ハイライトレポート

2024. 8. 27 Day1

法規制対応が急務に！
IoT/OTデバイスに求められるセキュリティ対策とは
～CRAの最新動向と対策～

ますます活発になるサイバー攻撃にどう立ち向かうか

サイバー攻撃は年を追うごとに増加の一途を辿り、2023年には攻撃対象への偵察行動が１IPアドレスあたり1日7,000件以上観測されています。また、サプライチェーンの弱点を突く攻撃がランサムウェアに次ぐ脅威になるなど攻撃手段が巧妙化し、ライフサイクル全体を通した今までより高度で包括的な対策が必要になってきています。セッション2ではこうしたサイバー攻撃に伴う各国の動向や、実際にセキュリティ対策で抑えるべきポイント、どこから対策するか？の最初の一手をご紹介しました。

主要各国サイバーセキュリティ規格の動向

加速するサイバー攻撃情勢を踏まえ、現在世界各国でサイバーセキュリティ規格や法案の策定が推進されています。欧州サイバーレジリエンス法（CRA）、無線機器指令（RED）、NIS2をはじめ、英国のPSTI、米国のラベリング制度など、早いものでは2024年から規制開始となる法案も存在します。普及させる政策に各国の違いはあれど、「脆弱性への対応、機器へのセキュリティ対策実装要件」は共通して求められる要件です。現実的には日々発見される新たな脆弱性に対して、製品開発部門のみ、保守部門のみといった一部門のみで対処することが容易ではないことは想像に難くありません。

サイバーセキュリティ対策の要点を抑える

サイバーセキュリティガイドライン・規格に対応するにも、理想とのGAP分析、言わば「現状把握」から取り組み始めることも重要です。先にゴールと課題を明らかにすることで、時間、費用、人員などのリソースを効率的に投入することが可能です。勿論、評価・分析だけではなく、次のフェーズで求められる具体的な脆弱性への対応や、脆弱性テストなどの規格準拠に向けた道のりを、総合的にご支援いたします。

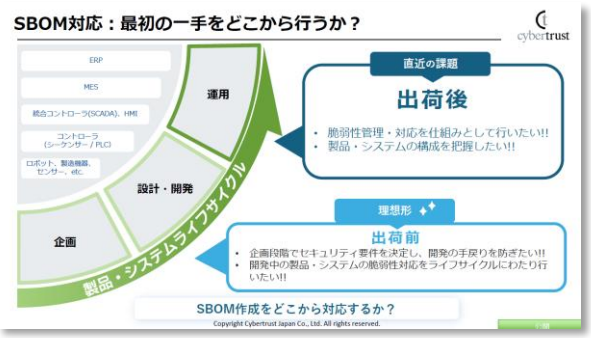
最初の一手をどこから行うか：SBOM対応

SBOMとは、作成するソフトウェアとそのソフトウェアで利用する外部のライブラリやソフトウェアの一覧と、ライセンス・コピーライト等のメタ情報で構成されるリストのことです。近年のオープンソースソフトウェアへのサプライチェーン攻撃の増加に伴い、ソフトウェア間の依存関係やライセンス情報を把握するためにSBOMの活用が重要になります。

リスクアセスメントを実施し上流工程から対策を行うことが理想ですが、出荷中の製品に対する「製造業者の報告義務」を先に実施しなければならない可能性もあります。現行製品の構成把握の最初の一手としてSBOM対応を実施することで、次期製品で守るべき対象を明確にすることができます。

■ 本日の登壇者 ■

サイバートラスト株式会社
OSS/IoT事業統括 IoT技術本部
執行役員本部長
岸田 茂晴 氏



SBOM対応：最初の一手をどこから行うか？
出所：投影資料より一部抜粋