PCJ-PR-20190408

<お知らせ>

２０１９年４月８日
フエニックス・コンタクト株式会社

フエニックス・コンタクト社「IEC 62443-4-1 および 2-4」に基づく認証を取得

～第三者認証機関 TÜVSÜD よりドイツで最初に取得した企業の１社に～

<※当プレスリリースは、２０１９年４月２日（現地時間）にフエニックス・コンタクト社（本社：ドイツ、ブロンベルグ）が発表したものの抄訳です。>

【２０１９年４月２日　ドイツ、ブロンベルグ発】産業用接続機器、制御製品および通信機器のマーケットリーダーであるフエニックス・コンタクト社（本社：ドイツ、ブロンベルグ）は、産業用自動化のセキュリティに関する**「IEC 62443-4-1および2-4」**シリーズの規格に基づく認証を、第三者認証機関TÜVSÜD（テュフズード）より、ドイツで最初に取得した企業の1社となりました。認証は当社が以下のプロセスを実行していることを確証するものです。

- **「IEC 62443-4-1」プロセスに準拠したセキュアな設計による製品の開発**
- **「IEC 62443-2-4」プロセスに準拠したセキュアな自動化ソリューションの設計**

今回の認証の取得は、当社の提供する製品、産業ソリューション、およびコンサルティングサービスにおいて標準化されたセキュリティを提供して、お客様の機械、システム、およびインフラの将来にわたる動作を確実にするというフエニックス・コンタクト社の企業方針に沿ったものです。

ハノーバーメッセにて（左がCTO ローランド・ベント）

セキュアに設計された製品は、開発段階でソフトウェアとハードウェアのセキュリティ要件が考慮されており、後のセキュリティ脆弱性発現を予防します。デバイスやセンサーがインターネットでネットワーク接続されるようになるので、セキュリティ対策はますます重要視されるようになっています。
ソフトウェアを介して実行されるプロセスがますます増えており、新たな攻撃対象が生まれています。したがって、継続的にセキュアな対策を提供できる体制が求められています。

フエニックス・コンタクト社のCTO、ローランド・ベント（Roland Bent）は次のように述べています。「フエニックス・コンタクト社の製品開発プロセスは、2018年秋にIEC 62443-4-1規格に基づいていると認定されました。セキュアな設計はセキュリティ製品の開発に不可欠です。」「そして次の一歩となる規格の認証取得が実現しました。当社がこの規格IEC 62443-2-4に基づいて、お客様のためのセキュアな自動化ソリューションを開発および実装できることが確証されました。」

■「IEC 62443」について

「IEC 62443」は自動化システムに向けたセキュリティの国際標準規格です。産業用自動化および制御システム（IACS）のITセキュリティを扱う一連の文書で構成されています。 IACSという用語は、自動生産システムをセキュアに運用するために必要な、システム、コンポーネント、プロセスなどのすべての要素を表します。特に産業用アプリケーションに焦点を当てることで、「IEC 62443」は「ISO 27001」とは一線を画しています。（ISO27001は従来のITシステムを扱う。）重要インフラの事業者にとって、ICE 62443はセキュアなソリューションの設計、立ち上げ、運用、およびメンテナンスのためのすべての要件を網羅しています。

■「IEC 62443-4-1および2-4」について

ITセキュリティ規格の「IEC 62443-4-1および2-4」の主な要素は、アプリケーションシナリオに基づく脅威とリスクの分析です。アプリケーション例と要求される対策がデバイスとシステムに対して定義されています。セキュリティの考え方が必要な予防策と共に、自動化ソリューションに対して考案されています。一方で、製品や

ソリューションにおいて、認識されているすべてのセキュリティ要件がトレーサビリティ付きで実装、検証、および文書化されることを保証する開発プロセスが規定されています。

■「製品セキュリティ・インシデント対応チーム（PSIRT）」

デバイス製造元は、セキュリティの脆弱性に適切に対応し、信頼性の高い方法でセキュリティアップデートを公開することが求められています。 フエニックス・コンタクト社は、新たに設立した製品セキュリティ・インシデント対応チーム（以下PSIRT）でこの要件を満たしました。このチームは、フエニックス・コンタクト製品のユーザーに既知のセキュリティ脆弱性を通知すると同時に、ユーザーが発見したセキュリティの脆弱性を秘密裏に報告する窓口としても機能します。PSIRTは、IEC 62443に規定されている報告された脆弱性レポートの処理、評価、発行、およびプロセスチェーンの更新に責任を負います。

■　あらゆる産業に関連するサイバーセキュリティ

サイバーセキュリティは産業界全般に関連しています。自動化技術とITの世界は互いに近づいています。その結果、システム境界があいまいになり、利用可能なデータ量が増え、データと情報の交換が増えています。産業用制御システム（ICS）も、これらのシステムのネットワーク化とインターネットへの接続の拡大により、ますますサイバー攻撃にさらされています。

- **遠隔制御技術**は、水管理システムの自動化に不可欠な要素です。デジタル化の過程で、イーサネットベースのソリューションには多くの利点がありますが、いくつかの課題もあります。イーサネットは外部設備とのデータ交換に一般的に使用されています。ただし、イーサネットベースのネットワークを使用してデジタル化の可用性に大きな影響を与えることもできます。マルウェア攻撃とその深刻な影響は、毎日のようにニュースになっています。プロセスのデジタル化には、強固なITセキュリティ実装戦略が不可欠です。
- **エネルギー供給とネットワーク制御**は、重要インフラの一部です。電力とガスがなければ、日常生活は非常に短い時間で停止してしまい、必要不可欠なサービスを提供することは不可能になります。どのようにエネルギー供給できるかは、情報通信技術が正常な状態かどうかにかかっており、ITセキュリティはエネルギー業界で不可欠です。
- 多くの**プロセス制御**の従事者は、既存のプロセス制御システムのデータを新しい技術のために使用できるようにしたいと考えていますが、その付加価値はクラウドベースのデータ分析によってもたらされます。既存のプロセス制御システムにインダストリー4.0技術を取り入れるには、まず運用データを照合する必要があります。プロセス制御システムデータへのフルアクセスが許可されている場合は、新しい分析および監視方法がより使いやすくなります。データアクセスがセキュアで影響を与えないことが重要です。
- 脅威となるのはインターネットだけではありません。サービスプロバイダーや社内スタッフによるミスも、誤動作や生産の中断につながる可能性があります。故障、破壊行為、またはデータの損失は、著しい損害を引き起こす可能性があります。これは、ダウンタイムが財務上の損失だけでなく、納期やその結果として会社のイメージや評判をも脅かすことにもなるためです。そのため、ICSセキュリティはますます重要になっています。

以上

<フエニックス・コンタクト株式会社について>

世界５５か国以上の海外支社を展開し、従業員１７、４００人以上、創業９５年以上の歴史を持つドイツの産業用接続機器、制御製品および通信機器のマーケットリーダー、フエニックス・コンタクト社の日本法人。日本では本社（神奈川県横浜市）をはじめ１０拠点、および配送センター（神奈川県川崎市）を通じ、ＤＩＮレール搭載用端子台・プリント基板用端子台・産業用コネクタなどの接続機器や、信号変換器・電源・リレーを中心とする電子機器、サージ保護機器、および産業用ネットワーク機器など約6万点におよぶ製品の販売およびカスタマーサービスを行う。詳細はHPをご覧ください。
http://www.phoenixcontact.co.jp

本件に関するお問合せ先：フエニックス・コンタクト株式会社　営業企画部　横井
Tel: 045-548-9796　Email: info@phoenixcontact.co.jp　HP:http://www.phoenixcontact.co.jp