EU　貿易管理制度

電子商取引・サイバーセキュリティ・個人情報保護に関する規制　詳細

1. 越境電子商取引に関する規則

(1) オンライン・コンテンツ・サービスの越境ポータビリティ

域内市場におけるオンライン・コンテンツ・サービスの越境ポータビリティに関する 2017 年 6 月 14 日付欧州議会・理事会規則 2017/1128（(2017 年 6 月 30 日付官報 L168 掲載）

http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32017R1128

欧州議会・理事会規則 2017/1128 は、2017 年 6 月 30 日に公布され、2018 年 3 月 20 日から適用が開始された。同規則は、EU 域内の居住者が、映画やスポーツ、ビデオゲームなど、居住国で契約した有料のオンライン・コンテンツ・サービスを、他の加盟国での一時滞在中にも利用できるようにすることを目的とする。コンテンツ利用のライセンスが特定の地域に限定されていることから、EU 域内でも従来は、他の加盟国での一時滞在中は、居住国で加入しているオンライン・コンテンツ・サービスを利用できなかった。

規則 2017/1128 に基づき、オンライン・コンテンツ・サービスの利用者が居住国以外の加盟国での一時滞在中にサービスを利用する際、居住国でのサービス利用と同様に扱われるようになった。すなわち、サービス提供者は、加入者の他の加盟国での一時滞在中にも、同じコンテンツと機能を、同数のデバイスとユーザーに対して追加料金なしで提供する義務が課せられる。なお、無償でコンテンツを提供するサービスの場合は、本規則を適用するか否かの選択が認められる。

同規則により、サービス提供者は、個々の加盟国でライセンスを取得する手続きが不要となった。ただし、不正利用防止の観点から、サービス提供者は、利用者の居住国を確認する必要がある。

(2) ジオブロッキング対策

域内市場における不当なジオブロッキング及び顧客の国籍・居住地・所在地によるその他の差別に対処し、規則 2006/2004、規則 2017/2394、及び指令 2009/22 を改正する 2018 年 2 月 28 日付欧州議会・理事会規則 2018/302（2018 年 3 月 2 日付官報 L60I 掲載）

http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32018R0302

欧州議会・理事会規則 2018/302 は、2017 年 3 月 2 日に公布され、2018 年 12 月 3 日から

適用開始された。ジオブロッキングとは、利用者の国籍や居住国などを理由とする、オンラインショップ等によるアクセス拒否や、アクセス可能でも購入取引を完了できない場合などを指す。規則 2018/302 は、こうした不当なジオブロッキングを禁止するものだ。

同規則は、利用者の国籍や居住国などを理由に、ウェブサイトへのアクセスを拒否・制限したり、同意なしに他のサイトに誘導したり、商品・サービスへのアクセスについて異なる一般条件や支払条件を提示することを原則として禁止する。なお、著作権で保護されるコンテンツや視聴覚サービス、運輸サービス、医療サービス、金融取引などは適用対象外となる。また、特定地域の利用者を対象に、異なる価格を提示することが可能であるなど、正当な根拠がある場合は適用の除外が認められる。

(3) 越境小荷物配送サービス

越境小荷物配送サービスに関する 2017 年 4 月 18 日付欧州議会・理事会規則 2018/644（2018 年 5 月 2 日付官報 L112 掲載）
http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32018R0644

欧州議会・理事会規則 2018/644 は、2018 年 5 月 2 日に公布され、罰則規定を除き 2018 年 5 月 22 日から適用開始した（罰則規定は 2019 年 11 月 23 日適用開始）。越境配送サービスにおける合理的な価格設定やサービスの質の向上を目的としており、インターネットを通じた商品の販売の容易化と信頼感の醸成が期待される。

EU では、一部加盟国の配送サービス分野の監督当局が価格情報を持ち合わせていないなど、加盟国によって市場の監視や規制監督における権限にばらつきがあった。規則 2018/644 は、競争を促進し価格の透明性を高めるために、全ての小荷物配送サービス事業者に、事業者名や住所、サービスの詳細、小荷物配送サービスの売上高、従業員数、取り扱い荷物数などを加盟国の監督当局に報告することを義務付けている。さらに、EU 域内の国境を越える配送サービスを提供する事業者は、同規則の付属書に定められた小荷物の年始時点での配送料金リストを、毎年 1 月 31 日までに加盟国の監督当局に提出しなければならない。加盟国監督当局は収集した料金表を欧州委員会に提出、欧州委員会はこのリストを毎年 3 月 31 日までに公示する。さらに、加盟国監督当局は、収集した価格データに基づき、価格の妥当性を定期的に検証する。

2. サイバーセキュリティに関する規則

(1) 適用法令

EU 共通の高度なネットワークと情報システムのセキュリティ対策に関する 2016 年 7 月 6 日付欧州議会・理事会指令 2016/1148（NIS 指令）（2016 年 7 月 19 日付官報 L194 掲載）（指令 2022/2555 により 2024 年 10 月 18 日に廃止予定）

https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32016L1148

規則 910/2014 および指令 2018/1972 を改正し指令 2016/1148 を廃止する EU 共通の高度なサイバーセキュリティ対策に関する 2022 年 12 月 14 日付欧州議会・理事会指令 2022/2555（NIS2 指令）（2022 年 12 月 27 日付官報 L333 掲載）

https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32022L2555

(2) 概要

欧州議会・理事会指令 2016/1148（NIS 指令）は、EU 共通の高度なセキュリティ環境を構築することを目的とする EU 初のサイバーセキュリティ関連法であり、2016 年 7 月 19 日に公布、8 月 8 日に適用開始した。

NIS 指令は、加盟国のサイバーセキュリティへの対応力の向上、EU 域内の国境を越えた協力体制の確立、重要分野における加盟国による監督の枠組みを定める。具体的に、加盟国は 1 つ以上のサイバーセキュリティ監督機関（複数の監督機関が存在する場合は単一連絡窓口も）、および加盟国レベルでのモニタリングや早期の注意喚起や警報の発信、情報発信、事故対応を担当する「コンピューター・セキュリティ事故対応チーム（CSIRT）」を創設する。

EU レベルでは、加盟国と欧州委員会、欧州ネットワーク・情報セキュリティ庁（ENISA）の代表からなる「協力グループ」を設置し、ネットワーク及び情報システムのセキュリティに関する加盟国間の戦略的協力の支援と円滑化を図る。また、加盟国の CSIRT および EU レベルのコンピューター危機管理チーム（CERT-EU）からなる「CSIRT ネットワーク」を設置し、サイバーセキュリティ事故に対して、実務レベルでの協調、リスク情報の共有などを行う。協力グループは CSIRT ネットワークの活動に関する戦略的ガイダンスを提供する一方、CSIRT ネットワークは協力グループに活動の報告を行う。

加盟国は、自国内に拠点を置く、社会経済に不可欠で情報通信技術に大きく依存する、エネルギー、運輸、水道、銀行、デジタルインフラ分野の「主要サービス事業者（Operators of

Essential Services：OES）」を特定し、技術・組織面において適切なセキュリティ対策が導入されるようにしなければならない。また、OES が提供する必要不可欠なサービスの継続に著しい影響を及ぼす事故が発生した場合は、加盟国の管轄当局または CSIRT に迅速に報告するようにしなければならない。同様の規定は、オンライン・マーケットプレイス、検索エンジン、クラウドサービスを提供する「デジタルサービス」にも適用される。

加盟国は 2018 年 5 月 9 日までに国内法を整備し、規制対象となる「主要サービス事業者（Operators of Essential Services：OES）」を 2018 年 11 月 9 日までに特定するよう定められていた。ENISA は専門的知見や助言の提供などを通じて、NIS 指令の導入・実施を支援する。

2023 年 1 月、指令 2022/2555（NIS2 指令）が発効し、加盟国は 2024 年 10 月 17 日までに国内法を整備し、同 18 日から適用を開始しなければならない。これに伴い、現行指令 2016/1148（NIS 指令）は、2024 年 10 月 18 日に廃止される。NIS2 指令は規制対象事業者を拡大し、サイバーセキュリティ対策の強靭化、インシデント報告のルールの明確化、執行当局の権限や監視の強化が図られている。基幹サービス運営者の範囲が拡大され、現行指令では対象とされていない下水道や行政機関などが追加される。また、デジタルサービス提供者以外にも、郵便、廃棄物処理、化学品、食品、医療機器の製造など、新たな業種も規制対象となる。リスクに対応したセキュリティ対策の導入が要請され、インシデント報告、サプライチェーンにおけるセキュリティ対応などにおける要件、方針や対策が強化される。重要セキュリティ事故は加盟国当局に報告する義務があり、事故発生からのタイムラインごとに具体的な報告内容などが明確にされた。対象事業者はコンプライアンス方針や実務手続きを整備することが求められる。準拠性違反が認められれば多額の罰金が科される可能性もある。

3. 個人データ保護に関する規則

(1) 適用法令

個人データの処理やその移転において自然人を保護し、指令 95/46/EC を廃止する 2016 年 4 月 27 日付欧州議会・理事会規則 2016/679（2016 年 5 月 4 日付官報 L119 掲載）（一般データ保護規則：GDPR）

https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32016R0679

個人情報保護法による日本での個人情報保護の十分性に関する欧州議会・理事会規則 2016/679 に準ずる 2019 年 1 月 23 日付欧州委員会実施決定 2019/419（2019 年 3 月 19 日付

官報 L76 掲載）

https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32019D0419

電子通信分野における個人データの処理およびプライバシーの保護に関する 2002 年 7 月 12 日付欧州議会・理事会指令 2002/58/EC（2002 年 7 月 31 日付官報 L201）（指令 2009/136 により改正）（e プライバシー指令）

https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32002L0058

（改正を反映した本文は、リンク中の「Current consolidated version」を参照）

(2) 概要

欧州議会・理事会規則 2016/679（一般データ保護規則：GDPR）は、域内の個人データ保護制度の調和と一貫性の改善を目的に、2016 年 5 月 4 日に公布、同 24 日に発効し、2018 年 5 月 25 日に適用開始した。GDPR は、EU において基本的人権の一部をなすプライバシー権の保護を目的に、域内における個人データの処理・移転に関する厳格なルールを定めるとともに、EU 域外への個人データの移動を原則禁止しており、違反が認められれば、多額の課徴金を科されるリスクがある。

個人データを管理する企業などは、データ保護の方針、内規、内部手続き等の体制整備が求められるとともに、説明責任が課される。データ管理者や処理者、もしくは、データ主体（個人）が欧州経済領域（EEA、EU27 カ国およびアイスランド、リヒテンシュタイン、ノルウェー）域内に存在する場合、及び、EEA 域外に拠点を持つ組織でも、EEA 域内で取得した個人データを取り扱う場合は、本規則への準拠が要請されるため注意が必要である。例えば、EEA 域外の企業が、インターネットを経由して EEA 所在者の個人情報を収集して購買活動をモニターし、マーケティングに利用する場合や、日本企業の EU 拠点が従業員データや取引先情報を日本本社と共有する場合も、GDPR の適用対象となる。

欧州委員会は 2019 年 1 月 23 日に、日本が EU と同水準の十分なデータ保護体制を確立していると認定した（欧州委員会実施決定 2019/419 による十分性認定）。これにより、EU から日本への個人データ移転については、事実上、EU 域内での移転と同じ取り扱いとなる。ただし、十分性認定により免除される法的義務は GDPR が定める移転にかかる部分のみであり、EU 域内で取得した個人データの処理を含む、その他の GDPR が定める規定は引き続き遵守する必要がある。

英国の EU 離脱後の移行期間が終了したことから、2021 年 1 月以降、英国は GDPR 規制上、個人データの移転が原則として禁止される EU 域外国（第三国）となった。ただし、2021 年 6 月 30 日までは、英国との通商・協力協定の暫定適用の規定により、従来通りの個人データの移転が暫定的に認められていた。その後、欧州委員会は 2021 年 6 月 28 日、英国が

EU と同水準の十分なデータ保護体制を有していると認定する実施決定（十分性認定）を採択した。これにより、今回の十分性認定の有効期限である 2025 年 6 月 27 日までは、EU から英国への個人データの移転が認められる。

一方、英国は、個人データの処理に関して EU の GDPR を国内法化した英国版 GDPR（UK GDPR）を適用しており、少なくとも 2024 年までは、EU に対する十分性認定を行っていることから、英国から EU への個人データの移転が認められる。

GDPR に関する情報は、次のジェトロ・ウェブサイトを参照。
ジェトロ：EU 一般データ保護規則（GDPR）について
https://www.jetro.go.jp/world/europe/eu/gdpr/

欧州議会・理事会指令 2002/58/EC（e プライバシー指令）は、インターネットや電話などにおける個人データ処理および EU 域内の電子通信におけるプライバシー権の保護と秘匿性を確保するためのルールを定めており、GDPR の先行法令であるデータ保護指令（95/46/EC）を補完するものと位置づけられる。

e プライバシー指令は、電子通信サービスの提供者に対して、個人データにアクセスできる人間の制限や個人データの破棄・喪失からの保護、個人データ処理におけるセキュリティ策の実施を要求し、個人データの侵害が発生した場合には、加盟国監督機関に通知することを義務付けている。また、加盟国に対しては、法的な根拠のない盗聴などの通信の傍受の禁止などを求めている。

なお、欧州委員会は、現行の e プライバシー指令の目標と原則は依然として有効であるものの、同指令が最後に改正された 2009 年以来の急速な技術と経済の進展に遅れをとっており、IP 電話（VoIP）やインスタント・メッセージ、ウェブベースの電子メールサービスなど新たな通信サービスにおけるプライバシー保護に空白が生じていると指摘。2017 年 1 月に同指令を置き換える規則案を提案した。同規則案は、GDPR と整合性を持たせ、かつ、EU 全域への統一的な適用を図るため、EU 規則として導入することが検討されている。加えて、規制対象を従来の通信サービスだけでなく、新たな通信サービスにまで拡大することが提案されている。

