EU サイバーレジリエンス法の官報掲載～適用開始日は 2027 年 12 月 11 日であるが、影響の甚大さと想定対応工数故に早期の着手は必至～

ヨーロッパニューズレター　　2024 年 11 月 27 日号

執筆者:
川島 章裕
a.kawashima@nishimura.com
服部 啓
k.hattori@nishimura.com

2024 年 11 月 20 日、EU において、サイバーレジリエンス法が官報に掲載され、同年 12 月 10 日に発効し、多くの規定は、2027 年 12 月 11 日より適用が開始される。これにより、ネットワーク等への接続が想定されるデジタル製品全般について、個別法令により対応が義務付けられていなくても、脆弱性への対処を含む所定のサイバーセキュリティ必須要件が課される。そして、それらの要件を確認する所定の製品安全性の手続を経なければ、EU 市場にそれらの製品を上市することができなくなるため、その影響は甚大である。適用開始まで 3 年の猶予が与えられているのは、対応に相応の工数を要することを受けてのことであり、EU 市場にそれらの製品を上市している可能性のある企業は、早急に、法令の概要の理解、該当製品の洗出し・分類、サイバーセキュリティ必須要件の充足に向けた取組み、その後求められる上市までのプロセスについて、対応の目処を付ける必要がある。本ニューズレターでは、そのような日系企業の早期の対応に資するよう、サイバーレジリエンス法の概要を速報的に解説する。

1. 適用範囲

(1) 適用対象となるデジタル製品

EU サイバーレジリエンス法（以下「CRA」という）は、スマートデバイスやソフトウェア等のデジタル要素を有する製品のサイバーセキュリティをそのライフサイクルを通じて確保することを目的としており、2024 年 10 月 17 日に加盟国法への移行期限を迎えた NIS2 指令等の既存の法令ではカバーできていない領域を補完する法令である。具体的には、CRA は、EU 域内市場において商業活動の過程で供給されるデジタル要素を含む製品（以下「デジタル製品」という）のうち、意図された又は合理的に予見される使用法の中にデバイス又はネットワークへの直接的又は間接的な、論理的又は物理的なデータ接続を想定したデジタル製品に適用される（2 条 1 項）。

ただし、CRA は、既に規制されているデジタル製品（医療機器規則（Regulation（EU）2017/745）、対外診断用医療機器規則（Regulation（EU）2017/745）、自動車の型式認証規則（Regulation（EU）2019/2144）が適用されるデジタル製品（2 条 2 項）、民間航空機における一般規則（Regulation（EU）2018/1139）に従って認証されているデジタル製品（2 条 3 項）等）や、国家安全保障又は防衛のみを目的として開発されるデジタル製品（2 条 7 項）等の一定の類型のデジタル製品については、適用されない。

(2) デジタル製品の意義

デジタル製品とは、あらゆるソフトウェア又はハードウェアの製品及びその遠隔データ処理ソリューショ

ンをいい、本体とは別個に上市されるソフトウェア又はハードウェアのコンポーネントも含む（3 条(1)号）。また、CRA は、通常のデジタル製品とは別に、特にサイバーセキュリティの重要性が高い類型のデジタル製品を重要な（important）デジタル製品（7 条）又はクリティカルな（critical）デジタル製品（8 条）として指定しており、重要なデジタル製品は、さらに Class I と Class II に分類される（7 条 2 項）。各デジタル製品は、その分類に応じて、サイバーセキュリティ必須要件への適合性を示すための適合性評価手続が異なる。

(3) 適用対象となる事業者

CRA は、デジタル製品の製造者（デジタル製品を自ら開発若しくは製造し、又は他者に設計、開発若しくは製造させて、自己の名称又は商標の下でデジタル製品を販売する者）、輸入者（EU 域内の者で、EU 域外に所在する者の名称又は商標が付されたデジタル製品を EU 域内市場に輸入する者）、販売者（EU 域内の者で、EU デジタル市場にデジタル製品を流通させる者であって、製造者又は輸入者に該当しない者）に適用される。

2. 主な義務内容

(1) サイバーセキュリティ必須要件

EU 域内市場においてデジタル製品を上市するためには、デジタル製品がデジタル製品の特性に関するサイバーセキュリティ必須要件を満たし、デジタル製品の製造者が導入するプロセスが脆弱性対処要件を満たしている必要がある（6 条、Annex I）（以下、両要件を総称して、「サイバーセキュリティ必須要件」という）。サイバーセキュリティ必須要件は、製造者がその確保に関する一次的な責任を負い、輸入者及び販売者はその遵守の確保等の二次的な責任を負う。

項目	内容
デジタル製品の特性に関するサイバーセキュリティ必須要件	①リスクに基づいて適切な水準のサイバーセキュリティを確保する形で設計、開発及び製造すること ②サイバーセキュリティリスクアセスメントに基づき、デジタル製品が以下の特性を備えること ・既知の悪用可能な脆弱性を有しないこと ・セキュア・バイ・デフォルト設定 ・セキュリティアップデートによる脆弱性への対処可能性の確保 ・不正アクセスからの保護の確保、不正アクセスの可能性が生じた場合における報告 ・処理データの機密性保護 ・処理データ、コマンド、プログラム及び設定の完全性保護並びに破損の報告 ・製品の使用目的に照らして関連性があり、必要最小限度のデータに限定した処理 ・必要不可欠な機能の可用性保護（DoS 攻撃への回復力及び緩和を含む） ・他のデバイス又はネットワークが提供するサービスの可用性への悪影響の最小化 ・攻撃対象領域を制限する設計、開発及び製造 ・適切な悪用緩和メカニズム等の使用によるインシデントの影響を緩和する設計、開

	発及び製造 ・内部アクティビティの記録・監視によるセキュリティ関連情報の提供 ・利用者が全てのデータ及び設定を安全かつ容易に永続的に削除する可能性の提供及び他の製品又はシステムへのデータ移転が行われる場合における安全な移転
脆弱性対処要件	・脆弱性及びコンポーネントの特定及び書面化 ・脆弱性に遅滞なく対応すること（機能アップデートとは別のセキュリティアップデート） ・効果的で定期的なテスト及びレビューの適用 ・セキュリティアップデートに伴い、解消済みの脆弱性に関する情報の公表 ・協調的脆弱性開示ポリシーの整備及び実施 ・製品及び製品中のサードパーティコンポーネントに関する潜在的な脆弱性についての情報共有を促進する措置の実施 ・悪用可能な脆弱性の適時修正又は緩和を確保する、セキュアなアップデート配布メカニズムの提供 ・特定のセキュリティイシューへの対応のために利用可能な場合、セキュリティアップデートが、ユーザーに対し、遅延なく、無料で、実施される措置等の関連情報を伝えるメッセージとともに配布されることの確保

(2) 適合性の推定

サイバーセキュリティ必須要件については、標準規格（harmonized standards）又は（標準規格が策定されない場合に欧州委員会が採択した）共通仕様（common specification）の策定が予定されており、デジタル製品がいずれかに適合する場合、サイバーセキュリティ必須要件への適合性が推定される（27 条 1、2、5 項）。また、サイバーセキュリティ法（Regulation (EU) 2019/881）に基づく欧州サイバーセキュリティ認証スキームに準拠する場合も、サイバーセキュリティ必須要件への適合性が推定される（27 条 8 項）。

(3) 適合性評価

デジタル製品の製造者は、サイバーセキュリティ必須要件が満たされているかを決定するために、デジタル製品及び製造者が実施するプロセスに関する適合性評価を実施しなければならない（32 条）。適合性評価の実施方法には、①内部管理手続による方法（Annex VIII のモジュール A）、②EU 型式認証手続（Annex VIII のモジュール B）の後に内部管理手続に基づく EU 型式適合（Annex VIII のモジュール C）を実施する方法、③完全品質保証に基づく適合性評価による方法（Annex VIII のモジュール H）、④欧州サイバーセキュリティ認証スキームによる方法がある。適合性評価の方法は、デジタル製品の分類によって異なる。

(4) 製造者の主な義務

製造者は、デジタル製品のサイバーセキュリティ必須要件の遵守の確保について、第一次的な義務を負う。具体的には、製造者は、主に、以下のような義務を負う（13 条）。
①設計・開発・製造段階における製品特性に関するサイバーセキュリティ必須要件の遵守の確保

②サイバーセキュリティリスク評価の実施、関連事項の文書化・アップデート
③脆弱性を検知した場合、及び、デジタル製品のサポート期間中における、脆弱性対処要件に適合する適切な対応、並びにそのためのポリシー及び手続きの策定
④デジタル製品を利用可能とした後少なくとも 10 年間、セキュリティアップデートをユーザーに提供
⑤適合性評価の実施、CE マークの表示
⑥デジタル製品のパッケージや付属文書における、製造者の名称・連絡先、サポート期間等、ユーザー向けの情報提供
⑦適切な文書作成の上、市場監視当局の求めに応じて提出
⑧デジタル製品の脆弱性の悪用又は重大なインシデント発生を認識してから 24 時間以内における CSIRT 及び ENISA への報告及び続報並びにユーザーへの通知

(5) 輸入者及び販売者の主な義務

輸入者及び販売者は、自らがデジタル製品のサイバーセキュリティ必須要件の適合性評価を実施する義務はないものの、デジタル製品を上市する又は流通させる前にデジタル製品がサイバーセキュリティ必須要件を遵守していることの確保又は確認を行う義務を含め、第二次的な義務を負う。輸入者及び販売者は、自己が上市又は流通させたデジタル製品が CRA に適合しない場合に取扱いを停止し、当該デジタル製品の製品回収又はリコールその他の是正措置を実施する義務、デジタル製品に脆弱性があると認識した場合に製造者への通知を行う義務、さらに重大なサイバーセキュリティリスクを生じさせ得ると考える合理的な理由がある場合には市場監視当局への適切な報告を行う義務、市場監督当局による調査等に協力する義務等を負う。また、輸入者は、ユーザーへの一定の情報提供や技術文書の一定期間の保管義務も負う（19、20 条）。

3. 制裁金

Annex I に記載されるサイバーセキュリティ必須要件又は製造者の義務の違反に対しては、1,500 万ユーロ又は前会計年度の全世界売上高の 2.5%のいずれか高い金額を上限とする制裁金が課され得る（64 条 2 項）。これら以外の義務違反に対しては、1,000 万ユーロ又は前会計年度の全世界売上高の 2%のいずれか高い金額を上限とする制裁金が課され得る（64 条 3 項）。また、不正確、不完全又は誤解を招く情報を報告先の機関又は市場監視当局に対して提供した場合、500 万ユーロ又は前会計年度の全世界売上高の 1%のいずれか高い金額を上限とする制裁金を課され得る（64 条 4 項）。なお、CRA の違反時に適用される制裁金に関するルールの制定及び執行は各加盟国が行うこととされている（64 条 1 項）。

4. 法令横断的な視点の必要性

CRA は、EU AI Act のサイバーセキュリティ要件の適合性に関するルールについても、規律を定めている。EU AI Act においてハイリスク AI システムとして分類されるデジタル製品は、以下の全ての要件を満たす場合、同法 15 条に定められたサイバーセキュリティ要件に適合するとみなされる（12 条）。
①デジタル製品は、上記 2(1)のデジタル製品の特性に関するサイバーセキュリティ必須要件に定められたサイバーセキュリティ必須要件を満たす。
②製造者が導入するプロセスは、上記 2(1)の脆弱性対処要件に定められたサイバーセキュリティ必須要件を満たす。

③EU AI Act 15 条で要求されるサイバーセキュリティ保護レベルの達成は、CRA に基づいて発行された EU 適合性宣言書で実証されている。

このように、CRA の適合性の評価は、EU AI Act の製品安全性確保のメカニズムにも組み込まれているが、EU のデジタル領域の法令は、基本権の保護という観点から相互にリンクする形で規制を設けていることが少なくないため、個別の法令への対応という視点だけでなく、法令横断的な視点を踏まえた対応を行うことが重要であるように思われる。

西村あさひ 広報課 newsletter@nishimura.com