ドイツ・会計税務ニュースレター

第 10 回　サイバーセキュリティ

欧州の重要 IT セキュリティ法案（2023 年）

2023 年 3 月

はじめに

EU では 2023 年以降、サイバーセキュリティに関する様々な新規制の導入が予定されています。規制の対象となる重要なインフラに該当しない企業であっても、その動向に留意する必要があります。

本稿では、その中でも重要な法案の概要と、実践するためにどのような準備が必要かを解説します。

※　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・加筆したものです。原文（英語）はこちらをご参照ください。

Contents

背景

サイバーセキュリティ関連のインシデントの頻発に伴い、事業者が対応すべき事項はますます多くなっています。GDPR の取り組みがデータプライバシーをめぐる会話を一変させたように、サイバーセキュリティにおける取り組みも、株主、顧客、サプライチェーンに対する事業者の責任を問うものとなるでしょう。

新たな規制や指令の導入の背景として、AI の進歩や、組織のセキュリティを脅かすツールの高度化が挙げられます。現在では、多くのサイバー犯罪グループが、数年前までごく一部のハッカーのみが利用可能だった、またはそれ以上に悪質なツールに簡単にアクセスすることが可能です。

S&P Global Market Intelligence による 2020 年の調査では、サイバー賠償責任保険の加入率は、2011 年の 34%から、2020 年には 78%に大きく増加しました[1]。保険料は上昇を続けており、最近では、保険会社に保険の提供を拒否されるリスクすらも考えられます。

[1] 参考：https://www.spglobal.com/marketintelligence/en/news-insights/latest-news-headlines/as-threats-grow-cyber-insurance-seen-as-more-of-a-necessity-61377276

こうした状況を受けて、EU では 2023 年以降、サイバーリスクとレジリエンス[2]に関連する各種規制の導入が予定されています。

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の改訂（NIS 2）

EU で 2016 年 7 月に導入された、「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 指令）」は更に強化されました。NIS 指令は、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すが、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図った NIS2 指令[3]が、2023 年 1 月 16 日に EU の決議により発効しました。

従来の NIS 指令から対象となるセクターの範囲を大きく広げ、新たに基幹セクター（Essential Entity）と重要セクター（Important Entity）の 2 つのカテゴリが設定されました[4]。

当該セクターの事業者が遵守すべきサイバーセキュリティリスクへの対応方針についても強化が図られているほか、インシデントに関する当局への報告義務についてもより明確化・厳格化されています（インシデント後 24 時間以内に早期警告、72 時間以内にインシデント通知、1 か月以内に最終報告書など）。

デジタルオペレーショナルレジリエンスに関する規制（DORA）

2022 年 11 月、銀行、保険会社、投資会社を含む金融機関の情報セキュリティを強化する、「デジタルオペレーショナルレジリエンスに関する規制」の草案[5]が採択されました。DORA は、デジタル運用のレジリエンス確保に対応する規制の枠組みを構築するために、EU 各加盟国で内国法を制定し、組織がサイバー攻撃の脅威に対応することを目的とします。DORA はまた、情報通信技術に対するリスクに関連した規則を統合・更新し、これまで存在していた各規則間のギャップを埋めることも意図しています。加盟国による法制化は 2024 年に予定されています。

---

[2] レジリエンス：困難で脅威を与える状況に対し、適応する過程や能力。サイバーセキュリティの分野においては、サイバー攻撃や自然災害といった脅威下においても、事業を継続するための企業の適応能力を指す。

[3] Directive (EU) 2022/2555。加盟国は NIS2 指令の発効を受け、2024 年 10 月 17 日までに内国法を成立させる必要がある。（参考: https://eur-lex.europa.eu/eli/dir/2022/2555/oj）

[4] 基幹セクター：エネルギー、保健医療、運輸、銀行および金融、上水道、下水道、デジタルインフラストラクチャ、行政機関、宇宙
重要セクター：郵便・配送サービス、廃棄物管理、化学品の製造・生産・流通、食品の生産・加工・流通、製造業（医療機器、電子機器、機械、輸送機器）、デジタルプロバイダー

[5] Regulation (EU) 2022/2554。高度かつ共通のデジタル運用レジリエンスを達成するために、金融機関のネットワークおよび情報システムのセキュリティ要件を定めている。
（参考：https://www.consilium.europa.eu/en/press/press-releases/2022/11/28/digital-finance-council-adopts-digital-operational-resilience-act/）

サイバーレジリエンス法（CRA）

2022 年 9 月、デジタル機器やサービスのサイバーセキュリティに関する共通基準を定めた「サイバーレジリエンス法（CRA）」[6]の草案が公表されました。この法律では、欧州で販売されるハードウエア、ソフトウェア等のデジタル製品やサービスを対象に、製造業者・輸入事業者・販売者らに当該製品の品質要件の確保を要求しています。重要なデジタル製品については、そのリスクに応じて、ベンダーが製品の脆弱性を特定し、テストするための要件が規定されています。

2023 年 1 月が CRA の公開草案に対する意見提出期限でした。ドイツを含む一部の EU 加盟国は、すでにこの法案の適用範囲を SaaS にも拡大することを提案しています。EU では、CRA の 2023 年後半の最終化、2025 年後半の適用を見込んでいます。タイミングはまだ先ですが、既に実務への影響が注目されています。

重要インフラストラクチャー包括法（KRITIS）／RCE

2023 年末には、ドイツの「重要インフラストラチャー包括法」[7]によって、リスク評価、監視の義務付けなど、特定の重要インフラの運営者が要求される最低限の要件が確保されることが期待されています。同法は、その欠陥や損傷がサプライチェーンの分断、公共の利益の喪失など、重大な影響を及ぼすと考えられる特に重要なインフラ事業者に対し、その物理的保護に関する要件を包括的に規制することを目的とします。この法律のガイドラインは、EU における同様の法案「重要なエンティティのレジリエンスを強化するための法案（RCE）」[8]にも移管されています。

各規制のすみ分け

ここまでの説明で、同様の法案が濫立しているという印象を抱く方もいるかもしれません。確かに、これらの法案はいずれも IT インフラのレジリエンス強化を企図したものであり、部分的に重複があることは事実です。しかし各法案のメインターゲットにはすみ分けがあり、NIS2 は幅広い重要セクターのサイバーセキュリティ、DORA は金融機関のネットワークセキュリティ、CRA はデジタル製品やサービスの適合基準、そして KRITIS および RCE は特に重要なインフラの物理的リスクに対するレジリエンスを主な対象としています。

NIS2 と RCE の対象企業に関する情報・洞察はこちらをご覧下さい。

---

[6] 参考：https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act

[7] 参考：https://www.bundesregierung.de/breg-de/aktuelles/schutz-kritischer-infrastrukturen-2151164

[8] Directive (EU) 2022/2557。EU 加盟国は、2024 年 10 月 17 日までに対応する内国法を成立させる必要がある。（参考：The Commission proposes a new directive to enhance the resilience of critical entities providing essential services in the EU (europa.eu)）

次のアクション

私たちが定期的にコンサルティングを提供している企業では、効果的なサイバーレジリエンス方針を確立するための課題の 1 つとして、複雑な規制環境を挙げています。しかし、事業者はこれらの規制環境を理解し、適切に対応することで、コンプライアンスと、事業継続の脅威となりうるセキュリティリスクへの対応を両立することが可能になります。

サイバーリスクに対する自社の対応方針を持つことは非常に重要ですが、それだけでは十分ではありません。リスクの適切なモニタリングを行い、現状把握に基づく効果的かつ積極的な回避・防止策を備えた包括的なアプローチを導入することが必要です。新規制への対応として、次のステップから始めることをお勧めします。

ステップ 1 ：サイバーリスクに関する現状把握

サイバーリスクに対する組織の現状認識とリスク許容度を明確にし、組織のサイバーリスク対応の成熟度について初期的な評価を行います。以下のような質問が考えられます。

- サイバーセキュリティの管理責任者は誰か？
- どのような事前対策を行っているか？
- どのようにテストし、対策が有効であることを確認しているか？
- 最もリスクが高いのはどの分野か？

組織のサイバーレジリエンスレベルを把握することで、その成熟度を次のレベルに引き上げるために投資が必要な分野を明らかにすることができます。

ステップ 2 ：教育・権限付与

従業員レベルの教育が必要な組織であっても、外部のプロフェッショナルによるサポートが必要な組織であっても、ナレッジは常に力となります。進化するサイバーセキュリティの分野において、組織のサイバーリスク対応に責任を持つ人は、この急速に進化するリスクに満ちた領域に関する最新の洞察と教育を受けることが不可欠です。連邦情報セキュリティ局（BSI）等の組織が提供するオープンなリソース[9]の活用を検討してください。

次に、組織の目標を設定し、評価を実施し、ベストプラクティスを導入し、データの最小化やフィッシング対策などのリスク低減プログラムを推進する責任を負う担当者が社内にいることを確認してください。サイバー関連のあらゆることを誰に頼めばよいかを、従業員が把握していることを確認してください。

最後に、経営陣がこの取り組みを支持するようにします。サイバーレジリエンス計画を成功させるには、IT 部門だけでなく、組織全体の協力が必要です。

---

[9] 参考：BSI - Bundesamt für Sicherheit in der Informationstechnik

ステップ３：進捗の評価

第三者による定期的なサイバー監査、プロアクティブな監視戦略、およびフォローアップ評価を通じて、サイバーレジリエンス戦略の成熟期における進捗状況を確認します。定期的に目標を達成しているかどうかを判断し、規制環境が変化した際にはリスクを再評価します。

サイバーレジリエンスの明確かつ積極的な戦略は、常に発展し続けるサイバーリスクに対応するための十分な備えと、既存のリスクを排除する方法を企業に提供するものです。ここでも、Grant Thornton AG の専門家によるアドバイスが役立ちます。

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おります。監査・保証業務、移転価格、グローバルタックスマネジメントを含む税制サポート、内部統制、事業戦略コンサルティングなど、貴社のドイツへの進出の程度や事業規模に応じたサービスのご提供が可能です。

ドイツでのビジネスサポートをお探しの日系企業様がありましたら、是非グラントソントン・ドイツ ジャパンデスクにご相談ください。

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