Atsumi & Sakai Newsletter
JAPAN
NEW YORK
LONDON
FRANKFURT
BRUSSELS
HO CHI MINH

2026 年 4 月 20 日
No.IEU_004

NIS2 指令 ― EU サイバーセキュリティ規制の概要

執筆者：弁護士 金久直樹／弁護士 丸山るり子／弁護士 船橋桃子

I. NIS2指令の概要

2023年1月16日に発効したNIS2指令（Network and Information Security Directive 2）[1]は、EU域内におけるサイバーセキュリティ及びレジリエンスの強化を目的として制定されたEU指令であり、適用対象となる事業者に対して、統一的なリスク管理体制の整備及びインシデント発生時の報告義務等を課している。NIS2指令は、従来のNIS指令を改訂するものであり、適用範囲及び義務内容のいずれについても大幅な拡充が図られている。グローバル展開する日本企業においては、EU加盟国内に存在するグループ会社が小規模であっても、親会社である日本企業の従業員数、売上高、総資産が合算されてNIS2指令の適用の対象となる場合があるため、留意する必要がある。

もっとも、NIS2指令は、EU加盟国の国内法に組み込まれるまで直接的な効力を生じるものではない。そのため、EU加盟国には、2024年10月17日までに同指令を国内法化することが義務付けられていたが、現時点においても、なお国内法の制定が完了していない国が存在する。

本稿では、NIS2指令のポイントを整理するとともに、EU加盟国における国内法制定の状況についても解説する。

II. Q&A

1. NIS2指令の適用対象となるのはどのような事業者か

(1) 原則的な適用対象

NIS2指令は、原則として、①EU域内でサービスを提供し、または事業活動を行い、②「高度にクリティカルなセクター」（NIS2指令付属書Ⅰ）または「その他のクリティカルセクター」（NIS2指令付属書II）に属し、③中規模企業以上に該当する事業者に適用される。ここでいう

[1] https://eur-lex.europa.eu/eli/dir/2022/2555/2022-12-27/eng

©Atsumi & Sakai 2026

中規模企業以上に該当する事業者とは、欧州委員会が2003年5月6日に公表した勧告[2]に定義され、従業員数が50人以上、かつ／または年間売上高もしくは総資産が1,000万ユーロ以上の事業者を指す。なお、③の事業者の規模の算定に関しては、「パートナー企業（partner enterprises）」（ある企業が他社の資本または議決権の25～50%を保有する場合）及び「関連企業（linked enterprise）」（ある企業が他社の資本または議決権の50%超を保有する場合）[3]の従業員数、売上高、総資産は合算して算定される[4]。具体的には、パートナー企業の場合、持分比率に対応する割合（例えば、持分比率が30%のとき、当該パートナー企業の30%分）、関連企業の場合、持分比率にかかわらず当該関連企業の100%分の従業員数、売上高、総資産が合算されることになるため、大規模なグループ企業の場合には、当該加盟国内では小規模な事業しか行っていない子会社であっても当該規模要件を満たし、規制対象となる可能性が高いため、グローバル展開する日本企業は注意が必要である。

(2) 対象となる主な事業分野

NIS2指令付属書I及び同IIに定められる「高度にクリティカルなセクター」及び「その他のクリティカルセクター」とは以下のとおりである。

- 「高度にクリティカルなセクター」：エネルギー、運輸、銀行業、金融市場インフラ、医療、飲料水、排水、デジタルインフラ、ICTサービス管理（BtoB）、公共行政、宇宙
- 「その他のクリティカルセクター」：郵便・物流、廃棄物管理、化学品の製造・生産・流通、食品の生産・加工・流通、特定の製造業（医療機器、コンピューター、電子製品、自動車、その他の輸送機器）、デジタルサービス提供者（オンラインマーケット、オンライン検索エンジン、SNS）、研究

日本企業のEU加盟国内に存在するグループ会社が上記にあてはまる事業を行っている場合、NIS２指令の適用可能性につき早急に確認を行う必要がある。

(3) 規模を問わず適用される事業者

DNSサービス提供者、トップレベルドメイン（TLD）レジストリ、適格トラストサービス提

[2] the Annex to Recommendation 2003/361/EC 第２条(https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32003H0361)

[3] the European Commission’s User Guide to the SME definition (https://www.europeanacademy.com/wp-content/uploads/2021/03/SME_definition_user_guide_en.pdf)

[4] the Annex to Recommendation 2003/361/EC 第２条及び第６条第２項(https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32003H0361)

©Atsumi & Sakai 2026

供者などは、上述の(1)③の企業規模にかかわらずNIS2指令が適用される[5]。

(4) 事業者区分

NIS2指令は、適用対象事業者を「必須事業者（essential entities）」と「重要事業者（important entities）」に区分しており、この区分は、監督の厳格さや制裁内容に影響を及ぼす。一般に、前者については、より厳格な監督及び執行措置が予定されている。必須事業者及び重要事業者は、セクターや事業規模、各国内法における特則を総合的に考慮して分類されるが、必須事業者の典型例は、高度にクリティカルなセクターに従事する大企業（従業員が250人以上、または、売上高が5,000万ユーロ超もしくは総資産が4,300万ユーロ超である場合）であり、重要事業者の典型例は、高度にクリティカルなセクターまたはその他のクリティカルなセクターに従事する中規模企業である。

2. NIS2指令に基づき事業者にはどのような義務が生じるか

(1) 登録義務

NIS2指令の適用対象となる必須事業者及び重要事業者は、事業者の名称や住所、連絡先等を管轄当局へ登録する義務を負い、具体的な登録義務の内容や手続は国内法に定められる。

(2) サイバーセキュリティに関するリスク管理措置

NIS2指令の適用対象事業者は、自社の業務やサービス提供に用いるネットワーク及び情報システムの安全性を確保するため、適切かつ相当で、最新の技術的・運用的・組織的措置を講じなければならない。これには、リスク分析及び情報セキュリティに関する方針の策定、インシデント対応、事業継続計画（インシデント発生時のバックアップ、災害復旧、危機管理）の策定、サプライチェーンにおけるセキュリティ確保、リスクマネジメントの有効性を評価するためのプロセスの実装、多要素認証の導入、暗号技術の使用または暗号化に関する方針及び手順の策定、アクセス制御方針の策定及び資産管理、脆弱性への対処及び開示を含むネットワーク及び情報システムの取得・開発・保守時におけるセキュリティ確保等が含まれる。

これらの措置は、事業者の規模やリスクの性質・深刻度を踏まえ、最新の技術水準に即して講じる必要がある。

(3) 経営層によるガバナンス

NIS2指令は、サイバーセキュリティ対策に関する経営層の関与と責任を強く求めている。具体的には、経営層がサイバーセキュリティに関するリスク管理措置を承認し、その実施状況を

[5] NIS2 指令第 3 条第 1 項(b)

©Atsumi & Sakai 2026

監督する義務を負う。経営層自身の研修参加や、従業員に対する定期的な教育・研修の実施も求められている。ただし、NIS2指令は、EU加盟国が国内法において経営層の責任を確保することを要求しており、EUレベルで直接個人責任を創設しているわけではないことには留意が必要である。

(4) インシデント発生時の報告義務

NIS2指令は、サービス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、管轄当局への迅速な報告を義務付けている。インシデントとは、保存・伝送・処理されたデータ、またはネットワーク・情報システムを通じて提供される、もしくはアクセス可能なサービスの可用性、真正性、完全性、機密性を損なう事象を指す[6]。インシデントが重大であるとは、(i) 当該事業者に対してサービスの深刻な運用障害もしくは財務的損失を引き起こした、または引き起こす可能性がある場合、(ii) 他の自然人もしくは法人に対して相当な物的・非物的損害を引き起こすことにより影響を与えた、または与える可能性がある場合を指す[7]。

NIS2指令は、インシデント報告につき三段階アプローチを採用している。具体的には、①インシデント認識から24時間以内の初期通報、②インシデント認識から72時間以内のインシデント報告、③インシデント報告から1か月以内の最終報告が必要となる。なお、具体的な報告手続や報告経路は国内法により定められる。

3. NIS2指令に違反した場合の罰則にはどのようなものがあるか

NIS2指令に違反した場合には、各加盟国の監督当局により行政処分として制裁が課されることとなり、その制裁金の金額が明確に定められている。必須事業者と重要事業者で基準が異なっており、必須事業者については、当該事業者の全世界売上高（当該事業者が属する企業グループの前会計年度における全世界年間売上高）の2%、または1,000万ユーロのいずれか高いほうが上限とされる[8]。一方、重要事業者については、当該事業者の全世界売上高（当該事業者が属する企業グループの前会計年度における全世界年間売上高）の1.4%、または700万ユーロのいずれか高いほうが適用される[9]。このように、NIS2指令違反の場合には、企業グループの全世界売上高を基準に巨額な制裁金が課される可能性があるため、グローバル展開する日本企業は注意が必要である。なお、各加盟国の国内法が、NIS2指令が要求している最低限の基準を超えて独自の要件や制裁を課すことは可能であることから、上記のNIS2指令で定められている

[6] NIS2 指令第 6 条第 6 項

[7] NIS2 指令第 23 条第 3 項

[8] NIS2 指令第 34 条第 4 項

[9] NIS2 指令第 34 条第 5 項

©Atsumi & Sakai 2026

制裁に加えて、各加盟国の国内法でさらなる制裁が課されている場合もあることに留意が必要である。

4. EU加盟国の国内法の制定状況はどうなっているか

NIS2指令は上述のとおり、2023年1月16日に発効し、EU加盟国は2024年10月17日までにNIS2指令に沿った内容の国内法を整備することが求められていたが、加盟国27カ国のうち23カ国が当該期限までに国内法の整備を完了できず[10]、2025年5月7日時点においても、19カ国が対応を完了していない状況であった[11]。欧州委員会による制裁の対象となることを回避するため、その後各加盟国により整備が進められ、最新の情報によると、2026年3月6日時点において、加盟国27カ国のうち21か国が国内法の整備が完了したとのことであり、いまだ整備が完了しておらず法案段階である加盟国6か国（エストニア・オランダ・アイルランド・フランス・スペイン・ルクセンブルグ）は、急ぎ国内法の整備を進めている状況となっている[12]。

5. EU加盟国の国内法の内容は具体的にはどのようなものか。NIS2指令より厳格化されている国はあるか

上記の通り、加盟国のうち 21 か国において国内法が整備されたが、そのうち以下の 3 か国を例に国内法の内容を検討し、NIS2 指令との相違点等につき言及する。

(1) ベルギー

ベルギーにおいては、2024年4月26日にNIS2指令の国内法[13]が制定され、2024年10月18日に発効した。適用対象となる事業者は、2025年3月18日までに管轄当局に登録しなければならない。ベルギー国内法は、NIS2指令の要件をほぼ踏襲しているが、主に以下の点で若干の相違がある：

- 適用対象：ベルギー国内法では、NIS2指令で定められた対象分野を基礎としつつ、王令（Royal Decree）により、対象となる分野を追加又は拡張することが可能とされている。これにより、将来的に追加の分野が対象とされる可能性がある。
- サイバーセキュリティに関するリスク管理措置：ベルギー国内法は、適用対象となる事業者に対し、「調整された脆弱性開示方針（Coordinated Vulnerability Disclosure Policy）」

[10] https://ecs-org.eu/activities/nis2-directive-transposition-tracker/

[11] https://digital-strategy.ec.europa.eu/en/policies/nis-transposition

[12] https://ecs-org.eu/activities/nis2-directive-transposition-tracker/

[13] https://www.ejustice.just.fgov.be/cgi_loi/article.pl?language=nl&lg_txt=n&type=&sort=&numac_search=&cn_search=2024042619&caller=eli&&view_numac=2024042619nx2024042619fr

©Atsumi & Sakai 2026

の策定及び実施を義務付けている。また、ベルギーの管轄当局であるCentre for Cybersecurity Belgiumは、調整された脆弱性開示の枠組みにおいて、信頼できる仲介機関として機能し得るとされており、脆弱性を報告する個人又は組織と、影響を受ける製品・サービスの製造者又は供給者との間の連絡・調整を促進する役割を担う。

(2) ハンガリー

ハンガリーでは、2024年12月20日にNIS2指令の国内法[14]が制定され、2025年1月1日に発効した。適用対象となる事業者は、2024年12月18日までに管轄当局に登録しなければならない。

ハンガリー国内法においては、主に以下の点でNIS指令と若干の相違がある：

- 電子情報システムの分類の実施：ハンガリー国内法では、電子情報システムの分類の実施が義務付けられており、関連する電子情報システムの完全性及び可用性に対するリスク、ならびに処理するデータの機密性、完全性、可用性に基づき、すべての関係事業者に電子情報システムを「基本」「重要」「高度」のセキュリティクラスに分類することを義務付けている。これに伴い、処理するデータの機密性、完全性、可用性に対する保護要件は段階的に厳格化されることとなる。さらに、特定の基準に基づき国内法の適用範囲が拡大された事業体は、外国（すなわちハンガリー国外）でのデータ処理や非プライベートクラウドサービスの利用に際し、自社の電子情報システムで処理されるデータを分類する必要がある。
- サイバーセキュリティ監査人の選任：ハンガリー国内法では、外部の指定されたサイバーセキュリティ監査人と2025年8月31日までに契約を締結し、二年毎の監査を実施する（第一回目のサイバーセキュリティ監査の実施の期限は2026年6月30日）ことが義務付けられている。
- 罰則：ハンガリー国内法では、NIS2指令で定められた制裁金に加え、国内法で定められた個々の義務に違反した場合に別途制裁金が定められており、義務違反の内容によっては当局は最大で150,000,000 HUFの制裁金を課すことが可能となっている。

(3) ドイツ

ドイツでは、2025年12月5日にドイツ国内法[15]が制定され、2025年12月6日に発効した。適用対象となる事業者は、NIS2指令の適用対象となった日から3か月以内に管轄当局に登録しなければならない。

ドイツ国内法においては、主に以下の点でNIS指令と若干の相違がある：

[14] https://njt.hu/jogszabaly/2024-69-00-00

[15] https://www.recht.bund.de/bgbl/1/2025/301/VO

©Atsumi & Sakai 2026

- 適用対象：ドイツ国内法では、適用対象について、付随的活動への適用除外が設けられており、これにより、適用対象となる活動への関与度が「軽微」とみなされる場合、当該企業は適用対象外となると定められている。もっとも、当該適用除外はNIS2指令との整合性に疑義があり、将来的に修正される可能性があると論じられている。
- 経営層によるガバナンス：ドイツ国内法では、NIS2指令で定められている上述の経営層による自社のサイバーセキュリティ対策の承認及びその実施の監督の義務を超えて、経営層は単に承認及び監督するだけでなく、そのような措置を「実施」することが要求されている。これにより、必要な措置の実施及び監督を怠った場合に経営層が会社法上の個人責任を問われる可能性がある。
- 罰則：ドイツ国内法では、NIS2指令で定められた制裁金に加え、国内法で定められた登録義務違反等の場合には最大で50万ユーロ、当局の命令違反等の場合には最大で10万ユーロの制裁金を課すことが可能となっている。

III. 結び

NIS2指令は、上記の通りEU加盟国内の一定規模以上の対象となる事業分野の企業に、サイバーセキュリティ対策を義務付ける、影響力の大きいEU指令である。対応措置の期限も定められており、違反した場合の制裁金も巨額であるため、適用可能性のある企業は、早期に対応を開始する必要がある。さらに、各EU加盟国の国内法において、NIS2指令よりも要件や義務が加重されている場合があるため、適用可能性のある各加盟国の国内法の内容を精査する必要もある。また、グローバル展開する日本企業においては、EU加盟国内に存在するグループ会社が小規模であってもNIS2指令の適用の対象となる場合があるため、適用対象の可否及び必要となる対応措置を慎重に検討すべきである。特に、国内法が最近発効した加盟国の国内法においては、上述した登録期限や対応措置の期限が近い可能性もあるため、注意が必要である。

©Atsumi & Sakai 2026

執筆者

弁護士　金久直樹（シニアパートナー、第一東京弁護士会）

Email: naoki.kanehisa@aplaw.jp

弁護士　丸山るり子（アソシエイト、東京弁護士会）

Email: ruriko.maruyama@aplaw.jp

弁護士　船橋桃子（アソシエイト、東京弁護士会）

Email: momoko.funahashi@aplaw.jp

お問い合わせ先

本ニューズレターに関する一般的なお問い合わせは、下記までご連絡ください。

渥美坂井法律事務所・外国法共同事業　ヨーロッパ/EUプラクティスチーム

Email: ipg_europe_eu@aplaw.jp

当事務所のニューズレターをご希望の方はニューズレター配信申込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よりご覧いただけます。

このニューズレターは、現行の又は予想される規制を網羅的に解説したものではなく、著者が重要だと考える部分に限って、その概要を記載したものです。このニューズレターに記載されている意見は著者個人の意見であり、渥美坂井法律事務所・外国法共同事業（「渥美坂井」）の見解を示すものではありません。著者は明白な誤りを避けるよう合理的な努力は行いましたが、著者も渥美坂井もこのニューズレターの正確性を保証するものではありません。著者も渥美坂井も読者がこのニューズレターに依拠することによって生じる損害を賠償する責任を負いません。取引を行う場合には、このニューズレターに依拠せずに渥美坂井の弁護士にご相談ください。

東京オフィス
Tokyo Head Office
〒100-0011 東京都千代田区
内幸町 2-2-2
富国生命ビル（総合受付：16F）

大阪提携オフィス
Osaka Affiliate Office
（A&S 大阪法律事務所）
〒530-0005 大阪府大阪市北区
中之島 2-3-18
中之島フェスティバルタワー16 階

福岡提携オフィス
Fukuoka Affiliate Office
（A&S 福岡法律事務所）
〒810-0001 福岡県福岡市中央区天神
2 丁目 12-1　天神ビル 10 階

ニューヨーク提携オフィス
New York Affiliate Office
1120 Avenue of the Americas,
4th Floor
New York, New York 10036

ロンドンオフィス
London Office
85 Gresham Street,
London EC2V 7NQ, United Kingdom

フランクフルト提携オフィス
Frankfurt Affiliate Office
Barckhausstraße 1 (8th Floor), 60325
Frankfurt am Main, Germany

ブリュッセルオフィス
Brussels Office
CBR Building, Chaussée de la Hulpe
185, 1170, Brussels, Belgium

ホーチミンオフィス
Ho Chi Minh Office
10F, The NEXUS building, 3A-3B Ton
Duc Thang Street, Sai Gon Ward, Ho
Chi Minh City, Vietnam

©Atsumi & Sakai 2026