西村あさひ法律事務所

サイバーレジリエンス法案の公表と日本企業への影響

ヨーロッパ/個人情報保護・データ保護規制ニューズレター　2022 年 9 月 20 日号

執筆者:
E-mail 石川 智也
E-mail 福島 惇央
E-mail 水口 敦喜

2022 年 9 月 15 日、「サイバーレジリエンス法案」(Cyber Resilience Act)が欧州委員会によって提案された。この法案は、IoT 機器等、カテゴリーを問わずあらゆるデジタル要素を有する製品に対してサイバーセキュリティ対策を広く包括的に求める世界初の規則となる可能性がある。対象とされる製品は、その性質に照らして EU 向けの製品だけ別規格で製造することが容易でない場合もあるように思われ、事実上、EU のルールが世界の基準となる可能性すら秘めている。また、製造業者から輸入・販売業者まで広く違反事業者に高額の制裁金を課すことが想定されている点でも、日系企業へのインパクトは小さくないように思われる。以下、速報的に概要を紹介する。

1. サイバーレジリエンス法案[1]の概要

近年、ランサムウェア攻撃が社会問題となっており、その被害額は世界で年間数百兆円に達するとの推計も報告されている[2]。また、増加する IoT 製品の脆弱性を悪用した DDoS(分散型サービス妨害)攻撃により大規模なインターネット接続障害が引き起こされるなど、1 つの製品におけるインシデントがサプライチェーン全体や社会・経済活動全体に深刻な混乱をもたらし、さらには生命が脅かされることになる危険性はますます高まっているといえ、高いレベルのサイバーセキュリティを確保して製品の脆弱性を低減することは喫緊の課題となっている。

このような状況下で提出されたサイバーレジリエンス法案の目的は、以下の 4 点を定めることにある(1 条)。

① デジタル要素を有する製品のサイバーセキュリティを確保するための、当該製品の上市に関する規制
② デジタル要素を有する製品の設計、開発及び製造に関する必須要件並びにこれらの製品のサイバーセキュリティに関する事業者の義務
③ デジタル要素を有する製品のサイバーセキュリティを製品のライフサイクル全体にわたって確保するために製造業者が実施する脆弱性対応プロセスに関する必須要件及び当該プロセスに関連する事業者の義務
④ これらの規制や要件についての市場監視及びエンフォースメント

サイバーレジリエンス法案は、意図され又は合理的に予見される使用法が、直接又は間接にデバイス又はネットワークへの論理的又は物理的データ接続を伴う「デジタル要素を有する製品」に適用される(2 条 1 項)。ここで、「デジタル要素を有する製品」とは、全てのソフトウェア又はハードウェアの製品並びにその遠隔データ処理ソリューション(別個に上市されるソフトウェア又はハードウェアの構成要素を含む)を指し(3 条(1)号)、その範囲は非常に広い。

サイバーレジリエンス法案は、ネットワークと情報システムのセキュリティに関する NIS 指令、近年閣僚理事会及び欧州議会の間で合意された NIS 2 指令、並びにサイバーセキュリティ法からなる EU のサイバーセキュリティに関する枠組みを補完することが期待されている。

1 https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act

2 https://joint-research-centre.ec.europa.eu/crosscutting-activities/facts4eufuture-series-reports-future-europe/cybersecurity-our-digital-anchor-european-perspective_en

2. 事業者の義務

(1) 製造業者の義務

デジタル要素を有する製品は、①正しくインストールされ、維持され、意図された目的のため又は合理的に予見できる状況で使用される条件の下で別紙 I セクション 1 に定められる「製品特性に関するセキュリティ必須要件」[3]を充足し、かつ、②製造業者が実施する脆弱性対応プロセスが別紙 I セクション 2 に定められる「脆弱性対応必須要件」[4]を充足する場合に限って、市場に流通させることが可能とされる(5 条)。

このようなルールを背景に、製造業者は、デジタル要素を有する製品を上市するにあたって、当該製品が上記の「製品特性に関するセキュリティ必須要件」に従って設計、販売及び製造され、かつ、上市から当該製品の期待寿命と 5 年のいずれか短い方の期間、上記の「脆弱性対応必須要件」に従って当該製品の脆弱性が取り扱われることを確保する義務等を負う(10 条 1 項・6 項)。そのほか、製造業者は、当該製品に関連するサイバーセキュリティリスクの評価・考慮(同条 2 項)、第三者から調達した構成要素のデューディリジェンスの実施(同条 4 項)、技術文書等の作成・保管(同条 3 項・5 項・7 項・8 項)、所定の情報・説明の添付(同条 10 項、別紙 II)等を義務づけられる。

また、製造業者は、当該製品が「製品特性に関するセキュリティ必須要件」及び「脆弱性対応必須要件」を充足する旨を確認する適合性評価手続を行い、EU 適合宣言の作成及び CE マークの貼付をする必要がある(10 条 7 項・11 項、20 条、22 条)[5]。適合性評価手続は、①内部管理手続(モジュール A)、②EC 型式検査手続(モジュール B)及び型式への適合性(モジュール C)、又は③完全品質保証(モジュール H)のいずれかの手続 [6]により行う必要がある(24 条 1 項)。ただし、別紙 III に列挙されたカテゴリーに属する「デジタル要素を有する重要製品」(6 条 1 項)[7]については、認証機関による関与なく自ら適合性を保証する①の手続によることはできないなど、より厳格な適合性評価が求められている(クラス I については 24 条 2 項、クラス II については 24 条 3 項)。

さらに、製造業者は、不当に遅延することなく、遅くとも当該製品に含まれる脆弱性が積極的に悪用されていることを知ってから 24 時間以内に、当該脆弱性及び講じた是正又は緩和措置(該当する場合)についての詳細を ENISA(欧州ネットワーク・情報セキュリティ機関)に報告する義務を負う(11 条 1 項)。

なお、AI 規則案 6 条において高リスク AI システムと分類されるデジタル要素を有する製品で、「製品特性に関するセキュリティ必須要件」を遵守し、「脆弱性対応必須要件」に対応している場合は、同規則案 15 条に定めるサイバーセキュリティに関する要件を遵守しているものとみなされる(8 条 1 項)。

(2) 輸入業者及び販売業者の義務

輸入業者は、「製品特性に関するセキュリティ必須要件」を遵守し、「脆弱性対応必須要件」に対応している場合にのみ、デジタル要素を有する製品を上市することができ(13 条 1 項)、上市に先立ち、当該製品が①適切な適合性評価手続を経ていること、②

---

3 例えば、①リスクに応じた適切なサイバーセキュリティの水準が確保されるように設計、開発及び製造されること、②既知の悪用可能な脆弱性なしに引き渡されることに加え、③リスク評価に基づき、かつ、該当する場合は、(i)デフォルト設定で安全に出荷されること、(ii)適切にデータへのアクセス制限が確保され、データの機密性(Confidentiality)が保護されていること(認証や暗号化等)、(iii)ユーザーが許可していない操作・変更から処理データ等の完全性(Integrity)が保護されていること、(iv)製品の利用目的に必要な範囲に処理データが限定されていること(データの最小限性)、(v)重要な機能の可用性(Availability)が保護されていること(DoS 攻撃へのレジリエンス等)等が規定されている。

4 例えば、①脆弱性及び製品の構成要素の特定及び文書化、②セキュリティアップデートの提供、③効果的かつ定期的な製品のセキュリティ試験・レビュー等が規定されている。

5 ソフトウェアの場合は、EU 適合宣言又は当該ソフトウェア製品のウェブサイト上に添付するものとされている(22 条 1 項)。

6 各モジュールは別紙 VI 及び Decision No 768/2008/EC (https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32008D0768)に規定されている。

7 サイバーセキュリティリスクのレベルに応じてクラス I とクラス II に分類されて列挙されている。クラス I としては、例えば、スタンドアローン・埋め込みブラウザ、パスワードマネージャ、マルウェア検知・除去・隔離ソフトウェア等が、より高いレベルのリスクを有するとされるクラス II としては、例えば、サーバ・デスクトップ・モバイル機器の OS、汎用マイクロプロセッサ、IC カード・IC カードリーダ・トークン等が挙げられている。

製造業者が技術文書を作成していること、及び③CE マークが貼付され所定の情報・説明が添付されていることを確保する必要がある(同条 2 項)。また、当該製品のパッケージ等に自身の連絡先を記載する必要がある(同条 4 項)。

他方、販売業者は、デジタル要素を有する製品を上市するにあたって、サイバーレジリエンス法案の必須要件に関連して十分な注意を払って行動するものとされ(14 条 1 項)、上市に先立ち、①CE マークが貼付されていること、②製造業者による所定の情報・説明の添付及び EU 適合宣言の提供並びに輸入業者による連絡先の記載がなされていることを確認する必要がある(同条 2 項)。

また、輸入業者及び販売業者のいずれも、当該製品が「製品特性に関するセキュリティ必須要件」又は「脆弱性対応必須要件」に適合していないと考えるか、又はそう信じるに足る理由がある場合には、当該製品が上記各必須要件に適合するまで、当該製品を上市することはできず、さらに、当該製品が重大なサイバーセキュリティリスクをもたらす場合、製造業者及び市場監視当局に通知する義務を負う(13 条 3 項、14 条 3 項)。

3. 市場監視とエンフォースメント

各加盟国が指定した市場監視当局は、上市されたデジタル要素を有する製品が「製品特性に関するセキュリティ必須要件」及び「脆弱性対応必須要件」を充足しているかを評価するために必要な場合、事業者に対し、当該製品に関連する内部文書を含むデータにアクセスする権限を付与されることが想定されている(41 条 1 項・2 項、42 条)。また、市場監視当局がデジタル要素を有する製品が重大なサイバーセキュリティリスクをもたらしていると判断する十分な理由があるときは、当該製品のサイバーレジリエンス法案の遵守に関する評価を実施することができ、当該製品の違反を認定した場合、市場監視当局は、当該製品の回収等の措置を講ずることを関連事業者に対して求めることができる(43 条 1 項)。

「製品特性に関するセキュリティ必須要件」又は「脆弱性対応必須要件」や製造業者に課せられた義務(10 条、11 条)の違反については 1500 万ユーロ又は前会計年度の全世界売上高の 2.5%のうち高い方を上限とする制裁金が、これら以外の義務の違反については 1000 万ユーロ又は前会計年度の全世界売上高の 2%のうち高い方を上限とする制裁金が、それぞれ違反者に課せられる(53 条 3 項・4 項)。

4. 今後の見込みと日本企業に求められる対応

今回公表されたサイバーレジリエンス法案は、この後、欧州議会及び閣僚理事会で法案が審議されることが予定されており、様々な関係者の声も参照しながらブラッシュアップされていくことが見込まれる。現時点では、成立・発効時期については見通せないが、EU 発の法案への対応については、いざ法律が成立してから情報収集に着手するのでは、成立過程を通じて検討を重ね、欧州当局とコミュニケーションを続けているような欧米を中心とする競合企業と比較して、対応が後手に回ってしまうおそれがあることには注意が必要である。

上記のとおり、本法案は、IoT 製品であれば、そのセクターを問わず、EU 域内に提供する日本企業に広く適用される可能性があり、これから販売を予定している製品について [8]、関連するサイバーセキュリティリスクを評価・考慮した上で適切な仕様変更やアップデートを講じること、及び、適切な適合性評価手続を経ることが必要になると考えられる。サイバーレジリエンスの確保への積極的な取組みは、経済安全保障の観点からも重視されるところであり、今後ますます高い水準で企業に求められていくものと予想される。

また、IoT 製品をめぐっては、IoT 製品のデータの権利関係を規律することになるデータ法案や、AI システムに該当する場合には AI 法案への対応も求められるようになるなど、今後成立すると考えられる複数の EU の関連法規制を横断的に理解し、その対応を検討していく必要があると考えられる [9]。

なお、いわゆるデータ保護・プライバシーの分野については、自社又は自社グループに適用される可能性のある各国の法令の動向をモニターする動きが広がってきているが、サイバーセキュリティ関連法令のモニターについては未だ手つかずということが多いのではないかと思われる。本法案の公表をきっかけに、サイバーセキュリティ関連法令の動向についても、自社又は自社グ

---

[8] 本法案の施行日より前に既に市場に売り出されている製品であっても、施行日以降、設計又は意図された目的に実質的変更が加えられた場合には、規制の対象となる(55 条 2 項)点に注意が必要である。

[9] AI 製品の賠償責任を規定する指令案も、9 月末に公表される予定であるとの報道も見受けられる(https://www.euractiv.com/section/digital/news/leak-commission-to-propose-rebuttable-presumption-for-ai-related-damages/)。

ループに適用される可能性のある各国の法令の動向のモニターを検討していくことが望ましい。

西村あさひ法律事務所　広報室　E-mail