経済産業省

EUサイバーレジリエンス法（草案概要）

2022年9月

経済産業省

サイバーセキュリティ課

背景

- 世界的な**サイバー攻撃増加**により、対策費用は5.5兆ユーロ/年と推定。対策のために以下２つの主要課題への対応が必要。
  ①低レベルのサイバーセキュリティや脆弱性の蔓延に対処するための**セキュリティアップデートが不十分。**
  ②ユーザが**適切にセキュリティ対策を備えた製品を選択できていない**。
- サイバーインシデントが組織全体・サプライチェーン全体に短時間で多大な影響を与えており、デジタル製品がEU市場全体で使用されるため、**国境を越えた対策が必須**。
- EUサイバーセキュリティ法（2019年）には、特定製品についての記載はあるものの、具体的なデジタル製品のサイバーセキュリティに関する必須要件が含まれない。
- EUサイバーレジリエンス法は、デジタル製品のサイバーセキュリティ要件を調和させ、流通/貿易の障壁を取り除くことで、**デジタル製品に関する包括的なサイバーセキュリティ要件を規定**するもの。

＜EUにおける近年のサイバーセキュリティ規制・認証制度＞

◆ **2016年　NIS指令**
　・・・　サイバーセキュリティに関するEU全体の法律

◇ **2019年　EUサイバーセキュリティ法**
　・・・　ENISAの権限強化、サイバーセキュリティ認証制度の整備

◆ **現在　　NIS２指令改定中**
　・・・　更に対象範囲拡大し、規制レベルを向上させる

◇ **現在　　EUCC策定中**
　・・・　サイバーレジリエンス法の適合性評価手法としても利用

EUサイバーレジリエンス法（草案）

- 2022年9月に草案提出。2023年後半の発効、**2025年後半の適用**を目指す。
- 例外を除き、**デジタル要素を備えた全ての製品が対象。SBOM作成や更新プログラム提供等セキュリティ要件への適合（自己適合宣言/第三者認証）が求められる。**
- **重要なデジタル製品について、低リスク製品でEUCCやEN規格対象外の製品は第三者認証を、高リスク製品には第三者認証を求める。**（中小企業の認証手続き減額）
- 適合性評価証明書にはEU適合宣言書（CEマーク）/EUCC証明書を用いる。
- **脆弱性の悪用やインシデント発見後24時間以内にENISAへの報告を義務化。**
- **罰則あり。**（最高1,500万ユーロ又は当該企業の全世界売上高の2.5%以内）

注：EUCCとは、IoT製品を対象とする欧州サイバーセキュリティ認証。
EN規格とは、欧州整合化規格

【対象】デジタル要素を備えた全ての製品

・デバイスやネットワークに直接的/間接的に接続されるものも含む。
・医療機器規則、体外診断用医療機器規則、民間航空機規則、自動車の型式承認規則の対象製品は適用除外。
・国家安全保障に関するデジタル製品や軍事目的・機密情報処理目的のものは除外。
・SaaSなどのソフトウェアサービスは対象外。研究開発目的のOSSなども対象外。

【適合性評価】使用環境等のリスクレベル毎に以下を求める。

- **「デジタル製品」　・・・　自己適合宣言か第三者認証を選択**
- **「重要なデジタル製品」のうちクラスI（低リスク）・・・EUCCやEN規格の対象外は第三者認証**
- **「重要なデジタル製品」のうちクラスII（高リスク）・・・第三者認証**

【適合性評価証明書】

・EU適合宣言書（CEマーク）に基づく証明書
・EUCCに基づく証明書（必要に応じてEUCCを必要とする製品を指定）
※この他、市場サーベイランスも行われる。
※第三国（日本も含む）との相互承認も可能。※条文上は見当たらず。

CEマーク

デジタル製品のセキュリティ要件/重要なデジタル製品の特定方針

- デジタル要素を有する製品は全て対象となるが、そのうち使用される環境や取り扱うデータの機密性、影響の範囲を考慮して「重要なデジタル製品」を特定し、その中でも更に低リスク・高リスクに分類。

デジタル製品（デジタル要素を備えた製品）は、以下への適合を**技術文書として作成し10年間保管する。**

- 附属書Iの１**「セキュリティ特性要件」**を満たし、適切に設置・維持され、目的どおりに使用されていること。
- 製造者は附属書Iの２**「脆弱性処理要件」**を満たすこと。

重要なデジタル製品は、以下を考慮して特定。

- アドミニスター権限が実行できるもの、ネットワークやコンピューティングリソースにアクセスできるもの、データやOTへのアクセス制御ができるもの、ネットワーク制御やエンドポイントセキュリティやネットワーク保護のための重要な機能を有するもの。
- 産業環境など機密性の高い環境下で使用されるものやNIS２指令に関連のあるもの。
- 個人データなど重要/機密性の高い機能を実施するもの。
- 広範囲に悪影響を及ぼすか複数の人へ影響を与えるもの。

デジタル製品
製造者は、SBOM作成、無料での更新プログラム提供を含む「脆弱性処理要件」を遵守し、製品が「セキュリティ特性要件」を満たすこと。
・・・自己適合宣言か第三者認証かを選択

重要なデジタル製品(低リスク)
重要ではあるがリスクの低いもの
・・・第三者認証（該当する場合はEUCC）

重要なデジタル製品(高リスク)
機密性の高いもの、広範囲へ影響を及ぼすもの
・・・第三者認証

重要なデジタル製品

以下の各クラスに規定された要素を主に有するデジタル製品

クラスI(低リスク)第三者認証(EUCC,EN規格以外)

1. ID管理システム、アクセス管理ソフト
2. スタンドアロン型/組込み型ブラウザ
3. パスワードマネジャー
4. マルウェア検知・削除・隔離ソフトウエア
5. VPN機能を持つ製品
6. ネットワーク管理システム
7. ネットワーク・コンフィグレーション管理ツール
8. ネットワーク・モニタリングシステム
9. ネットワーク・リソース管理
10. SEIM（セキュリティ情報イベント管理）
11. ブートマネジャーを含む更新・パッチ管理
12. アプリケーション構成管理システム
13. リモートアクセス/共有ソフトウェア
14. モバイル機器管理ソフトウェア
15. 物理ネットワークインターフェイス
16. OS（クラスII製品以外）
17. ファイアウォール、侵入検知・防止システム（産業用以外）
18. ルータ、モデム、スイッチ（産業用以外）
19. マイクロプロセッサ（クラスII製品以外）
20. マイクロコントローラ
21. NIS 2 指令の別添Iに示される目的でのASIC、FPGA
22. PLC、DCS、CNC、SCADAなどの産業用自動化制御システム（IACS）（クラスII製品以外）
23. 産業用IoT（クラスII製品以外）

クラスII(高リスク) 第三者認証

1. OSであってサーバ、デスクトップ、モバイル機器用のもの
2. OSや同様の環境の仮想化を実施するためのハイパバイザー及びコンテナー・ランタイム・システム
3. 公開鍵インフラ及びデジタル証明書発行
4. 産業用のファイアウォール、侵入検知・防止システム
5. 汎用マイクロプロセッサ
6. PLCやセキュアエレメントへの統合を目的としたマイクロプロセッサ
7. 産業用のルータ、モデム、スイッチ
8. セキュアエレメント
9. ハードウェア・セキュリティ・モジュール（HSMs）
10. セキュア暗号プロセッサ
11. スマートカード、スマートカードリーダー、トークン
12. 産業用のPLC、DCS、CNC、SCADAなどの産業用自動化制御システム（IACS）
13. NIS 2 指令の別添Iに記載された重要エンティティが使用する産業用IoT機器
14. ロボットセンシング/アクチュエーターコンポーネント及びロボット
15. コントローラー

製造業者の義務（10条）

① デジタル製品を市場に出す際、附属書Iの１**「セキュリティ特性要件」を遵守して**設計・開発・製造されていることを確認する。
② サイバーセキュリティ上の**リスクアセスメントを実施**し、その結果を設計・開発・製造・配送・メンテナンスの際の考慮に入れる。
③ デジタル製品を市場に出する際、上記のリスクアセスメントの結果を技術文書に含める。
④ 第三者から提供された部品を使用する際には、その部品により製品のセキュリティリスクを高めないことを保証する。
⑤ リスクに比例した方法でデジタル製品に関するサイバーセキュリティ側面を体系的に文書化する。
⑥ **上市後5年間**または製品寿命のうち短い期間の間、**脆弱性に効果的に対処**する。製造業者は脆弱性開示ポリシー等、適切なポリシーや手続きを有する。
⑦ 上市前に製造業者は**技術文書を作成**する。対応する適合性評価手続きを行い、適合性が実証された場合は**CEマーキングを貼付**する。
⑧ **上市後10年間**、**技術文書と（該当する場合は）EU適合性証明書を**市場監視当局が自由に使えるように**保管する**。
⑨ 一連の製造の中で、適合性を維持するための手順が整備されていることを確認する。
⑩ 附属書IIに規定される情報が製品に付属されていることを確認する。
⑪ EU適合性証明書を提供するか、その情報を記載したURLを提供する。
⑫ **上市後5年間**または製品寿命のうち短い期間の間、附属書Iの１**「セキュリティ特性要件」を遵守しない場合、直ちに必要な是正措置を講じ、製品の撤回またはリコールを行う**。
⑬ **市場監視当局からの要求**に応じて製品の**適合性を証明する情報・文書を提出**する。
⑭ 操業を停止し義務を遵守できなくなる場合、操業停止前に市場監視当局やユーザに通知する。
⑮ （欧州委員会は実施法の中で、SBOMの形式と要素を指定することができる。）

製造業者の報告義務（11条）

① デジタル製品の中に**積極的に悪用された脆弱性を発見してから24時間以内にENISAに通知する。**通知には、その脆弱性の情報、講じられた是正措置・緩和措置を含む。
（ENISAは正当なサイバーセキュリティリスク等の事由が無い限り、NIS2指令に基づいて遅滞なく脆弱性開示目的で指定されているCSIRTに転送し、市場監視当局にも通知する。）

② 製品のセキュリティに影響を与える**インシデントを認識してから24時間以内にENISAに通知する。**インシデント通知には、インシデントの深刻度・影響、国境を越える影響があるか等を含む。
（ENISAは、 正当なサイバーセキュリティリスク等の事由が無い限り、NIS2指令に基づいて指定されたコンタクト先に通知を転送し、市場監視当局にも通知する。 ）

③（運用レベルでの大規模なインシデントや危機管理に関する場合、ENISAはその情報をNIS２指令に基づいて設立されたEU CyCLONe(欧州サイバー危機連絡組織ネットワーク)に提出する。）

④ 製造業者は、必要に応じて**インシデントの影響を緩和するための是正措置について遅滞なくユーザーに通知する。**

⑤（欧州委員会は、通知された情報をの種類、形式、手順を更に指定することができる。）

⑥（ENISAはNIS２指令の協力グループに対して、サイバーセキュリティに関する最新の傾向を技術レポートとして2年に1度提出する。）

⑦ 製造業者が製品に統合されている**OSSコンポーネントの脆弱性**を特定した場合、その脆弱性をコンポーネントを**維持する個人/団体に報告する**。

全てのデジタル製品に求められるセキュリティ特性要件（附属書I）

附属書Iの１「セキュリティ特性要件」

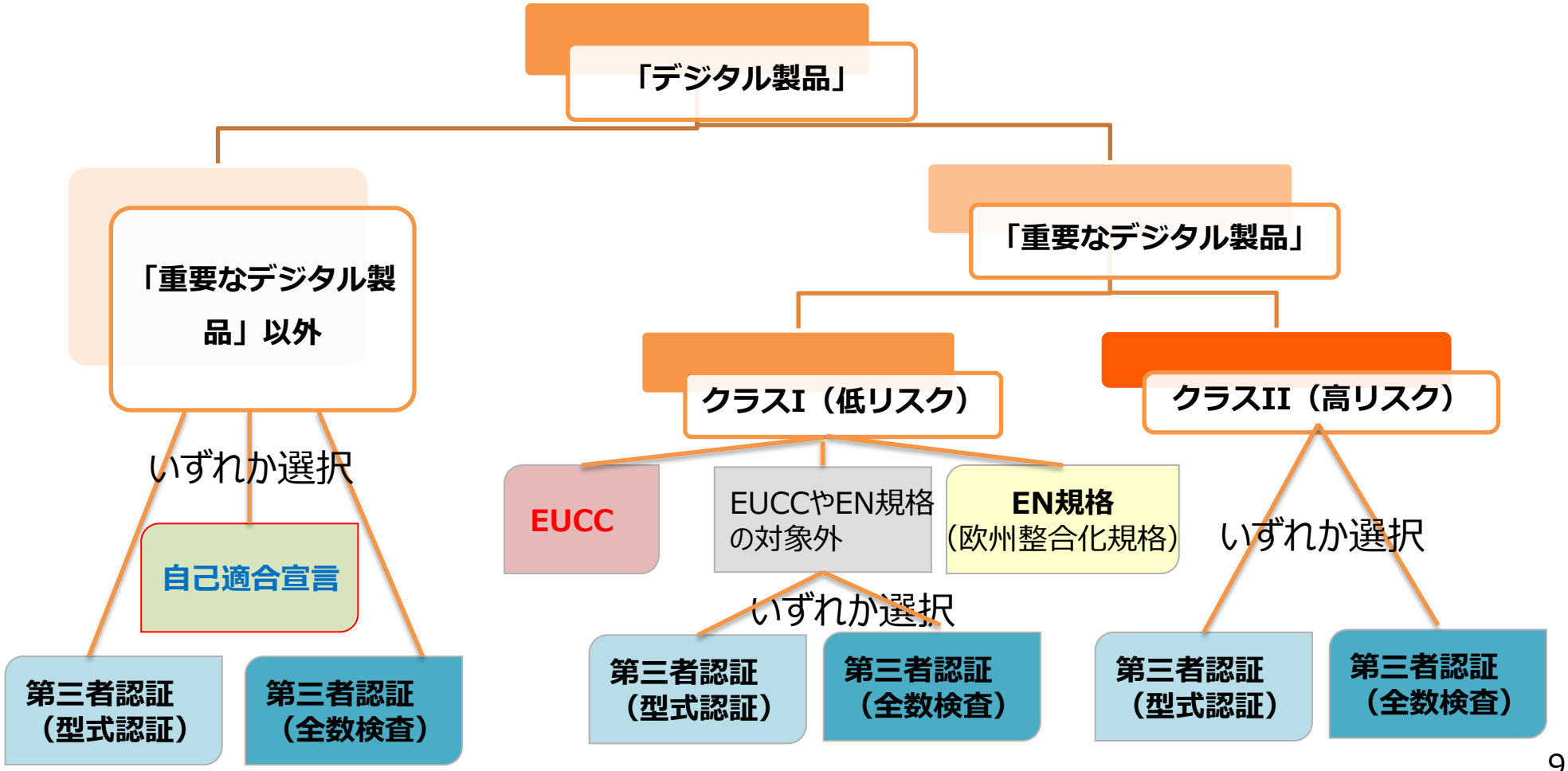
（１）リスクに基づいて適切なサイバーセキュリティを確保するよう設計・開発・生産されていること。
（２）悪用可能な脆弱性が含まれないこと。
（３）リスクベースアセスメントに基づいて、以下を満たすこと。
(a) 製品を元の状態にリセット可能である等、安全な構成となっていること。
(b) 適切な制御メカニズムにより不正アクセスからの保護が確保されていること。
(c) 最先端の暗号化などにより個人データ・その他のデータの機密性を保護すること。
(d) データやプログラムなどの完全性を許可されていない操作から保護し、破損についても報告すること。
(e) 必要なデータに限定して処理を行うこと。（データの最小化）
(f) DoS攻撃からの回復・緩和などの重要な可用性の機能を保護すること。
(g) 他の機器やネットワークからのサービスの可用性について自身への悪影響を最小化すること。
(h) 外部インターフェース等の攻撃対象領域を制限して設計・開発・製造されていること。
(i) インシデントの影響を軽減するように設計・開発・製造されているころ。
(j) アクセス、データ修正、サービス、機能などの内部活動を記録・監視し、セキュリティ情報を提供すること。
(k) 自動更新やユーザーへのアップデート通知などによりセキュリティアップデートによる脆弱性対応を確実に行えること。

附属書Iの２「脆弱性処理要件」　・・・製造業者が満たすべき要件

（１）製品に含まれる脆弱性とコンポーネントを特定し、文書化すること。そのために、機械読み取り可能な形式で一般的に使用されるSBOM作成（少なくとも最上位レベルの依存関係含む）を行うこと。
（２）セキュリティアップデートの提供など、遅滞なく脆弱性に対処・緩和すること。
（３）効果的かつ定期的なテストとレビューを行うこと。
（４）脆弱性情報の公開及び修正を行うこと。
（５）脆弱性開示ポリシーを導入し、実施すること。
（６）製品やサードパーティコンポーネントの潜在的な脆弱性に関する情報共有を行い、連絡先を提供すること。
（７）悪用可能な脆弱性が適時に修正・緩和されるように安全にアップデートを配布するメカニズムを提供すること。
（８）セキュリティパッチや更新プログラムが遅滞なく無料で配布され、ユーザーへの助言メッセージも添付すること。

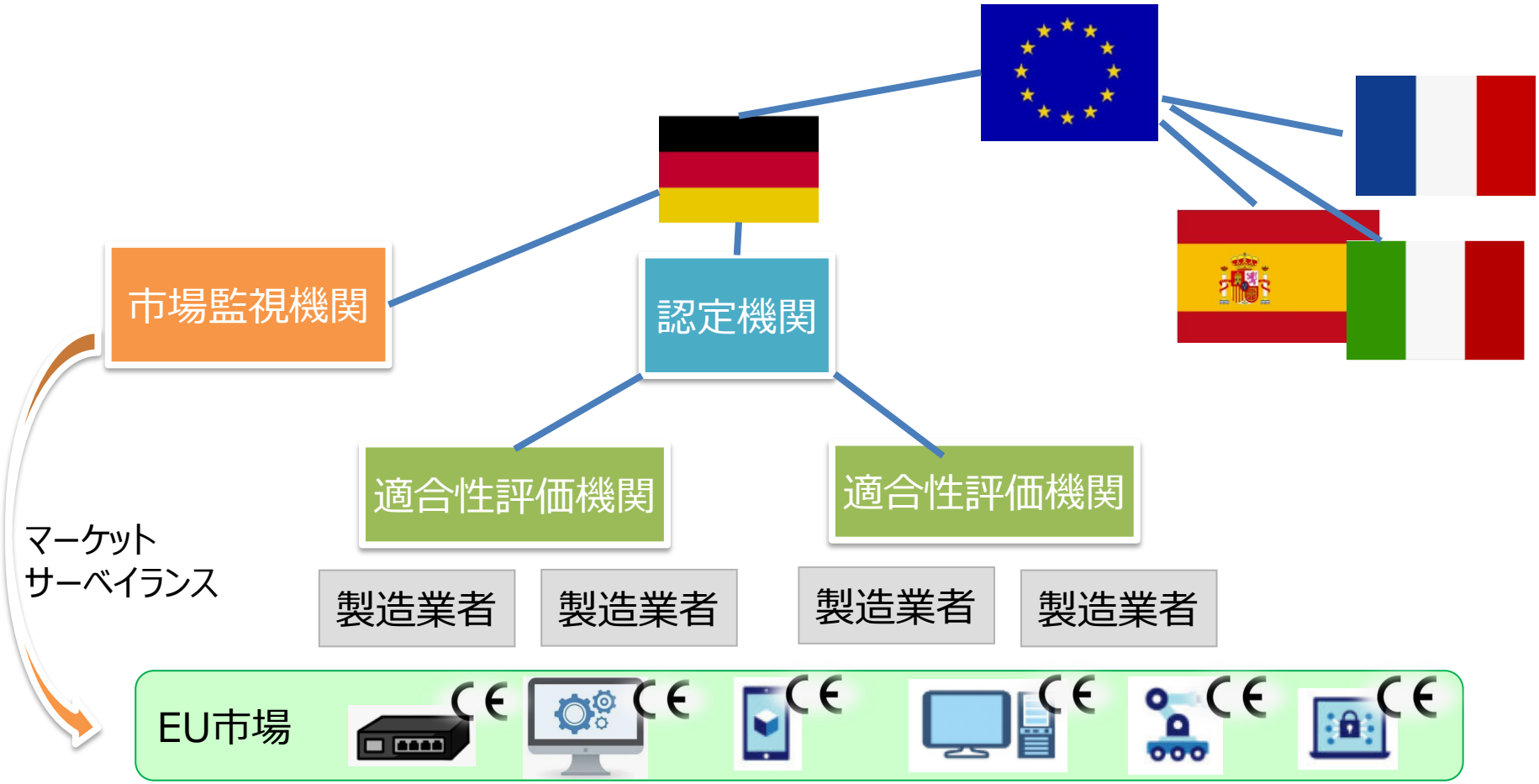
適合性評価方法　（24条、附属書VI）

- **「重要なデジタル製品」以外**は、**自己適合宣言か第三者認証かを選択**可能。
- **「重要なデジタル製品」**は、**クラスII（高リスク）は第三者認証、クラスI（低リスク）かつ**EUCCやE欧州整合化規格に準拠していない場合は**第三者認証**の取得が必要。



EU、EU加盟国、適合性評価機関の関係

- EUサイバーレジリエンス法は、EU規則であるためEU加盟国は修正を加えずに国内法として適用することとなる。
- 各EU加盟国において認定機関が国内の適合性評価機関を認定する。各EU加盟国は自国で認定された適合性評価機関の名称等をEU及び他のEU加盟国に通知する。
- 各EU加盟国は、市場監視機関を指定し、マーケットサーベイランスを行う。



他の指令・規制との関係

- 既に他のEU規則においてセキュリティ要件が課されている対象製品は適用除外となる。（第2条）
- 現在、法案策定中の「一般製品安全規則」及び「AI規則」についての関係性も整理されている。
- また、EU適合宣言（CEマーク）に関する記述も引用されている。

第2条：以下の規則の対象製品は適用除外
・「医療機器規則」　（EU 2017/745）
・「体外診断用医療機器規則」（EU 2017/746）
・「民間航空機規則」　（EU 2019/2144）
・「自動車の型式承認規則」（EU 2018/1139）
・他の規制によっても適用除外となる場合もある。

第７条：「一般製品安全規則（法案策定中）」における製造者の義務などはこの規制ではカバーされていない安全上のリスクに関して、この規制の対象製品にも適用される。

第８条：「AI規則（法案策定中）」におけるサイバーセキュリティ要件について、この規則で遵守していることをもって、AI規則上の要件も満たしているものとする。

（参考）サイバーレジリエンス法　主要な条文

第５条：デジタル製品の要件（附属書I,II）
第６条：重要なデジタル製品（附属書III）
第７条：一般的な製品安全（EU一般製品安全規則）
第８条：高リスクAIシステム（EU AI規則）
第９条：機械製品（EU機械指令）
第１０条：製造者の義務（証明書、技術文書の取得と保管）
第１１条：製造者の報告義務（脆弱性/インシデントの発見後２４時間以内）
第１８条：適合性の推定（EUCCの利用）
第２０条：EU適合宣言（附属書IV, CEマーク）
第２３条：技術文書（附属書V）
第２４条：適合性評価手順（モジュールB、C、H）
第２５～４０条：適合性評価機関
第４１～４９条：マーケットサーベイランス
第５２条：守秘義務
第５３条：罰則
第５７条：発効及び適用（官報掲載20日後に発効、その24ヶ月後に適用）
※第11条は発効後12ヶ月後に適用

＝＝＝＝＝＝＝＝＝＝＝＝

附属書 I：サイバーセキュリティ要件（①製品特性、②脆弱性対応）
附属書II：製品に添付すべき情報
附属書III：対象製品（①クラスI、②クラスII）
附属書IV：EU適合宣言　（CEマーク）
附属書 V：技術文書
附属書VI：適合性評価手順