的。</li> <li>ただし、第三者が不正に取得したデータをさらに流通した場合における差止を規定してなく、民事的救済は不可。</li> </ul>
	<p style="text-align: center;"><b>権利付与（著作権）</b></p>	<ul style="list-style-type: none"> <li>主たる保護対象がインターネット上でのコンテンツ、データベースであり、データそのものは保護対象としていない。</li> <li>また著作権では、権利保護が強すぎるため、データ流通に適しておらず、産業界への寄与も小さいと認識されている。</li> </ul>
<ul style="list-style-type: none"> <li>プライバシーデータについては、連邦取引委員会（FTC）が厳格に取締り、産業界は負担（ガイダンスの数が膨大）を感じながらも遵守せざるを得ない状態。国際ハーモナイゼーションについては、欧州一般データ規則（GDPR）で定める細かなデータ取扱いルールの全てに対応することは困難と認識している。</li> </ul>		



## 欧州委員会

価値あるデータは、契約による保護を基本としている。契約外の第三者による不正取得に対しては、営業秘密、競争法、サイバーセキュリティ法、内部告発者保護法等の各国現行法の範囲内で保護されるものがあると認識されている。

データ保護に関する認識	データ保護に関する法制度	制度運用・評価	
<ul style="list-style-type: none"> <li>欧州・各国のそれぞれのレベルにおいて、固有の権利を付与するようなデータ流通を規制する制度導入に対しては否定的な意見が多い。</li> <li>➢ データ所有権については否定的で、データアクセス権を保護する志向。</li> <li>契約を基本とし、契約外の第三者による不正取得に対しては、営業秘密、競争法、サイバーセキュリティ法、内部告発者保護法等の各国現行法の範囲内で保護されるものがあると認識されている。</li> </ul>	<p>データベース保護</p>	<ul style="list-style-type: none"> <li>データベース保護指令で、著作権、sui generisによる保護を制定。</li> <li>保護対象は、コンテンツの選択又は配列によって知的創作物を構成するデータベース、及び「相当の投資」がなされているデータベース。(ただし、無造作に素材を集めただけのものはデータベースに該当しないと指摘されている)</li> </ul>	<ul style="list-style-type: none"> <li>特にsui generisによる保護については早い時期から批判も多く、判例でも多くのデータベースがsui generisによって保護されないことが示される。</li> <li>同指令について当初から産業界は好意的ではなく、10年ほど前に見直しの機運が高まった際にも評価はネガティブであったとの指摘があった。</li> </ul>
	<p>営業秘密保護指令</p>	<ul style="list-style-type: none"> <li>2016年に採択された営業秘密保護指令で、欧州域内での営業秘密の定義、規制行為、救済措置の統一を図る。</li> <li>保護対象は、営業秘密がノウハウ、営業情報、技術情報を含む概念とし、非公知性・有益性・秘密管理性を保護要件とする。</li> <li>規制行為は、不正取得、同意を得ない開示又は使用等。</li> <li>救済措置として民事による差止請求、損害賠償請求を提示。</li> </ul>	<ul style="list-style-type: none"> <li>指令策定のプロセスが長引き過ぎ、妥協の産物となっているとの指摘あり。</li> <li>必ずしもデータ保護を意図して策定されていないが、ドイツからはインターネット上での市場のつながりが発展する中、欧州域内での制度協調が図られる点において好意的な評価を受けている。</li> </ul>
	<p>単一デジタル市場戦略</p>	<ul style="list-style-type: none"> <li>2015年に欧州委員会が文書として「A Digital Single Market Strategy for Europe」を公表し、その後2017年1月に「欧州データ経済の構築」としてコンサルテーションペーパーを公表。</li> <li>自動集積されるローデータの保護について当該データへの匿名アクセスの促進、共有促進、投資や資産の保護、秘密情報の開示の回避、データのロックイン効果の最小化について、ガイドンス、契約ルール等の詳細な議論の必要性を指摘。</li> </ul>	<ul style="list-style-type: none"> <li>コンサルテーションペーパーへの関心は高い。</li> <li>2017年6月時点で同コンサルテーションを所管する担当の欧州委員が空席であり、新たなペーパーによる方向性提示までには数か月～1年程度は要する可能性があるとの見解があったが欧州委員不在状況は解消。現在、欧州委員会のウェブサイトには、「2017年秋にデータ・フリーフローの協力枠組みに関する提案を準備」等との情報が公表されている。</li> </ul>
	<p>契約</p>	<ul style="list-style-type: none"> <li>欧州委員会DG JUSTICEによりデータに関するモデル契約開発中。</li> </ul>	<ul style="list-style-type: none"> <li>価値あるデータ保護については企業間の契約を基本とするという意見。</li> <li>DG JUSTICEによるデータに関するモデル契約については、一定程度有用であろうが、どの程度活用が広がるかは不明という見解。</li> </ul>

• プライバシーデータは、GDPRによって保護・規制される。国際ハーモナイゼーションについては、GDPRの詳細さ、厳格さの観点からEU域外とのハーモナイゼーションは不可能と認識されている

## ドイツ

価値あるデータは、契約による保護を基本としており、第三者による不正取得は当該データが営業秘密に該当する場合には営業秘密で規制するという考え。また、自動車業界による自主的ガイドラインを策定する動きがあり、産業界から注目されている。

データ保護に関する認識	データ保護に関する法制度	制度運用・評価
<ul style="list-style-type: none"> <li>データは「21世紀の石油」と認識されており、その最大限の活用が志向されている。</li> <li>個人データ活用によるビジネスではアメリカ系企業に水をあけられたため、Industrie4.0にも見られるIoTや強みがある自動車産業等における「価値あるデータ」を活用したビジネスにおける巻き返しのためにもデータの利活用の重要性が強く認識されている。</li> <li>基本的には契約による保護とし、第三者による不正取得はそのデータが営業秘密に該当する場合には営業秘密で規制するという考えである。（ただし、契約と営業秘密のみで必ずしも十分ではないと認識）</li> <li>データ所有権については否定的で、データアクセス権を保護する志向。</li> <li>特に産業界は現状では契約とセキュリティによって保護されており、データ所有権を設定するような制度のようにデータの利活用を阻害しうような新たな法律は現時点で不要という認識。</li> </ul>	<p><b>営業秘密</b></p> <ul style="list-style-type: none"> <li>2004年施行の不正競争防止法(UWG)17条が営業秘密漏えいについて刑事罰を設けている。また、民法においてUWG17条に該当する行為に対する損害賠償請求と差止請求を定めている。</li> <li>「営業秘密」の定義規定はなく、判例に依る。</li> <li>欧州指令を受けて本年10-11月の本案提出に向けて営業秘密法案の準備が進められている(2017年6月時点)。</li> </ul>	<ul style="list-style-type: none"> <li>UWG全体の保護対象のあいまいさや、営業秘密の提示が限定的に判示されてきたことから活発な運用はなされていない。</li> <li>UWG17条は新法に移管され欧州指令と整合化されるが、新法成立後も運用に委ねられる余地が大きいと見られる。</li> </ul>
	<p><b>契約</b></p> <ul style="list-style-type: none"> <li>B to Bの価値あるデータの保護や取扱いについては企業間契約に依るべきとの意見が太宗である。</li> <li>自動車産業団体は基本的に契約に委ねるべきとの立場で、これを補完するデータの分類と取扱いに関するガイドラインの整備に取組んでいる。</li> </ul>	<ul style="list-style-type: none"> <li>データの取扱いを定めたB to Bの契約に係る大きな紛争は取り沙汰されていない。</li> <li>データの取扱いが分野毎に展開することに対する期待は大きい。</li> </ul>
	<p><b>不正アクセスの規制</b></p> <ul style="list-style-type: none"> <li>刑法典202a,b条が秘密に管理されているデータに対する権限のないアクセスと取得を禁止、同203条が他者から開示を受けた者の第三者開示を禁止、同204条が他者から当該秘密の開示を受けた者の利用禁止を規定。</li> <li>内部からの牽制の有用性が認識され、内部告発者保護の制度の整備が進んでいる。</li> </ul>	<ul style="list-style-type: none"> <li>1986年に当時の東側諸国の産業スパイを念頭に導入。今日的なデータ保護は必ずしも射程にない。</li> <li>内部告発者の保護に関する制度はドイツは進んでいなかったため、欧州レベルでの対応の進捗を受け、国内で注力されている。</li> </ul>
	<p><b>権利付与</b></p> <ul style="list-style-type: none"> <li>欧州データベース保護指令に基づき1998年までに国内法を整備。</li> <li>同指令に対して欧州委員会はコンサルテーションを実施中。</li> </ul>	<ul style="list-style-type: none"> <li>データベース保護法は活用されなかった。</li> <li>コンサルテーションに対しても、同指令の延長では今日的なデータをカバーし得ないとの見解が太宗。</li> </ul>
<ul style="list-style-type: none"> <li>プライバシーデータについては、ドイツは欧州他国より厳格に保護していた伝統があると認識されている。GDPRについて、EU域内のハーモナイゼーションに寄与するという点で肯定的である</li> </ul>		

## フランス

価値あるデータは、契約及び営業秘密で対応可能なものについてはそれぞれに基づいて保護するという考え。フランス国内法において営業秘密は製造秘密としての刑事的保護と民法による一般不法行為の規制により保護される。

データ保護に関する認識	データ保護に関する法制度	制度運用・評価
<ul style="list-style-type: none"> <li>価値あるデータについては、基本的には契約及び営業秘密で対応可能なものについてはそれぞれに基づいて保護するという考えである。               <ul style="list-style-type: none"> <li>フランスにおいて価値あるデータの保護を明示的に対象とする法制度は存在しない。</li> <li>営業秘密については、製造秘密としての刑事的保護と民法による一般不法行為の規制により保護されている。</li> </ul> </li> </ul>	<p><b>営業秘密</b></p> <ul style="list-style-type: none"> <li>営業秘密に係る事項は、一般法である民法典1382条及び1383条に定める民事上の責任の原則及び不法行為の適用に準拠。ただし、運用事例はほとんどない。</li> <li>また、営業秘密侵害に相当する行為は、刑法典311 2条(窃盗)・刑法典313 1条(詐欺)で定める刑事罰の対象となる可能性がある。</li> <li>特定の場合には労働法における「製造上の秘密の開示」として刑事罰の対象。</li> <li>全体としては不法行為又は契約に基づいた合意に係る判例法に準拠(成文法の定義規定はない)。</li> <li>「製造秘密」及び「営業秘密」は知的財産法典621-1条に規定され、これが労働法典1227-1条にも規定され、労働法典152-7条が定める刑事罰の対象となっている。</li> </ul>	<ul style="list-style-type: none"> <li>営業秘密侵害に際する差止請求に関する判例は、10年以上に渡り低調。</li> <li>2014年と2015年に2度に渡り営業秘密に特化した法案が提出されたが成立せず。</li> <li>データに関連する法令については、新政権下で現状よりも正確になることが期待される。複数のEU指令を受けた法改正を含め、今後5年間は動向が注目される。</li> </ul>
	<p><b>データベース保護</b></p> <ul style="list-style-type: none"> <li>データベース保護に係る事項は、知的財産法典341-1条により規定。</li> <li>保護を受けるには、データの内容の構成、検証又は呈示が実質的な財政的、物的又は人的投資の証明が必要。</li> </ul>	<ul style="list-style-type: none"> <li>判例において、データベースが保護対象となるかはケース・バイ・ケース。</li> </ul>
	<p><b>不正アクセスの規制</b></p> <ul style="list-style-type: none"> <li>刑法典323 1条は、コンピュータへの不正アクセスを禁止し、違反行為への懲役又は罰金を規定する。</li> <li>刑法典323 3条は、不法なコンピュータへのデータ入力、コンピュータ内のデータの消去・改変を禁止し、違反行為への懲役又は罰金を規定する。</li> </ul>	<ul style="list-style-type: none"> <li>第三者の故意による不正アクセス、損害を与える行為を規制している。</li> <li>ただし、コンピュータへの第三者が不正に取得したデータをさらに流通した場合における差止を規定してなく、民事的救済は不可。</li> </ul>
	<p><b>契約</b></p> <ul style="list-style-type: none"> <li>価値あるデータの企業間における法的枠組みは契約によるとの認識が一般的。</li> <li>契約は、従業員との間の労働契と、第三者である顧客、サービス提供者等に営業秘密等のデータを開示又は移送するにあたっての、非開示合意(NDAs)や移送契約(transfer agreement)等。</li> </ul>	<ul style="list-style-type: none"> <li>営業秘密に関する法制度が存在しないことから、営業秘密や製造秘密は、知的財産法典の判例によって進展してきたことと並行して、営業秘密を阻害する契約又は不正競争に関わる申し立てによっても進展。</li> </ul>

• プライバシーデータについては、フランスデータ保護法及びCNILにより保護・規制されている。GDPR発効を含むEU域内での動きに先駆けて自国の法改正をしている。

## イギリス

価値あるデータは、営業秘密（機密情報の保持）、競争法、コンピュータ不正使用法で対応可能な範囲内で保護されるという考え。営業秘密はコモン・ローに基づいている。

データ保護に関する認識	データ保護に関する法制度		制度運用・評価
<ul style="list-style-type: none"> <li>価値あるデータについては、コモン・ローによる営業秘密保護（機密情報の保護）、競争法による「商業的にセンシティブな情報の保護、コンピュータ不正使用法による不正アクセスの規制によって対応可能な範囲内で保護されるという考えである。               <ul style="list-style-type: none"> <li>機密情報の保護は、差止、損害賠償が認められる。</li> <li>競争法による保護では、制裁金の支払、及び刑事措置を規定。</li> <li>コンピュータ不正使用法では刑事措置を規定。</li> <li>EU営業秘密保護指令については、イギリスがEU離脱に先立ち本指令にもとづく新たな制度を導入する可能性は低いとみられている。</li> </ul> </li> </ul>	営業秘密	<ul style="list-style-type: none"> <li>営業秘密を含む技術的、商業的、その他の情報はコモン・ロー上の信頼関係の法理 (the law of confidence) の下で保護される。</li> <li>営業秘密の対象として、化学式のような技術に関する秘密、工業プロセスのような機械に関する秘密、製品やプロセスの改善、財務・統計情報、見積額、仕入れ値、事業戦略等の商業的情報、顧客や供給元の商業的記録、ソフトウェアのソースコード等が判例によって示されている。</li> <li>違反者に対しては、差止、損害賠償による民事措置が認められている。</li> </ul>	<ul style="list-style-type: none"> <li>EU営業秘密保護指令については、イギリスがEU離脱に先立ち本指令にもとづく新たな制度を導入する可能性は低いとみられている。</li> </ul>
	競争法	<ul style="list-style-type: none"> <li>1998年競争法によって、イギリス国内における取引に影響を与える反競争的協定 (第1章) 及び支配的地位の濫用 (第2章) を規定。</li> <li>「商業的にセンシティブな情報」は競争法において定義されていないが、実務においては公的なドメインではない分野における再販売価格や、製造能力又はコスト等の情報が、商業的にセンシティブであり競争法の範疇となる可能性が高いとされている。</li> </ul>	<ul style="list-style-type: none"> <li>法律専門家の見解によれば、本調査の対象である「価値あるデータ」も「商業的にセンシティブな情報」として捉えられる可能性がある。</li> </ul>
	不正アクセスの規制	<ul style="list-style-type: none"> <li>1990年コンピュータ不正使用法により、アクセスを許可されていないプログラムやデータへ不正 (同法第1条) 及びさらなる違反行為を行う意図をもって違反行為を行うこと (同法第2条) を禁止。</li> <li>違反者には、禁固刑又は罰金刑が科される。</li> </ul>	<ul style="list-style-type: none"> <li>第三者の故意による不正アクセス、損害を与える行為を規制している。</li> <li>ただし、コンピュータへの第三者が不正に取得したデータをさらに流通した場合における差止を規定してなく、民事的救済は不可。</li> </ul>
	契約	<ul style="list-style-type: none"> <li>情報を共有する際に機密性を保持するための方法として、イギリス特許庁が秘密保持契約 (non-disclosure agreements) に関するガイダンスを公表。ガイダンスにおいて、秘密保持契約は原則として、記録されておりかつ「機密」であることが記された情報のみを保護し、また会合やプレゼンテーションで共有された情報も保護するとされている。</li> </ul>	<ul style="list-style-type: none"> <li>法律専門家の見解によれば、契約のみで価値あるデータの保護は困難であり、複数の制度の組み合わせによる保護となる旨が指摘され、具体的には、セキュリティにおける保護、データ管理、契約による機密保持等、複数手段によってデータが不正取得・公開されることを防ぐべきという意見が述べられている。</li> </ul>
<ul style="list-style-type: none"> <li>プライバシーデータについては、EUデータ保護指令を受けて設置された1989年データ保護法により保護されている。GDPRに則したパーソナルデータの保護制度の策定に加え、現在新たなパーソナルデータの保護のための新法策定が計画されているが、この新法とGDPRの整合性については明らかではない。</li> </ul>			

中国

価値あるデータは、営業秘密に該当する場合には営業秘密で保護するという考え。サービス業革新発展大綱による知的財産権保護制度の整備については、本報告書作成時点では具体的な法制度の検討・立案は確認されていない。

データ保護に関する認識	データ保護に関する法制度	制度運用・評価
<ul style="list-style-type: none"> <li>価値あるデータについては、反不正競争法に基づき当該データが営業秘密に該当する場合には営業秘密によって保護するという考えである。             <ul style="list-style-type: none"> <li>営業秘密の保護は、反不正競争法で対象を規定、民法通則で差止、損害賠償、刑法で懲役・罰金を規定。</li> <li>サービス業革新発展大綱が2017年7月に公表され、知的財産権保護制度の整備が記載されているも、本報告書作成時点では具体的な法制度の検討・立案は確認されていない。</li> </ul> </li> </ul>	<p><b>営業秘密</b></p> <ul style="list-style-type: none"> <li>営業秘密の対象として、反不正競争法で非公知性・有益性・秘密管理性を満たす技術情報及び経営情報を規定。</li> <li>規制される行為については、反不正競争法で、不正取得、不正使用、約定・秘密保持契約に反する公開・使用・他者への使用許諾、違反行為を明らかに知った又は知りうる第三者による不正取得、不正使用、暴露について、営業秘密侵害行為として規定。</li> <li>民法通則第118条において、技術情報の侵害への保護として、著作権、特許権、商標権等と併せて、発明又はその他の技術成果の剽窃・改ざん・冒用等の侵害に対する、差止(侵害の停止、影響の除去)、損害賠償を規定。</li> <li>刑法第219条において、営業秘密侵害罪を規定しており、反不正競争法で定める営業秘密に対する、不正取得・不正使用に対して懲役又は罰金を規定。</li> </ul> <p><b>サービス業革新発展大綱</b></p> <ul style="list-style-type: none"> <li>2017年7月21日に国家発展改革委員会が「サービス業革新発展大綱(2017～2025年)」を発表。</li> <li>知的財産権保護制度について、専利権、商標権、著作権、営業秘密保護等の法律・法規の整備、ビジネス・モデル特許保護制度の研究、知的財産権審査、登録手続の改善、簡素化、知的財産権の情報資源の共有推進、知的財産権侵害に関する懲罰的賠償制度の整備、企業の海外における権利保護支援メカニズムの整備について言及されている他、インターネット、ビッグデータ、電子商取引等の分野の知的財産権保護規定の整備が示されている。</li> </ul>	<ul style="list-style-type: none"> <li>データの不正取得・不正使用に関する判例としては、インターネットを通じて競合他社のデータを不正取得し、事業において利用することで、反不正競争法に抵触したものが存在している。</li> <li>法律専門家の見解として、保護対象の広さ、国際ハーモナイゼーションの観点で、他の制度と比較し、「価値あるデータ」は営業秘密による保護が適しているという意見が聞かれた。</li> </ul> <p>左記で示されている規定整備について本調査報告書作成時点では方針にとどまっており、本報告書作成時点では具体的な法制度の検討・立案は確認されていない。</p> <p>ただし、中国では過去にも全国人民代表大会(National People Congress)において、電子商取引に関する規制が検討されたが、2017年9月末時点において未だ2013年に提出した法案が通過していないことも踏まえると、サービス業核心発展大綱はスローガンを示しているものの、具体化には時間を要するという指摘もある。</p>
<ul style="list-style-type: none"> <li>プライバシーデータについては、サイバーセキュリティ関連法において保護する方針。</li> </ul>		