

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化と呼応して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部品やソフトウェア・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、3Days・5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年後半より施行されます。またNIS2の正式発効と同じ年の2022年に草案が発表されたCRAは2026年の部分施行（第11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以外に製造業者自身の取組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、以下のプロセス構築から製品のセキュア化に取り組んで頂きます

- 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（脆弱性評価、ペネトレーションテスト）
- ⑤IEC 62443-4-1 Maturity Level3&4-2認証取得（製品のセキュリティ機能を強化）

サプライチェーンセキュリティ & レベルの評価

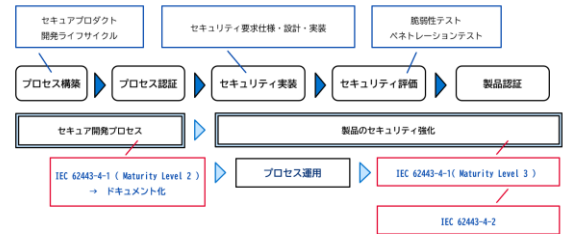
IEC 62443にはサプライチェーンセキュリティを実現する管理システムを有しています。サプライチェーンセキュリティの強化に向けてアセットオーナーはインテグレーターに対して、インテグレーターはコンポーネントメーカーに対してIEC 62443を活用してサプライチェーンセキュリティの強化を図ることが可能です。。またIEC 62443にはセキュリティ面での構築、実装能力（Maturity Level）、更にシステム、コンポーネントのセキュリティ保護レベル（Security Level）を数値化し、それを評価する側面も有しています。

■ 本日の登壇者 ■



テ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



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

[他記事、ウェビナ情報はこちら](#)



エンジニアよりそうマガジンサイト