IDEC

Think Automation and beyond...

セキュリティに関する注意事項

昨今のインターネット社会の急速な発展と比例して、ネットワークにおけるセキュリティ確保の重要度が高まっています。そこで、弊社製品をご使用する際、必ずご配慮頂きたいセキュリティに関する注意事項を、以下にご案内いたします。これら内容をご理解の上、ご使用いただくようお願い申し上げます。

セキュリティに関する注意事項

一般的には、セキュリティに関する対策を適切に行わずにネットワークを構築すると、以下のような問題が発生する可能性があります。

- 外部ネットワークからの不正侵入に伴うシステムの停止や不正操作、機密情報の搾取、データの改ざんや破壊、マルウェア感染
- マルウェア感染によって踏み台にされ、被害者から加害者へ転じて他のネットワーク機器を攻撃
- ネットワークサービスの許可に伴う思いもよらない情報の漏洩や流出
- なりすましによる不正な操作

上記問題に伴う二次被害（傷害、損害賠償、風評被害、機会損失など）

上記のような問題を防止するため、後述のセキュリティ対策事例を参考に、弊社製品、同じネットワーク内の他の機器、およびそれらがサポートしているセキュリティ機能を適切に設定した上で、弊社製品をネットワークに接続してください。また、必要に応じて、その他セキュリティリスク回避のための十分な措置を講じてください。

なお、弊社製品は電気通信事業者（移動通信会社、固定通信会社、インターネットプロバイダ）等）の通信回線（公衆無線 LAN を含む）に直接接続することはできません。弊社製品をインターネットに接続する場合は、必ずルータ等を経由して接続してください。

不正アクセスの手段や制御システムの脆弱性は、常に新たに発見されており、どんなにセキュリティ対策を実施していても、セキュリティリスクは残ります。ネットワーク接続には常に危険が伴うことをご理解いただくとともに、常に新しい情報を入手し、セキュリティ対策を行うことを強くおすすめします。

不正アクセス等により直接または間接的に生じた損失、損害その他の費用については、弊社は、一切の責任を負いかねますので、ご了承ください。

セキュリティ対策事例

閉域網の構築および暗号化

外部ネットワークと接続する場合、専用ネットワークや VPN など閉域網を使用してネットワークを構築してください。また、可能な限り、暗号化（SSL/TLS）等の処置を講じてください。なお、閉域網を使用してネットワークを構築したとしても、特殊な方法によりセキュリティが破られることもあり得ますので、本リスクをご理解の上、運用してください。

パスワード

以下を参考にして、パスワードを設定してください。弊社製品のパスワード設定方法は、対象製品のマニュアルを参照してください。

- デフォルトパスワードから変更する
- 推測されにくく強度の高いパスワードとする（大小の英字と数字等を含み、桁数が多いもの）
- パスワードを定期的に変更し、厳重に管理する

アクセス制限

以下を参考にして、ネットワーク接続する機器にアクセス制限を設定してください。弊社製品の設定方法は、対象製品のマニュアルを参照してください

- 不要なネットワークサービスやポートは停止する
- 特定のアクセス元からの接続だけを許可する
- アカウント毎にアクセス権を制限する

その他の参考情報

セキュリティに関する様々なガイドラインが国内外で公開されていますので、それらガイドラインに沿ったネットワーク構築および運用を行ってください。2021 年 1 月現在公開されているガイドラインの一例を以下に示します。なお、新しい情報が公開された場合はその新しい情報を参照してください。

NECA 制御システムセキュリティ運用ガイドライン

https://www.neca.or.jp/anzen/control_system_security/

制御システムに関わる人（管理者、設計者、保守担当者、オペレータ）を対象として、制御システムをよりセキュアに構築・運用し、操業を安全に継続するための指針がまとめられています。

総務省／経済産業省 IoT セキュリティガイドライン ver 1.0

https://www.soumu.go.jp/menu_news/s-news/01ryutsu03_02000108.html

IoT 機器やシステム、サービスの供給者及び利用者を対象として、サイバー攻撃などの新たなリスクによる影響を踏まえ、IoT 機器やシステム、サービスに対してリスクに応じた適切なサイバーセキュリティ対策を検討するための考え方が、分野を特定せずまとめられています。

経済産業省／NEDO IoT セキュリティ対応マニュアル産業保安版（第２版）

https://www.meti.go.jp/policy/safety_security/industrial_safety/sangyo/hipregas/files/20190425iotsecuritymanualver2.pdf

産業プラントの管理者を対象として、プラントデータ活用の際のサイバー攻撃による新たなリスクに対して、適切なセキュリティ対策を検討するためのポイントがまとめられています。