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

2026 年 5 月 11 日
No.IEU_004

NIS2 指令——欧盟网络安全监管概述

作者：律师 金久直树 / 律师 丸山瑠璃子 / 律师 船桥桃子

翻译：外国法事务律师（中华人民共和国法） 陈凤琴

I. NIS2指令概述

2023年1月16日生效的NIS2指令（网络与信息安全指令2/ Network and Information Security Directive 2）[1]，是一项旨在加强欧盟境内网络安全及韧性的欧盟指令，要求适用对象企业建立统一的风险管理体系，并规定了发生安全事件时的报告义务等。NIS2指令是对原有NIS指令的修订，其适用范围及义务内容均得到了大幅扩展。对于开展全球业务的日本企业而言，即使位于欧盟成员国境内的集团子公司规模较小，若将其母公司（即日本企业）的员工人数、销售额及总资产进行合并计算后，仍可能成为NIS2指令的适用对象，因此需予以注意。

不过，NIS2指令在被纳入欧盟成员国的国内法之前并不产生直接效力。因此，尽管欧盟成员国被要求在2024年10月17日之前将该指令转化为国内法，但截至目前，仍有部分国家尚未完成国内法的制定。

本文将梳理NIS2指令的核心要点，并就欧盟成员国国内法制定情况进行解读。

II. 问答

1. NIS2指令的适用对象是哪些企业？

(1) 原则上的适用对象

原则上，《NIS2指令》适用于满足以下条件的经营者：①在欧盟境内提供服务或开展业务活动；②属于“高度关键行业”（《NIS2指令》附件I）或“其他关键行业”（《NIS2指令》附件II）；③属于中型企业及以上规模。此处所指的中型及以上企业，系依据欧盟委员会于2003年5月6日发布的建议[2]所定义，指员工人数在50人以上，且或年营业额或总资产在1,000万欧元以上的企业。此外，关于③类企业的规模计算，需将“合作企业（partner enterprises）”（某企业持有另一家企业25%至50%的资本或表决权的情况）及“关联企业（linked enterprise）”（某企业持有另一家企业超过50%的资本或表

[1] https://eur-lex.europa.eu/eli/dir/2022/2555/2022-12-27/eng
[2] 《2003/361/EC 号建议书》附件第 2 条（https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32003H0361）

决权的情况）[3] 的员工人数、销售额、总资产进行合并计算[4]。具体而言，对于合作企业，按持股比例对应的份额进行计算（例如，持股比例为30%时，即该合作企业30%的份额）；对于关联企业，则无论持股比例如何，均将该关联企业的100%员工人数、销售额及总资产计入合计。因此，对于大型集团企业而言，即使是在该成员国内仅开展小规模业务的子公司，也可能满足相关规模要求并成为监管对象，因此，开展全球业务的日本企业需予以注意。

(2) 主要适用业务行业

《NIS2指令》附件I及附件II所规定的“高度关键行业”及“其他关键行业”如下：

- “高度关键行业”：能源、运输、银行业、金融市场基础设施、医疗、饮用水、排水、数字基础设施、ICT服务管理（B2B）、公共行政、航天
- “其他关键行业”：邮政与物流、废物管理、化学品制造、生产与流通、食品生产、加工与流通、特定制造业（医疗器械、计算机、电子产品、汽车及其他运输设备）、数字服务提供商（在线市场、在线搜索引擎、社交媒体）、研究

如果日本企业在欧盟成员国境内的集团子公司从事上述业务，则需尽快确认是否适用《NIS 2指令》。

(3) 无论规模大小均适用该指令的经营者

DNS服务提供商、顶级域名（TLD）注册管理机构、合格信任服务提供商等，无论是否符合上述(1)③所述的企业规模，均适用NIS2指令[5]。

(4) 企业分类

《NIS2指令》将适用对象企业分为“关键实体（essential entities）”和“重要实体（important entities）”，这一划分将影响监管的严格程度及制裁内容。一般而言，针对前者将采取更为严格的监管及执法措施。关键实体与重要实体的划分需综合考虑行业领域、业务规模以及各国国内法的特别规定，其中关键实体的典型代表是从事高度关键行业的大型企业（员工人数250人以上，或营业额超过5,000万欧元，或总资产超过4,300万欧元），而重要实体的典型例子则是从事高度关键行业或其他关键行业的中型企业。

2. 根据《NIS2指令》，企业需承担哪些义务？

(1) 注册义务

属于NIS2指令适用范围的关键实体及重要实体，有义务向主管当局登记企业名称、地址、联系方式等信息，具体的登记义务内容及程序由成员国国内法规定。

(2) 网络安全风险管理措施

NIS2指令的适用对象企业必须采取适当、合理且符合最新技术水平的技术性、运营性及组织性的措施，以确保其业务及服务所使用的网络和信息系统的安全性。这包括制定风险分析及信息安全政策、制定事故响应机制、业务连续性计划（包括事故发生时的备份、灾难恢复及危机管理）、确保供应链安全、实施风险管理有效性评估流程、引入多因素认证、制定加密技术使用或加密相关政策及程

[3] 欧盟委员会《中小企业定义用户指南》（https://www.europeanacademy.com/wp-content/uploads/2021/03/SME_definition_user_guide_en.pdf）
[4] 第 2003/361/EC 号建议书附件第 2 条及第 6 条第 2 款(https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32003H0361)
[5] 《NIS2 指令》第 3 条第 1 款(b)

序、制定访问控制政策及资产管理、以及在网络和信息系统的采购、开发及维护过程中确保安全（包括漏洞处理与披露）等。

这些措施需结合企业规模以及风险的性质和严重程度，并按照最新的技术水平予以实施。

(3) 管理层治理

《NIS2指令》强烈要求管理层在网络安全措施方面发挥作用并承担责任。具体而言，管理层有义务批准网络安全相关的风险管理措施，并监督其实施情况。此外，还要求管理层亲自参加培训，并对员工实施定期教育和培训。但需注意的是，NIS2指令要求欧盟成员国在国内法中确保管理层责任的落实，而非在欧盟层面直接设立个人责任。

(4) 发生安全事件时的报告义务

NIS2指令规定，当发生对服务提供造成重大影响的事件时，必须迅速向主管当局报告。所谓事件，是指损害通过网络和信息系统存储、传输或处理的数据，或损害通过该系统提供或可访问服务的可用性、真实性、完整性或保密性的情形[6] 。所谓重大事件，是指：(i) 已导致或可能导致相关企业的服务出现严重运营障碍或财务损失的情况；(ii) 已造成或可能造成对其他自然人或法人产生相当程度的物质或非物质损害的情况[7]。

《NIS2指令》在事件报告方面采用了三阶段机制。具体而言，必须：①在发现事件后24小时内进行初步通报；②在发现事件后72小时内提交事件报告；③在提交事件报告后1个月内提交最终报告。此外，具体的报告程序和报告途径由国内法规定。

3. 违反NIS2指令将面临哪些处罚？

若违反NIS2指令，各成员国的监管机构将作为行政处分予以制裁，且罚款金额有明确规定。关键实体与重要实体的标准不同，对于关键实体，上限为该企业全球销售额（即该企业所属企业集团上一会计年度的全球年度销售额）的2%，或1000万欧元，以较高者为准[8] 。另一方面，对于重要实体，适用其全球销售额（即该企业所属企业集团上一会计年度的全球年度销售额）的1.4%，或700万欧元，以较高者为准[9]。由此可见，若违反NIS2指令，可能依据企业集团的全球销售额被处以巨额罚款，因此开展全球业务的日本企业需格外注意。此外，由于各成员国的国内法可以在NIS2指令规定的最低标准基础上设定更严格的要求或追加制裁，因此需要注意，除了上述NIS2指令规定的制裁外，各成员国的国内法可能还会施加进一步的制裁。

4. 欧盟成员国的国内法制定情况如何？

如前所述，NIS2指令已于2023年1月16日生效，要求欧盟成员国须在2024年10月17日前制定符合NIS2指令内容的国内法。然而，在27个成员国中，有23个国家未能在该期限前完成国内法制定[10]，截至2025年5月7日，仍有19个国家尚未完成相关工作[11] 。为避免受到欧盟委员会的制裁，此后各成员国加快了立法进程，据最新消息，截至2026年3月6日，27个成员国中有21个已完成国内法修订；其余6

[6] NIS2 指令第 6 条第 6 款
[7] NIS2 指令第 23 条第 3 款
[8] NIS2 指令第 34 条第 4 款
[9] NIS2 指令第 34 条第 5 款
[10] https://ecs-org.eu/activities/nis2-directive-transposition-tracker/
[11] https://digital-strategy.ec.europa.eu/en/policies/nis-transposition

个尚未完成修订、仍处于法案阶段的成员国（爱沙尼亚、荷兰、爱尔兰、法国、西班牙、卢森堡）正加紧推进国内法修订工作[12] 。

5. 欧盟成员国的国内法具体内容如何？是否有国家比NIS2指令更为严格？

如上所述，虽然已有21个成员国完成了国内法的制定，但本文将以其中以下3个国家为例，探讨其国内法的内容，并介绍与NIS2指令的差异等。

(1) 比利时

比利时于2024年4月26日制定了NIS2指令的国内法[13]，并于2024年10月18日生效。适用对象企业须在2025年3月18日前向主管机关完成登记。比利时国内法基本沿袭了NIS2指令的要求，但主要在以下方面存在若干差异：

- 适用对象：比利时国内法以NIS2指令规定的适用领域为基础，同时允许通过王令（Royal Decree）追加或扩展适用领域。因此，未来可能会有更多领域被纳入适用范围。。
- 网络安全风险管理措施：比利时国内法要求适用对象企业制定并实施“协调漏洞披露政策（Coordinated Vulnerability Disclosure Policy）”。此外，比利时主管机关Centre for Cybersecurity Belgium可在协调漏洞披露框架下作为可信赖的中介机构发挥作用，负责促进报告漏洞的个人或组织与受影响产品或服务的制造商或供应商之间的联系与协调。

(2) 匈牙利

匈牙利于2024年12月20日制定了NIS2指令的国内法[14]，并于2025年1月1日生效。适用对象企业须在2024年12月18日前向主管机关完成登记。

匈牙利国内法主要在以下方面与NIS2指令存在若干差异：

- 实施电子信息系统分类：匈牙利国内法规定必须实施电子信息系统分类，并要求所有相关企业根据相关电子信息系统的完整性及可用性风险，以及所处理数据的机密性、完整性和可用性，将电子信息系统分为“基础”、“重要”和“高级”三个安全等级。随之，对所处理数据机密性、完整性及可用性的保护要求将逐步收紧。此外，根据特定标准被纳入国内法适用范围的企业，在境外（即匈牙利境外）处理数据或使用非私有云服务时，必须对其电子信息系统中处理的数据进行分类。
- 网络安全审计员的选任：根据匈牙利国内法，企业必须在2025年8月31日前与指定的外部网络安全审计员签订合同，并每两年进行一次审计（首次网络安全审计的截止日期为2026年6月30日）。
- 处罚规定：根据匈牙利国内法，除NIS2指令规定的罚款外，若违反国内法规定的具体义务，还将另行处以罚款；根据违规内容的不同，主管机关最高可处以1.5亿匈牙利福林（HUF）的罚款。

[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

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

(3) 德国

德国于2025年12月5日制定了NIS2指令的国内[15]，并于2025年12月6日正式生效。适用对象企业须在成为NIS2指令适用对象之日起3个月内向主管机关完成登记。

德国国内法主要在以下方面与NIS2指令存在若干差异：

- 适用范围：德国国内法针对适用范围，设定了附带活动的豁免条款，规定若企业参与相关适用活动的程度被视为“轻微”，则该企业不属于适用范围。不过，有观点认为该豁免条款与NIS2指令的协调性存疑，未来可能进行修订。
- 管理层的治理：德国国内法要求管理层不仅要批准并监督公司网络安全措施的实施，还必须亲自“实施”这些措施，这超出了NIS2指令中规定的管理层仅需批准及监督的义务。因此，若管理层疏于实施及监督必要措施，可能需承担公司法规定的个人责任。
- 处罚：根据德国国内法，除NIS2指令规定的罚款外，若违反国内法规定的登记义务等行为，最高可处以50万欧元罚款；若违反主管机关命令等行为，最高可处以10万欧元罚款。

III. 结语

如上所述，NIS2指令是一项影响深远的欧盟指令，要求欧盟成员国内一定规模以上的特定行业企业必须采取网络安全措施。鉴于该指令规定了应对措施的截止期限，且违规时的罚款金额巨大，可能适用该指令的企业有必要尽早着手应对。此外，由于各欧盟成员国的国内法中，其要求和义务可能比NIS2指令更为严格，因此，有必要仔细审查各适用成员国国内法的内容。此外，对于开展全球业务的日本企业而言，即使在欧盟成员国内的集团子公司规模较小，也可能属于NIS2指令的适用对象，因此应慎重评估是否属于适用对象以及所需采取的应对措施。特别是对于近期国内法才生效的成员国，其国内法中规定的上述登记期限或应对措施的截止日期可能已临近，需格外注意。

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

作者

律师　金久直树（高级合伙人，第一东京律师协会）
Email: naoki.kanehisa@aplaw.jp

律师　丸山瑠璃子（律师，东京律师协会）
Email: ruriko.maruyama@aplaw.jp

律师　船桥桃子（律师，东京律师协会）
Email: momoko.funahashi@aplaw.jp

翻译：外国法事务所律师（中华人民共和国法）　陈凤琴（高级合伙人、第二东京律师协会）
Email: fengqin.chen@aplaw.jp

联系方式

如您对本简报(Newsletter)有一般性咨询，欢迎联系以下作者。

渥美坂井律师事务所・外国法共同事业 欧洲/欧盟业务团队
Email: ipg_europe_eu@aplaw.jp

若您希望订阅本事务所简报，请通过《简报订阅申请表》进行申请。
此外，您亦可通过**此处**查阅往期简报。

东京办公室
邮编 100-0011
东京都千代田区内幸町 2-2-2
富国生命大厦 16 层

大阪合作办公室
邮编 530-0005
大阪府大阪市北区中之岛 2-3-18
中之岛 Festival Tower 16 层

福冈合作办公室
邮编 810-0001
福冈市中央区天神 2-12-1
天神大厦 10 层

纽约合作办公室
1120 Avenue of the Americas,
4th Floor
New York, New York 10036

伦敦办公室
85 Gresham Street,
London EC2V 7NQ,
United Kingdom

法兰克福合作办公室
Barckhausstraße 1 (8th Floor),
60325 Frankfurt am Main,
Germany

布鲁塞尔办公室
CBR Building, Chaussée de la
Hulpe 185, 1170,
Brussels, Belgium

胡志明市办公室
10F, The NEXUS building, 3A-
3B Ton Duc Thang Street,
Sai Gon Ward,
Ho Chi Minh City, Vietnam