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～

セキュリティ対策に乗り遅れないために

産業制御機器のIoT化と巧妙化するサイバー攻撃の脅威に備えるべく、早急なセキュリティ対策が求められています。2027年にはサイバーレジリエンス法の全面施行が予定されている等、サイバーセキュリティを義務とする法制化の動きも世界全体に広がりを見せています。ウェビナでは、サイバーセキュリティ対策のカギとなるIEC 62443から、法規制の対象とされる製品やソフトウェア・IC選び・脆弱性管理から構築すべきシステム要件まで、様々な情報とノウハウを厳選し、2Days・4セッションに渡って開催いたします。

EUサイバーセキュリティ規制のタイムライン

2022年の正式発効を経たNIS2指令は2024年秋より施行されます。またNIS2の正式発効と同じ2022年に草案が発表されたCRAは2026年の部分施行（第14条　報告義務）を経て、2027年には全面施行を予定しています。法規制は技術対応に加えセキュア開発、脆弱性処理への適用を義務として課しているため、その対策には相当の時間を要することが予想されます。施行までのタイムラインが明確となった今、早急にサイバーセキュリティ対策を開始しなければなりません。

IEC 62443　取り組みに向けたステップ

法規制対策に向けIEC 62443-4-2製品認証まで進むには、以下に取り組む必要があります。

①製品のライフサイクルに合わせた開発プロセスを構築
　（セキュア開発プロセスを策定し開発手順を確立）
②IEC 62443-4-1 Maturity Level2を認証取得
③開発プロセスを運用しセキュリティ機能を製品に実装
④実装されたセキュリティ機能の耐性評価を確認
　（脆弱性テスト、ペネトレーションテスト）
⑤IEC 62443-4-1 Maturity Level3&4-2認証取得

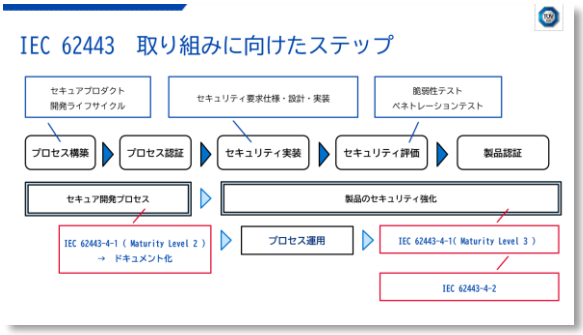
サプライチェーンセキュリティ & レベルの評価

IEC 62443にはサプライチェーンセキュリティを実現する管理システムを有しています。サプライチェーンセキュリティの強化に向けて、アセットオーナーはインテグレータに対して、インテグレータはコンポーネントメーカに対してIEC 62443を活用することで全体のセキュリティ強化を図ることが可能です。

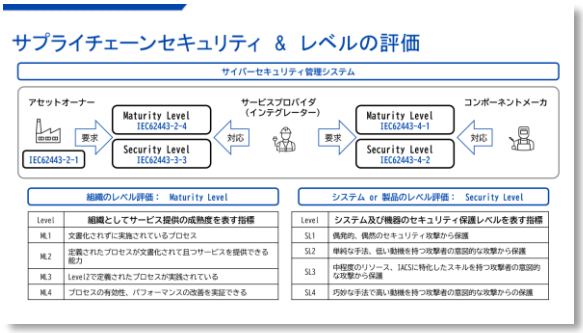
また、IEC 62443にはセキュリティ面でのインテグレータ、コンポーネントメーカの成熟度（Maturity Level）、更にシステム及び機器のセキュリティ保護レベル（Security Level）を第3者評価で数値化する側面も有しています。

■ 本日の登壇者 ■

テュフズードジャパン株式会社
登山 慎一　氏
COM事業部　IEP部
シニアセールスエクゼクティブ



IEC 62443　取り組みに向けたステップ
出所：投影資料より一部抜粋



サプライチェーンセキュリティ　&　レベルの評価
出所：投影資料より一部抜粋

[他記事、ウェビナ、お問い合わせはこちら]

リョーサン テクラボ
エンジニアによりそうマガジンサイト