ANDERSON MŌRI & TOMOTSUNE

INDIA LEGAL UPDATE

2022 年 9 月 29 日

インド IT 法上のサイバーセキュリティ規則の施行

弁護士 琴浦 諒 / 大河内 亮

インド政府の電子情報技術省(Ministry of Electronics and Information Technology)の機関である Computer Emergency Response Team は、2022 年 9 月 25 日付けで、Information Technology Act 2000 の 70-B 条 6 項に基づき、情報技術を取り扱う事業者(法人、政府機関を含む)が情報セキュリティのために遵守すべき実務及び手続、情報流出等の防止策の策定、サイバー犯罪にあった場合の報告義務等について定めたサイバーセキュリティ規制を全面的に施行しました。

インドのサイバーセキュリティ規則は、日本企業のインド子会社や関連会社のみならず、日本企業自体にも適用がある規制であり、かつインド国内の連絡先(Point of Contact)の CERT-In への通知や、サイバーインシデントが起きた場合の 6 時間以内の CERT-In への報告義務など、日本企業側におけるさまざまなアクションが実際に必要となる規制でもあります。また、違反の場合の罰則規定も定められています。

本ニュースレターでは、インドのサイバーセキュリティ規則の概要と、同規則が日系企業に与える影響について解説します。

1. インドサイバーセキュリティ規則の施行

インド政府の電子情報技術省(Ministry of Electronics and Information Technology)の機関である Computer Emergency Response Team (以下「**CERT-In**」といいます)は、2022 年 4 月 28 日付けで、Information Technology Act 2000(以下「**インド IT 法**」といいます)の 70-B 条 6 項に基づき、情報技術を取り扱う事業者(法人、政府機関を含む。以下「**対象事業者**」といいます)が情報セキュリティのために遵守すべき実務及び手続、情報流出等の防止策の策定、サイバー犯罪にあった場合の報告義務等について定めた通達(Direction)(以下「**インドサイバーセキュリティ規則**」といいます)を発行しました。

インドサイバーセキュリティ規則は、対象事業者においてサイバーインシデント(下記 3(1)参照)があった場合に、そのことを直ちにユーザー、カスタマーに通知すべきこと等を定めた CERT-In の 2021 年 1 月 20 日付け通達に続き、サイバー犯罪に対するインド政府の対策の一環として発行されたものです。

インドサイバーセキュリティ規則は、当初、同規則の通達日の 60 日後の施行が予定されていましたが、対象事業者側の対応が間に合わない等の懸念から、2022 年 6 月 27 日付で CERT-In から発行された通達により、その一部の施行が同年 9 月 25 日まで延期されていました。その後、2022 年 9 月 25 日付けで、インドサイバーセ

キュリティ規則は全面的に施行されました。

2. インドサイバーセキュリティ規則の適用範囲

インドサイバーセキュリティ規則の適用対象となる対象事業者は、同規則の別紙 1 で定義されており、サービスプロバイダやサービス仲介業者、データセンター等の情報技術を専門的に扱う事業者のみならず、一般の法人や政府機関等、広い意味で情報技術を取り扱う者を含むものとされています。そのため、サービスプロバイダやサービス仲介業者、データセンター等でない法人事業者であっても、同法の適用対象となりえます。今日において、ビジネスを行っている法人事業者で、情報技術を取り扱わない事業者はほとんど存在しないと思われるため、実質的にほとんど全ての法人事業者が規制対象となると考えられます。

また、インドサイバーセキュリティ規則は、インド IT 法の施行規則の一種として制定されたものですが、インド IT 法自体が適用対象をインド国内の個人、法人等に限っていないこと、またインドサイバーセキュリティ規則も適用対象を特に限定していないことから、（日本企業のインド子会社や関連会社に限らず）日本に所在する日本企業も適用対象となります。CERT-In のウェブサイト上で公開されている FAQ[1]（以下「**CERT-In FAQ**」といいます）の Q26 にも、その旨が明記されています。

そのため、下記 3 に述べる各種規制については、インドへの輸出、あるいはインドに代理店がある等の形でインドにビジネスを有しており、したがって何らかの形でインドに関わる IT を利用した情報（インド国内の顧客情報、売上情報、流通網に関する情報等）の管理を行っている、またはこれらの情報を有している日本企業も、これを遵守しなければ、インドにおいて、インドサイバーセキュリティ規則に基づく処罰を受ける可能性があることに留意が必要です（下記 4 参照）。

3. インドサイバーセキュリティ規則の概要

（1） サイバーインシデントの報告義務

インドサイバーセキュリティ規則の別紙 1 で規定されているサイバーインシデント（対象事業者の重要な IT ネットワークやシステムに対するスキャニングやプロービング、重要なシステム及び情報の漏洩、IT システムやデータへの不正アクセス、ウェブサイトへの侵入・改ざん、ウィルス等によるコード攻撃、システムへの攻撃等）があった場合、そのようなサイバーインシデントを覚知した対象事業者は、6 時間以内にCERT－In に対して、所定の書式により報告をしなければならないとされています。

この「6 時間以内」という要件については、期限が短すぎて非現実的である、との批判もありましたが、結局そのまま施行されるに至っています。なお、CERT-In FAQ の Q30 によれば、「覚知した時点でわかっていることだけを取り急ぎ報告し、詳細は事後の報告とすることでも構わない」とされています。

また、CERT-In FAQ の Q22 によれば、ユーザーやカスタマーとの契約、規約上、対象事業者が守秘義務を負っている場合であっても、この報告義務は、当該守秘義務に優先するとされています。

（2） Infomration and Communication Technology （ICT） system の時計の同期義務

全ての対象事業者は、インドの National Informatics Centre (NIC)の Network Time Protocol (NTP)と呼ばれるサーバーまたは National Physical Laboratory (NPL)と呼ばれるサーバー等に、対象事業者のInfomration and Communication Technology （ICT） system（以下「**ICT System**」といいます）の時計を同期させな

[1] FAQs_on_CyberSecurityDirections_May2022.pdf (cert-in.org.in)

ければならないとされています。

なお、インド国外の対象事業者については、上記 NIC や NPL と同等の正確な時計を有するサーバーに同期することで、上記義務を代替することができるとされています。

(3) インド国内でのログの保存義務

全ての対象事業者は、その ICT System について、インド国内に過去 180 日分のログを保存しなければならないとされています。このログは、CERT-In から要請があった場合、または当該対象事業者においてサイバーインシデントが起きた場合、CERT-In に提供されなければなりません。

なお、インドサイバーセキュリティ規則上は、「インド国内のログ保存義務」が規定されていますが、CERT-In FAQ の Q35 によれば、日本企業を含む外国の対象事業者については、CERT-In に対して合理的な時間内に報告することができるのであれば、インド国外にログを保存しても構わないとされています。

(4) インド国内の連絡先(Point of Contact)の通知義務

全ての対象事業者は、CERT-In の所定の書式により、CERT-In がコンタクトするためのインド国内の連絡先(Point of Contact)を CERT-In に通知しなければならないとされています。また、代理店の変更や担当者の変更等により、この連絡先に変更があった場合、直ちにその旨を CERT-In に通知しなければならないとされています。

日本企業を含む外国の対象事業者であっても、インドに関わる IT を利用した情報を取り扱っている限りにおいて、インド国内の連絡先(Point of Contact)を CERT-In に報告する必要があります(CERT-In FAQ の Q29 参照)。そのため、たとえば専らインドに対する輸出だけを行っており、インド国内に代理店や子会社・関連会社等が存在しない日本企業の場合であっても、インドに関わる IT を利用した情報(インド国内の顧客情報、売上情報、流通網に関する情報等)の管理を行っている、またはこれらの情報を保有している限り、このインド国内の連絡先(Point of Contact)を CERT-In に通知する義務を負うことに注意が必要です。

(5) データセンター、VPS プロバイダー、クラウドサービスプロバイダ及び VPN プロバイダー、並びにバーチャル資産産業に対する規制

インドサイバーセキュリティ規則は、データセンター、VPS プロバイダー、クラウドサービスプロバイダ及び VPN プロバイダーを営む業者や、暗号資産や仮想通貨等のバーチャル資産産業を営む業者など、特定の対象事業者に対し、通常の対象事業者とは異なる、一定の厳格な規制を定めています。

以上の他、インドサイバーセキュリティ規則については、CERT-In FAQ に詳細な FAQ が記載されているため、こちらをご参照ください。

4. 違反の場合の罰則

インドサイバーセキュリティ規則上、同規則に違反した対象事業者に対しては、インド IT 法 70-B 条 7 項に基づき、1 年以下の懲役もしくは 10 万ルピー以下の罰金、またはその併科の罰則が課せられる可能性があります。

勿論、インド国内法による罰則規定を日本にいる日本企業にどうやって執行するのか、そもそも実際にインド政府がインド国内法に基づいて外国企業まで処罰しようとするのか(たとえば、上記 3(4)の CERT-In への インド国内の連絡先(Point of Contact)の通知義務に違反している外国企業をどこまで手間とコストをかけて処罰しようと

するのか）等の実務上の問題は数多くあると思われますが、理論上は、日本企業がインドサイバーセキュリティ規則に違反した場合、同規則に基づく処罰を受ける可能性があることに十分に注意が必要です。

5. 日系企業への影響

上に述べたとおり、インドサイバーセキュリティ規則は、日本企業のインド子会社や関連会社のみならず、日本企業本体にも適用がある規制であり、かつインド国内の連絡先（Point of Contact）の CERT-In への通知や、サイバーインシデントが起きた場合の 6 時間以内の CERT-In への報告義務など、日本企業側におけるさまざまなアクションが実際に必要となる規制でもあります。

そのため、インドにビジネスを有する日系企業においては、必要に応じて弁護士等の外部の専門家に相談しつつ、同規制に応じた体制を整備していくことが必要となると思われます。

■ 本ニュースレターの内容は、一般的な情報提供であり、具体的な法的アドバイスではありません。お問い合わせ等ございましたら、下記弁護士までご遠慮なくご連絡下さいますよう、お願いいたします。

■ 本ニュースレターの執筆者は、以下のとおりです。
弁護士　琴浦　諒（ryo.kotoura@amt-law.com）
弁護士　大河内　亮（ryo.okochi@amt-law.com）

■ ニュースレターの配信停止をご希望の場合には、お手数ですが、お問い合わせにてお手続き下さいますようお願いいたします。

■ ニュースレターのバックナンバーは、こちらにてご覧いただけます。