制御システム・ネットワークのセキュリティーに関する留意事項

製造業に関わる多くの企業では各自の競争力を維持するために、自社のオートメーションおよび制御システムをその工場内でより一体化する必要性があることを認識しています。
システムは多くの場合、上位のエンタープライズ・データ・システムと統合する必要があり、さらに複数の工場にわたって情報のアクセスが可能な統合化、またはインターネットを介した統合化が必要になることがあります。この IT の世界とオートメーションの世界の一体化に伴い、安全なシステムの維持、並びに工程、従業員、データ、および知的財産権への投資の保護において課題が生じます。
オートメーション・ネットワークおよびシステムは、内蔵のパスワード保護スキームを備えますが、これは自社のシステムの安全性を確保するための 1 つの小さなステップに過ぎません。オートメーション制御システム・ネットワークは、少なくとも通常のビジネス・コンピューター・システムと同等の堅牢性を備えたデータ保護およびセキュリティー手段を組み込まなければなりません。当社では、PLC、HMI 製品のお客様が、自社の用途に必要な適切なセキュリティーのレベルを決定するために、自社のネットワーク・セキュリティー解析を実施することを推奨します。

防護手段の１つとして、ファイアーウォールの背後に制御システム・ネットワークを配置、それらのビジネス・ネットワークからの隔離、侵入検知システムの採用、並びに仮想プライベート・ネットワーク（VPN）などの遠隔アクセスのための安全な手段の採用などが含まれます。
さらに、ユーザーはすべての制御システム・デバイスのネットワークへの露出を最小限に抑える必要があり、これらのシステムを直接インターネットに接続して露出させるべきではありません。これらの手順に従うことによって、外部および内部の両ソースからのリスクを大きく低減することが可能になり、より安全なシステムを提供することができます。
このようなシステムを防護することは、コンピューターおよびビジネス・システムを防護することとまったく同様に、お客様の責任です。
光洋電子工業は、お客様が自社の安全システムに下記の 1 つまたは複数のリソースを同時に採用することを推奨します。

これらに関連する情報は，以下の機関から参考情報を入手することが出来ます。
⇒経済産業省の情報セキュリティに関する政策，緊急情報など。ウェブ・アドレスは以下のとおりです。
http://www.meti.go.jp/policy/netsecurity/vulhandlingG.html

⇒JP-CERT の情報提供，インシデント報告，制御システムセキュリティなど。ウェブ・アドレスは以下のとおりです。
http://www.jpcert.or.jp/

⇒IPA の情報セキュルティ対策など。ウェブ・アドレスは以下のとおりです。
http://www.ipa.go.jp/security/index.html

上記の一連のリソースは、制御システム・ネットワークの安全性を確保すること、並びにセキュリティー侵害に対するリスクおよびこれに対して露出することを低減するための包括的なアプローチを示唆しています。
インターネットにアクセスするあらゆるシステムの特性を考慮すると、お客様が自社の適用方法に対するセキュリティーの必要性およびその要件の評価を行うこと、並びに自社の制御システムに固有の特定のセキュリティー・リスクを緩和するための措置を講ずることは、それぞれのお客様に課せられた義務です。

光洋電子工業株式会社