サイバーセキュリティ

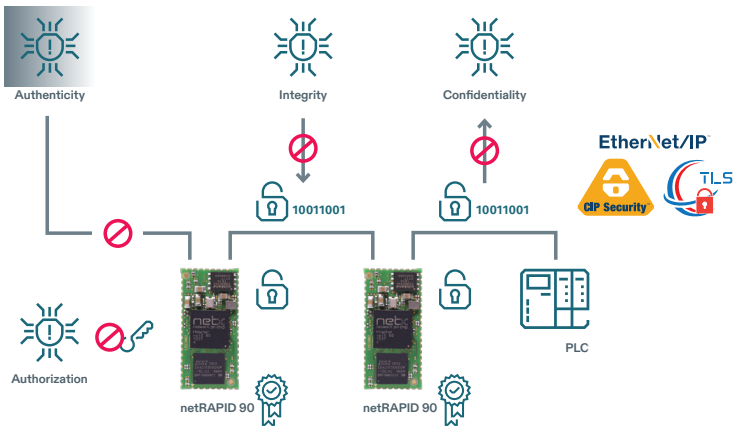
セキュア・フィールドレベル

- **Integrity（完全性）: データの不正操作からの保護**
  EtherNet/IP CIPセキュリティ・ファームウェアでサポートされるIOデータ署名
- **Authenticity（真正性）：信頼できるデバイスのみへの通信を確立**
  EtherNet/IP CIPセキュリティ・ファームウェアは、デバイスID証明書
  Webサーバ証明書によるデバイスID検証に対応
- **Authorization（認証）:認証されたユーザのみがデバイスとデータにアクセス可能**
  netX 90のセキュアブートに対応
  EtherNet/IP CIPセキュリティ・ファームウェアに統合されたユーザ管理
- **Confidentiality（機密性）:不正なデータの読み取りを防止し、データの機密性を保持**
  EtherNet/IP CIPセキュリティ・ファームウェアで対応される
  IOデータ暗号化コンフィデンシャリティ・プロファイル付き

ヒルシャー製品におけるサイバーセキュリティ対応

IIoTとそれに関連するOT/IT融合の重要性が高まるにつれ、サイバーセキュリティの重要性はますます高まっています。システムの堅牢性と可用性と確保するためには、4つのサイバーセキュリティの目標である完全性、真正性、認証、機密性を達成する必要があります。

ヒルシャーの製品は、これらの目標に対応しています。当社のハードウェアとソフトウェアは、IEC62443の要件を満たす機能を提供し、フィールドレベルでのサイバーセキュリティを大幅に向上させます。



→ QRコード リンク: サイバーセキュリティ

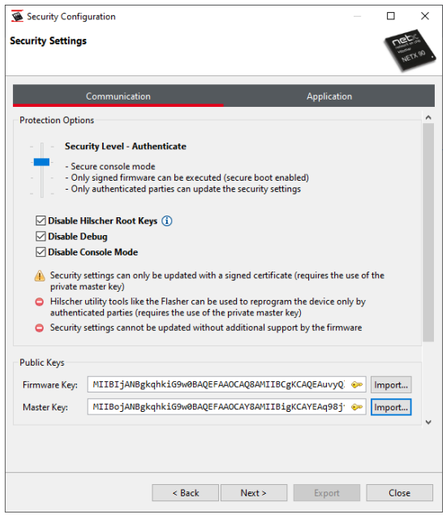
P 03-5362-0521
www.hilscher.jp

セキュア・フィールドレベル – サイバーセキュリティ

セキュアブート

セキュアブートはデバイスの起動段階でアクティブになるため、“ハードウェアに近い”機能です。この機能により、改ざんのないオリジナルのファームウェアのみがデバイス上で起動および実行されることが保証されます。

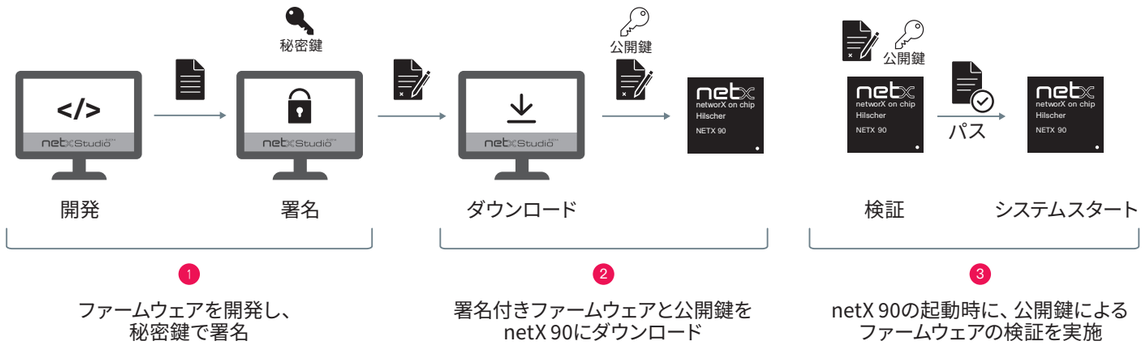
ファームウェアの署名、公開鍵のインストール、セキュアブートの設定は、netX Studio IDE（右図）で実行されます。プロダクション環境では、コマンドライン・ツールが利用可能です。



4つのセキュリティレベルと任意の追加オプションを設定することにより、保護のレベルを上げることが可能です。

- → **Disabled（無効）**
  オープンシステム
- → **Development（開発）**
  ファームウェアの検証は有効だが、セキュリティ設定は制限なく変更可能
- → **Authenticate（認証）**
  ファームウェアの検証は有効で、セキュリティ設定の変更には秘密鍵が必要
- → **Immutable（不変）**
  セキュリティの設定は変更可能

JTAGおよびコンソール・インターフェースはロック可能



セキュア通信

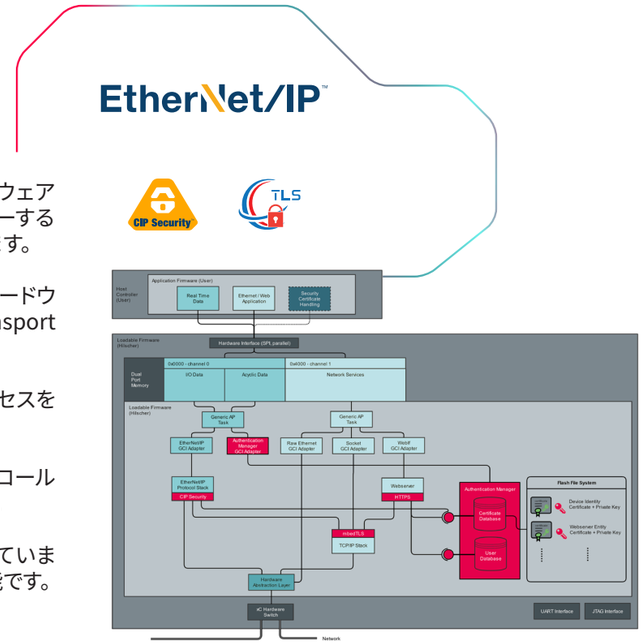
ヒルシャーのnetX 90用のEtherNet/IPプロトコル・ファームウェア（CIPセキュリティ対応）は、完全性、真正性、機密性をカバーする「EtherNet/IP Confidentiality Profile」をサポートしています。

セキュア通信機能の多くは、TCP/IPスタックと、netX 90上にハードウェア実装された暗号アクセラレータ上で実行されるTLS（Transport Layer Security）スタックをベースにしています。

HTTPSプロトコルのサポートにより、安全なWebサーバ・アクセスを実現しています。

実装されたユーザ・データベースにより、ユーザ・グループ、ロール（役割）、関連するデータへのアクセス権の定義が可能です。

セキュリティ機能は、ヒルシャーのファームウェアに内包されています。アプリケーション側の負担が少なく、迅速な市場投入が可能です。



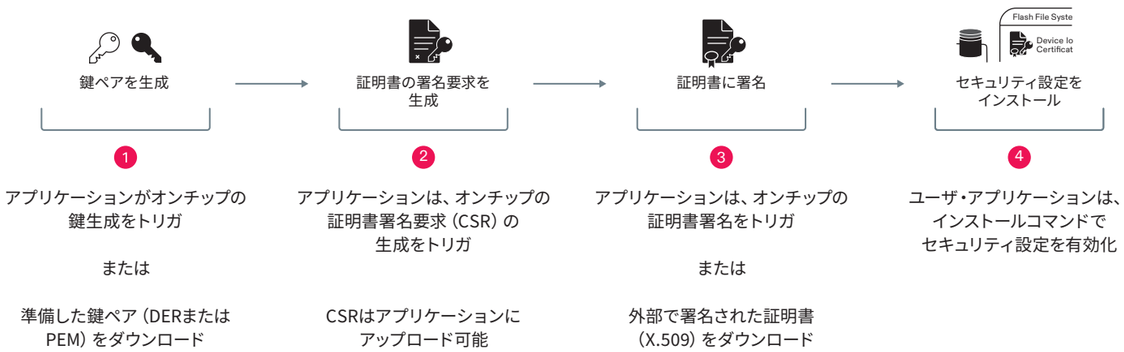
証明書の展開

ヒルシャーのセキュリティ・ファームウェアは、PKI（公開鍵基盤）の有無にかかわらず、セキュリティ証明書の生成と展開に大きな柔軟性を提供しています。

2つの主な方法：

- → デュアルポートメモリ・インターフェース経由のAPIを使用したアプリケーションによるセキュリティ設定
- → EtherNet/IP CIPセキュリティのためのRockwell Factory® Policy Managerなど、プロトコル固有の方法とツール

アプリケーションによるセキュリティ設定は、4つのステップで構成されています。



→ QRコード リンク: サイバーセキュリティ
P 03-5262-0521
www.hilscher.jp

製品情報
技術データ

技術データ

エンドポイント認証
X.509v3証明書（PEM/DER format）、Pre-Shared Key（PSK）

暗号技術
シンメトリック：AES（128、256ビット）、
非シンメトリック：ECC、RSA（2048、3072、4096ビット）

対応楕円曲線
secp256r1、secp384r1

ハッシュ関数
SHA-1、SHA-256、SHA-384

EtherNet/IP over (D)TLSポート・ナンバ
TCP/UDP：2221

HTTPSポート・ナンバ
TCP：443

HTTPS接続番号
1

TLSバーション
1.2

対応セキュリティ・プロファイル
EtherNet/IP Confidentiality Profile

証明書オプション
自己署名証明書、ベンダ署名証明書

ソフトウェアの互換性
Rockwell FactoryTalk® Policy Manager バージョン6.20.00互換

技術データ

EtherNet/IP対応 (D)TLS暗号スイート
ECDHE-ECDSA： SHA-1（暗号化なし）
ECDHE-ECDSA： AES-128ビット CBCモードおよびSHA-256
ECDHE-ECDSA： AES-128ビット、GCMモードおよびSHA-256
ECDHE-ECDSA： AES-256ビット、CBCモードおよびSHA-384
RSA： SHA-256（暗号化なし）
RSA： AES-128ビット、CBCモード、SHA-256
RSA： AES-256ビット、CBCモード、SHA-256
ECDHE-PSK： SHA-256（暗号化なし）
ECDHE-PSK： AES-128ビット、CBCモードおよびSHA-256
ECDHE-PSK： AES-128ビット、GCMモードおよびSHA-256
ECDHE-PSK： ChaCha20 Poly1305モードおよびSHA-256

定義済みの標準オブジェクト
ファナル・オブジェクト（0x37）
CIPセキュリティ・オブジェクト（0x5D）
EtherNet/IPセキュリティ・オブジェクト（0x5E）
認証管理オブジェクト（0x5F）
TCP/IPインターフェース・オブジェクト（0xF5）
Ingress Egressオブジェクト（0x3AC）（Rockwellより）

対応済みの機能
セキュアI/O通信（Class 0/1）
セキュアExplicit Messaging（Class3、UCMM）
Certificate provisioning（Pushモデル経由）
Default Security Configuration（DPM経由）

注: すべての技術データは予告なしに変更される場合があります。

→ QRコード リンク: サイバーセキュリティ
P 03-5262-0521
www.hilscher.jp