NAGASHIMA OHNO & TSUNEMATSU
長島・大野・常松法律事務所
NO&T Technology Law Update
テクノロジー法ニュースレター

2024年7月
テクノロジー法ニュースレター　No. 52
欧州最新法律情報　No. 32

欧州サイバーレジリエンス法（Cyber Resilience Act）の概要（2024年11月28日更新版）

弁護士 鈴木 明美
弁護士 松宮 優貴

※本ニュースレターは、欧州サイバーレジリエンス法が2024年12月10日に発効するのを受け、2024年11月28日付で記事のタイトル及び内容をアップデートしています。
※2025年2月7日付で「デジタル製品の重要性に応じた分類と必須セキュリティ要件」の内容をアップデートしています。

はじめに

欧州では、近年、データ法（Data Act）やAI法（AI Act）等、新しいテクノロジー分野に関する規制が次々と定められていますが、サイバーセキュリティに関する規制も様々存在します。本ニュースレターにおいては、それらのサイバーセキュリティに関する規制のうち、**本年12月10日**に発効することになったサイバーレジリエンス法（Cyber Resilience Act）（以下「サイバーレジリエンス法」）について、概要を説明します。

サイバーレジリエンス法は、分野や業種に関わらず、広くデジタル製品一般について、設計・開発・上市・販売後までのライフサイクルを通じたサイバーセキュリティ要件を定めています。成立後は、一定の猶予期間を経て、法に定めるセキュリティ要件が事業者に課され、違反した企業には高額の制裁金が科される可能性があります。また、欧州域内にIoT製品等のデジタル製品を流通させる事業者であれば、欧州域内に拠点を持たない事業者であっても適用の可能性があります。

したがって、欧州市場に向けてデジタル製品を販売する可能性のある日本企業におかれましては、猶予期間が経過するまでに必要な体制整備を完了できるよう、十分な事前検討・準備を行う必要があります。

制定の背景・経緯

欧州におけるサイバーセキュリティに関する規制としては、2016年に発効したNIS指令（Directive on Security of Network and Information Systems）が一定の基幹サービス及びオンラインサービスを対象としたサイバーセキュリティ対策について定めており、その改訂版であるNIS2指令（2023年1月発効）はさらに対象範囲を拡大し、一定の重要分野におけるリスク対策やインシデントの報告義務等を定めています。

さらに、特にリスクの高い分野に関しては、クリティカルインフラに関するCER（Directive on the Resilience of Critical Entities）や、2025年1月から適用が開始される金融システムに関するDORA（Regulation on Digital Operational Resilience of the Financial Sector）、さらに、特定の製品群に関する規制として、医療機器、自動車や航空機に関する個別の規制も存在します。

しかし、これら個別規制の対象とならないデジタル製品は多く存在し、一般に流通するデジタル製品の多くがサイバーセキュリティに関する最低限の要素も備えておらず、深刻化するハッキング等のサイバー攻撃に対して脆弱であることが問題視されていました。また、一旦市場に出たデジタル製品について継続的なサイバーセキュリティ対策が提供されることは少なく、新しいサイバー攻撃への対応が期待できないことも問題とされました。

そのため、2022 年 9 月に、欧州委員会がサイバーレジリエンス法案を上程し、2023 年 11 月に欧州議会と欧州閣僚理事会との政治的合意を経て、2024 年 3 月 12 日に欧州議会において修正後のサイバーレジリエンス法案が承認されました。同法案は、**同年 10 月 10 日**に欧州閣僚理事会によって承認され、所定の手続を経て **2024 年 12 月 10 日**に EU 法として発効することになりました。

発効後は、対象となる事業者が必要な対応を進める期間を確保するため、適用開始までに所定の猶予期間が設けられており、適用開始時期は、全体については同法の発効後 36 ヶ月後**（2027 年 12 月 11 日）**からとされていますが、インシデント発生や脆弱性に関する報告義務（第 14 条）については同法の発効後 21 ヶ月後**（2026 年 9 月 11 日）**から、適合性評価機関に関する規定（第 4 章）については同法の発効後 18 ヶ月後**（2026 年 6 月 11 日）**からとされています。

対象となるデジタル製品及び事業者

1. 対象となるデジタル製品

サイバーレジリエンス法は、欧州市場において流通するデジタル要素を有するあらゆる製品に対して、一定の必須セキュリティ要件を課すことを目的としています。

「デジタル要素を有するあらゆる製品（products with digital elements）」とは、ソフトウェア又はハードウェア製品及びその遠隔データ処理ソリューションを意味します（以下「デジタル製品」）（第 3 条第 1 項）。IoT 製品やネットワーク機器からデジタル通信機能を持った玩具まで、さまざまな製品がこれに含まれます。

一方、型式認証規則（医療機器規則、対外診断用医療機器規則、民間航空機規則及び自動車）の対象製品、国家安全保障に関するデジタル製品や軍事目的・機密処理目的のもの、SaaS 等のソフトウェアサービス、並びに、研究開発目的のオープンソースソフトウェアは、それぞれ個別の法令によってセキュリティ要件が課されていることから、サイバーレジリエンス法との関係では適用除外とされています。

2. 対象となる事業者

サイバーレジリエンス法に基づいて義務を負う主体は以下の通りであり、それぞれについて異なる内容の義務が定められています。

① 製造者：対象となるデジタル製品を開発若しくは製造し、又はデジタル製品を設計、開発若しくは製造させ、自己の名において販売する主体

② 輸入者：EU 域外に所在する事業者等の名称又は商標が付されたデジタル製品を EU 市場に輸入する EU 域内の主体

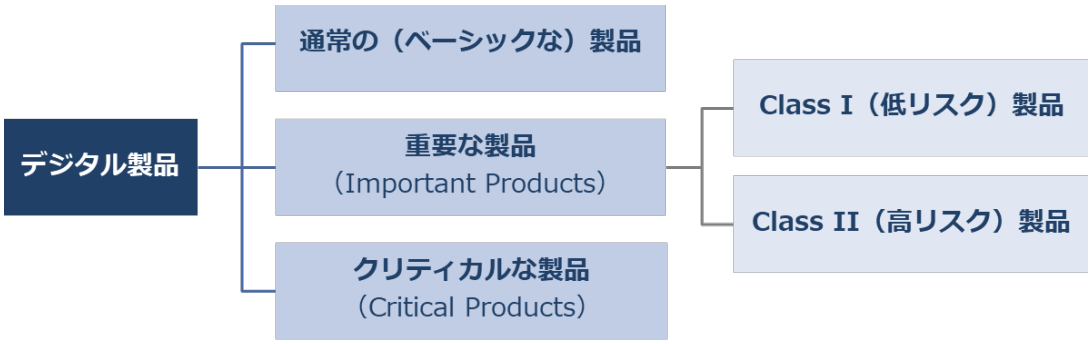
③ 販売者：EU 市場においてデジタル製品を販売する EU 域内の主体で、製造者又は輸入者ではない者

なお、輸入者又は販売者が、自らの名称や商標を付してデジタル製品を販売したり（例：OEM）、市販されているデジタル製品に自ら重要な改変を加えて販売したりする場合、あるいは製造者、輸入者及び販売者以外の者がデジタル製品に自ら重要な改変を加えて販売する場合には、製造者と見做されます（第 21 条、第 22 条）。

デジタル製品の重要性に応じた分類と必須セキュリティ要件

1. デジタル製品の分類

対象となるデジタル製品は、以下の通り分類されます。



（1）重要な製品（Important Products）

重要な製品とは、サイバーレジリエンス法の附属書 III（Annex III）に定めるカテゴリに分類される中核機能を有するデジタル製品であって、以下のいずれかの基準を満たすものを言います（第 7 条）。

a	当該デジタル製品が、主に他の製品・ネットワーク又はサービスのサイバーセキュリティにとって重要な役割（例えば、認証及びアクセスの確保、侵入防止及び侵入検知、エンドポイントセキュリティ又はネットワーク保護等）を果たすデジタル要素を備えること
b	当該デジタル製品が、ネットワーク管理、構成制御、仮想化又はパーソナルデータの処理を含む中央システム機能など、直接操作により他の大量の製品又はそのユーザーの健康、セキュリティ又は安全性を攪乱し、支配し又は損害を与える能力及び強度において重大な悪影響を生じさせるリスクを有する機能を実行すること

附属書 III に記載されている製品カテゴリは以下の通りです。

Class I（低リスク）製品	Class II（高リスク）製品
▪ ID 管理システム、アクセス管理ソフトウェア及びハードウェア（生体認証等の認証用リーダーを含む） ▪ スタンドアローン/組み込み型ブラウザ ▪ パスワードマネジャー ▪ マルウェア検知、削除又は隔離用ソフト ▪ VPN 機能を持つ製品 ▪ ネットワーク管理システム ▪ SIEM（セキュリティ情報イベント管理） ▪ ブートマネジャー ▪ 公開鍵インフラ及び電子証明書発行ソフトウェア ▪ 物理及び仮想ネットワークインターフェース ▪ OS ▪ ルータ、モデム、スイッチ ▪ セキュリティ関連機能を有するマイクロプロセッサ ▪ セキュリティ関連機能を有するマイクロコントローラ ▪ セキュリティ関連機能を有する ASIC 及び FPGA ▪ スマートホーム汎用目的バーチャルアシスタント ▪ セキュリティ機能を有するスマートホーム製品（スマートロック、セキュリティカメラ、ベビーモニター及び警報システムを含む） ▪ 規制 [1]の対象となるデジタル通信機能を持った玩具であって、ソーシャルコミュニケーション機能又は位置情報	▪ OS や同様の環境の仮想化を実施するためのハイパーバイザー及びコンテナ・ランタイム・システム ▪ ファイヤーウォール、侵入検知・防止システム ▪ 不正防止機能を備えたマイクロプロセッサ ▪ 不正防止機能を備えたマイクロコントローラ

1 Directive 2009/48/EC

トラッキング機能を持つもの ▪ 身体に装着して健康状態のモニタリングを行うためのウェアラブル製品であって規制[2]の対象とならないもの、及び子供が使用することを想定したウェアラブル製品	

（2）クリティカルな製品（Critical Products）

クリティカルな製品とは、サイバーレジリエンス法の附属書 IV（Annex IV）に列挙する各カテゴリを中核機能とするデジタル製品であって、その強度や多数の他のデジタル要素を含む製品に混乱、制御、又は損害を生じさせる能力及び強度において重大な悪影響を及ぼすリスクを伴うサイバーセキュリティ関連の製品を言います（前文(46)、第 8 条）。具体的には以下の通りです。

クリティカルな製品
▪ セキュリティボックスを含むハードウェア製品 ▪ 一定の要件を備えたスマートメーターシステム[3]内のスマートメーターゲートウェイ ▪ セキュアエレメントを含む、スマートカード又は類似の製品

（3）通常の（ベーシックな）製品（General Products）

通常の製品は、重要な製品及びクリティカルな製品以外の全てのデジタル製品を指します。

2. 必須セキュリティ要件

デジタル製品を EU 市場に流通させるためには、当該製品が一定の必須セキュリティ要件を満たし、それが証明されている必要があります。必須セキュリティ要件の詳細は附属書 I（Annex I）に定められており、サイバーセキュリティ要件（パート I）と製造者が遵守すべき脆弱性対応に関する要件（パート II）に分かれます。サイバーセキュリティ要件には、主に以下の内容が含まれます。

① 悪用可能な既知の脆弱性がないこと
② デフォルト設定で安全な状態であること
③ セキュリティアップデートが適用されること
④ 不正アクセスを防止するための認証システムを備えること
⑤ 当該デジタル製品が取り扱うデータについて機密性が保たれていること
⑥ 当該デジタル製品が取り扱うデータ及びコマンド等について外部からの改変等を防止すること
⑦ 当該デジタル製品の目的との関係で必要なデータのみを取り扱うこと
⑧ インシデント等が発生した場合でも必須基本機能を維持できるよう保護すること
⑨ 他の機器やネットワークへの悪影響を最小化すること
⑩ ユーザーによるデータや設定の移行可能性（データポータビリティ）を確保すること

3. 適合性評価

デジタル製品の製造者は、デジタル製品を EU 市場に流通させる前に、一定の適合性評価を行うことにより、当該製品がセキュリティ要件を満たすことを証明しなければなりません（第 32 条）。適合性評価の手法は、上述したデジタル製品の分類によって異なります。

クリティカルな製品については、主として、今後クリティカルな製品に関して定められるサイバーセキュリティ認証規格による認証を受けなければならないこととされています。

重要な製品については、①附属書 VIII のモジュール B に従った EU 型式審査機関による型式認証及びモジュー

2 Regulation (EU) 2017/745 又は Regulation (EU) 2017/746

3 送電網に供給される電力または送電網から消費される電力を測定することができ、従来のメーターよりも多くの情報を提供し、電子通信の形式を使用して、情報、監視、制御の目的でデータを送受信することができる電子システム。（Directive (EU) 2019/944、第 2 条第 23 項）

ルCに基づく内部生産コントロール、②附属書VIIIのモジュールHに従った完全品質保証（full quality assurance）ベースの適合宣言、③サイバーセキュリティ法（Regulation (EU) 2019/881）に基づくサイバーセキュリティ認証規格が適用される場合、同認証規格において「Substantial」レベル以上の適合性を得ることのいずれかが必要となります。但し、Class I（低リスク）製品については、今後欧州標準化機関（European Standards Organisations）が策定し欧州委員会が承認する標準規格（harmonised standards）に適合する場合、あるいは、欧州委員会が定める共通仕様（common specifications）に適合する場合は、上記の手法は要求されません。

通常の製品については、附属書 VIII のモジュール A に従った内部コントロール手続に則った自己適合宣言に拠ることが認められています。

製造者の義務

デジタル製品の製造者に課される主な義務の内容は、以下の通りです。

1. デジタル製品を上市する前に、そのセキュリティ適合性を確認すること

製造者は、デジタル製品を上市するにあたっては、当該デジタル製品が、附属書 I パート I に定めるサイバーセキュリティ要件を満たすよう設計、開発及び製造しなければなりません（第 13 条第 1 項）。

さらに、当該義務の遵守のために、製造者は、サイバーセキュリティのリスク評価を行い、その結果を、企画、設計、開発、製造、販売及びメンテナンスの過程を通して考慮する必要があります（第 13 条第 2 項）。このように、製品のライフサイクル全体を通じてサイバーセキュリティに配慮するという考え方を、「サイバーセキュリティ・バイ・デザイン」といいます。

また、当該デジタル製品に第三者の製品（フリーソフト及びオープンソースソフトウェアを含む。）を組み込む場合は、当該第三者製品にかかるデュー・ディリジェンスを行い、当該第三者製品がデジタル製品のセキュリティリスクを高めるものでないことを確認しなければなりません（第 13 条第 5 項）。

上述した適合性評価を行った上で、適合性が確認されたデジタル製品は、EU 適合宣言書（「CE マーク」）をつけなければなりません（第 13 条第 12 項、第 28 条、第 30 条）。

2. デジタル製品の上市後も、セキュリティ適合性を維持すること

製造者は、デジタル製品の上市後も、開発及び製造プロセスやデザインの変更、サイバーセキュリティに関する基準の変更等への対応を継続し、本法に定めるセキュリティ要件への適合性を維持するための手続を継続しなければなりません（第 13 条第 14 項）。

3. サイバーセキュリティに関する事項を文書にまとめ、適時にアップデートすること

製造者は、その製造するデジタル製品を市場に投入する前に行ったリスクアセスメントの結果を文書化し、当該製品の「サポート期間」中、当該文書を必要に応じてアップデートしなければなりません（第 13 条第 3 項）。「サポート期間」とは、製造者が附属書 I パート II に定める脆弱性対応を行うべき期間であり、当該デジタル製品に関するユーザーの合理的な期待や製品の性質等を踏まえた製品寿命その他の諸要素をベースに定められますが、最低でも上市後 5 年間（想定使用期間がそれより短い場合はその期間）とされています。

また、製造者は、当該製品と共に提供する技術文書中に、当該アセスメント関連文書を含める必要があります（第 13 条第 4 項）。

さらに、その製造するデジタル製品のリスクの程度に応じて適切な方法で、当該製品に関するサイバーセキュリティ関連事項、すなわち、製造者が認識する脆弱性の内容、第三者から提供を受けた関連情報等を文書にまとめた上、必要に応じて当該文書を適時にアップデートしなければなりません（第 13 条第 7 項）。

4. 脆弱性を発見した場合に適切な対応をとること

製造者は、その製造するデジタル製品を構成する部品に含まれる脆弱性（当該製品に組み込まれるオープンソースソフトウェアの脆弱性を含む。）を発見した場合、当該部品またはソフトウェアの製造又は維持を行う主体に当該脆弱性について報告し、附属書 I パート II に定める要求事項に沿って当該脆弱性に対応しなければなりません（第 13 条第 6 項）。

さらに、デジタル製品のサポート期間中、附属書 I パート II に従って当該製品またはその部品の脆弱性への効

果的な対応を継続する必要があり、脆弱性への対応に係るポリシー及び手続を定めておく必要があります（第 13 条第 8 項）。

また、サポート期間中、製造者は、自社製品が附属書 I に定める必須セキュリティ要件に適合していないと判断した場合、直ちに、不適合を是正し、必要に応じて製品回収やリコールを行う等の是正措置を行う必要があります（第 13 条第 21 項）。

5. デジタル製品の上市後 10 年間セキュリティアップデートや技術文書等を保持すること

当該製品の上市後 10 年間又は当該製品のサポート期間のいずれか長い方の期間、附属書 I パート II に定めるセキュリティアップデートがユーザーによって利用可能な状態におく必要があります（第 13 条第 9 項）。

また、同期間中、当該デジタル製品に関する技術文書及び当該デジタル製品の EU 適合宣言書を、市場監督当局が閲覧できるよう保持しなければなりません（第 13 条第 13 項）。

6. 旧バージョンのサポート終了に一定の条件が課されること

製造者があるソフトウェア製品の新バージョンを上市した場合、製造者は、過去製品のユーザーが当該最新版に無料でアクセスできるようになっており、最新版を利用することに追加のコストがかからない場合に限り、セキュリティアップデートの提供を通じて脆弱性対応を行う対象を新バージョンのみとすることができます（第 13 条第 10 項）。

7. デジタル製品と共に一定の情報をユーザーに提供すること

製造者は、デジタル製品の型番号、バッチまたはシリアルナンバー等、当該デジタル製品を特定する情報を製品自体（それができない場合にはパッケージ又は付属文書）に記載し、製造者の名称その他コンタクト情報等を、製品自体、パッケージ又は付属文書に記載しなければなりません（第 13 条第 15 項、第 16 項）。製造者は、ユーザーから製造者へのコンタクトのための単一の問い合わせ窓口を設定しなければなりません（自動案内のみは不可）（第 13 条第 17 項）。

また、当該製品に関する一定の情報及び指示説明（製造者の特定に関する情報、当該製品の脆弱性に関する報告先、当該製品の使用環境に関する指示説明、誤った使用方法の例等）をユーザー及び市場監督当局にわかりやすい形でまとめ、紙又は電子的いずれかの方法で当該デジタル製品に添付してユーザーに提供し、上市後 10 年間または当該製品のサポート期間のいずれか長い方の期間を通じて、ユーザー及び当局が閲覧できる状態に置かなければなりません（第 13 条第 18 項、附属書 II）。

さらに、当該製品のサポート期間の終期について、ユーザーが当該デジタル製品を購入する際に明確に認識できるように明示しなければならず、さらに、当該デジタル製品の性質上可能な場合は、サポート期間が終了したことをデジタル製品に表示することによりユーザーに通知しなければなりません（第 13 条第 19 項）。

製造者は、当該製品にかかる適合宣言書のコピーを当該デジタル製品と共に提供しなければなりません（第 13 条第 20 項）。

8. 市場監督当局による調査等に協力すること

市場監督当局による要請を受けた場合に必要な資料を提供する等、その調査に協力し、デジタル製品に関するサイバーセキュリティリスクの低減に向けて協力しなければなりません（第 13 条第 22 項）。

9. 事業の終了等に関する報告を行うこと

デジタル製品の製造者がその事業を終了する場合等、サイバーレジリエンス法に基づく義務を履行することができなくなる場合は、事前に、市場監督当局及びユーザー（可能な限り）に対して報告を行わなければなりません（第 13 条第 23 項）。

10. 脆弱性発見・インシデント発生時に、期限内に適切な報告を行うこと

自らが製造するデジタル製品について積極的に悪用される可能性のある脆弱性が発見された場合、又は重大なインシデントが発生した場合には、コーディネーターとして指定された CSIRT（Computer Security Incident Response Team）及び ENISA（European Network and Information Security Agency）に同時に通知しなければなりません（第 14 条第 1 項、第 3 項）。当該通知は、①対象となる脆弱性を認識してから 24 時間以内に行う速報と、②72 時間以内に行う第 2 報、③当該脆弱性への対策を行ってから 14 日（インシデント発生の場合は第

２報から１ヶ月）以内に行う最終報告からなるものとされています（第 14 条第 2 項、第 4 項）。

さらに、当該脆弱性又はインシデントによる影響を受けるユーザー（適切な場合は、全てのユーザー）に対して、当該脆弱性又はインシデントの情報、及び、必要な場合は、インシデントの影響を軽減するためにユーザーが取れる対応等について通知しなければなりません（第 14 条第 8 項）。

輸入者の義務

1. デジタル製品を市場に投入する前に、セキュリティ要件への適合性を保証すること

輸入者は、附属書Ⅰパート I に定めるサイバーセキュリティ要件を満たすデジタル製品であって、製造プロセスが附属書 I パート II に定める脆弱性対応に関する要件を満たすもののみを市場に投入しなければならず、当該デジタル製品を市場に投入する前に、製造者が当該デジタル製品について適切な適合性評価を実施し、技術文書を作成し、CE マークが付されており、製造者による必要な情報提供が行われていること等を確認しなければなりません（第 19 条第 1 項、第 2 項）。

2. 自らが取り扱うデジタル製品が法令に適合しなくなった場合に取扱を停止し、適切な報告を行うこと

輸入者は、自らが取り扱うデジタル製品又はその製品の製造者による製造プロセスが本法に適合していない場合、不適合が解消されるまではこれを市場に提供せず、その取扱を停止する等の措置を講じなければなりません。また、当該デジタル製品に係るセキュリティリスクが重大なサイバーセキュリティリスクにつながる場合、市場監督当局に通知を行う必要があります（第 19 条第 3 項）。

3. 一定の情報をユーザーに提供すること

輸入者は、自らに関する一定の情報（輸入者の特定に関する情報、連絡先等）をユーザーにわかりやすく提供しなければなりません（第 19 条第 4 項）。

4. 自らが流通させたデジタル製品が法令に適合しなくなった場合に適切な対応及び報告を行うこと

輸入者は、自らが EU 市場に流通させたデジタル製品が本法に適合していない場合、直ちに、不適合を是正し、（適切な場合には）製品回収やリコールを行う等の是正措置を行う必要があります。また、自らが取り扱うデジタル製品に関する脆弱性を発見した場合、当該デジタル製品の製造者に対して遅滞なく報告を行い、さらに当該デジタル製品が重大なセキュリティリスクを伴う場合には市場監督当局にも直ちに情報提供を行う必要があります（第 19 条第 5 項）。

5. デジタル製品の上市後 10 年間技術文書等を保持すること

輸入者は、その取り扱う製品の上市後 10 年間またはサポート期間のうちいずれか長い方の期間、当該デジタル製品にかかる適合宣言書及び技術文書を、市場監督当局が閲覧できるよう保持しなければなりません（第 19 条第 6 項）。

6. 市場監督当局による調査等に協力すること

輸入者は、市場監督当局による要請を受けた場合に必要な資料を提供する等、その調査に協力し、自らが取り扱うデジタル製品に関するサイバーセキュリティリスクの低減に向けて協力しなければなりません（第 19 条 7 項）。

7. 事業の終了等に関する報告を行うこと

輸入者は、自らが取り扱うデジタル製品の製造者がその事業を終了し、サイバーレジリエンス法に基づく義務を履行することができなくなっていることを認識した場合は、市場監督当局及びユーザー（可能な限り）に対して報告を行わなければなりません（第 19 条第 8 項）。

販売者の義務

1. デジタル製品を市場に投入する前に、セキュリティ要件への適合性を保証すること

販売者は、デジタル製品を市場に投入する前に、サイバーレジリエンス法に定める要求事項に留意の上、当該デジタル製品に CE マークが付されており、製造者及び輸入者がサイバーレジリエンス法上の一定の義務を履行し、必要な情報提供を行っていることを確認しなければなりません（第 20 条第 1 項、第 2 項）。

2. 自らが取り扱うデジタル製品が法令に適合しなくなった場合に取扱を停止し、適切な報告を行うこと

販売者は、自らが保有する情報に基づいて、自らが取り扱うデジタル製品が附属書 I に定めるサイバーセキュリティ要件に適合しないと判断した場合、不適合が解消されるまではこれを市場に提供せず、その取扱を停止する等の措置を講じなければなりません。また、当該デジタル製品に係るセキュリティリスクが重大なサイバーセキュリティリスクにつながる場合、遅滞なく市場監督当局に通知を行う必要があります（第 20 条第 3 項）。

3. 自らが流通させたデジタル製品が法令に適合しなくなった場合に適切な対応及び報告を行うこと

販売者は、自らが保有する情報に基づいて、自らが EU 市場に流通させたデジタル製品又はその製品の製造者による製造プロセスが本法に適合していないと判断した場合、適合性を確保するための是正措置、又は（適切な場合には）製品回収やリコールが行われるようにしなければなりません。また、自らが取り扱うデジタル製品に関する脆弱性を発見した場合、当該デジタル製品の製造者に対して遅滞なく通知し、さらに当該デジタル製品が重大なセキュリティリスクを伴う場合には市場監督当局にも直ちに情報提供を行う必要があります（第 20 条第 4 項）。

4. 市場監督当局による調査等に協力すること

販売者は、市場監督当局による要請を受けた場合に必要な資料を提供する等、その調査に協力し、自らが取り扱うデジタル製品に関するサイバーセキュリティリスクの低減に向けて協力しなければなりません（第 20 条第 5 項）。

5. 事業の終了等に関する報告を行うこと

販売者は、自らが保有する情報に基づいて、自らが取り扱うデジタル製品の製造者がその事業を終了し、サイバーレジリエンス法に基づく義務を履行することができなくなっていることを認識した場合は、市場監督当局及びユーザー（可能な限り）に対して遅滞なく報告を行わなければなりません（第 20 条第 6 項）。

罰則

附属書 I に定める必須サイバーセキュリティ要件又は本法第 13 条若しくは第 14 条に定める義務（製造者の義務）の違反に関しては、最大で 1,500 万ユーロまたは当該事業者の前年度の全世界の年間売上高の 2.5%のうちいずれか高い金額の制裁金を科せられる可能性があります。また、その他同法が定める特定の義務（輸入者及び販売者の義務を含みます。）に違反した場合、最大で 1,000 万ユーロまたは当該事業者の全世界の年間売上高の 2%のうちいずれか高い金額の制裁金を科せられる可能性があります（第 64 条）。

最後に

サイバーレジリエンス法は EU 市場にデジタル製品を販売する事業者であれば EU に拠点を持たない企業であっても適用の可能性があります。デジタル製品の定義は非常に広範であるため、多くの日本企業において検討の必要のある法令であると言えます。

サイバーレジリエンス法には、適合性評価のプロセスやセキュリティ文書の作成と具備、上市した後の継続的なモニタリングやアップデート等、一朝一夕には対応が難しい規定が含まれています。適用の可能性のある日本企業においては、必要に応じて対応期限までに適切な対応ができるよう、自らの製品への適用の有無及び具体的な対応策の検討を行う必要があります。

2024 年 7 月 22 日
2024 年 11 月 28 日更新
2025 年 2 月 7 日更新

[執筆者]

鈴木 明美（弁護士・パートナー）
akemi_suzuki@noandt.com
1999 年慶應義塾大学法学部法律学科卒業。2000 年弁護士登録（第一東京弁護士会）、長島・大野・常松法律事務所入所。2006 年スタンフォード・ロースクール修士（LL.M.）課程修了。2007 年米国ニューヨーク州弁護士登録。
主な取扱分野は、クロスボーダーを中心とする企業法務一般のほか、国内外の企業に対するデータ保護規制、その他データにまつわる様々な法律問題に関する助言。

松宮 優貴（弁護士）
yuki_matsumiya@noandt.com
2011 年東京大学法学部卒業、2012 年東京大学法科大学院（司法試験合格により）退学。2013 年弁護士登録（第一東京弁護士会）、長島・大野・常松法律事務所入所。2019 年シカゴ大学ロースクール修士（LL.M.）課程修了。2020 年米国ニューヨーク州弁護士登録。
AI、HR テック、データプロテクションやサイバーセキュリティ等、テクノロジーに関する様々な法律問題に関するアドバイスのほか、テクノロジー系企業を中心とした国内外の M&A に関するアドバイスも提供している。

[編集者]

殿村 桂司（弁護士・パートナー）
keiji_tonomura@noandt.com
企業買収（M&A）取引・知財関連取引を中心に企業法務全般に関するアドバイスを提供している。TMT 業界の案件にも幅広い経験を有しているほか、シェアリング・エコノミー、Fintech、IoT、AI などテクノロジーの発展が生み出す新しい事業分野の案件も数多く取り扱っている。

長島･大野･常松 法律事務所　www.noandt.com

〒100-7036　東京都千代田区丸の内二丁目７番２号　ＪＰタワー
Tel: 03-6889-7000（代表）　Fax: 03-6889-8000（代表）　Email: info@noandt.com

長島・大野・常松法律事務所は、約 600 名の弁護士が所属する日本有数の総合法律事務所であり、東京、ニューヨーク、シンガポール、バンコク、ホーチミン、ハノイ、ジャカルタ*及び上海に拠点を構えています。企業法務におけるあらゆる分野のリーガルサービスをワンストップで提供し、国内案件及び国際案件の双方に豊富な経験と実績を有しています。
（*提携事務所）

テクノロジー法ニュースレター及び欧州最新法律情報の配信登録を希望される場合には、<https://www.noandt.com/newsletters/>よりお申込みください。テクノロジー法ニュースレターに関するお問い合わせ等につきましては、<newsletter-technology@noandt.com>まで、欧州最新法律情報に関するお問い合わせ等につきましては、<newsletter-europe@noandt.com>までご連絡ください。なお、配信先としてご登録いただきましたメールアドレスには、長島・大野・常松法律事務所からその他のご案内もお送りする場合がございますので予めご了承いただけますようお願いいたします。