海外プライバシー保護の動向

寺田 眞治 ●一般財団法人日本情報経済社会推進協会 主席研究員
柊 紫央璃 ●一般財団法人日本情報経済社会推進協会 客員研究員

COVID-19のパンデミックがあぶり出した、プライバシーに関する考え方の違い。多くの国では基本的人権であり本人の判断に委ねられるものとする一方、個人情報を国が管理する中国のような例もある。

■分断が進むプライバシー保護制度

2020年に発生した新型コロナウイルス感染症（COVID-19）のパンデミックは、はからずも各国のプライバシーに関する考え方の違いをあらわにすることになった。罹患者やクラスター発生などの把握、濃厚接触者の把握に関する対応策に、それは如実に表れている。

欧米先進国の大半はプライバシーを基本的人権であり本人の判断に委ねられるべきものとして、対策アプリにおける個人情報や位置情報の利用を厳密に制限し、さらにアプリのダウンロードも義務化することはしなかった。日本もこれに倣っている。一方で、中国では罹患の有無にかかわらず、様々な手段による位置情報や行動履歴の取得によって個人にヘルスコードを付し、カメラや人工知能（AI）の利用による個人識別によって監視をも含む対策を講じた。この両極端な例以外にも、個人情報を国家が管理するタイプと国家が管理しないタイプ、特定の個人を識別するタイプと匿名のタイプなど、プライバシーへの影響度が異なるものが様々あり、それぞれの国のプライバシーに対する考え方が明確にうかがえる。

2020年は、こういった特別な危機対応とは別に、ここ数年続いてきた世界的なプライバシー保護制度の拡充についても各国の違いが鮮明になった1年でもあった。表面的には最も厳しい規制と考えられているEUのGDPR（General Data Protection Regulation、一般データ保護規則）に追随するような法制度の整備が各国で進んでいるように見受けられる。米国では2020年1月にCCPA（California Consumer Privacy Act、カリフォルニア州消費者プライバシー法）[1]が施行され、同年11月にはこれを補完し塗り替えることになるCPRA（California Privacy Rights Act、カルフォルニア州プライバシー権利法）が住民投票で承認された。中国では2017年に施行されたオンライン上の個人情報保護を含むサイバーセキュリティ法[2]に続いて、オンライン以外も対象とする個人情報全般の保護を目的とする個人情報保護法（案）が審議されており、草案のパブリックコメントが2020年11月まで行われていた。日本においては、3年ごとの見直しに伴う改正が大詰めを迎えている。その他、アジア各国でも次々と新たな法律の制定や改正が進んでいる。

これらに共通していることは、企業と個人の関係という面では、個人のプライバシーに関する権利を重視したGDPRにきわめて近い、あるいは近づくものであるということである。その一方で、

国家と個人の関係においては、同様に個人のプライバシーに関する権利を重視するタイプと、国家が個人を管理することを重視するタイプに分かれる。

国内の個人情報を海外に移転する際に課せられる規制（越境移転規制）の厳しさについても、おおむね国家の個人情報の管理の程度に応じているとみることができる。データローカライゼーション（国内の個人情報を国内に保存すること）については、個人のプライバシーを保護するための場合と、国家が管理するための場合とでは意味が大きく異なり、後者では国外との情報の流通を監視し規制することが目的となる。その根拠とされるのは国家の安全やサイバー空間の主権であり、中国やロシアをはじめとする独裁傾向の強い国や発展途上国で多く見られる。

このように、一見すると世界はGDPRの制度をベースとする法制度に収斂しつつあるようだが、実態は、個人のプライバシーを基本的人権として国家の介入を極力排除する方向性と、国家の体制維持や海外からの干渉を抑えるために個人を管理する目的でプライバシー保護制度を利用する方向性に大別される。2020年は、この色分けが各国の法律の制定や改正で、より明確になった1年と言えるであろう。

■EUの動向

EUではGDPRの施行以降、定着させるために様々な対応が進められているが、十分な成果がありデジタル単一市場としての安定した運用になっているとは言い難い状況が続いている。特にCookieを利用したターゲティング広告については、業界団体であるIAB（Interactive Advertising Bureau）EuropeがGDPRに準拠するために策定したTCF（Transparency & Consent Framework）[3]に対して、各国の機関でも肯定的な意見と不十分だとする意見が錯綜しており、いまだ確たる状況には達していない。

そんな中、2020年12月、フランスのデータ保護機関であるCNIL（Commission Nationale de l'Informatique et des Libertés、情報処理・自由全国委員会）が、米グーグルと米アマゾン・ドット・コムに対して事前同意なしのCookie取得や説明不足などの透明性欠如をGDPR違反として、それぞれ1億ユーロと3500万ユーロという巨額の制裁金を科すと発表している。今後、両社が司法的手続きを取るのか、その場合の結果がいかなるものとなるのかは見通せないが、大きな分岐点となることは間違いないだろう。

また、国ごとの意見の相違は、COVID-19対策としてのコンタクト・トレーシング・アプリの仕様策定時にも見られた。英国やフランスなどは罹患者と濃厚接触者の情報を一元的に中央サーバーで管理できる方法を模索し、ドイツとスイスは本人が申告しない限り当局が把握することができない分散型の方法を選択した。英国とフランスも、結局、公衆衛生ではなくプライバシーを重視する分散型の方向に落ちついたものの、デジタルの特徴を有効に活用できない結果となり、今後に課題を残すこととなった。

法制度の充実の面でも、オンラインに限定しない普遍的なGDPRを電子通信のセグメントで補完することを目的としたePrivacy規則は、本来、2018年に同時施行を目指していたにもかかわらず、2年以上を経た現時点でも成立のめどが立っていない。さらに、企業などのプライバシー保護対策を審査し、認証を与える仕組みの構築も大幅に遅れている。

これらはいずれも、EUがデジタル単一市場を目指す上で必要となる域内の環境をそろえることを重要な目的の一つとしている。理念や総論では意見に大きな隔たりはないものの、現実的な対応

となると各国、産業ごとなど様々なステークホルダーの間で利害関係が対立し、それが進捗の阻害要因となっていると考えられる。

■米国の動向

EUが足踏みをしている間に米国ではプライバシー保護に関する動きが加速し、国際的な影響力も増大している。前述のように、2020年1月に施行となったCCPAが日本企業にも大きな影響を及ぼすとして話題になったが、同年11月にはCPRAが住民投票によって可決された。

CPRAはCCPAを改正して消費者の権利をより拡大するもので、州独自の個人情報保護機関が法の執行を行うことを定めている。さらに、センシティブ情報を定義した規制の強化、第三者提供や共同利用についての明確化と制限、児童のプライバシー保護の強化などを含む消費者の権利が追加されている。事前の同意取得を求めるまでには至っていないが、それ以外ではGDPRにさらに近づいた見ることができる。施行は2023年1月1日とまだ先ではあるが、罰則などの強化もあり、CCPA以上に対応に追われることになるだろう。

米国の特徴であった州独自あるいはセクターごとのプライバシー保護の動きに対し、連邦法によって米国全体としての法制度策定の動きも本格化しつつある。現在、民主党からはCOPRA（Consumer Online Privacy Rights Act、消費者オンラインプライバシー権利法）[4]、共和党からはSDA（SAFE DATA Act、セーフデータ法）[5]が提案されており、いずれもこれまでのものと比べると、包括的なプライバシー保護を目指したものとなっている。米国内での制度乱立を避けたいという企業の思惑もあり、これまでになく連邦法成立への期待は高まっており、両党の意見の差も縮まってきている。しかしながら具体的な内容の議論となると、各ステークホルダーの意見の整理すら不十分で、成立の見通しは立っていない。2020年の大統領選で民主党が政権を担うことになったことから規制は強化の方向に向かうとみられているが、その場合、産業界の反発は強くなるだろう。

一方、こういった厳しい法制度を回避するための自主的な規制についても大きな進展が見られた。NIST（National Institute of Standards and Technology、国立標準技術研究所）による2020年1月のプライバシーフレームワーク[6]と同年9月のSP 800-53 Rev.5[7]のリリースである。NISTは実態としては商務省傘下であり、今回のドキュメントも政府機関の調達要件でもあることから必ずしも純粋な自主規制とは言えないが、産官学が共同して策定しているものでもあり、法律とは一線を画す。事実上、グローバルでのデファクトスタンダードとなっているCSF（Cyber Security Framework）[8]と合わせた3点セットで、セキュリティとプライバシー保護を統合した評価基準と管理策を策定している。これらに準拠していれば、セキュリティとプライバシー保護に関しては政府機関の要求をも満たすと判断されるハイレベルなものである。

CSFと前バージョンのSP800-53は2020年に登録申請が始まった日本のISMAP（Information system Security Management and Assessment Program、政府情報システムのためのセキュリティ評価制度）[9]のひな型であるなど、世界中の多くの企業が準拠あるいは参照するといった実績があることから、追加・統合されたプライバシー保護管理策も広く普及する可能性が高い。さらに、これらとISOの国際標準規格などを機械可読化するOSCAL（Open Security Controls Assessment Language）[10]もVersion 1.0が公開され、評価や認証における可視化・共有化・簡便化が格段に進むことが予想されている。

政策のみではなく、産官学の協力により、実務

において一気に世界の最先端に躍り出る流れが生まれつつあることは、米国らしい現象と言える。

■中国の動向

2020年から2021年にかけて最もダイナミックな動きを見せたのは中国だろう。COVID-19を契機とする個人の健康状態を表すヘルスコードの普及や様々な監視システムによる国民管理の急激な進展に目が行きがちであるが、それらの根拠となる法体系も急ピッチで完成系に近づきつつある。

2020年5月に可決され2021年1月1日から施行される民法典[11]では「プライバシーおよび個人情報保護」という章が新たに設けられた。さらに、現在審議中の個人情報保護法（案）は、民法典の個人情報保護の原則を受け継いで、個人情報処理規則、個人情報越境移転、個人の権利および個人情報処理者の義務などに対して具体的なルールを提供している。

これまで、中国の個人情報保護に関する法体系の整備は、主に以下の2つのアプローチで並行して行われてきた。

①刑法や民法などの基本法で個人情報が守られる権利・プライバシー権を定義し確立させた上で、一般法で特定のシナリオにおける個人情報保護のルールを作る
②インターネットの普及に伴い、国家インターネット情報弁公室が主導するサイバーセキュリティ関連の法整備に合わせてサイバー空間における個人情報保護の規程を整理する

①について、基本法では、2009年の刑法改正案（七）で「個人情報の不正提供罪、個人情報の不正入手罪」を定め、2015年に可決された刑法改正案（九）で2つの罪を個人情報侵害罪として合併し、情報セキュリティ管理義務履行拒否罪を追加した。2013年には、消費者権益保護法（改正）で個人情報が守られる権利を消費者の基本的権利として規定し、消費者の個人情報の収集や利用、保護などについて事業者の法的義務を明確化した。民法においては、2017年10月1日施行の中国民法総則で「自然人の個人情報は、法律による保護を受ける。他者の個人情報を取得する必要がある組織および個人は、法令に従って個人情報を取得し、個人情報の安全を確保しなければならず、他人の個人情報を違法に収集、利用、処理、または譲渡することは禁止される」（第111条）と規定された。これらの流れが、民法典および個人情報保護法（案）へとつながっている。

②のサイバー空間における個人情報保護の規程は、2012年12月にインターネット情報保護の強化に関する決定が出されたことを皮切りに開発が急ピッチで進み、2017年のサイバーセキュリティ法へとつながる。さらに、2019年1月1日施行の電子商取引法[12]では、ネットワーク運営者と電子商取引経営者に対して個人情報を適切に取り扱う義務が課された。

この2つの流れは、以下により、統合される。民法典で個人情報を処理する場合は個人情報保護の責任があるとするとともに、個人情報保護法（案）において組織・個人が国内で自然人の個人情報処理活動を行う際に本法が適用されるとし、先に制定されたサイバーセキュリティ法の対象者であるネットワーク運営者から、個人情報を取り扱うあらゆる組織・個人に適用対象を拡大する。個人情報保護法（案）ではさらに、一部の場合において国外まで適用対象を拡張している。

このように、民法典で普遍的な権利として確立し、個人情報保護法（案）で具体的な規則を制定し、さらにサイバーセキュリティ法でサイバー空間における情報セキュリティの観点が補強される構図により、法体系として一通りの完成形に近づ

いたと言えるだろう。

世界に先駆けて個人情報とプライバシーを分けて定義し明文化したことは、注目に値する。民法典ではプライバシー情報を私密信息と呼び、自然人の私生活の平穏、および他人に知られたくない私生活や私的な活動、プライバシー情報と定義しており、日本の判例に極めて近いものとなっている。一方で個人情報保護法（案）は機微な個人情報の概念を、漏えいしたり不法に使用されたりすると、個人が差別を受けたり身体や財産の安全が著しく脅かされたりする可能性のある個人情報と定義している。両者の重なり合いの範囲は明らかではなく、今後、どのように整理されていくかが注目される。

中国の法制度において最も特徴的なのは、国家安全保障の観点である。サイバーセキュリティ法は「重要情報インフラ運用の安全」の章を設けている。そこでは、重要情報インフラの運営者は個人情報および重要データを国内に保存しなければならないとし、データローカライゼーションを規定している。国外に提供する必要がある場合は、国家インターネット情報部門が国務院の関係部門と共に、制定した規則に従って安全評価を行わなければならない。個人情報保護法（案）ではさらに、対象者を重要情報インフラの運営者だけでなく個人情報の処理件数が国家インターネット情報部門の定める件数に達した個人情報処理者にまで拡大していることに注意が必要である。また、中国に敵対的な国家による個人情報侵害行為に対しては対抗措置を講じることができるとあり、海外からの干渉排除など、国家管理の明確な意思を示している。

実務においては、2020年10月に発行された国家規格の個人情報安全規範であるGB/T 35273-2020[13]が最も重要である。個人情報、機微な個人情報、個人生体情報を定義した上で、個人情報コントローラーがそれぞれの情報に対し、処理における収集や保管、利用、共有、譲渡、公開、域外移転などの行動に関する要件を明確化したものだ。個人情報の定義を特定の自然人の活動を反映できる情報にまで拡張しており、保護対象の範囲の広さではGDPRに近いと考えられる。適用の除外として国家安全や公共衛生関連を含めているのも、中国的特徴と言える。

全体として、要件の厳しさは日本の個人情報保護法を上回っている。例えば、個人情報の保管について、個人情報コントローラーが個人情報を収集後、「速やかに仮名加工（De-identification）し」、個人の身元を復元するために使用できる情報と別々に保管するように求めている。さらに、機微な個人情報を取り扱う際の暗号化措置を義務付け、生体情報について「原則的にローデータを保管しない」としている。また、ユーザープロファイリングの利用、パーソナライズされたディスプレー（ターゲティングマーケティング）の利用要件を新たに追加し、情報システムの自動意思決定メカニズムの利用へのガイドラインを提供するなど、GDPRの要素をも取り込んでいる。組織における個人情報セキュリティ管理要件には、プライバシー・バイ・デザインの思想や、いわゆるPIA（Privacy Impact Assessment、プライバシー影響評価）の実施を取り入れており、どのようなときに評価または再評価が必要なのか、どのような内容を評価するのか、そして評価レポートの作成と保管、公開にも言及している。

以上、中国の社会信用システムのニーズを満たしつつ、新しい技術分野において欧米の標準に足並みをそろえようとする意図が見て取れるものとなっている。

■国際協調と国際標準化

国ごとの法制度が分断する中で、これらの法制

度を順守しつつグローバルでのデータ流通を実現するための方法の模索が続いている。

EUは、相手国の法制度の整備がGDPR並みに十分であることを認定することでデータの越境を認める規定を設けている。日本の個人情報保護法にも同様の規定があり、各国にも広がりつつある。このような2国間での認定方法は、基本的に、より厳しい法制度に合わせなければならないものであり、これが最も厳しいとされるEUのGDPRが世界的に広がる要因でもある。

例外的なものとして、EUと米国の間でのプライバシーシールドという仕組みがある。これは、企業がGDPRに準拠した取り扱いを行うことを米国商務省が保証するものであるが、2020年7月にEUの最高裁判所に当たる欧州司法裁判所（ECJ）は、これを無効であると判断した。仕組みの問題ではなく、CLOUD Act（Clarifying Lawful Overseas Use of Data Act、クラウド法）[14]に代表されるように、政府が個人の情報を自由に検閲・取得できるガバメントアクセスの可能性が排除されないためである。この衝撃は大きく、ガバメントアクセスに関する法律がある限り企業間の契約でこれを拒否するという条項は成り立たなくなる。現在、EUと米国で対応を急務としているが、どのように解決されるかは不明である。

一方、多国間での枠組みとして、APEC（Asia Pacific Economic Cooperation、アジア太平洋経済協力会議）はCBPR（Cross Border Privacy Rules、越境プライバシールール）[15]を策定し、APEC域内の個人情報に対する消費者や事業者、行政機関における信用を構築するための認証システムの提供を開始している。日本、米国、メキシコ、カナダ、シンガポール、韓国、オーストラリア、台湾、フィリピンが参加しており、特に米国はこれを強力に推進するとして、英国とインドの参加を求めているといわれている。ただ、その意図には中国包囲網的な戦略も含まれており、陣営ごとの分断を助長する可能性も高い。日本はCBPRにプラスアルファすることで、アジア太平洋地域とEUの越境データ移転を可能にできないかを模索しているが、相違が大きくハードルは高い。

法制度の違いを乗り越えようとする試みとは別に、国際標準規格による認証によって企業間でのデータ流通を確保しようとする動きも加速している。特にISO（International Organization for Standardization、国際標準化機構）およびIEC（International Electrotechnical Commission、国際電気標準会議）による標準規格は、WTO（World Trade Organization、世界貿易機関）のTBT協定（Agreement on Technical Barriers to Trade、貿易の技術的障害に関する協定）により、加盟国が国内の規格を定めるときに国際標準規格に準じることが求められるため、各国が国際連携の認証基盤として重視する傾向が強まっている。

近年普及が著しいISMS（Information Security Management System、情報セキュリティマネジメントシステム）を代表とするISO/IEC 27000シリーズに、個人情報を取り扱う場合の拡張管理策としてISO/IEC 27701が2019年に発行され、認証も始まっている。これにより、グローバルにおけるPIMS（Personal Information Management System、個人情報マネジメントシステム）としての普及が有望視されている。さらに、ISO/IEC 29134（プライバシー影響評価）が2017年に発行され、日本でもJIS X 9251としてJIS化している。日本提案のISO/IEC 29184（オンラインのプライバシー通知と同意）も2020年6月に発行されており、企業間での認証に必要な主要なものはそろいつつある。

これ以外にも多くの標準化が各国から提案されているが、特に米国と中国が積極的であり、主導権争いの様相を呈している。両国とも他国に比べ

て国内における標準化の整備が早く、前述のように米国はNISTドキュメントの国際標準化、中国はGB規格と呼ばれる国家標準規格の国際標準化を目指している。

中国はサイバー空間主権主義の下、個人を管理しようとする考え方に基づき、ガバメントアクセスを標準化しようとするもくろみが見え隠れする。特にCOVID-19のパンデミックに対するパブリック・ヘルス・エマージェンシー（公衆衛生上の緊急事態）という名目で、スマートシティをはじめとする様々な分野での個人情報の取得と利用、越境ECにおける個人の評価システムなど多数提案している。公衆衛生上の緊急事態におけるガバメントアクセスについては、2020年11月に国連をはじめとする関連機関などによる共同声明（Joint Statement on Data Protection and Privacy in the COVID-19 Response）[16]が発表されている。概要は、緊急事態の期間は目的を限定した最小限のデータを利用し、緊急事態終了後はデータの廃棄を行うこと、およびそのような仕組みとなることを保証するメカニズムや手順を整えることなどである。この指針が今後の基本線として認識されていくものと思われる。

■最後に

個人情報の取り扱いやプライバシーの保護に関する考え方は、先進国ではOECD（Organisation for Economic Co-operation and Development、経済協力開発機構）の8原則がベースとなるものの、グローバル全体で統一されたものはないとみられる。さらに、文化的な背景だけではなく政治や経済、安全保障にも影響を及ぼすことから、国ごとの法制度の整備は分断を助長する傾向を強めている。一方でグローバルでのデータ流通に対する需要は高まっており、データ主体（本人）との同意関係をベースとする個人情報の取り扱いについて、企業や事業単位での取り組みを標準化し、相互認証する仕組みが急速に進んでいる。

ただ、個人情報の取り扱いを規定するだけでプライバシーが保護されるわけではないという考えも広がってきており、EUは基本的人権、米国は消費者保護という観点からアウトカムベース、リスクベースでの制度化を加速しつつある。日本でも、経済産業省と総務省が共同で『DX時代における企業のプライバシーガバナンスガイドブック』を2020年8月に発行した[17]。本書では個人情報保護に限られないプライバシー保護が企業の社会的信頼を得るために重要であるとしており、今後、制度化も含めた議論が活発化すると思われる。

以上を俯瞰すると混とんとした様相のようだが、プライバシー保護における複雑な要素が個々に分解されつつあり、各要素の方向性も現れ始めている。国ごとの思惑の違いにより、分断が加速するのか一定の方向に再構成されるかは、今のところ見通せない。しかし、COVID-19のパンデミックがプライバシーに関して一般の人にも考える機会を提供し、規制側の考え方の違いを浮かび上がらせたことは間違いなく、すでに様々な動きが顕在化しつつある。今後は国家も産業界も受動的に動向を注視するのではなく、積極的に働きかけていくことで自らの立場を確保していく流れが顕著になると考えられる。

1. California Consumer Privacy Act (CCPA)（https://oag.ca.gov/privacy/ccpa/）
2. 中国サイバーセキュリティ法（http://www.cac.gov.cn/2016-11/07/c_1119867116.htm）
3. TCF – Transparency & Consent Framework（https://iabeurope.eu/transparency-consent-framework/）
4. Text - S.2968 - 116th Congress (2019-2020): Consumer Online Privacy Rights Act（https://www.congress.gov/bill/

116th-congress/senate-bill/2968/text/）

5. Text - S.4626 - 116th Congress (2019-2020): SAFE DATA Act（https://www.congress.gov/bill/116th-congress/senate-bill/4626/text/）
6. Privacy Framework（https://www.nist.gov/privacy-framework ）
7. SP 800-53 Rev. 5, Security and Privacy Controls for Info Systems and Organizations（https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final）
8. Cybersecurity Framework（https://www.nist.gov/cyberframework）
9. 政府情報システムのためのセキュリティ評価制度（ISMAP）（https://www.ipa.go.jp/security/ismap/）
10. OSCAL（https://pages.nist.gov/OSCAL/）
11. 中国民法典（http://www.npc.gov.cn/npc/c30834/202006/75ba6483b8344591abd07917e1d25cc8.shtml）
12. 中国電子商取引法（http://www.npc.gov.cn/zgrdw/npc/lfzt/rlyw/2018-08/31/content_2060827.htm）
13. 国家規格「個人情報安全規範」2020版が正式にリリース（https://www.secrss.com/articles/17713 ）
14. Text - H.R.4943 - 115th Congress (2017-2018): CLOUD Act（https://www.congress.gov/bill/115th-congress/house-bill/4943/text）
15. Cross Border Privacy Rules System（http://cbprs.org/ ）
16. Joint Statement on Data Protection and Privacy in the COVID-19 Response（https://www.un.org/en/coronavirus/joint-statement-data-protection-and-privacy-covid-19-response/）
17. 企業のプライバシーガバナンスモデル検討会（http://www.iotac.jp/wg/data/govenance/）

インターネット白書 ARCHIVES

1996,1997,1998,1999,2000....

［インターネット白書ARCHIVES］ご利用上の注意

このファイルは、株式会社インプレスR&Dが1996年～2021年までに発行したインターネットの年鑑『インターネット白書』の誌面をPDF化し、「インターネット白書ARCHIVES」として以下のウェブサイトで公開しているものです。

https://IWParchives.jp/

このファイルをご利用いただくにあたり、下記の注意事項を必ずお読みください。

- 記載されている内容（技術解説、データ、URL、名称など）は発行当時のものです。
- 収録されている内容は著作権法上の保護を受けています。著作権はそれぞれの記事の著作者（執筆者、写真・図の作成者、編集部など）が保持しています。
- 著作者から許諾が得られなかった著作物は掲載されていない場合があります。
- このファイルの内容を改変したり、商用目的として再利用したりすることはできません。あくまで個人や企業の非商用利用での閲覧、複製、送信に限られます。
- 収録されている内容を何らかの媒体に引用としてご利用される際は、出典として媒体名および年号、該当ページ番号、発行元（株式会社インプレスR&D）などの情報をご明記ください。
- オリジナルの発行時点では、株式会社インプレスR&D（初期は株式会社インプレス）と著作権者は内容が正確なものであるように最大限に努めましたが、すべての情報が完全に正確であることは保証できません。このファイルの内容に起因する直接的および間接的な損害に対して、一切の責任を負いません。お客様個人の責任においてご利用ください。

お問い合わせ先 | 株式会社インプレスR&D | ✉ iwp-info@impress.co.jp