西村あさひ法律事務所

TCOR (Terrorist Content Online Regulation)の施行

個人情報保護・データ保護規制ニューズレター　2022 年 11 月 22 日号

執筆者:
E-mail 岩瀬　ひとみ
E-mail 菊地　浩之
E-mail 河合　優子
E-mail 村田　知信
E-mail 五十嵐　チカ
E-mail 松本　絢子
E-mail 菅　悠人
E-mail 佐々木　将也

目次

Ⅰ　TCOR (Terrorist Content Online Regulation)の施行

はじめに

2022 年 7 月 7 日、テロ関連コンテンツ規則(Regulation on preventing the dissemination of terrorist content online (TCOR))[1]が施行された。同規則は、オンライン上のテロ関連コンテンツの拡散を防止することを目的とし、EU 域内で一定のサービスを提供するホスティングサービス提供者に対して新たな義務を課すものである。この中では、一定の要件を満たすホスティングサービス提供者は、EU 加盟国による通知後 1 時間以内にテロ関連コンテンツの削除等をしなければならないとされている。また、違反した場合の制裁の内容については、EU 加盟国が詳細を定めるものとされているが、削除等をしない場合、最大で全世界売上高の4%もの制裁金が課され得る等、GDPR と同等の水準の制裁が規定されるものと見込まれる。

本稿では、TCOR の概要及び日系企業にとって特に注意すべきと思われる点について、簡潔に紹介する。加えて、TCOR と EU のデジタルサービス法(Digital Service Act (DSA))[2]との関連性や、米国における関連規制の動向についても簡単に触れることとする。

1.　適用対象者

TCOR は、EU 域内で情報社会サービス(information social service)[3]を提供するホスティングサービス提供者(hosting service

---

1　Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online 参照。

2　DSA は、安全、予測可能かつ信頼できるオンライン環境の整備を目的とした規則(Regulation)として、2022 年 10 月 27 日に EU 官報に掲載された(*Publications Office (europa.eu))。同年 11 月 16 日付けで発効し、2024 年 2 月 17 日から施行されることになる(DSA93 条 2 項。ただし一部の条文については別途の施行日が定められている)。DSA(案)の概要については、当事務所ヨーロッパニューズレター2022 年 8 月 25 日「デジタルサービス法案(Digital Services Act)の概要及び日本への影響」参照。

3　情報社会サービスとは、通常、有償で、隔地間で、電子的手段によって、サービス受領者の個別の要求に応じて提供されるあらゆるサービスをいう(Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services 1 条 1 項(b))。

provider)に適用される(1 条 2 項)。適用の有無を判断するうえで特に重要となる要件は、以下(1)及び(2)である。

(1) 保存及び公衆への伝播

TCOR 上、ホスティングサービス提供者は、コンテンツ提供者[4]の要求により、提供された情報を保存(storage)する者と定義されている(2 条 1 項)。ここで「保存」とは、物理的なメモリ又は仮想的なサーバーにデータを保持することを意味しており、したがって、単なる導管(mere conduit)やキャッシング(caching)等、インターネットインフラの他の層で提供され保存を伴わないサービスは TCOR の適用対象とはならない(前文(13))。

「コンテンツ提供者の要求」との要件については、TCOR 上必ずしも明確な定義は与えられていないものの、コンテンツ提供者から直接要求を受ける立場になくかつコンテンツ提供者に間接的にしか利益をもたらさないサービス(例:クラウドインフラ)の提供者は TCOR の適用範囲外であるとされている点が参考になる(前文(14))。

そして、そのようなホスティングサービス提供者のうち、TCOR の適用対象となるのは、上記のように保存された情報を公衆へ伝播(dissemination to the public)するものであるとされている(2 条 1 項)。ここでいう「公衆への伝播」とは、情報が潜在的に無制限の者に対して利用可能となることをいい(2 条 3 項)、当該情報に対して現にアクセスがあったか否かは問題とされていない。また、「無制限」という点については、仮に当該サービス上の情報に到達するために登録・承認のプロセスが設定されている場合であっても、そのような登録が自動的に行われる場合や、誰を承認するかについて人為的な決定が介在していないような場合には、当該情報は公衆に伝播したとみなされる(前文(14))。そして、以上のように公衆への伝播が要件とされていることから、E メールやプライベートメッセージサービスといった個人間でのコミュニケーションサービス(interpersonal messaging service)[5]は TCOR の適用対象外とされている(前文(14))。

したがって、TCOR の適用対象となるサービスの具体例としては、SNS、映像・画像・音声共有サービス、ファイル共有サービス、レンタルサーバーなどが想定される[6](前文(14))。

(2) EU との実質的な関連性

EU 域内においてサービスを提供するホスティングサービス提供者のうち、TCOR の適用対象となるのは、一つ又は複数の EU 加盟国との間に実質的関連性(substantial connection)を有するものに限定される(2 条 4 項)。この実質的関連性が認められる具体例としては、以下①乃至③が挙げられている(2 条 5 項)。

① ホスティングサービス提供者の拠点が EU 域内に存在する場合
② ホスティングサービスのユーザーが EU 加盟国内に相当数存在する場合
③ ホスティングサービスが一つ又は複数の EU 加盟国を対象とする場合

これらのうち、②「相当数」や③「対象とする」の意義については TCOR 上必ずしも明確にされてはいないものの、TCOR 同様 EU 内のホスティングサービス提供者を規制する DSA における解釈が参考になるものと思われる。すなわち、DSA においては、「相当数(のサービス受領者)」は、当該 EU 加盟国の人口に応じて相対的に決定されるとされ、また、「対象とする」か否かを判断するに際しては、当該サービスが当該 EU 加盟国において使用されている言語及び通貨、製品・サービスの受発注の可能性、使用されているトップレベルドメインなどの事情が考慮されると規定されているところ(DSA 前文(8)、2 条(e))、当該判断枠組みは、TCOR の下においても同様に妥当する可能性が高いと考えられる。

なお、後述のとおり、EU 域内に主たる拠点を有しないホスティングサービス提供者は、EU 加盟国内に EU 代理人を選任しなければならない。

---

4 「コンテンツ提供者」(content provider)とは、サービスのユーザーであって、ホスティングサービス提供者によって保存され又は公衆へ伝播される情報を提供した者をいう(2 条 1 項)。

5 Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code 2 条 5 項参照。

6 なお、ホスティングサービス提供者が複数のサービスを提供している場合には、上記の要件に該当するサービスのみが TCOR の適用対象となる(DSA 前文(15))。

2. 適用対象となるコンテンツ

(1) テロ関連コンテンツ

TCOR は、オンライン上のテロ関連コンテンツ(terrorist content)に対して適用される。「テロ関連コンテンツ」とは、大要、以下①乃至③を内容とする資料・データを意味する(2 条(7)[7])。

① テロ犯罪(生命身体に対する攻撃、誘拐略取、政府公共関係施設の大規模破壊行為、交通機関の乗っ取り、爆発物又は武器の製造・所持・取得・移転・供給・使用(R&D 含む)、ライフラインの妨害若しくは違法なシステム障害の惹起)を煽動又は勧誘するもの
② テロリストグループの活動への参加を勧誘するもの
③ ①のテロ犯罪に関与・貢献する目的で、爆発物等の有害物質その他の技術について指導するもの

(2) 除外事由及び判断枠組み

表現の自由への配慮から一定の除外事由が規定されている。具体的には、教育、報道、芸術若しくは研究を目的とするもの又はテロ対策を目的とするものについては、TCOR の適用対象から除外され(1 条 3 項)、この除外事由に該当するか否かは、伝播の真の目的及び現にそのような目的のために伝播されているかという観点から判断される(同条)。

判断枠組みの全体像は以上のとおりであるが、テロ関連コンテンツの外縁は必ずしも明確とはいえないように思われる。例えば上記②については、テロリストグループがプロパガンダとして使用している画像・映像がコラージュされ拡散されるといった事例も想定され得るところ、そのような拡散行為がテロリストグループの活動への参加を勧誘するものであるか、それとも単なるユーモアを目的としたものなのか、判断に窮する場面もあり得る。また、仮にユーモアを目的としたものであると認定されたとしても、それが上記除外事由のいずれに該当するのかは必ずしも判然としない[8]。実務上、TCOR の適用対象となるホスティングサービス提供者は、後述する 1 時間以内の削除義務の履行を巡って難しい判断を強いられることも想定され得るように思われる。

3. ホスティングサービス提供者の義務

TCOR の適用対象となるホスティングサービス提供者の義務のうち主要なものとしては、大要、以下(1)乃至(5)が挙げられる。

(1) 1 時間以内の削除又はアクセス遮断

ホスティングサービス提供者は、EU 加盟国の管轄当局[9]から削除命令を受領してから 1 時間以内に、問題となっているテロ関連コンテンツの削除又はアクセス遮断を行わなければならない(3 条 3 項)[10]。削除命令は、ホスティングサービス提供者の主たる拠点又は EU 代理人(17 条)に対して発出され(3 条 5 項前段)、同時に、電子的手段により問い合わせ先に対して転送されるものとされている(3 条 5 項後段)。

また、ホスティングサービス提供者は、削除命令の内容に重大な過誤があるか又は命令を実行するのに十分な情報が記

---

7 また、Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA 3 条(1)も参照。

8 ユーモアの取り扱いの困難性については、TCOR の立案過程において、人権団体により指摘されていた(EU: German Presidency Proposal for Terrorist Content Online Regulation fails to protect freedom of speech - ARTICLE 19 参照)。

9 各 EU 加盟国の管轄当局のリストについては、List of national competent authority (authorities) and contact points (europa.eu) 参照。

10 なお、当該管轄当局が当該ホスティングサービス提供者に対して過去に削除命令を発令したことがない場合には、当該管轄当局は、原則として、削除命令の発出の遅くとも 12 時間前までに当該ホスティングサービス提供者に対して適用可能性のある手続及び期限について情報提供をしなければならないとされている(3 条 2 項)。

載されておらず削除命令を遵守できない場合には、不当な遅滞なく、管轄当局に対してその旨を通知し、必要な求釈明をしなければならない(3 条 8 項)。

そして、ホスティングサービス提供者は、削除命令に基づきテロ関連コンテンツの削除等を行った場合には、当該管轄当局に対して通知するとともに(3 条 6 項)、削除等されたテロ関連コンテンツ及びそれに関連するデータで、行政・司法上の事後審査やテロ犯罪予防のための手続において必要となるものについて、適切な保護措置を施したうえで保存しておく義務を負う(6 条 1 項・3 項)。

(2) 特別措置の実施

ホスティングサービス提供者は、管轄当局により当該ホスティングサービス提供者がテロ関連コンテンツの伝播に悪用されている(exposed to terrorist content)と認定された場合には、そのようなサービスの悪用に対処するための規定を作成し、サービスの利用規約に組み込まなければならない(5 条 1 項・4 項)[11]。また、実際にサービスを提供する際にも、削除やアクセス遮断の実現可能性を担保するためのスタッフの配置やユーザによる報告メカニズムの構築など、具体的な措置を講じることが必要となる(5 条 2 項・3 項)。

(3) 透明性報告書の作成

ホスティングサービス提供者は、その利用規約において、テロ関連コンテンツの伝播に対処するための方針を明確に規定することを義務付けられている(7 条 1 項)。また、ホスティングサービス提供者は、実際に対処措置を講じた場合などには、対処措置の内容などを記載した透明性報告書(transparency report)を年に一度公表することとされている(7 条 2 項・3 項)。

(4) 削除命令に対する異議申立て

ホスティングサービス提供者及びコンテンツ提供者は、削除命令が発出された EU 加盟国の裁判所において、削除命令の適法性等について異議申立てをすることができる(9 条 1 項・2 項)[12]。

また、ホスティングサービス提供者は、特別措置の実施によりコンテンツが削除等されたコンテンツ提供者に対して、削除等に対する異議申立てのメカニズムを構築しなければならない(10 条)。

(5) 問い合わせ先及び EU 代理人の設置

ホスティングサービス提供者は、削除命令に関連する処理のために、問い合わせ先(contact point)を指定又は設置したうえで、その情報を公表しなければならない(15 条 1 項)[13]。

また、EU 域内に主たる拠点を有しないホスティングサービス提供者は、管轄当局により発出される削除命令やその他の決定の受領、遵守及び執行のため、サービスを提供する EU 加盟国に居住又は設立された自然人又は法人を法的な代理人(legal representative(EU 代理人))として選任し、当該 EU 代理人に対して、管轄当局と協力するために必要な権限及び

---

11 なお、上記の認定がされるための要件は、①管轄当局が客観的事情(例:過去 12 か月以内に 2 以上の削除命令を受領していること)により決定し、かつ②当該ホスティングサービス提供者に対して①の決定を通知することであるとされている(5 条 4 項)。

12 なお、ホスティングサービス提供者が主たる事務所又は EU 代理人を置いていない EU 加盟国において削除命令が発出された場合には、当該削除命令の写しが、当該ホスティングサービス提供者が主たる事務所又 EU 代理人を設置する EU 加盟国の管轄当局に対して提出され、その後は当該管轄当局を中心に手続が進行することになる(4 条、越境削除命令手続)。具体的には、ホスティングサービス提供者又はコンテンツ提供者は、当該越境削除命令等を受領してから 48 時間以内に、当該管轄当局に対して、当該削除命令が TCOR 若しくは EU 基本権憲章上の基本権又は自由を重大若しくは明白に侵害するか否かについて審査を請求することができる(同条 4 項)。当該管轄当局は、当該請求を受領してから 72 時間以内に審査し決定しなければならず、審査の結果、削除命令に侵害が認められた場合には、ホスティングサービス提供者は、削除等したコンテンツを直ちに回復させなければならない(同条 7 項)。

13 本稿執筆時点では Regulation on Dissemination of Terrorist Content Online (EU) Removal Order | Facebook や、Terrorist Content Online Regulation | TikTok などの例が見られた。

リソースを提供しなければならない(17 条 1 項・2 項)。

EU 代理人を指名することの実務上の大きな効果の一つは、特別措置(5 条)及び制裁(18 条)の管轄権を限定できることにある。すなわち、EU 域内に主たる拠点を有しないホスティングサービス提供者については、特別措置及び制裁の管轄権は、指名された EU 代理人の居住又は設立されている EU 加盟国のみが有するとされているのに対し(16 条 1 項)、そのようなホスティングサービス提供者について EU 代理人が指名されていない場合には、全ての EU 加盟国が上記の管轄権を有することとされているため(同条 2 項)、EU 代理人の設置の有無は、ホスティングサービス提供者が制裁を受ける可能性及び受けた場合の実務対応に大きく影響するように思われる。

4. 義務違反に対する制裁

TCOR 上の義務を違反するホスティングサービス提供者に対しては、EU 加盟国の管轄当局により、制裁が課され得る。制裁の具体的な内容については、各 EU 加盟国が定めるものとされており(18 条 1 項前段)、各 EU 加盟国に一定の裁量が認められているものの(18 条 2 項)、少なくとも、GDPR83 条 1 項と同様、「効果的、比例的かつ抑止力のあるもの」(effective, proportionate and dissuasive)であることが要求されている(18 条 1 項後段)。

また、テロ関連コンテンツの 1 時間以内の削除義務を長期にわたり遵守しないホスティングサービス提供者に対しては、最大で直前の事業年度の全世界売上高の 4%の額の制裁金が課され得ることが確保されなければならないとされており注意を要する(18 条 3 項)。ここでの「全世界売上高」には、当該ホスティングサービス提供者の売上総額のみならず、親会社及び関連する全ての子会社によって形成される経済単位の稼得した売上総額が算入されることが想定されていると解され[14]、TCOR の上記制裁規定は、GDPR とほぼ同等の水準に達しているともいえる。

5. DSA との関係及び米国における関連規制の動向

(1) TCOR と DSA との関係

DSA 上にも違法コンテンツへの対処するための規定が置かれているが、DSA は TCOR の規定の効力を排除しないとされている(DSA 前文(10)、前文(34)第 2 パラ、2 条 4 項(c))。論理的には、TCOR は DSA の特別法として位置づけられるものと思われる。

DSA 上は、ノーティスアンドアクションメカニズム(利用者からの通知を受け付け、それに応じて一定の行動を起こさなければ免責を受けられなくなる)が採用されているのに対し(DSA16 条)、TCOR 上はそのような枠組みは採られておらず、原則として管轄当局が命令を発することで初めてホスティングサービス提供者の義務が生じることとなる。また、そのような規律が採用されている帰結として、TCOR は、DSA とは異なり、ホスティングサービス提供者の免責枠組みを用意していない。

(2) 米国における関連規制の動向

テロ関連コンテンツを巡るホスティングサービス提供者の責任については、米国においても新たな動向が存在する。米国においては、かねてより米国通信品位法 230 条(c)[15]が、サービス上でやり取りされる第三者の情報から生ずるホスティングサービス提

---

14 29 条作業部会による Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679 によれば、GDPR 上、管轄当局は、効果的、比例的かつ抑止力のある制裁金を課すために、TFEU101 条及び 102 条における事業(undertaking)概念を採用すべきものとされている。そして、そこにいう「事業」とは、CJEU の判例上、事業体の法的地位や資金調達方法にかかわらず、「経済活動に従事する全ての事業体」を含み(Case C-41/90 Höfner and Elsner, para 21, ECLI:EU:C:1991:161)、「法律上、その経済単位が自然人・法人の複数の者から構成されている場合であっても、経済単位を指すものと理解されなければならない」(Case C-217/05 Confederación Española de Empresarios de Estaciones de Servicio, para 40, ECLI:EU:C:2006:784、Case 170/83 Hydrotherm [1984] ECR 2999, paragraph 11, ECLI:EU:C:1984:271)とされる。以上を前提に、TCOR18 条 1 項が、GDPR83 条 1 項と同様、効果的、比例的かつ抑止力のある制裁金を要求していることを考慮すれば、TCOR 上の制裁規定においても、上記の「事業」概念が採用されているものと考えられる。

15 47 USC 230: Protection for private blocking and screening of offensive material (house.gov)参照。

供者の責任を免除してきたが、近時、米国連邦最高裁は、Gonzalez v. Google[16]及び Twitter v. Taamneh[17]の審理を受理した。いずれの事件においても、ホスティングサービス提供者が実装しているアルゴリズムに基づくレコメンデーション機能によりテロ関連コンテンツが利用者に表示されることが問題視されており [18]、このような場面においても同法によるホスティングサービス提供者の免責が認められるかについて判断が示される見込みである。両事件が米国連邦最高裁において審理されることには、テロ関連コンテンツの規制の是非に関する世界的な議論の高まりを看取できるように思われる。

結び

本稿では、TCOR の規制の概要について簡潔に解説した。TCOR のエンフォースメントをめぐっては不透明な部分も少なからず存在し、TCOR 上の義務を一度違反しただけで直ちに満額の制裁金が課されるといったことが想定されるわけではない。とはいえ、制裁の内容を決定するにあたっては、違反の性質、重大性及び期間や、違反が故意にされているか否か、過去の違反歴、さらには管轄当局に対する協力の度合いといった点も考慮されることからすれば(18 条 2 項)、適用を受ける事業者においては、将来的な事業活動を念頭に置いた対策が求められよう。

Ⅱ 個人情報保護・データ保護規制 各国法アップデート

1. 欧州

- 2022 年 10 月 10 日、欧州データ保護評議会(EDPB)は GDPR に基づく個人データ侵害の通知に関するガイドラインのアップデート版ドラフトを公開した。当該ドラフトにおいては、個人データ侵害が発生した際に要求される原則 72 時間以内の通知(GDPR 33 条 1 項)について、単に EU 代理人が存在するのみではワンストップショップシステムは適用されず、当該 EU 代理人の所在する EU 加盟国に対してだけでなく、当該個人データ侵害により影響を受けるデータ主体が居住する加盟国のすべての当局に対して行われる必要があるということが明確化されている(パラグラフ 73)。当該ドラフトが採用された場合、個人データの管理者は広範な通知義務を負うこととなり得るため、GDPR の適用を受ける企業としては注意が必要である。当該ドラフトについては、2022 年 10 月 18 日から 2022 年 11 月 29 日までの期間、パブリック・コメントが募集されている。

- 2022 年 10 月 12 日、デジタル市場法(DMA。当事務所ヨーロッパニューズレター2022 年 9 月 9 日号「デジタル市場法(Digital Markets Act)の成立及び日本への影響」参照。)が EU 官報に掲載された。デジタルサービスを提供する巨大企業を規制する DMA は、2022 年 11 月 1 日付けで発効し、2023 年 5 月 2 日から施行されることとなる(ただし、一部の条文については別途の施行日が定められている。)。
  また、2022 年 10 月 27 日、デジタルサービス法(DSA。当事務所ヨーロッパニューズレター2022 年 8 月 25 日号「デジタルサービス法案(Digital Services Act)の概要及び日本への影響」参照。)が EU 官報に掲載された。DSA は、2022 年 11 月 16 日付けで発効し、2024 年 2 月 17 日から施行されることになる(ただし、一部の条文については別途の施行日が定められている。)。

- 欧州司法裁判所は、2022 年 10 月 20 日、ハンガリーの大手 ISP(管理者)が、サービス提供のために事前に収集した顧客情報のコピーを、サーバーの「技術的エラーのテスト・修正の目的」での処理については顧客の同意を取得していなかったにもかかわらず、サーバーの「技術的なエラーのテスト・修正の目的」で立ち上げた別個のデータベースに保存し処理を継続していた事件において、大要、以下のとおり、判決を下した。

16 Docket for 21-1333 (supremecourt.gov)参照。

17 Docket for 21-1496 (supremecourt.gov)参照。

18 特に、Gonzalez v. Google は、2015 年 11 月のフランス・パリにおける同時多発テロ事件で、当時パリに留学していて事件の犠牲となった米国人留学生の親族が原告となって提起している事件であり、YouTube 上で生成されるコンテンツのレコメンデーションに係るアルゴリズムが、テロ関連コンテンツをもレコメンドする内容となっていたことは違法であり、これによる損害を原告が YouTube を擁する Google に対して請求するものとなっている。

① **GDPR5 条 1 項 b 号の目的限定原則**:サービス提供のために事前に収集した顧客情報を「技術的エラーのテスト・修正目的」で立ち上げた別のデータベースに保存するという追加処理は、それが当該顧客情報が当初収集された際の特定の目的に関連する限り、5 条 1 項 b 号によっては禁止されない。
② **同項 e 号の記録保存制限原則**:上記の追加処理は、同項 e 号の規律に服し、「技術的エラーのテスト・修正」の実行のために必要な期間を超えて行うことはできない。

欧州司法裁判所は、2022 年 10 月 27 日、通信事業者からその加入者の個人データを受領して、電子的に一般公開された電話帳に掲載するベルギーの会社が、加入者から削除要求を受けたにもかかわらず、受領元の通信事業者からの情報に基づき当該個人データを公開の電話帳上に掲載した事案において、大要、以下とおり、判決を下した。

① **ePrivacy 指令における加入者の同意の意味とその対象**:通信事業者や電話帳の発行者が、加入者の個人データを一般に公開された電話帳に掲載するには、当該加入者の「同意」が必要であり(ePrivacy 指令 12 条 2 項、2 条(f)、GDPR95 条)、その「同意」は GDPR4 条 11 号の「同意」と同義である。ただし、当該同意は、当該通信事業者又は電話帳の発行者のいずれかに与えられれば足りる。
② **GDPR17 条の消去の権利**:電話帳から個人データを削除してほしいという加入者の要求は、GDPR17 条の消去の権利の行使として解される。
③ **GDPR5 条 2 項、24 条の管理者の責任**:EU 加盟国の当局は、電話帳の発行者に対して、管理者として、当該発行者に個人データを提供した通信事業者だけでなく、当該発行者が当該個人データを提供した他の電話帳発行者も当該撤回に関する通知を受領するために、適切な技術上及び組織的上の措置を講じるよう求めることができる。
④ **GDPR17 条 2 項の合理的な措置の解釈**:EU 加盟国の当局は、電話帳の発行者に対して、当該発行者が加入者から自己に関する個人データを今後公表しないよう要求された場合、当該要求を検索エンジン事業者に通知するための「合理的な措置(reasonable steps)」を講じるよう求めることができる。

2. ブラジル

ブラジルデータ保護当局(ANPD)は、2022 年 10 月 18 日、Cookie に関するガイダンスを公表した。同ガイダンスには、Cookie Notice や Cookie バナー等についてデータ管理者が採ることを推奨される措置(ベストプラクティス)、Cookie の利用に関する法的根拠等が記載されている。

3. タイ

2022 年 11 月 2 日、データブリーチが発生した場合の個人情報保護法上の報告義務に関するガイドラインの草案がパブリックコメントのために公表された。同草案には、データブリーチ発生時に報告義務の有無を判断するためのリスク評価の方法や報告事項等の詳細が規定されている。

4. オーストラリア

2022 年 10 月 26 日、法務長官は、情報漏洩事故への罰則の強化を含む改正法案(Privacy Legislation Amendment (Enforcement and Other Measures) Bill 2022 (Privacy Bill))を提出し、2022 年 11 月 7 日まで意見募集を行った。同法案は、個人情報の漏洩に対する罰則の強化、個人情報の漏洩事件の対応に関する Australian Information Commissioner(AIC)の権限の強化及び AIC とオーストラリア政府の管轄官庁である Australian Communications and Media Authority(ACMA)が情報を共有する機能の拡張を含むものである。同法案は可決された場合には、ただちに施行される。

当事務所では、クライアントの皆様のビジネスニーズに即応すべく、弁護士等が各分野で時宜にかなったトピックを解説したニューズレターを執筆し、随時発行しております。N&A ニューズレター購読をご希望の方は N&A ニューズレター　配信申込・変更フォームよりお手続きをお願いいたします。また、バックナンバーはこちらに掲載しておりますので、あわせてご覧ください。

本ニューズレターはリーガルアドバイスを目的とするものではなく、個別の案件については当該案件の個別の状況に応じ、日本法または現地法弁護士の適切なアドバイスを求めていただく必要があります。また、本稿に記載の見解は執筆担当者の個人的見解であり、当事務所または当事務所のクライアントの見解ではありません。

西村あさひ法律事務所　広報室　E-mail