

TECH, IP AND TELECOMS LAW UPDATES

2023年9月号 (Vol.5)

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 榑良 拓 TEL. 03 6266 8771 hiromu.nagira@mhm-global.com	

1. 総務省：「Web3 時代に向けたメタバース等の利活用に関する研究会」報告書の公表
2. 経済産業省：「ソフトウェア管理に向けた SBOM（Software Bill of Materials）の導入に関する手引」の策定
3. 総務省：「ICT サイバーセキュリティ総合対策 2023」の公表

平素は格別のご高配を賜り、厚く御礼申し上げます。

このたび、森・濱田松本法律事務所では、テクノロジー・知的財産、電気通信における最新情報を集めて、「TECH, IP AND TELECOMS LAW UPDATES」9月号 (Vol.5) を作成いたしました。実務における一助となれば幸いに存じます。

1. 総務省：「Web3 時代に向けたメタバース等の利活用に関する研究会」報告書の公表

2023年7月18日、総務省は、「Web3 時代に向けたメタバース等の利活用に関する研究会」においてとりまとめられた[報告書](#)を、パブリックコメントの結果とともに公表しました。この報告書は、2022年8月から約1年かけて行われた当該研究会での議論をまとめたもので、メタバースの利活用に向けた現状及び今後の課題、課題解決の方針が整理されています。

当該報告書が取り上げているメタバース等の発展に向けた課題は、多岐に亘りますが、例えば、アバターに関する権利性の問題やプラットフォーム事業者等の責任、メタバース空間内で生成されたデータの取扱いの問題などが検討されています。当該報告書においては、こうした課題の解決にあたっては、イノベーションを阻害しないように、メタバース関連サービス提供者向けガイドラインを策定することが、課題解決の一つの方向性として提起されており、注目に値します。メタバースを巡る課題については、引き続き法的整理が不明確な部分も多く残されていますが、官民間問わず、現在様々な関係者による課題の解決に向けた取組みが進められていることから、引き続き最新の動向をフォローしていくことが必要といえるでしょう。

TECH, IP AND TELECOMS LAW UPDATES

2. 経済産業省：「ソフトウェア管理に向けた SBOM（Software Bill of Materials）の導入に関する手引」の策定

経済産業省は、2023年7月28日、「[ソフトウェア管理に向けた SBOM（Software Bill of Materials）の導入に関する手引](#)」を公表しました。この手引きは、「[サイバー・フィジカル・セキュリティ確保に向けたソフトウェア管理手法等検討タスクフォース](#)」における検討結果を踏まえたものです。

製品に使用されているソフトウェアに対するセキュリティ上の脅威が増大している一方で、製品にはコンポーネントを含め多種多様なソフトウェアが含まれており、それを全て把握することが困難という課題があります。近年では、2021年12月にJavaベースのオープンソースのロギングライブラリである「Apache Log4j」に関する脆弱性が発見され、国内でも大きな影響がありました。

こうした背景もあり、ソフトウェアの脆弱性対応及びライセンスの管理のため、ソフトウェア部品表とも呼ばれる SBOM（Software Bill of Materials）を用いた管理手法が注目されています。この手引きは、SBOM のメリットや導入に当たって認識／実施すべきポイントをまとめたものです。

SBOM は、ソフトウェア業界はもちろん、自動車業界や医療業界でも活用の検討が進んでいます。2023年3月31日厚生労働省通知「[医療機器のサイバーセキュリティ導入に関する手引書の改訂について](#)」に添付された「医療機器のサイバーセキュリティ導入に関する手引書（第2版）」においても、SBOM の取扱いに関する記述があります。

今後、法令に基づく義務として SBOM の作成が必要となる可能性がありますので、SBOM を取り巻く制度については今後も注目が必要です。

3. 総務省：「ICT サイバーセキュリティ総合対策 2023」の公表

総務省は、2023年8月10日、サイバーセキュリティに係る課題や情報通信分野において講ずべき対策等をまとめた「[ICT サイバーセキュリティ総合対策 2023](#)」を公表しました。「総合対策 2023」では、①情報通信ネットワークの安全性・信頼性の確保、②サイバー攻撃への自律的な対処能力の向上、③国際連携の推進、④普及啓発の推進を柱として、総務省が今後重点的に取り組むべき施策を示しています。

このうち、①に関して、サイバー攻撃に悪用されるおそれのある IoT 機器の調査及び当該機器の利用者への注意喚起を行う取組みである「[NOTICE](#)」の継続的な実施や拡充が掲げられています。NOTICE とは、総務省、国立研究開発法人情報通信研究機構（NICT）及びインターネット・サービス・プロバイダ（ISP）が連携し、NICT がインターネット上の IoT 機器に対して、容易に推測されるパスワード等を入力することなどにより、サイバー攻撃に悪用されるおそれのある機器を調査し、当該機器の情報を ISP に通知し、ISP が NICT から受け取った情報を基に当該機器の利用者を特定し、注意喚起を行う仕組みです。「総合対策 2023」では、具体的に、(i)脆弱性等のある IoT 機器の調査につい

TECH, IP AND TELECOMS LAW UPDATES

て、NOTICE の枠組みを活用した調査を延長・拡充すること、(ii)利用者への注意喚起等の実効性を向上させるため、情報発信・周知啓発を強化すること、(iii)メーカーや Sier 等の幅広い関係者との連携による総合的な対処を効果的に実施すること、(iv)NOTICE の運営体制を強化するため、司令塔としての役割を担う体制（NOTICE ステアリングコミッティ）を整備・確立することなどを挙げています。

(i)に関し、NOTICE は、国立研究開発法人情報通信研究機構法（NICT 法）の 2018 年の改正により、2024 年 3 月までの期間限定の措置として導入されたもの（NICT 法附則 8 条 2 項）でしたが、今後、期間延長等のための法改正が予想されます。