データ・セキュリティ NEWSLETTER

2024 年 12 月 13 日

欧州サイバーレジリエンス法
～IoT 製品を含むデジタル製品のサイバーセキュリティ～

森・濱田松本法律事務所

弁護士　林 浩美
TEL. 03 5220 1811
hiromi.hayashi@mhm-global.com

弁護士　田中 浩之
TEL. 03 6266 8597
hiroyuki.tanaka@mhm-global.com

弁護士　湯川 昌紀
TEL. 03 6266 8764
masaki.yukawa@mhm-global.com

弁護士　蔦 大輔
TEL. 03 6266 8769
daisuke.tsuta@mhm-global.com

弁護士　若林 慶太郎
TEL. 03 5220 1974
keitaro.wakabayashi@mhm-global.com

本稿では、欧州において 2024 年 12 月 10 日に新たに成立したサイバーレジリエンス法（以下「CRA」といいます。）をご紹介します。

CRA は、欧州内で販売される IoT 製品を含むデジタル製品に対して包括的なサイバーセキュリティ要件を遵守することを義務付け、また、デジタル製品の脆弱性への対応やユーザーへのセキュリティアップデートの提供等を規定し、サイバーセキュリティリスクから、欧州内のデジタル製品のユーザーを保護することを目的とした法律です。CRA の成立に至る背景には、欧州サイバーセキュリティ法[1]に基づく認証制度があくまで任意の認証制度であり、デジタル製品に対して義務的にサイバーセキュリティ対策を求めるものではないことや、デジタル製品の多くが十分なセキュリティ対策を備えておらず、ユーザーが安全な製品を選択できていないことなどが挙げられています。

CRA を遵守しなければ、欧州市場においてデジタル製品を販売することができなくなるため、各企業は、CRA において規定されている内容を確認し、CRA が要求する要件を充足することができるように対応する必要があります。以下では、別途の言及がない限り、CRA の条文を引用しています。

[1] 欧州サイバーセキュリティ法とは、欧州全体のサイバーセキュリティレベル向上を目的として 2019 年に成立した法律であり、欧州全体における認証制度の導入や当局である ENISA（The European Union Agency for Cybersecurity）の役割の明確化等を主な内容としています。

Ⅰ. 適用対象

1. 総論

CRA は、デバイス又はネットワークに直接又は間接に、論理的又は物理的に接続されて利用される（又は利用されることが合理的に想定される）、デジタル要素を備える製品（products with digital elements）（以下「デジタル製品」といいます。）に適用されます（2 条 1 項）。デジタル製品は、すべてのソフトウェア、ハードウェア（典型的にはネットワークに接続するいわゆる IoT 機器）及びその遠隔データ処理ソリューション[2]を意味し、別途市場に供されるソフトウェア、ハードウェアの構成要素及び部品を含みます（3 条(1)号）。ただし、医療機器や航空、自動車等、既存の法令で規律されているものは CRA の対象外とされています（2 条 2 項乃至 6 項）。

なお、本法が適用されるためには、デジタル製品は、「市場で入手可能」でなければなりません。「市場で入手可能」とは、有償・無償を問わず、「商業活動の一環」として EU 市場での流通や使用のために製品を供給することを意味します（3 条(22)及び前文(15)）。典型的には、有償のデジタル製品が「商業活動の一環」として供給されるものになりますが、その製品自体が有償でなくても、①テクニカルサポートに対する対価を請求する場合（実費を超える場合のみ）、②製造業者がほかのサービスを収益化するためのプラットフォームを提供する場合、③セキュリティ、互換性、相互運用性の向上以外の理由で、個人データを処理することを利用条件として要求する場合なども、「商業活動の一環」として供給されるものに含まれます（前文(15)）。自社内部で開発・利用されているにすぎない製品は適用対象外となります。

デジタル製品は、各製品の潜在的な脆弱性が悪用された場合の悪影響の深刻さに応じて、その重要度が区別され、具体的には、通常の製品（General Products）、重要な製品（Important Products with Digital Elements）及びクリティカルな製品（Critical Products with Digital Elements）に分けられます（重要な製品については 7 条、クリティカルな製品については 8 条）。重要な製品については、さらにクラス I とクラス II（クラス I より高リスク）に分類されています（7 条 2 項）。

2. セキュリティ必須要件

デジタル製品を欧州内で流通させるためには、附属書 I で定められたセキュリティ必須要件を充足し、その充足が証明されている必要があります。セキュリティ必須要件は、デジタル製品として満たすべきサイバーセキュリティ要件（附属書 I-1）と

[2] 製造業者によって又は製造業者の責任のもとで設計及び開発されたソフトウェアのための遠隔からのデータ処理であって、その処理がないとデジタル製品の機能の一つを果たすことができなくなるであろうものを意味します（3 条(2)）。クラウドソリューションが「遠隔データ処理ソリューション」としてデジタル製品に当たるかどうかは、定義への該当性次第とされ、例えば家庭用スマート機器の製造業者が、ユーザーが遠隔から当該機器をコントロールすることができるように提供するクラウド機能は、この定義に該当するとされています（前文(12)）。

製造業者として満たすべき脆弱性処理要件（附属書 I-2）に分かれています。

デジタル製品として満たすべきサイバーセキュリティ要件には、セキュリティリスクに基づき適切なレベルのサイバーセキュリティが確保されるように設計、開発、製造されていることや、悪用可能な既知の脆弱性がないこと、必要なセキュリティのアップデートによる脆弱性対応を確実に行うことができることなどの条件が規定されています。

そして、製造業者として満たすべき脆弱性処理要件としては、製品に含まれる脆弱性とコンポーネントの特定（SBOM[3]を含みます。）及び文書化を行うこと、機能に加えてセキュリティも適時かつ自動的にアップデートされる仕組みがあること、脆弱性情報を公開及び修正すること、脆弱性開示ポリシーを策定することなどの条件が定められています。

3. 適合性評価

製造業者は、デジタル製品について、上記 2 のセキュリティ要件の充足性について、自己適合宣言や第三者認証による適合性評価を実施する必要があります（32 条）。これに基づき、適合宣言書を作成し、CE マーキングを貼付することとされています（13 条 12 項）。

適合性評価は、自己適合宣言や型式認証、第三者認証等、複数の方法が定められているところ、その方法は上記 1 のデジタル製品の分類によって異なります。通常の製品であれば、自己評価を含めた様々な方式から適合性評価方法を選択することができますが、重要な製品とクリティカルな製品については、第三者を含めた認証等の追加要件が課されることとなります。

Ⅱ. 製造業者等の義務

1. 主要な義務

欧州内におけるデジタル製品の製造業者は、適合性評価を行う義務のほか、様々な義務を負います。また、輸入業者及び販売業者は、製造業者が適合性評価を実施しているかの確認等、セキュリティ要件の充足性を確保するための義務を負います。製造業者、輸入業者及び販売業者の主要な義務はそれぞれ下表に記載されているとおりです。

［製造業者（13 条）］

① 設計、開発、製造におけるセキュリティ必須要件の充足
② セキュリティに関するリスクマネジメント及びその文書化
③ デジタル製品の脆弱性対応

[3] Software Bill of Materials の略であり、ソフトウェア部品表のことを指しています。

④	ユーザーに対するセキュリティアップデート提供（最低 10 年間）
⑤	EU 適合宣言書及び技術文書等の保管（最低 10 年間）

［輸入業者（19 条）］

①	セキュリティ必須要件を充足した製品のみを上市
②	デジタル製品が法令に適合しなくなった場合における取扱いの停止及び監査当局への適切な報告
③	デジタル製品の脆弱性を認識した場合の製造業者への通知
④	EU 適合宣言書及び技術文書等の保管（最低 10 年間）

［販売業者（20 条）］

①	セキュリティ必須要件を充足した製品のみを上市
②	デジタル製品の脆弱性を認識した場合の製造業者への通知
③	デジタル製品が法令に適合しなくなった場合における取扱いの停止及び監査当局への適切な報告

2. 報告義務

製造業者は、上表の各義務に加え、脆弱性又は重大なインシデントに関する報告義務（14 条）を負うこととなりますが、その具体的な内容は下表のとおりです。製造業者が、ENISA が用意する単一の報告用プラットフォームを通じて、各国の窓口として機能する CSIRT 及び ENISA に通知を行う仕組みとなっています。

［デジタル製品に含まれる、積極的な悪用される脆弱性を認識した場合］

①	早期報告：脆弱性を認識してから 24 時間以内の速報
②	脆弱性報告：脆弱性を認識してから 72 時間以内に、当該デジタル製品の一般的な情報、当該脆弱性の性質、講じられた是正措置又は緩和措置、及びユーザーが講じることのできる是正措置又は緩和措置を内容として含む報告
③	最終報告：是正措置又は緩和措置が利用可能となった後 14 日以内に、脆弱性の重大性及び影響を含む当該脆弱性の説明、悪用する主体についての情報、セキュリティのアップデートその他の対応策を内容として含む報告

［デジタル製品のセキュリティに影響を及ぼす重大なインシデントが発生したことを認識した場合］

①	早期報告：インシデントを認識してから 24 時間以内の速報
②	インシデント報告：インシデントを認識してから 72 時間以内に、インシデントの性質、初期評価、講じられた是正措置又は緩和措置、及びユーザーが講じることのできる対応策を内容として含む報告
③	最終報告：②の報告の 1 か月以内に、インシデントの重大性及び影響を含む当該インシデントの説明、原因、対応策を内容として含む報告

Ⅲ. 制裁等

欧州委員会や ENISA、欧州各国当局には市場の監督や調査、規制権限等が与えられています。欧州各国は、CRA 違反に対して適用される制裁に関する規則を制定し、その制裁を実行するために対策を講じなければなりません（64 条 1 項）。

また、CRA において、違反類型ごとに制裁が定められています。附属書 I における義務、製造業者の各義務（13 条）及び報告義務（14 条）に違反した場合には、最大 1,500 万ユーロ又は全世界の年間売上高の最大 2.5%のいずれか高い金額の制裁金が課せられます（64 条 2 項）。その他の義務（19 条及び 20 条を含む）に違反した場合には、最大 1,000 万ユーロ又は全世界の年間売上高の最大 2.5%のいずれか高い金額の制裁金が課せられます（64 条 3 項）。また、不正確で不完全な誤解を招く情報を当局に対して提供した場合には、最大 500 万ユーロの罰金又は年間売上高の最大 1%のいずれか高い金額の制裁金が課せられます（64 条 4 項）。

Ⅳ. 施行日等

CRA は、2024 年 12 月 10 日に発効した後、段階的に適用開始されます。

具体的には、適合性評価における第三者認証機関に対する通知に関する規定は 2026 年 6 月 11 日、上記 2 の報告義務に関する規定は 2026 年 9 月 11 日、その他の規定は 2027 年 12 月 11 日に適用される予定です。

Ⅴ. 今後の展開

CRA は、上記のとおり、段階的に施行されるところ、各企業は CRA を遵守することができるような体制を整える準備をすることが求められます。欧州においてデジタル製品を製造、輸入及び販売する場合には、CRA の要件を充足しているかを確認することが求められます。

CRA に関する今後の動向を引き続き注視していく必要があります。

セミナー情報

- セミナー　『メタバース空間での法的課題』
  開催日時　2024 年 12 月 16 日（月）19:00～20:30
  講師　増田 雅史
  主催　次世代労働政策勉強会

- セミナー　『Animoca Brands Japan が描く Web3 の世界 日本の IP コンテンツで日本と世界を繋ぐ』
  開催日時　2024 年 12 月 17 日（火）18:00～20:30

講師　増田 雅史
主催　渋谷 Web3 大学

- セミナー　『個人情報保護法改正に向けた検討状況とプライバシーを巡る諸状況（NCA Annual Conference 2024）』
  開催日時　2024 年 12 月 19 日（木）14:40～15:20
  講師　蔦 大輔
  主催　一般社団法人日本シーサート協議会

- セミナー　『重要情報の漏えいと情報管理の対策～営業秘密・個人情報漏えい時の対応と、情報の漏えいを未然に防止するための対策を解説～』
  開催日時　2025 年 1 月 8 日（水）14:00～17:00
  講師　佐々木 奏
  主催　一般社団法人企業研究会

- セミナー　『「セキュリティインシデント対応の総点検」ビジネス法務 2025 年 1 月号特集連動セミナー（第 2 回 ランサムウェア攻撃）』
  開催日時　2025 年 1 月 15 日（水）16:00～17:00
  講師　林 浩美、蔦 大輔、嶋村 直登、二神 拓也
  主催　株式会社中央経済社

- セミナー　『オンラインサービスにおける電気通信事業法の実務対応 ―施行後の状況・最新動向を踏まえたポイント解説―』
  開催日時　2025 年 1 月 15 日（水）12:00～13:00
  講師　呂 佳叡
  主催　BUSINESS LAWYERS／弁護士ドットコム株式会社

- セミナー　『オンラインサービスに関する電気通信事業法の基礎と実務－法改正後の対応事例・「スマートフォン プライバシー イニシアティブ」改定など最新動向を踏まえて－』
  開催日時　2025 年 1 月 30 日（木）13:30～16:30
  講師　呂 佳叡
  主催　株式会社 FN コミュニケーションズ

- セミナー　『先端分野における知的財産実務上の課題～AI・NFT・メタバース～』
  開催日時　2025 年 2 月 10 日（月）10:00～11:50
  講師　増田 雅史

主催　中央大学法科大学院

- セミナー　『「セキュリティインシデント対応の総点検」ビジネス法務 2025 年 1 月号特集連動セミナー（第 3 回 委託先における情報漏えい）』
  開催日時　2025 年 2 月 19 日（水）16:00～17:00
  講師　林 浩美、蔦 大輔、嶋村 直登、二神 拓也
  主催　株式会社中央経済社

- セミナー　『 EU 市場へコネクティッドデバイス・デジタル製品等を上市する企業が知っておくべき最新法規制～EU データ法、サイバーレジリエンス法、改正製造物責任指令を含む EU の製品安全性の規制、NIS2 指令、AI 法、GDPR への具体的対応～』
  ※本セミナーの名称変更予定のため、詳細は当事務所ウェブサイトをご確認ください。
  開催日時　2025 年 2 月 28 日（金）9:30～12:30
  講師　田中浩之
  主催　経営調査研究会

文献情報

- 論文　「連載 テクノロジー×著作権理解を深めるキーワード⑥プロンプトエンジニアリング」
  掲載誌　月刊コピライト No.761 Vol.64
  著者　岡田 淳（単著）

- 論文　「AI 事業者ガイドライン（第 1.0 版）［初版］」
  掲載誌　別冊 NBL No.190
  著者　岡田 淳

- 論文　「連載 テクノロジー×著作権理解を深めるキーワード⑦ファインチューニング」
  掲載誌　月刊コピライト No.762 Vol.64
  著者　岡田 淳（単著）

- 本　『ゲノム法』
  出版社　株式会社商事法務
  著者　吉田 和央

- 論文　「『個人情報保護法 いわゆる３年ごと見直しに係る検討の中間整理』について」
  掲載誌　会計・監査ジャーナル Vol.36 No.11
  著者　北山 昇

- 論文　「特集：AI と法～生成 AI 時代におけるリスクと展望～ 第２部《論文》日本政府における AI 法政策の現状と今後」
  掲載誌　法の支配 No.215
  著者　岡田 淳

- 論文　「連載 テクノロジー×著作権理解を深めるキーワード⑧カリフォルニア州の AI 関連規制（1）：デジタルレプリカ」
  掲載誌　月刊コピライト No.763 Vol.64
  著者　岡田 淳

- 論文　「〈サイバー攻撃手法別 セキュリティインシデント対応の総点検〉攻撃手法と対応（1）ランサムウェア攻撃」
  掲載誌　ビジネス法務 Vol.25 No.1
  著者　林 浩美、蔦 大輔、二神 拓也（共著）

- 論文　「〈サイバー攻撃手法別 セキュリティインシデント対応の総点検〉攻撃手法と対応（2）委託先における情報漏えい」
  掲載誌　ビジネス法務 Vol.25 No.1
  著者　林 浩美、蔦 大輔、二神 拓也（共著）

- 論文　「〈サイバー攻撃手法別 セキュリティインシデント対応の総点検〉攻撃手法と対応（3）内部不正による情報漏えい」
  掲載誌　ビジネス法務 Vol.25 No.1
  著者　湯川 昌紀、蔦 大輔（共著）

- 論文　「〈サイバー攻撃手法別 セキュリティインシデント対応の総点検〉攻撃手法と対応（4）フィッシング詐欺および不正送金」
  掲載誌　ビジネス法務 Vol.25 No.1
  著者　蔦 大輔、嶋村 直登、長尾 勇志（共著）

- 論文　「〈サイバー攻撃手法別 セキュリティインシデント対応の総点検〉攻撃手法と対応（5）アカウントへの不正ログイン」
  掲載誌　ビジネス法務 Vol.25 No.1

著者　　蔦 大輔、嶋村 直登、長尾 勇志（共著）

- 書籍　　『グローバルデータ保護法対応 Q&A100』
  著者　　田中 浩之 編著、梅津 英明、石川 大輝、細川 怜嗣、森・濱田松本法律事務所グローバルデータ保護法研究チーム（共著）

NEWS

- 蔦 大輔 弁護士のインタビューが、UNITIS の『ランサムウェア身代金は払っていいのか？ 法令や判断基準、事前策を弁護士が解説』と題した記事に掲載されました
- 岡田 淳 弁護士が岩手県議会・デジタル社会・新産業創出調査特別委員会において、有識者として意見陳述を行いました
- 蔦　大輔　弁護士のインタビューが、UNITIS の『ダークウェブに流出した情報の取得・拡散は違法？　抵触する法律や企業の対応策を弁護士が解説』と題した記事に掲載されました
- 蔦 大輔 弁護士のインタビューが、UNITIS の『ランサムウェア被害時にとるべき初動・広報対応を弁護士が解説』と題した記事に掲載されました
- 岡田 淳 弁護士が、TOKYO MX の番組「田村淳の訊きたい放題！ニュースの裏側：あなたは誘導されている？ ダークパターンを知っていますか？ ネット通販の課題を考える」に出演いたしました
- 蔦 大輔 弁護士が登壇したセミナーが、UNITIS の『2024 上期のセキュリティ事件・動向を弁護士 4 名が解説 -「サイバーセキュリティ法務に詳しい弁護士 4 名が徹底議論 第 3 弾」レポート』と題した記事に掲載されました
- 岡田 淳 弁護士のコメントが、読売新聞夕刊『「在庫わずか」「ニセのお客様の声」など消費者欺く「ダークパターン」対策、官民で始まる…被害 1 兆円の試算も』と題した記事に掲載されました