TECH, IP AND TELECOMS LAW UPDATES

2024 年 11 月号（Vol.12）

弁護士　岡田 淳
TEL. 03 5220 1821
atsushi.okada@mhm-global.com

弁護士　蔦 大輔
TEL. 03 6266 8769
daisuke.tsuta@mhm-global.com

弁護士　呂 佳叡
TEL. 03 6266 8995
kaei.ro@mhm-global.com

弁護士　輪千 浩平
TEL. 03 6266 8750
kohei.wachi@mhm-global.com

弁護士　佐藤 真澄
TEL. 03 5293 4915
masumi.sato@mhm-global.com

弁護士　棚良 拡
TEL. 03 6266 8771
hiromu.nagira@mhm-global.com

1. ダークパターンに関する近時の動向ー総務省：「スマートフォン プライバシー イニシアティブ」改定などー

近年、「ダークパターン」と呼ばれる、ユーザーを欺いたり操作したりしてユーザーの選択を損ない、又は歪める手法に関する問題意識が高まっており、欧米では、EU の DSA（Digital Services Act）などの法令による明示的な禁止、EDPB（欧州データ保護会議）、米国 FTC（連邦取引委員会）、OECD（経済開発協力機構）といった各国の機関によるガイドラインや報告書が策定され、執行も行われています。

こうした動向を踏まえ、日本でも政府の各種ガイドライン・文書において、ダークパターン回避のための注意喚起等が行われています。2024 年 11 月 8 日までパブリックコメントにかけられていた、総務省「利用者情報に関するワーキンググループ報告書（案）」中の「スマートフォン プライバシー イニシアティブ」改定案（改定後のタイトルは「スマートフォン プライバシー セキュリティ イニシアティブ」）では、利用者情報の取扱いに関するダークパターンの具体的な事例を挙げ、アプリ提供者等はダークパターンを回避することが望ましい旨記載されています。2024 年 10 月 31 日に改正された総務省「電気通信事業法の消費者保護ルールに関するガイドライン」においても、対象となる電気通信役務の利用契約に関してウェブページで基本説明事項の確認やプラン選択が行われる場合にダークパターンとならないよう留意することが求められるとして、ウェブページのデザイン等の望ましい例と不適切な例を掲載しています。

また、2024 年 10 月 17 日に公表された内閣府消費者法委員会「消費者法制度のパラダイムシフトに関する専門調査会 中間整理」においては、デジタル取引におけるダークパターンの拡大・深刻化を指摘し、悪質な行為に対する厳格な対応、及び健全な事業活動を促進するインセンティブを設計する等のメリハリの利いた規律の在り方を検討

することや、実効的なエンフォースメントの観点から、越境取引や多数の海外デジタルプラットフォームの存在を踏まえた対応を検討することの重要性を提言し、さらに、消費者団体をはじめとする多様な団体の活躍への期待が述べられています。

民間の取組としては、2024 年 10 月に一般社団法人 ダークパターン対策協会が発足しました。同協会では、ガイドライン策定や、ダークパターンではない Web サイトを審査して認定する NDD（Non-Deceptive Design）認定制度を実施する予定としており、今後の活動が注目されます。

2. AI に関する政策アップデート

AI に関する法規制の動向について、様々な法分野においてアップデートがありました。

2024 年 10 月 2 日、公正取引委員会がディスカッションペーパー「生成 AI を巡る競争」を公表し、生成 AI 関連市場の実態を把握するため、広く情報・意見を募集しました。当該ディスカッションペーパーは、生成 AI 関連市場の市場構造を、インフラストラクチャー（計算資源、データ、専門人材）、モデル、アプリケーションに分けたうえで、生成 AI を巡る独占禁止法、競争政策上論点となり得る点を複数取り上げています。具体的な論点としては、アクセス制限・他社排除、自社優遇、抱き合わせ、生成 AI を用いた並行行為、パートナーシップによる高度専門人材の獲得といったテーマを掲げています。今後、提出された情報等を踏まえ、公正取引委員会は、適時に事実関係を整理したうえで、必要に応じて独占禁止法・競争政策上の考え方を示すこととしています。現時点ではいまだ調査段階であり、公正取引委員会が今後どのような対応をとっていくかについては十分な予測が難しい状況ですが、公正取引委員会の動向を注視する必要があります。

また、2024 年 11 月 15 日、「AI 時代の知的財産権検討会『中間とりまとめ』―権利者のための手引き―」が内閣府知的財産戦略推進事務局から公表されました。これは同年 5 月に AI 時代の知的財産権検討会がまとめた中間とりまとめのポイントを、権利者の視点から解説をしたものとなります。この手引きにおいては、権利者が AI 学習用にデータを提供したい場合、あるいは、AI 学習に利用されるのを避けたい場合などについて、権利者が取るべき法的、技術的、契約的な対応方法について整理をしています。例えば、AI 学習に利用されることを防ぐための技術的措置としては、クローラによる収集を拒絶するために robot.txt をウェブサイトに設定すること、学習を妨害するノイズを画像に付与しておくことなどが挙げられています。なお、中間とりまとめと同様、この手引きは法的な拘束力を有するものではありません。

その他にも、2024 年 10 月 30 日、経済産業省の下で、AI 利活用に伴う契約時の留意事項検討会が開催されました。同検討会は、今後 AI 利活用に関する契約を締結する際に留意すべき事項のチェックリストの内容について議論をすることが予定されています。チェックリストの最終版は 2025 年 1 月以降に公開される予定です。

加えて、特許庁においては、生成 AI を用いて、大量のデザインや発明品が公開され

た場合であってもなお、正規の発明者等の権利を保護することができるようにするため、今後、意匠法と特許法について必要な法整備について議論を進めていくことが予定されています。今後も各省庁や業界団体などから AI の利活用に伴って発生する問題に対処するため、法改正やガイドラインなどの制定が続くことが予想されます。AI を巡る法規制、ガイドライン等の制定動向についてタイムリーに確認をすることが必要です。

3. 金融庁:「金融分野におけるサイバーセキュリティに関するガイドライン」の公表

金融庁は、2024 年 10 月 4 日に、「金融分野におけるサイバーセキュリティに関するガイドライン」を公表しました。2024 年 6 月 28 日から 7 月 29 日にかけて、ドラフトについて意見募集が実施され、意見募集の結果、若干の補足説明や脚注が追加されましたが、内容について本質的な変更はありません。

このガイドラインは、3 つの節から構成され、特に第 2 節「サイバーセキュリティ管理態勢」では、ガバナンス、特定、防御、検知、対応、復旧、サードパーティリスク管理のそれぞれについて、金融機関等における「基本的な対応事項」及び「対応が望ましい事項」を明確化しています。

いずれについても、一律の対応を求めるものではなく、金融機関等が、自らを取り巻く事業環境、経営戦略及びリスクの許容度等を踏まえた上で、サイバーセキュリティリスクを特定、評価し、リスクに見合った低減措置を講ずること（いわゆる「リスクベース・アプローチ」を採ること）が求められることに留意が必要であるとしています。

なお、このガイドラインの詳細については、データ・セキュリティ / FINANCIAL REGULATION BULLETIN「金融分野におけるサイバーセキュリティに関するガイドライン」（2024 年 10 月号）もご参照ください。

4. セキュリティ要件適合評価及びラベリング制度（JC-STAR）の公表

情報処理推進機構（IPA）は、2024 年 9 月 30 日に「セキュリティ要件適合評価及びラベリング制度」（JC-STAR: Labeling scheme based on Japan Cyber-Security Technical Assessment Requirements）（本制度）を公表しました。本制度は、経済産業省が同年 8 月に公表した「IoT 製品に対するセキュリティ適合性評価制度構築方針」に基づくもので、調達者が、自らが求めるセキュリティ水準の IoT 製品を容易に選定できるようにするとともに、適切なセキュリティ対策が講じられた IoT 製品が普及する仕組みを構築することを目的としています。

主目的及び概要

本制度の主な目的は以下の 3 つです。

①政府機関や企業等で調達する製品について、共通的な物差しで製品のセキュリティ

機能を評価・可視化すること

②特定分野において、セキュリティが確保された IoT 製品のみが採用されるようにすること

③IoT 製品を輸出するベンダーの負担軽減のため、諸外国の制度と相互承認を図ること

対象製品と適合性評価レベル

本制度では、消費者向け・企業向けを問わず、幅広い IoT 製品が対象とされ、以下の適合基準のレベルが設定されています。

★1：IoT 製品共通の最低限の脅威に対応するための共通の適合基準・評価基準

★2～★4：IoT 製品類型ごとの特徴に応じた適合基準・評価基準

★1 及び★2 については、制度の普及促進のため、ベンダーによる自己評価等を通じた自己適合宣言とされ、★3 及び★4 については第三者認証とされています。

適合基準

要求される適合基準は、ETSI EN 303 645 や NISTIR8425 等の国内外の規格とも調和させつつ、独自に定められます。本制度の公表とともに★1 レベルの適合基準・評価方法（JST-CR-01-01-2024）が定められており、不正アクセスによる情報漏えいや機能異常、通信の盗聴、廃棄機器からの情報漏えい、停電等発生時の機能異常等が、★1 で考慮すべき脅威として挙げられています。

JC-STAR の公表及び今後の導入スケジュール

適合製品には二次元バーコード付きのラベルが付与され、適合評価等の情報を容易に取得できるようになります。★1 については、2025 年 3 月から申請受付を開始予定であり、★2 以上については、一部の製品類型を対象として 2025 年度下期以降の制度の開始が目指されています。

諸外国の取り組み状況

英国、米国、EU でも同様の評価制度の検討・導入が進行中であり、日本の制度との相互承認が重要となります。英国では、法的な義務付けを伴う PSTI 法が 2024 年 4 月に施行され、米国では、任意制度である U.S. Cyber Trust Mark が 2024 年中に運用開始される予定です。また、EU では、2024 年 10 月に、法的な義務付けを伴う Cyber Resilience Act が採択され、成立しました。

なお、本制度に関しては、2024 年 11 月 6 日に、経済産業省が「特定分野システムの IoT 製品における JC-STAR 制度活用ガイド（1.0 版）」を公表していますので、併せてご参照ください。