NEWSLETTER

見逃しがち、EUのサイバーセキュリティ法令「NIS2指令」のインパクト：域外適用の可能性、EU域内の現地拠点（特に製造業）への適用可能性につき要確認

ヨーロッパニューズレター　　2025年1月17日号

執筆者:
石川 智也　n.ishikawa@nishimura.com
川島 章裕　a.kawashima@nishimura.com

近時、EU域内の拠点（中でも、これまでGDPRをはじめとするデジタル関連法制のリスクが高くないと思われてきた製造拠点）に、サイバーセキュリティ法令であるNIS2指令の適用があることが判明し、対応に追われるケースが少なくない。NIS2指令とは、EU初のサイバーセキュリティに関する法であるNIS指令（Network and Information Systems Directive）を改訂したもので、適用範囲が従前に比して著しく拡大するとともに、義務の内容も加重されている。EU加盟国は2024年10月17日までにNIS2指令の内容に沿った国内法の整備が義務づけられており、順次国内法の適用が開始されている。以下では、NIS2指令の概要と留意すべきポイントについて説明する。

1. NIS2指令の概要

NIS2指令は、高重要分野（エネルギー、運輸、銀行、金融市場インフラ、保健衛生、飲料水、廃水、デジタルインフラ、ICTサービスマネジメント、行政機関、宇宙）及びその他の重要分野（郵便宅配サービス、廃棄物管理、化学物質の生産、製造及び流通、食品の生産、加工及び流通、製造業（医療機器の製造、コンピュータ、電気製品及び光学製品の製造、電気設備の製造、機械設備の製造、自動車、トレーラー及びセミトレーラーの製造、その他輸送設備の製造、デジタルプロバイダー、研究機関））における事業者を主な適用対象としている。**特に、日系企業においては、製造業においてNIS2指令への対応が必要となる場合があるにもかかわらず、確認がなされていないケースが少なくないように思われる。上記にあてはまる事業を行っている場合には、NIS2指令の適用可能性がないか速やかに確認を行うことが望ましい。**

NIS2指令に基づく国内法の違反に関しては、必須事業者（essential entity）については1000万ユーロ又は事業者が属する事業体（企業グループ等の経済単位）の前年度の全世界売上高の2%のいずれか高い方を上限とする制裁金、重要事業者（important entity）については700万ユーロ又は事業者が属する事業体の前年度の全世界売上高の1.4%のいずれか高い方を上限とする制裁金の規定が定められており、GDPRに匹敵する巨額の制裁金リスクがある。

NIS2指令の適用対象となる事業者は、ネットワーク及びシステムのセキュリティに係るリスクを管理するために適切かつ相当な技術的、運営的及び組織的措置を講じる義務を負う（情報システムセキュリティに関するポリシー、サプライチェーンのセキュリティ等に関する措置）。また、事業者のサービスの提供に重大な影響を及ぼすインシデントが発生した場合には、事業者はCSIRT又は加盟国の監督当局に通知する義務を負う。

2. NIS2 指令の域外適用及び EU 代理人の選任義務

NIS2 指令の適用範囲に関しては、適用対象となる事業者は、原則として、当該事業者の拠点がある加盟国の法令の適用を受ける旨が規定されている。もっとも、下記に該当する事業者は、EU 域内に拠点がない場合でも、EU 域内でサービスの提供を行う場合、EU 域内に代理人（以下「EU 代理人」という）を選任する義務を負う。EU 代理人は、サービスが提供される加盟国のいずれか一つにおいて設置されなければならず、当該事業者は EU 代理人を設置した加盟国の法令の適用を受ける。当該事業者が EU 代理人を設置しない場合、当該事業者によるサービス提供がなされるすべての加盟国が、当該事業者に対して NIS2 指令の違反に対する法的措置を講じることが可能となることに注意が必要である。

- ドメイン名システム（DNS）サービス提供事業者、トップレベルドメイン（TLD）名レジストリ、ドメイン名登録サービス提供事業者、クラウドコンピューティングサービス提供事業者、データセンターサービス提供事業者、コンテンツデリバリーネットワーク提供事業者、マネージドサービス提供事業者（例：ICT 製品等の管理等に関連するサービス提供事業者）、マネージドセキュリティサービス提供事業者、オンラインマーケットプレイス提供事業者、オンライン検索エンジン提供事業者、SNS プラットフォーム提供事業者

3. 欧州委員会による NIS2 指令の実施規則の採択

欧州委員会は、2024 年 10 月 17 日、NIS2 指令に関する初めての実施規則（以下「本実施規則」という）を採択した。本実施規則は、デジタルサービス（クラウドコンピューティングサービス、データセンターサービス、オンラインマーケットプレイス、オンライン検索エンジン、SNS プラットフォーム等）の提供事業者を対象としている。そして、NIS2 指令に規定されるサイバーセキュリティのリスク管理対策や、NIS2 指令の適用対象となる企業におけるインシデントが重大であると判断され、加盟国の監督当局への報告が必要となる事案について、より具体的な内容を規定している。本実施規則は、2024 年 10 月 18 日付けで官報に掲載されており、2024 年 11 月 7 日から発効している。

4. 加盟国法の制定状況及び日本企業における対応

欧州委員会は、国内法の制定期限である 2024 年 10 月 17 日を徒過し、立法手続が遅滞している状況を踏まえ、2024 年 11 月 28 日の時点で国内法を制定していなかった 23 の加盟国（ベルギー、イタリア、クロアチア、リトアニア以外の加盟国）に対して義務違反手続を開始し、2 か月以内に回答を行うよう通知を行った。現時点で国内法が未制定の加盟国においても、ドイツ、フランス、オランダ、ポーランドを含め、国内法の整備が進められている。

上記のとおり国内法の違反に対して巨額の制裁金の規定が定められており、法令違反におけるリスクの高いルールであることから、NIS2 指令に基づくルールの適用開始を踏まえて、日本企業においても適切にコンプライアンス対応を実施していく必要がある。また、EU 域内に拠点がない事業者に関しても、EU 域内で上記の特定のデジタルサービスを提供する場合、域外適用を受け、EU 代理人の選任義務が課されること、そして、EU 代理人を選任しなかった場合には、サービスを提供している全ての加盟国の当局が管轄当局となることに注意が必要である。

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。

西村あさひ 広報課 newsletter@nishimura.com