欧米企業の欧州サイバーレジリエンス法案（EU Cyber Resilience Act）対応準備状況

～見えてきた日本企業との大きな温度差～

PwCコンサルティング合同会社

欧州連合で議論が進んでいるデジタル製品のセキュリティ対策を義務付ける新法「サイバーレジリエンス法案」について、現時点での欧米企業の対応準備状況と、日本企業が改めて認識すべき課題を提言します。

欧米企業はCRAにどう対応しているのか

欧州連合（EU）でデジタル製品のセキュリティ対策を義務付ける新法「サイバーレジリエンス法案（以降、CRA）」の議論が進んでいます。個人情報保護法制の一般データ保護規則（GDPR）と同じく、EU市場に参入する幅広い業種の企業を対象とし、違反には巨額の制裁金を科す内容が提案されています。

CRAは、既にセキュリティ規制の存在する自動車、医療、航空分野や国家安全保障に関わる製品などを除き、ほぼ全てのデジタル製品を対象としており、製品メーカーに対して設計開発段階から販売後の5年間まで、EU圏内で販売する製品の脆弱性対応を義務付ける点で一定の負担を強いることになります。2022年9月に公開された草案に基づくCRA要求事項の概説は過去記事「欧州サイバーレジリエンス法案（EU Cyber Resilience Act）概説～日本の製造業への影響と最低限押さえるべき要点～」を参照ください。

こうした法規制案に対応すべく、多くの日本の製造業は一斉に準備を始めています。先の記事を公表した際、多くのお問い合わせやご相談を頂きました。一方で、海外からはCRAに対して大きな波紋のような声があまり聞こえてこないことに少し違和感を覚えたことをきっかけに、PwCでは、グローバルネットワークを通じて欧米のメジャー企業のCRA対応準備状況を確認したところ、日本の製造業と大きな温度差が見えてきました。本記事では現時点での欧米企業の対応準備状況と、日本企業が改めて認識すべき課題を提言します。

余裕をもってCRA最終要件を確認する欧米メジャー企業

2023年5～6月にかけて、PwCグローバルネットワークで欧米メジャー企業（少なくとも国際的に知名度のあるブランドを持つ企業）のセキュリティ関係者にCRA対応状況を聴取した結果、各社とも既に準備できており、冷静に対応していることが見えてきました。

「CRA要求の多くは、セキュリティに配慮した製品を提供するために必要な取り組みとして従来からさまざまなガイドラインや標準などで言われてきたことであり、いくつかCRA特有の要件はあるものの、それら以外は既に対応できている」と認識している企業が多く、各社に特段の焦りは見られませんでした。顧客に提供する製品のセキュリティ品質の確保はメーカー責任として当然という欧米企業の意識の高さがうかがえる結果でした。

pwc

特に次の3点が共通した意見として聞かれました。

1. セキュリティを製品ライフサイクルに組み込むことは基本認識であり、セキュア開発プロセスおよび脆弱性管理・インシデント報告に対応するPSIRT（Product Security Incident Response Team）の基本的な取り組みは既に組織として確立済み
2. 製品セキュリティの責任を明確化するため、CPSO（Chief Product Security Officer）（もしくは管理責任者）をアサイン済み
3. CRA法案の段階から、PSIRT以外の関係者（製品コンプライアンス部門や品質保証部門など）と要件を追跡し、自社にとって対応が厳しい条項や不明確な点について、法規策定当局へパブリックコメントを提出済み

外部コンサルタントの支援を受けて情報収集している、という企業もありましたが、一様に基本的な対応や意見表明も済んでいる状況を踏まえると、これから要件を確認しよう、そのための対応体制の検討を始めよう、という段階の企業が欧米企業と対峙するには、相当のスピード感を持って対応体制作りを進める必要があるでしょう。

ENISA報告義務やSBOM対応は欧米企業にとっても大きなチャレンジ

一方で、CRAの要件には、今までの法規やガイドラインには見られない要件もあり、特に広範な分野の製品が対象となっていることから、CRA要件を満たすべき対象になるのか、どこまでやれば要件を満たしていることになるのかを明確に判断できないといった声も聞かれました。

特にCRA特有の要件として指摘のあった主なチャレンジは以下2点に集約されました。

1. 24時間以内の脆弱性・インシデント報告義務（条項11）

CRAは、デジタル製品に発見された脆弱性やインシデントについて、欧州連合サイバーセキュリティ機関（ENISA）への24時間以内の通知を義務化しています。この条項は、CRA発効後12か月で施行されるため、非常に注目されていました。なぜなら、この条項の内容は現在施行されている他の法規（例えば、GDPRやNIS等）より厳しく、PSIRTの初動能力が問われるからです。この要件に対しては、以下のような声も多く聞かれたため、この要件は今後、見直されること予想されます。

- 24時間報告の起点となるトリガーが不明確
- どのレベルの問題を報告すればよいかが不明瞭
- 具体的な脆弱性、インシデントの深刻度と重大さを定義する必要がある
- また、分析不十分な状況でENISAに報告することになれば、ENISAは毎日のように大量な脆弱性情報を入手し、ENISAがボトルネックとなるため制度設計にも問題がある
- ユーザー報告より先にENISAへ報告する要件の意図が不明瞭
- 重大なインシデントがあれば、ENISAより、まず顧客への連絡が第一と考える

2. SBOM情報による脆弱性管理

脆弱性管理において、CRAの付属書にSBOM（Software Bill of Material）の利活用が明示されました。SBOMを導入し、SBOMのデータを基にデジタル製品のライフサイクルで脆弱性を管理すること、企業間の情報共有や欧州委員会への報告のために、委員会より指定のフォーマットに従ってデータを作成し、公開可能とすることが要求されています。昨今、SBOM管理は多くガイドラインでも指摘されており、企業でも導入が始まっているものの、まだまだ成熟途上の取り組みなため、運用面での課題として次のような声が聞かれました。

- 指定されるフォーマットが既に導入したSBOM管理システムで対応可能かが不明
- 欧州委員会へのSBOM報告の意図とタイミングが不明。欧州委員会は大量に寄せられるSBOM情報を管理しきれるのか、ここにもボトルネックとなる制度上の問題がある

欧米企業は既にSBOM管理についてPSIRTオペレーションの運用上の課題として検討しています。SBOMは脆弱性管理における基本台帳となる存在です。このSBOM情報をどのように効率的に管理し、どのように効果的に脆弱性対応の取り組みに活かすかを欧米企業は議論しています。将来直面する課題を見通すに至れていない日本企業は、早くそれらの課題を自己の課題として認識できるところまで成熟度を引き上げる必要があるでしょう。

日本企業は早急に製品セキュリティの対応体制の整備を

今回の聴取によって、欧米のメジャー企業は既に主要なCRA要件の基本的対応は済んでおり、CRA要件案に対し意見を挙げて、最終化を待つ状態にあるため、日本の製造業に見られるような大きな波紋が起きていない理由がよく理解できました。法的対応義務が発生する前から、製品セキュリティ対応は企業責任として当然のこと、という理解が根底にあり、製品のセキュリティ品質の認識が日本企業と大きく違っていることを改めて確認できました。

製造業として製品セキュリティに取り組むことは、コンプライアンス上、そして事業リスク管理の面でも、海外では当たり前となっているということを、日本企業は認識すべきででしょう。また欧州地域にデジタル要素を持つ製品を展開している日本企業は、欧米企業が既に到達しているレベル、主要なCRA要件の対応は済んでいるといえるレベルまで、早々にたどり着かなければ、欧州での市場競争力を失うことになりかねないリスクを認識すべきでしょう。そこで製品セキュリティの取り組みレベルに応じて、以下のように提言します。

1. まだ製品セキュリティの取り組みを始められていない企業

- 欧州市場を失いかねない事業リスクであることをトップマネジメントは理解する（CEマークによる上市、違反時の制裁金グローバル売上2.5%）
- とにかく製品セキュリティ体制づくりを始める
- CRA要件を満たす以前の基本的なセキュア開発プロセスと脆弱性対応プロセス（PSIRT機能構築）と体制を早期に構築する（海外に追い付くには2023年度中が理想、最終ゴールをCRA要件準拠とする）
- 欧州拠点との製品セキュリティに関する情報連携体制を構築する

2. 既に製品セキュリティの取り組みを開始している企業

- CRA要件の修正動向のモニタリングを行って自社対応状況との差分を確認し、充足させるための取り組みを計画する
- 修正案に対して、自社の都合に合わない要件に対しては、積極的にコメントを提言する
- 欧米企業もチャレンジと認識するポイントの業界動向のモニタリングと対策を検討する

製品セキュリティの対応体制を実行性ある形にすることは一朝一夕には難しく、人・環境整備への投資を数年単位で行い、成熟度を高める取り組みが必要になります。したがって、CRAの要件が決まってから動きだすのではまず間に合いません。CRAの修正案では、発効後の猶予期間が伸びる方向で議論されていますが（CRA修正案の動向については別途レポートを発行予定）、それでも製品投入タイミングから開発期間を差し引いて考えれば、いまセキュア開発をスタートさせておく必要があるのではないでしょうか。

対応に向けた取り組みとして必要となるのは以下のステップです。

ステップ	取り組み
STEP 1	情報収集と社内共有、課題認識、取り組み推進（旗振り）役の設定
STEP 2	CRA要件との現状との差分把握から差分を埋める取り組み計画の策定
STEP 3	計画に沿った製品セキュリティのマネジメントシステムの構築
STEP 4	システムに沿った運用に向けた教育や訓練と製品戦略

PwCでは、今後も本法案についての調査を継続し、要件への対応方法やとるべき対応について、より具体的に解説してまいります。また、CRA要件準拠に必要な一連の取り組みをPwCグローバルネットワークを通じて総合的にご支援する体制を整えております。

執筆者

林 彦博

PwCコンサルティング
合同会社
マネージングディレクター

奥山 謙

PwCコンサルティング
合同会社
ディレクター

伊藤 公祐

PwCコンサルティング
合同会社
マネージャー

亀井 啓

PwCコンサルティング
合同会社
マネージャー

周 文琦

PwCコンサルティング
合同会社
マネージャー

PwC Cyber Security & Privacy

https://www.pwc.com/jp/ja/services/digital-trust.html