ドイツ会計・税務ニュースレター

第 37 回　サイバーセキュリティ

改正ネットワークおよび情報セキュリティ指令（NIS2）

2024 年 8 月

はじめに

欧州連合（EU）は 2022 年 12 月、欧州におけるサイバーセキュリティの向上を企図して、NIS2 指令を公表しました。多くの企業や業界に加盟国で共通の厳格なセキュリティ要件を課すことで、サイバー脅威に対するレジリエンスを強化することを目的としています。

※　本稿は、Grant Thornton AG（グラントソントン・ドイツ）が作成したものを、和訳・編集したものです。原文（ドイツ語）はこちらをご参照ください。

Contents

背景

NIS2 は、2016 年 7 月に EU で導入された「ネットワークと情報システムのセキュリティに関する指令（NIS）」を改正・強化したものです。当初の NIS は、加盟国が情報システムのセキュリティに関する共通の包括的ルールを策定することを要求するものでしたが、その後の 5G 技術の台頭や COVID19 に起因する情報システムへの依存度の高まり、サイバーセキュリティインシデントの増加を受け、更なる規制の強化を企図した NIS2 が発効しました。

EU 加盟国は 2024 年 10 月 17 日までに NIS2 に対応する国内法を制定する必要があります。推定によるとドイツ国内の 25,000－40,000 社が NIS2 の適用範囲に含まれるとされています。対象企業は NIS から範囲を広げ、新たに郵便および宅配サービス、廃棄物管理および化学品（化学物質の生産、

製造、取引を行う企業）、各種メーカーも含まれることになりました[1]。これらの業種の中会社以上の企業[2]が NIS2 の適用対象となります。

セキュリティ要件の増加

NIS2 は、対象企業が適切なサイバーセキュリティを構築することを目的としています。企業は、セキュリティインシデントの発生確率や重要度などのリスク評価に基づいて、自社のサイバーセキュリティの適切性をチェックし、対策を講じます。この対策には、情報システムのリスク分析、セキュリティインシデントへの対応、事業継続対策（バックアップ管理、災害時の復旧）が含まれます。

企業はまた、サプライチェーンの IT セキュリティを確保し、ネットワークおよび情報システムの調達、開発、保守時にセキュリティ対策を講じ、とりわけサイバーセキュリティ分野におけるリスク管理の有効性の評価手順を確立する必要があります。重要な IT システムには、暗号化と多要素認証を含める必要があります。

コスト、投資、ノウハウ

NIS2 の導入には資金と人的資源が必要であり、特に中堅企業は大きな課題に直面しています。新たなセキュリティと IT インフラを実装するには、テクノロジーへの投資が必要です。これらのコストに加えて、既存の従業員の資格取得やトレーニング、または追加の IT スタッフの採用により、必要なノウハウを社内で構築または利用できるようにする必要があります。外部のセキュリティ専門家も NIS2 対応を支援できますが、いずれの場合でも、企業はコストの増加に直面します。IT インフラ、特にサイバーセキュリティの分野で熟練した技術者が不足していることを考えると、これは特に大きな課題です。

インシデントの報告義務と文書化

技術的要件に加えて、企業はセキュリティインシデントの報告要件も満たさなければなりません。重大なインシデントは一定期間内に報告される必要があり[3]、その為には確立されたコミュニケーションチャネルが必要です。また、すべてのサイバーセキュリティ対策とインシデントを包括的に文書化する必要があり、管理上の負担も増大します。企業は、社内の組織分析およびプロセス分析を通じて自社のガバナンス構造の見直しを行い、NIS2 の要件に適応させる必要があります。

---

[1] 主要エンティティ： エネルギー、輸送、銀行、金融市場インフラ、ヘルスケア、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
重要エンティティ： 郵便・宅配、廃棄物管理、化学品、食品、製造業（医療機器、コンピュータ・電気電子・光学製品、機械、自動車、輸送機器）、デジタルプロバイダー、研究

[2] 中会社は以下 3 つの基準値のうち 2 年連続して 2 つ以上の基準を満たす企業をいう。
- 売上高：15 百万ユーロ超 50 百万ユーロ以下
- 総資産：7.5 百万ユーロ超 25 百万ユーロ以下
- 従業員：50 名超 250 名以下

[3] 重大なインシデントを認識してから 24 時間以内に早期警告、72 時間以内にインシデントの重大度、影響、ならびに入手可能な場合には侵害の兆候などについての初期評価を含めたインシデント通知を行い、インシデント通知から 1 か月以内にインシデントの原因や範囲、是正措置等を含めた最終報告を行う必要がある。

ペナルティ

NIS2 に遵守していない企業は多額のペナルティを科される可能性があります。また、十分なサイバーセキュリティが確保できていないことによる、レピュテーションリスクやそれに伴うビジネス上の障壁が生じるリスクもあります。NIS2 の不遵守は取締役会および経営陣の直接の責任となります。

法令順守をイノベーションに繋げるために

これらの課題の一方で、NIS2 はドイツの中小企業に機会も創出します。IT とサイバーセキュリティの強化は、顧客の信頼を醸成し、競争上の優位性をもたらします。サイバーセキュリティ対策への投資は、企業の技術的、組織的、手続上の可能性を広げ、必要なイノベーションを促進し、デジタルトランスフォーメーション対策を加速することができます。

お問い合わせ先

Grant Thornton AG（グラントソントン・ドイツ）では、ドイツに進出する日系企業のために、デュッセルドルフ・オフィスにジャパンデスクを設けています。監査・保証業務、税務申告、給与計算、記帳代行、M&A トランザクションアドバイザリー、内部統制構築支援、事業戦略コンサルティングなど、各種の会計税務サービスをご提供しています。

担当者

井上 広志 Hiroshi Inoue
Grant Thornton AG | Head of Japan Desk | Partner
公認会計士（日本）
E hiroshi.inoue@de.gt.com
W grantthornton.de