第 8 章　自由な越境データ流通と多様な公共政策目的の調整

城山　英明

1. 基本的課題

デジタル経済化の下では、モノやサービスの提供にはしばしば国境を越えた様々な主体のネットワークが関わっており、そのような主体間で情報の流通が不可欠となっている。そのため、自由な越境データ流通を確保することが重要な課題となっている。

しかし、自由な越境データ流通と様々な公共政策目的とのトレードオフが生じうる。例えば、個人情報保護、サイバーセキュリティ、金融規制等の規制の実効的な実施、産業政策、ELSI、安全保障等の観点から、自由な越境データ流通を規制し、データ・ローカライゼーション等を求める動きが出てきている。また、多様な公共政策目的のうち、どの公共政策目的を重視するのかは、各国・各地域で異なる。データ流通に関しては、アメリカ、欧州連合（EU）、中国は異なった 3 つの領域を構成しているといわれる [1]。

アメリカは自由なデータ流通への制約を限定しようとしてきた。例えば、2012 年に発効した米韓自由貿易協定においては、電子商取引章に初めて自由な情報流通に関する規定が置かれた [2]。

他方、EU では個人データの保護は基本権であると考えられ、個人データ保護を目的とする制度枠組みが構築されてきた。1995 年 10 月には「個人データ処理に係る個人の保護および当該データの自由な移動に関する指令」（データ保護指令）が採択され、同指令第 25 条において、個人データの第三国への移転は、当該第三国が十分なレベルの保護（adequate level of protection）を確保している場合に限って行うことができると規定された。これを引き継ぎ、2016 年 4 月に採択された「個人データの取り扱いに係る自然人の保護と当該データの自由な移動に関する規則」（一般データ保護規則：GDPR）でも、個人データの「十分なレベルの保護」が EU 域外に個人データを移転する条件とされた [3]。

また、中国では安全が重視されてきた。例えば、2017 年に制定されたネットワーク安全法第 37 条では、「重要情報インフラストラクチャーの運営者が中華人民共和国の国内での運営において収集、発生させた個人情報及び重要データは、国内で保存しなければならない。業務の必要性により、国外に対し確かに提供する必要のある場合には、国のネットワーク安全情報化機関が国務院の関係機関と共同して制定する弁法に従い安全評価を行わなければならない。法律及び行政法規に別段の定めのある場合には、当該定めに基づいて行う」と規定されている [4]。「個人情報」、「重要データ」という鍵となる概念がネットワーク安全法に規定されてる点、また、データの国内保存が求められている点に特色がある。

このような状況の中で、自由な越境データ流通と様々な公共政策目的を具体的にどのように調整するのかが課題となる。本稿では、まず 2. において、このような調整を二国間あるいは地域レベルでの自由貿易協定（FTA）あるいは経済連携協定（EPA）がどのように試みているのかを確認する。具体的には、自由な越境データ流通、コンピュータ関連施設の設置、ソース・コードの開示についてどのような規定を置いているのかに焦点を当てる。その上で、3. では、FTA/EPA において、個人情報保護、サイバーセキュリティ、あるいは ELSI の確保といった課題に関して、どのような規定を置いているのかを検討する。

自由な越境データ流通と公共政策目的の調整を図るためには、各公共政策目的に即した国際的調和化の契機が重要だと思われる。その上で、4. において、世界貿易機関（WTO）といったグローバルレベルでの対応の現状について確認する。

2. FTA/EPA におけるデータ流通関連規定のあり方－共通性と差異

ここでは、環太平洋パートナーシップに関する包括的及び先進的な協定（CPTPP）、米国・メキシコ・カナダ協定（USMCA）、日米デジタル貿易協定、日 EU 経済連携協定、地域的な包括的経済連携（RCEP）協定、シンガポール、チリ、ニュージーランドによるデジタル経済連携協定（DEPA：Digital Economy Partnership Agreement）、オーストラリア・シンガポール・デジタル経済連携協定（DEA：Digital Economy Agreement）におけるデータ流通関連規定を検討する。

（1）CPTTP

CPTPP は、オーストラリア、ブルネイ、カナダ、チリ、日本、マレーシア、メキシコ、ニュージーランド、ペルー、シンガポール、ベトナムの 11 カ国により 2018 年 3 月に署名された。まず、越境データ流通に関する規定[5]としては、第 14・11 条（情報の電子的手段による国境を越える移転）、第 14・13 条（コンピュータ関連設備の設置）、第 14・17 条（ソース・コード）がある。第 14・11 条 1 では、各締約国が情報の電子的手段による移転に関する自国の規制上の要件を課することができることを認めるとしつつ、第 14・11 条 2 では、原則的に各締約国は、対象者の事業の実施のために行われる場合には、情報の電子的手段による国境を越える移転を許可するとする。また、第 14・13 条 1 では、各締約国がコンピュータ関連設備の利用に関する自国の法令上の要件を課することができることを認めるとしつつ、第 14・11 条 2 では、いずれの締約国も、自国の領域において事業を遂行するための条件として、対象者に対し、当該領域においてコンピュータ関連設備を利用し、又は設置することを要求してはならないとする。また、第 14・17 条 1 でも、いずれの締約国も、他の締約国の者が所有するソフトウェア又は当該ソフトウェアを含む製品の自国の領域における輸入、頒布、販売又は利用の条件として、当該ソフトウェアのソース・コードの移転又は当該ソース・コードへのアクセスを要求してはならないとする。

このように、データの自由流通が原則ではあるが、公共政策の正当な目的による制限は認めている。第 14・11 条 3 では、この条のいかなる規定も、締約国が公共政策の正当な目的を達成するために第 14・11 条 2 の規定に適合しない措置を採用し、又は維持することを妨げるものではない、ただし、当該措置が、次の要件を満たすことを条件とする、(a) 恣意的若しくは不当な差別の手段となるような態様で又は貿易に対する偽装した制限となるような態様で適用されないこと、(b) 目的の達成のために必要である以上に情報の移転に制限を課するものではないこと、と規定している。第 14・13 条 3 においても、基本的には同様の規定が置かれている。さらに、ソース・コードに関する第 14・17 条 2 では、第 14・17 条 1 の規定の対象となるソフトウェアは、大量販売用ソフトウェア又は当該ソフトウェアを含む製品に限定するものとし、中枢的な基盤（critical infrastructure）のために利用されるソフトウェアを含まないと規定され、対象が限定されている。

（2）USMCA

2018 年 12 月に署名された USMCA では、越境データ流通に関する規定[6]として、第 19・11 条（情報の電子的手段による国境を越える移転）、第 19・12 条（コンピュータ関連設備の設置）、第 19・16 条（ソース・コード）がある。第 19・11 条 1 では、いかなる締約国も、個人情報を含む情報の電子的手段による国境を越えた移転が、その活動が対象者の事業の遂行のためである場合には、これを禁止又は制限してはならないとする。また、第 19・12 条では、いかなる締約国も、対象者が当該締約国の領域において事業を行うための条件として、当該領域においてコンピュータ設備を使用し、又は配置することを要求してはならないとする。また、第 19・16 条 1 でも、いかなる締約国も、自国の領域における当該ソフトウェア又は当該ソフトウェアを含む製品の輸入、流通、販売又は使用の条件として、他の締約国の者が所有するソフトウェアのソース・コード又は当該ソース・コードに表されたアルゴリズムの譲渡若しくは入手を要求してはならないとする。USMCA では、CPTPP より幅広く、アルゴリズムの要求も禁止されている。

USMCA においても公共政策の正当な目的による制限は認めている。第 19・11 条 2 では、締約国が、正当な公共政策の目的を達成するために必要な、第 19・11 条 1 と適合しない措置を採択し又は維持することを妨げるものではない、ただし、当該措置は、(a) 恣意的若しくは不当な差別の手段となるような態様で又は貿易に対する偽装された制限となるような態様で適用されるものでないこと、(b) 目的の達成のために必要である以上に情報の移転に制限を課するものではないこと、と規定している。また、ソース・コードに関する第 19・16 条 2 では、締約国の規制機関または司法当局が、不正な開示に対する保護措置を条件として、他の締約国の者に対し、特定の調査、検査、審査、執行措置または司法手続のためにソフトウェアのソース・コードまたはそのソース・コードに表されたアルゴリズムを保存し、利用可能にするよう求めることを排除するものではないと規定している。ただし、コンピュータ設備設置については、公共政策目的による介入を認めていない。

（3）日米デジタル貿易協定

2019 年 10 月に署名された日米デジタル貿易協定における越境データ流通に関連する規定[7]としては、第 11 条（情報の電子的手段による国境を越える移転）、第 12 条（コンピュータ関連設備の設置）、第 13 条（対象金融サービス提供者のための金融サービスのコンピュータ関連設備の設置）、第 17 条（ソース・コード）がある。第 11 条 1 では、いずれの締約国も、情報（個人情報を含む）の電子的手段による国境を越える移転が対象者の事業の実施のために行われる場合には、当該移転を禁止し、又は制限してはならないと規定している。また、第 12 条 1 では、いずれの締約国も、自国の領域において事業を実施するための条件として、対象者に対し、当該領域においてコンピュータ関連設備を利用し、又は設置することを要求してはならないと規定している。また、第 17 条 1 でも、いずれの一方の締約国も、他方の締約国の者が所有するソフトウェア又は当該ソフトウェアを含む製品の一方の締約国の領域における輸入、流通、販売又は使用の条件として、当該ソフトウェアのソース・コードの移転若しくは当該ソース・コードへのアクセス又は当該ソース・コードにおいて表されるアルゴリズムの移転若しくは当該アルゴリズムへのアクセスを要求してはならないと規定している。日米デジタル貿易協定でも、USMCA と同様、対象範囲はアルゴリズ

ムに拡大している。

日米デジタル貿易協定においても公共政策の正当な目的による制限は認めている。第 11 条 2 では、この条のいかなる規定も、第 11 条 1 の規定に適合しない措置であって、締約国が公共政策の正当な目的を達成するために必要なものを採用し、又は維持することを妨げるものではない、ただし、当該措置が、次の要件を満たすことを条件とする、(a) 恣意的若しくは不当な差別の手段となるような態様で又は貿易に対する偽装した制限となるような態様で適用されないこと、(b) 目的の達成に必要な範囲を超えて情報の移転に制限を課するものではないこと、と規定している。

また、コンピュータ関連設備の設置に関する第 12 条 2 においては、この条の規定は対象金融サービス提供者については適用せず、次条において取り扱うと規定している。その上で、第 13 条 1 において、両締約国は、対象金融サービス提供者の情報への締約国の金融規制当局による迅速、直接的、完全及び継続的なアクセスが金融に係る規制及び監督のために不可欠であることを認識し、並びに当該アクセスへの潜在的な全ての制限を撤廃することの必要性を認識するとし、規制のためのアクセスの必要性を認める。しかし、このような必要性が、コンピュータ設備の領域内設置要求を常に正当化するわけではなく、第 13 条 2 において、当該締約国の金融規制当局が、規制及び監督を目的として、迅速、直接的、完全及び継続的なアクセスを認められる場合には、対象金融サービス提供者に対し、当該締約国の領域において事業を実施するための条件として、当該領域において金融サービスのコンピュータ関連設備を利用し、又は設置することを要求してはならないと規定する。

ソース・コードに関する第 17 条 2 では、この条の規定は、一方の締約国の規制機関又は司法当局が、他方の締約国の者に、特定の調査、検査、検討、執行活動又は司法手続のため、ソフトウェアのソース・コード又は当該ソース・コードにおいて表現されるアルゴリズムを保存し、又は入手可能なものとすることを要求することを妨げるものではないと規定する。

また、第 4 条において、安全保障に関する一般的な例外規定も置かれている。この協定のいかなる規定も、次のいずれかのことを定めるものと解してはならない、(a) 締約国に対し、その開示が自国の安全保障上の重大な利益に反すると当該締約国が決定する情報の提供又はそのような情報へのアクセスを要求すること、(b) 締約国が国際の平和若しくは安全の維持若しくは回復に関する自国の義務の履行又は自国の安全保障上の重大な利益の保護のために必要であると認める措置を適用することを妨げること、と規定されている。

(4) RCEP

2020 年 11 月に署名された RCEP（地域的な包括的経済連携）協定では、越境データ流通に関する規定[8]として、第 12・15 条（情報の電子的手段による国境を越える移転）、第 12・14 条（コンピュータ関連設備の設置）が規定されている。ソース・コードに関する規定はない。第 12・15 条 1 では、締約国は各締約国が情報の電子的手段による移転に関する自国の規制上の要件を課することができるとしつつも、第 12・15 条 2 では、締約国は、情報の電子的手段による国境を越える移転が対象者の事業の実施のために行われる場合には、当該移転を妨げてはならないとする。また、第 12・14 条 1 でも、締約国は、各締約国がコンピュータ関連設備の利用又は設置に関する自国の措置をとることができることを認

識するとしつつ、第 12・14 条 2 では、いずれの締約国も、自国の領域において事業を実施するための条件として、対象者に対し、当該領域においてコンピュータ関連設備を利用し、又は設置することを要求してはならないとする。

他方、正当な公共政策の扱いについては、TPP 等とは大きく異なる面がある。第 12・15 条 2 では、まず、この条のいかなる規定も、締約国が公共政策の正当な目的を達成するために必要であると認める措置を採用し、又は維持することを妨げるものではない、ただし、当該措置が恣意的若しくは不当な差別の手段となるような態様で又は貿易に対する偽装した制限となるような態様で適用されないことを条件とするとする。ここまでは、TPP 等と基本的には同様である。しかし、注が付記されてる。その内容は、この規定の適用上、締約国は、正当な公共政策の実施の必要性については実施する締約国が決定することを確認するというものである。また、第 12・15 条 2 では、締約国が自国の安全保障上の重大な利益の保護のために必要であると認める措置を採用し、又は維持することを妨げるものではないとされ、他の締約国は当該措置については争わないとされる。そして、第 12・14 条 3 においても、同様の規定が置かれている。

(5) 日 EU 経済連携協定

2018 年 7 月に署名された日 EU 経済連携協定[9]には、現状ではデータの流通に関する実質的規定はない。第 8・81 条（データの自由な流通）においては、両締約国は、この協定の効力発生の日から 3 年以内に、データの自由な流通に関する規定をこの協定に含めることの必要性について再評価するとのみ規定されている。

ただし、越境データ流通に関連する規定として、第 8・73 条（ソース・コード）が置かれており、第 8・73 条 1 には、いずれの一方の締約国も、他方の締約国の者が所有するソフトウェアのソース・コードの移転又は当該ソース・コードへのアクセスを要求することができないと規定している。

なお、第 8・81 条 2 においては、この条のいかなる規定も、次の要求又は権利に影響を及ぼすものではないとされ、(a) 競争法令の違反を是正するための司法裁判所、行政裁判所又は競争当局による要求、(b) 知的財産権の保護及び行使に関する司法裁判所、行政裁判所又は行政当局による要求等が例示されている。この点で、公共政策目的での制約が認められているといえる。

(6) DEPA

2020 年 6 月に署名された DEPA の越境データ流通に関連する規定[10]としては、第 4・3 条（情報の電子的手段による国境を越える移転）、第 4・4 条 コンピュータ関連設備の設置がある。ソース・コードに関する規定はない。第 4・3 条 1 では、締約国は、各締約国が電子的方法による情報の移転に関する自国の規制上の要件を課すことができることを認めるとしつつ、第 4･3 条 2 では、各締約国は、対象者の事業の実施のために行われる場合には、電子的手段による情報（個人情報を含む）の国境を越えた移転を許可すると規定する。また、第 4・4 条 1 では、締約国は、各締約国が、コンピュータ関連設備の使用に関する独自の規制要件を課することができることを認めるとしつつ、第 4･4 条 2 では、いずれの締約国も、自国の領域において事業を遂行するための条件として、対象者に対し、当該領域において

コンピュータ関連設備を利用し、又は設置することを要求してはならないと規定する。

DEPA においても正当な公共政策目的による制限は認めている。第 4・3 条 3 では、締約国が、正当な公共政策の目的を達成するために、第 4・3 条 2 と適合しない措置を採用し又は維持することを妨げるものではない、ただし、(a) 恣意的若しくは不当な差別の手段となるような態様で又は貿易に対する偽装した制限となるような態様で適用されないこと、(b) 目的の達成のために必要である以上に情報の移転に制限を課するものではないこと、と規定している。第 4・4 条 3 においても、同様の規定が存在する。

また、第 15・2 条には、安全保障に関する一般的な例外規定も置かれている。第 15・2 条においては、この協定のいかなる規定も、次のいずれかのことを定めるものと解してはならない、(a) 締約国に対し、その開示が自国の安全保障上の重大な利益に反すると当該締約国が決定する情報の提供又はそのような情報へのアクセスを要求すること、(b) 締約国が国際の平和若しくは安全の維持若しくは回復に関する自国の義務の履行又は自国の安全保障上の重大な利益の保護のために必要であると認める措置を適用することを妨げること、と規定されている。

(7) オーストラリア・シンガポール DEA

2020 年 8 月に署名されたオーストラリア・シンガポール DEA（Digital Economy Agreement）の越境データ流通に関連する規定[11]としては、第 23 条（情報の電子的手段による国境を越える移転）、第 24 条（コンピュータ関連設備の設置）、第 25 条（金融サービスのためのコンピュータ関連設備の設置）、第 28 条（ソース・コード）がある。第 23 条 1 では、締約国は、各締約国が電子的方法による情報の移転に関する自国の規制上の要件を課すことができることを認めるとしつつ、第 23 条 2 では、各締約国は、対象者の事業の実施のために行われる場合には、電子的手段による情報（個人情報を含む）の国境を越えた移転を許可すると規定する。また、第 24 条 1 では、締約国は、各締約国が、コンピュータ関連設備の使用に関する独自の規制要件を課することができることを認めるとしつつ、第 24 条 2 では、いずれの締約国も、自国の領域において事業を遂行するための条件として、対象者に対し、当該領域においてコンピュータ関連設備を利用し、又は設置することを要求してはならないと規定する。また、第 28 条 1 においても、いずれの一方の締約国も、他方の締約国の者が所有するソフトウェア又は当該ソフトウェアを含む製品の一方の締約国の領域における輸入、流通、販売又は使用の条件として、当該ソフトウェアのソース･コードの移転若しくは当該ソース・コードへのアクセスを要求してはならないと規定している。

オーストラリア・シンガポール DEA においても正当な公共政策目的による制限は認めている。第 23 条 3 では、本条は、締約国が、正当な公共政策の目的を達成するために、第 23 条 2 と適合しない措置を採用し又は維持することを妨げるものではない、ただし、(a) 恣意的若しくは不当な差別の手段となるような態様で又は貿易に対する偽装した制限となるような態様で適用されないこと、(b) 目的の達成のために必要である以上に情報の移転に制限を課するものではないこと、と規定している。また、コンピュータ関連設備の設置に関する第 24 条 3 にも、同様の規定が存在する。さらに、金融サービスについては、別途第 25 条が設定されており、金融規制の観点からコンピュータ関連設備の利用又は設定に関する制限に配慮がされている。ただし、第 25 条 2 においては、いずれの締約国も、金融

サービス提供者が当該締約国の領域外において利用し、又は設置する金融サービスのコンピュータ関連設備において処理され、又は保存される情報に、当該締約国の金融規制当局が、規制及び監督を目的として、迅速、直接的、完全及び継続的なアクセスを認められる場合には、金融サービス提供者に対し、当該締約国の領域において事業を実施するための条件として、当該領域において金融サービスのコンピュータ関連設備を利用し、又は設置することを要求してはならないと規定しており、当該領域におけるコンピュータ関連設備利用・設置を求めることができる場合を限定している。

また、ソース・コードに関する第 28 条 2 においては、この条の規定は、一方の締約国の政府機関、規制機関又は司法当局（関連機関）が、他方の締約国の者に対し、特定の調査、検査、検討、執行活動、又は司法あるいは行政手続のため、関連機関に対しソフトウェアのソース・コードを保存し、又は入手可能なものとすることを要求することを妨げるものではないと規定する。

(8) 比較

以上のような様々な FTA/EPA における規定を比較すると対応には一定のバリエーションが存在することが確認される。

第 1 に、そもそもデータの自由な流通を FTA の実質的な対象範囲に含めるか否かで差異がある。日 EU 経済連携協定では、現状においてデータの流通に関する実質的規定はない。そして、第 8・81 条においては、この協定の効力発生の日から 3 年以内に、データの自由な流通に関する規定をこの協定に含めることの必要性について再評価するとのみ規定されている。これは、個人データ保護の問題を基本権の問題と認識し、基本的には貿易規制の枠外と考える EU の考え方を反映している。そのため、個人データの越境流通については、別途、日本と EU との間で 2019 年 1 月に合意された個人情報保護に関する十分性認定に基づく域外データ移転の相互承認によって可能とされた。

第 2 に、日 EU 経済連携協定以外の FTA/EPA では、基本的には情報の電子的手段による国境を越える移転を認めている。ただし、公共政策の正当な目的による制限は認め、その際の条件として、(a) 恣意的若しくは不当な差別の手段となるような態様で又は貿易に対する偽装した制限となるような態様で適用されないこと、(b) 目的の達成のために必要である以上に情報の移転に制限を課するものではないこと、と規定するというのが共通の構造となっている。

ただし、正当な公共政策の扱いについては、RCEP と CPTPP 等とは大きく異なる。RCEP 第 12・15 条 2 には注が付記されており、この規定の適用上、締約国は、正当な公共政策の実施の必要性については実施する締約国が決定することを確認している。また、締約国が自国の安全保障上の重大な利益の保護のために必要であると認める措置を採用し、又は維持することを妨げるものではないとされ、他の締約国は、当該措置については争わないとしている。

第 3 に、コンピュータ関連設備の設置に関しては、原則的に、いかなる締約国も、対象者が当該締約国の領域において事業を行うための条件として、当該領域においてコンピュータ設備を使用し、又は配置することを要求してはならないと規定されている。ただ、多くの FTA において、公共政策の正当な目的による制限は認め、その際の条件として、(a)

恣意的若しくは不当な差別の手段となるような態様で又は貿易に対する偽装した制限となるような態様で適用されないこと、(b) 目的の達成のために必要である以上に情報の移転に制限を課するものではないこと、と規定している。ただし、USMCA には例外規定がない。

また、金融規制上の観点から、領域内におけるコンピュータ利用・設置を要求する可能性がある金融サービスについては、日米デジタル貿易協定、オーストラリア・シンガポール DEA において、別途の規定が設けられている。いずれも、金融サービス提供者が当該締約国の領域外において利用し、又は設置する金融サービスのコンピュータ関連設備において処理され、又は保存される情報に、当該締約国の金融規制当局が、規制及び監督を目的として、迅速、直接的、完全及び継続的なアクセスを認められる場合には、対象金融サービス提供者に対し、当該締約国の領域において事業を実施するための条件として、当該領域において金融サービスのコンピュータ関連設備を利用し、又は設置することを要求してはならないと規定している。

第 4 に、ソース・コードに関しては、USMCA 第 19・16 条 1 は、いかなる締約国も、自国の領域における当該ソフトウェア又は当該ソフトウェアを含む製品の輸入、流通、販売又は使用の条件として、他の締約国の者が所有するソフトウェアのソース・コード又は当該ソース・コードに表されたアルゴリズムの譲渡若しくは入手を要求してはならないとすると規定しており、CPTPP 等より幅広く、アルゴリズムの要求も禁止している。日米デジタル貿易協定においても、同様に対象範囲はアルゴリズムに拡大されている。

他方、CPTTP 第 14・17 条 2 においては、この条の規定の適用上、第 14・17 条 1 の規定の対象となるソフトウェアは、大量販売用ソフトウェア又は当該ソフトウェアを含む製品に限定するものとし、中枢的な基盤（critical infrastructure）のために利用されるソフトウェアを含まないと規定され、対象が限定されている。

第 5 に、日米デジタル貿易協定第 4 条や DEPA 第 15・2 条には、安全保障一般に関する例外規定が置かれている。また、CPTTP の場合には、例外及び一般規定が置かれている第 29 章において、第 29･2 条として安全保障のための例外として同様の内容が規定されている。

3. FTA/EPA における公共政策目的の国際的調和化の契機

公共政策目的間の調整を行うためには、各公共政策目的に関して一定の国際的調和化を志向することが必要になる。ここでは、そのような契機がどの程度存在するのかを確認しておきたい。

(1) 個人情報保護

第 1 に、CPTPP では第 14・8 条 1 において、消費者の信頼確保のための個人情報保護の重要性を指摘する。その上で、第 14・18 条 2 において、各締約国は、個人情報の保護のための自国の法的枠組みを作成するに当たり、関係国際機関の原則及び指針を考慮すべきであると規定する。また、第 14・18 条 5 では、異なる制度の間の一貫性（compatibility）を促進する仕組みの整備を奨励すべきであるとする。このように、関係国際機関の原則及び指針を考慮すべきこと、各国間の制度の一貫性を促進することを重視している。

第 2 に、USMCA では第 19・8 条 1 において、消費者の信頼確保のための個人情報保護の重要性を指摘する。その上で、第 19・8 条 2 において、各締約国は APEC プライバシー

フレームワーク及び OECD プライバシー保護及び個人データの国境を越えた流通に関するガイドラインに関する理事会勧告（2013 年）等の関連する国際機関の原則及びガイドラインを考慮するものとすると規定する。また、第 19・8 条 3 では、個人情報の国境を越えた流れに対するいかなる制限も必要かつ提示されたリスクに見合ったものであることを確認することの重要性を指摘する。さらに、第 19・8 条 6 では、異なる制度間の一貫性（compatibility）を促進する仕組みの整備を奨励するとともに、両締約国は、それぞれの管轄区域で適用されているメカニズムに関する情報を交換し、両締約国間の一貫性を促進するためにこれら又は他の適切な取り決めを拡張する方法を探求するよう努めなければならないとし、その際、両締約国は、APEC 越境プライバシー規則が、個人情報を保護しつつ越境的な情報伝達を促進するための有効なメカニズムであることを認識するとする。

第 3 に、日米デジタル貿易協定では、第 15 条に個人情報の保護に関する規定が置かれている。具体的には、第 15 条 3 において、異なる制度の間の相互運用性（interoperability）を促進する仕組みの整備を奨励すべきであるとし、第 15 条 4 では、個人情報を保護するための措置の遵守を確保すること及び個人情報の国境を越える流通に対する制限が当該流通によりもたらされるリスクとの関係で必要であり、かつ、当該リスクに比例したものであることを確保することの重要性を認識するとする。

第 4 に、RCEP では、第 12・8 条 1 において、各締約国は、電子商取引の利用者の個人情報の保護を確保する法的枠組みを採用し、又は維持するとし、第 12・8 条 2 において、個人情報の保護のための自国の法的枠組みを策定するに当たり、関係する国際的な機関又は団体の国際的な基準、原則、指針及び規準を考慮するとする。

これらの規定には、一定の共通性が見られる。まず、CPTTP、USMCA においては、個人情報保護が消費者の信頼の確保のために重要であることが強調されている。また、CPTTP、USMCA、日米デジタル貿易協定、RCEP のいずれにおいても、一定の国際機関等の基準・指針等を参照すべきであるとし、一定の国際調和化への配慮を行っている。ただし、その規範性の程度、具体性においては各々異なる。CPTTP においては、異なる制度の間の一貫性（compatibility）を促進する仕組みの整備を奨励すべきであり、関係国際機関の原則及び指針を考慮すべきとする。RCEP においては、関係する国際的な機関又は団体の国際的な基準、原則、指針及び規準を考慮するという、やや弱い表現となっている。他方、USMCA においては、参照すべき国際的仕組みとして APEC プライバシーフレームワーク及び OECD プライバシー保護及び個人データの国境を越えた流通に関するガイドラインに関する理事会勧告を明示する。また、実質的な規制方法に関しては、USMCA や日米デジタル貿易協定は、個人情報を保護するための個人情報の国境を越える流通に対する制限がリスクに基づく方法に依拠することの重要性を指摘している。

（2）サイバーセキュリティ

第 1 に CPTPP では、第 14・16 条において、（a）コンピュータの安全性に係る事件への対応について責任を負う自国の機関の能力を構築すること、（b）締約国の電子的なネットワークに影響を及ぼす悪意のある侵入又は悪意のコードの拡散を特定し、及び軽減するために協力することを目的として、現行の協力の仕組みを利用することの重要性を認識する。

第 2 に USMCA では、第 19・15 条 1 において、両締約国はサイバーセキュリティに対す

る脅威がデジタル貿易に対する信頼を損なうものであることを認識するとし、その上で、(a) サイバーセキュリティ事象対応について責任を負うそれぞれの自国機関の能力を構築すること、(b) 電子ネットワークに影響を及ぼす悪意のある侵入又は悪意のあるコードの流布を特定及び軽減するために協力するための既存の協力メカニズムを強化し、サイバーセキュリティ事象に迅速に対処し、また認識及びベストプラクティスのための情報を共有するためにこれらのメカニズムを利用することに努めるとする。また、第 19･15 条 2 では、両締約国は、サイバーセキュリティの脅威の進化する性質に鑑み、当該脅威に対処するに当たって、定められた規制よりもリスクに基づくアプローチが一層効果的なものとなることができることを認識するとする。

第 3 に日米デジタル貿易協定では、第 19 条 1 において、両締約国は、サイバーセキュリティに対する脅威がデジタル貿易に対する信頼を損なうものであることを認識するとし、(a) コンピュータの安全性に係る事象への対応について責任を負うそれぞれの権限のある当局の能力を構築すること、(b) 電子的なネットワークに影響を及ぼす悪意のある侵入又は悪意のコードの拡散を特定し、及び軽減するために協力するための現行の協力の仕組みを強化すること並びに当該仕組みをサイバーセキュリティに係る事象への迅速な対処のために並びに意識の向上及び良い慣行に関する情報の共有のために利用することに努めるとする。また、第 19 条 2 では、サイバーセキュリティの脅威の進化する性質に鑑み、当該脅威に対処するに当たって、定められている規制よりもリスクに基づいた方法が一層効果的なものとなることができることを認識するとする。

第 4 に RCEP では、第 12・13 条において、(a) コンピュータの安全性に係る事象への対応について責任を有するそれぞれの権限のある当局の能力を構築すること、(b) サイバーセキュリティに関連する事項について協力するために既存の協力の仕組みを利用することの重要性を認識するとする。

第 5 に DEPA では、第 5・1 条 2 において、(a) コンピュータ・セキュリティ事象対応を担当する自国機関の能力を高めること、(b) 既存の協力メカニズムを用いて、締約国の電子ネットワークに影響を及ぼす悪意のある侵入又は悪意のあるコードの流布を特定し、これを緩和するために協力すること、(c) 資格の相互承認、多様性及び平等に関する可能なイニシアティブを含む、サイバーセキュリティの分野における人材育成（workforce development）の重要性を認識するとする。オーストラリア・シンガポール DEA においても同様の規定が存在する。また、DEPA では、第 5･2 条において、オンラインの安全･セキュリティ一般についても規定されており、具体的には第 5・2 条 2 において、オンラインの安全及びセキュリティの問題に対処するために、マルチステークホルダーアプローチをとることの重要性を認識するとしている。

これらの規定においても、各国機関の協力強化、既存の協力メカニズムの活用に関しては共通性がみられるが、差異もみられる。CPTTP、RCEP においては、各国機関の能力強化、既存の協力の仕組みの活用に焦点を当てたシンプルな規定になっているのに対して、USMCA、日米デジタル貿易協定においては、リスクに基づいた方法が効果的であることが強調され、一定の規制のあり方についても示されている。また、DEPA では人材育成の重要性が指摘され、安全及びセキュリティの問題への対処におけるマルチステークホルダーアプローチの重要性も認識されている。

（3）新たな課題－ AI 倫理・ガバナンス

個人情報保護やサイバーセキュリティが多くの FTA/EPA において触れられてきた公共政策課題になるのに対して、近年新たに触れられるようになった課題もある。そのような課題の例として、DEPA が規定している AI 倫理・ガバナンスがある。オーストラリア・シンガポール DEA にも類似の規定がある。

DEPA 第 8･2 条では、人工知能について規定する。第 8･2 条 2 では、AI 技術が信頼され、安全かつ責任を持って使用されるためには、倫理及びガバナンスの枠組みを開発することが経済的及び社会的に重要であること、それぞれの管轄区域を越えた AI 技術の採用及び利用を可能な限り促進するために、相互理解を深め、最終的に当該枠組みが国際的に整合されることを確保することの利益を認識するとする。その上で、第 8・2 条 3 において、信頼され、安全で責任ある AI 技術の利用を支援する倫理及びガバナンスの枠組み（AI ガバナンス枠組み）の採用を促進するよう努めるものとし、第 8・2 条 4 において、AI ガバナンス枠組みの採用にあたり、締約国は、説明可能性、透明性、公平性及び人間中心の価値を含む国際的に認められた原則又はガイドラインを考慮するよう努めるものとする。

このように AI 倫理・ガバナンスに関しても、国際的な原則・ガイドラインが参照されている。

4. 世界レベルでの政策動向

（1）G7、G20 によるアジェンダセッティング

データの自由な越境流通と様々な公共政策目的の調整に関するデータガバナンスに関しては、FTA/EPA において具体的規定が検討されるのと並行して、世界レベルでは、G7、G20 といった場において、一定のアジェンダセッティングが行われてきた。

2016 年 5 月に開催された G7 伊勢志摩サミットにおいては、サイバーに関する G7 の原則と行動が採択され、目指すべきサイバー空間においては、情報の自由な流通がグローバルな経済及び開発を促進することが基本原則であり，デジタル経済の全ての活動主体によるサイバー空間への公平かつ平等なアクセスを確保するものであること、プライバシー，データ保護及びサイバーセキュリティを促進することの重要性が再確認された。同時に、知的財産の開発及び保護の重要性を確認するとともに，市場へのアクセスの条件として，それらの製品のソース・コードへのアクセス又はその移転を求める政策に反対するとした[12]。

また、2019 年 6 月に大阪で開催された G20 では、首脳宣言において、デジタル化を伴うイノベーションを進めるために、データ・フリー・フロー・ウィズ・トラスト（DFFT：信頼性のある自由なデータ流通）という方針が示された。そして、電子商取引に関する共同声明イニシアティブの下で進行中の議論に留意し、WTO における電子商取引に関する作業計画の重要性を再確認するとされた[13]。

（2）WTO における検討

G7、G20 等におけるアジェンダ設定も踏まえ、WTO における検討も最近進みつつある。2017 年 12 月にブエノスアイレスで開催された第 11 回閣僚会議において、電子商取引に関する共同声明[14]が発出され、有志国グループで将来の交渉に向けた探求的作業を開始することになった。71 加盟国により 2018 年 3 月に電子商取引に関する第 1 回有志国会合が開

催され、2018 年 12 月まで計 9 回開催された。そして、2019 年 1 月にダボスで開催された非公式閣僚会合で、電子商取引に関する共同声明[15]が再度出され、可能な限り多くのメンバーとともに高いレベルのルール作成を目指し、交渉開始の意思が確認された。そして、中国等も含む 76 加盟国が参加して、交渉が開始された。

2020 年 12 月には電子商取引共同声明イニシアティブが共同議長国（日、豪、シンガポール）による進捗報告として出された[16]。そこでは、主要な進展が、電子署名及び電子認証、ペーパーレス貿易、電子的な送信に対する関税、公開された政府データ、インターネット・アクセス、消費者保護、迷惑メール、ソース・コード等について見られたとされた。他方、データ流通を促進する規律については、高い水準で商業的に意義のある成果には必須であり、2021 年前期にはこれらの議論を一層深める必要があるとされた。例えば、交渉過程における中国の主張[17]においては、1）技術進歩、ビジネスの発展、正当な公共政策目的のバランスを踏まえたリーゾナブルな目標設定が重要である、2）当面はモノの貿易に焦点を当てるべきである、3）発展段階や政策関心も異なる発展途上国にも配慮すべきである、4）データ流通、データ保存等の議論を一部の国は主張するが、様々な議論があるのであり、交渉に先立ってより探求的議論が必要である、5）データ流通の基礎にはセキュリティがあるべきだ、といった原則的な議論がみられ、交渉の難しさが垣間見られた。

その後、2021 年 12 月には、WTO 電子商取引交渉の共同議長国である日本、オーストラリア及びシンガポールは、これまでの交渉の実質的な進捗を確認するとともに、今後の目標を示す、共同議長国閣僚声明[18]を発表した。その中では、8 つの条文（①オンラインの消費者保護、②電子署名及び電子認証、③要求されていない商業上の電子メッセージ、④政府の公開されたデータ、⑤電子契約、⑥透明性、⑦ペーパーレス貿易、⑧開かれたインターネット・アクセス）について意見の収斂が達成され、その結果、消費者の信頼性の向上、オンラインで取引するビジネスの支援といった便益がもたらされることが確認された。他方、電子的な送信に対する関税、国境を越えるデータ流通、データ・ローカライゼーション、ソース・コード、サイバーセキュリティ等の分野については条文提案の統合は進んだものの、これらの分野の交渉を 2022 年初めから強化する必要があることが確認された。その上で、データ流通を可能とし、促進する規定が、高い水準かつ商業的に意義のある成果のための鍵であること、途上国及び後発開発途上国の関与を支援することの重要性の認識が示された。

5. おわりに

公共政策目的間の調整可能性については、ベトナムを含む TPP、中国を含む RCEP においても一定の規定が可能であったことを考えると条文レベルでは WTO において一定の合意が行われる可能性もあると思われる。ただし、特に RCEP の規定に見られるように、公共政策目的の判断、特に安全保障の観点からの判断が各国に委ねられる可能性も高く、その場合、実質的な公共政策目的間バランスの差異は持続する可能性が高い。また、貿易枠組みの下における政策目的間調整は容易ではない[19]。このような状況の中で、公共政策目的間のバランスに関して一定の調整を図るためには、個人情報保護、サイバーセキュリティ、ELSI といった実質的な公共政策目的の各々に関して一定の国際的調和化の方向性が必要であろう。3. において検討したように、そのような方向性もある程度はみられるもの

の、現時点では限定的である。

経済安全保障が議論される中で、狭義の安全保障と、個人情報保護、サーバーセキュリティ、実効的規制、産業政策、倫理的法的社会的課題（ELSI）への対応強化等との境界も曖昧になりつつあり、「安全保障」が肥大化する恐れがある。このような広義の「安全保障」を適切にマネジメントするためにも、個別の公共政策毎に国際調和化を図ることは重要である。

また、データガバナンスの検討プロセスにおいては、政策的調整の場としては FTA/EPA が先行し、最近になって WTO における試みもみられるようになってきた。また、その過程では、G7、G20 等の横断的な場も触媒として活用されてきた。そのなかで、日本は G20 等を通して、データ・フリー・フロー・ウィズ・トラストをかかげて議論を主導することを試みている。日本は、米国、EU、中国といったデータに関する主要領域に比べれば小さな単位ではあるのが、EU との個人情報保護に関する十分性認定の取得、日米デジタル貿易協定、TPP、中国を含む RCEP 等様々な仕組みの実験の結節点になっている面はあり、様々な立場の橋渡しを行うには、興味深い場所にいるとは言える。

―注―

1 Susan Ariel Aaronson and Patrick Leblond, “Another Digital Divide: The Rise of Data Realms and its Implications for the WTO”, *Journal of International Economic Law*, Vol. 21, 2018.

2 Ibid. 255.

3 須田祐子『データプライバシーの国際政治：越境データをめぐる対立と協調』勁草書房、2021 年、18、20、39 頁。

4 「ネットワーク安全法（大地法律事務所仮訳）」（https://www.jetro.go.jp/ext_images/world/asia/cn/law/pdf/others_005.pdf）。

5 「第 14 章　電子商取引」（https://www.cas.go.jp/jp/tpp/tppinfo/kyotei/tpp_text_yakubun/pdf/160308_yakubun_14.pdf）。

6 “Chapter 19 Digital Trade”（https://ustr.gov/sites/default/files/files/agreements/FTA/USMCA/Text/19-Digital-Trade.pdf）.

7 「デジタル貿易に関する日本国とアメリカ合衆国との間の協定」（https://www.mofa.go.jp/mofaj/files/000527426.pdf）。

8 「第 12 章電子商取引」（https://www.mofa.go.jp/mofaj/files/100129065.pdf）。

9 「経済上の連携に関する日本国と欧州連合との間の協定」（https://www.mofa.go.jp/mofaj/files/000382088.pdf）。

10 “Digital Economy Partnership Agreement”（https://www.mti.gov.sg/Improving-Trade/Digital-Economy-Agreements/The-Digital-Economy-Partnership-Agreement）.

11 “Australia-Singapore Digital Economy Agreement”（https://www.dfat.gov.au/sites/default/files/australia-singapore-digital-economy-agreement.pdf）.

12 「サイバーに関する G7 の原則と行動」（https://www.mofa.go.jp/mofaj/files/000160315.pdf）。

13 「G20 大阪首脳宣言」（https://www.mofa.go.jp/mofaj/gaiko/g20/osaka19/jp/documents/final_g20_osaka_leaders_declaration.html）。

14 WTO, “Joint Statement Initiative on Electric Commerce” (WT/MIN (17)/60).

15 WTO, “Joint Statement Initiative on Electric Commerce” (WT/L/1056).

16 WTO, “Joint Statement Initiative on E-commerce: Co-convenors’ Update”（https://www.wto.org/english/news_e/news20_e/ecom_14dec20_e.pdf）.

17 WTO, “Joint Statement Initiative on Electric Commerce- communication from China” (INF/ECOM/19 24 April 2019).

18 “WTO Joint Statement Initiative on E-commerce: Statement by Ministers of Australia, Japan and Singapore”（https://www.wto.org/english/news_e/news21_e/ji_ecom_minister_statement_e.pdf）.

19 SPS 協定、TBT 協定運用における政策目的間調整の課題については、以下を参照。城山英明『国際行政論』（有斐閣、2013 年）、106 － 108 頁。