IP Tech
Tokyo

Client Alert
30 March 2023

EU における、ネットワーク・情報システムのセキュリティに関する指令 2（NIS 指令 2）の留意点

本アラートに関する
お問い合わせ先：


高瀬　健作
パートナー
03 6271 9752
Kensaku.Takase@bakermckenzie.com


達野　大輔
パートナー
03 6271 9479
Daisuke.Tatsuno@bakermckenzie.com


藤原　総一郎
アソシエイト
03 6271 9707
Soichiro.Fujiwara@bakermckenzie.com

デジタルトランスフォーメーション、リモートワーク、地政学的な問題などを背景として、サイバー空間における脅威やサイバー攻撃は増加の一途を辿り、サイバー犯罪は社会全体にとってますます緊急性の高い問題になっている。この問題に対応するため、2016 年、欧州議会はサイバーセキュリティに関する初の EU 全体の法律である、「ネットワーク・情報システムのセキュリティに関する指令（NIS 指令）」を採択したが、この度、その改正法である通称「NIS 指令 2」が公布された。

NIS 指令は、基幹エネルギー網や医療、交通網といったインフラストラクチャーを運営する事業者、そして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やクラウドコンピューティングサービスを提供する特定の事業者であるデジタルサービスプロバイダー（DSP）といった重要な役務を提供する事業者（OES）に、一定のリスク管理と報告の義務を課していた。しかし、その運用は EU 加盟国間でもまちまちであり、実際に報告されたインシデントは多くはなかった。そこで 2020 年、欧州委員会は NIS 指令の改正となる新指令の導入を提案し、当該新指令が 2022 年 12 月 27 日に公布され、2023 年 1 月 16 日に発効した（「NIS 指令 2」）。NIS 指令 2 は、NIS 指令の欠陥に対処し、必要不可欠で重要な事業者やインフラストラクチャーをサイバー上の脅威やサイバー攻撃から保護し、EU 全体で共通する高いレベルのセキュリティを実現することを目的としているものである。NIS 指令 2 の EU 加盟国による国内法化は、2024 年 10 月 17 日までに行われなければならないとされている。

欧州委員会は、NIS 指令 2 が「安全で堅牢かつ適切な情報共有を促進」し、ひいては事業者がフィッシング、マルウェア、不正アクセスなどの脅威から情報システムを守るのに役立つと説明している。更に、NIS 指令 2 では、セキュリティ要件の強化、サプライチェーンのセキュリティへの対応、報告義務の合理化、EU 全域での制裁の調和など、より厳しい監督措置及び執行要件の導入が期待されている（ただし、NIS 指令 2 はあくまで「指令」であり、直接加盟国に効力が発生する「規則」ではない）。

NIS 指令 2 となり変わること

1. 適用対象の拡大

NIS 指令 2 は、NIS 指令よりも広範な産業やサービスに適用される。NIS 指令が主に OES と DSP に適用されていたのに対し、NIS 指令 2 はこの区別をなくし、代わりに「最重要（essential）」事業者と「重要（important）」事業

者という、より幅広い概念を導入している。また、各カテゴリーに分類される事業者の種類も増えている。

「最重要」事業者は、社会・経済活動に不可欠な事業者で、例えば、エネルギー、運輸、金融、衛生分野の事業者が該当する。また、「重要」事業者は、例えば、製造、食料、研究開発分野の事業者が該当する。NIS 指令 2 では、廃棄物及びその管理サービス、特定の重要製品（医薬品、医療機器、化学品など）の製造業者、郵便・宅配サービス、デジタルサービス（SNS、データセンターサービスなど）が対象に追加された。適用対象となる事業者には、より厳しい義務が課せられ、リスク管理及び情報システムのセキュリティポリシー、インシデントの処理（インシデントの予防、検出及びこれへの対応）、ネットワーク及び情報システムのセキュリティ、サプライチェーンのセキュリティ、暗号化及び危機管理などに関して、技術及び組織の構造並びに能力の面から対応する必要が生じる。

2. インシデント報告義務の改正

NIS 指令では、事業者は特定のインシデントやサイバー上の脅威を認知した場合、「不当な遅延なく」関連する監督当局に報告することが求められているだけであった。従って NIS 指令のもとで報告されたインシデントはそれほど多くはなかったとも言われている。NIS 指令 2 では、報告義務が段階的に細分化され、「重大な」インシデント、すなわちサービスの供給に重大な影響を与えたか、又は影響を与える可能性のあるインシデントに気づいてから 24 時間以内に、関連する監督当局に最初の報告を行うことが義務づけられた。さらに、事業者は最初の報告から 1 か月以内に最終報告を行うことも義務づけられた。実際には、インシデントの種類によっては、最初の報告が非常に簡潔なものとなり、また 1 か月以内に最終報告を行うことが困難である可能性も想定される。

NIS 指令 2 は、セキュリティに関するインシデントを報告する手順、内容及び時間枠に関する詳細な規定も含まれている。

3. 経営層に課せられた義務

NIS 指令 2 の下で、EU 加盟国は、サイバーセキュリティのリスク管理及び報告義務違反に対して、最高 1,000 万ユーロ又は事業者の全世界年間総売上高の 2%のいずれか高い方の額の罰金を課せるようになった。NIS 指令 2 におけるアプローチの主な変更点として、事業者が法律に定められた義務の遵守を怠った場合、その事業者の経営層も個人としての責任を問われる可能性がある。その潜在的な影響として、罰金に加え、経営機能の遂行の一時的な停止がありえることになる。この背景としては、取締役会及び上級幹部がサイバーリスクについて理解していない、十分に取り組んでいないという以前からの懸念があった。ただ、当事務所の経験上、この 2 年から 3 年で、状況は大きく改善されてきているといえる。

経営層にコンプライアンスに関する責任を負わせることは、その行動を促進し、セキュリティガバナンスの強化につながるはずである（ただし、これが実際に起きるかどうかはまだ不明である。経営層に個人責任を課すことは、

他の分野では必ずしも望ましい行動につながっておらず、サイバー領域全般に関しても、既にスキルと知識の大きなギャップが存在している）。経営層は、法律で規定されている措置の実施と監督において、より積極的な役割を果たす必要がある。また、この新たな仕組みにより、特定の役職に対する個人責任保険の適用範囲の拡大が求められる可能性がある。

4. サプライチェーンのセキュリティ

NIS 指令 2 の主な変更点の 1 つは、NIS 指令よりもさらに踏み込んだ、EU 全体で協調したサプライチェーンのリスク評価である。NIS 指令 2 は、事業者に対して、セキュリティリスクの軽減及びサードパーティーのサプライヤー／サービスのデューデリジェンスを含む、サイバーリスク管理策の実施を求めている。サードパーティとサプライチェーンは、ここ数年、サイバーリスクの主な発生源となっており、サプライチェーンを経由した世界的なサイバーインシデントが多発している。しかし、サードパーティのサイバーリスクの効果的な監査は困難である。多くの監査は紙面上で行われるためである。SBOM（ソフトウェアが含んでいるライブラリやモジュールを一覧化した構成情報）のようなコンセプトも助けとなると思われるが、効果的なサイバーサプライチェーンのリスク評価及び監査のプロセスを開発するためには、依然として課題が数多く存在する。

今後の展望

NIS 指令 2 は、EU 及び EU で活動する事業者全体のサイバーディフェンスとレジリエンスを高めることを目的とした、近年に制定されたあるいは今後制定される様々な EU 法の一部に過ぎない。最近になってサイバーセキュリティ法が採択され、現在提案されているサイバーレジリエンス法については、現在 EU 加盟国の意見を聴取しているところである。また、英国では、英国法のもとで施行されている NIS を英国版 NIS2 に置き換えることが提案され、最近では通信セキュリティの要件が変更されている。このように、欧州全体でもサイバー法の大きな変革が生じている。様々な法律がどのように相互に関連し、運用されるかを明確にする試みはなされているものの、それが実際に達成されるかどうかは未だ明らかではない。明確なのは、サイバーコンプライアンスのマトリクスがさらに複雑化するということである。異なる製品や事業分野にどの法律が適用されるのか、どのように異なる法律への対応を実現するのか、どのようにインシデント及び監督当局から課される可能性がある報告義務に対応するかを明確にすることは、事業者におけるサイバーハイジーン（サイバー衛生）の備えとして、さらに重要な一部分となる。