White paper

国際規格に適合した IT/OT コントローラのサイバーセキュリティ

- 考え方とニーズ
- 適用技術概要(注力・強化機能等)
- 現場適用法と留意点
- 導入メリットと今後の課題・開発方向

PHOENIX CONTACT

① 考え方とニーズ

デジタル化という言葉をよく聞くようになってからしばらく経っているが、その流れはますます加速していくと考えられる。大目標である脱炭素のためにはデジタル化データを基にして、ライフタイムでの低炭素化になるような判断や、セクターカップリングのための最適な自動処理が欠かせなくなり、IT/OT が融合したデジタル化が進む。

ただし、デジタル化が進むほどサイバー攻撃の対象領域も増加する。意図しない OT の操作は破壊的な問題となるため、OT のサイバーセキュリティは必須になる。

このような状況下で欧州ではいち早くサイバーセキュリティを強化するための法制化が進んでいる。欧州における組織のサイバーセキュリティ対策のための NIS2 指令は 2023 年に発効され、2024 年度中に欧州各国で法制化される。欧州で使用されるあらゆるデジタル機器が対象となるサイバーレジリエンス法(CRA)は 2027 年から適用される。CE マークを付ける即ちサイバーレジリエンス法への適合を宣言していることになる。サイバー攻撃によって引き起こされる安全性の劣化から保護する条項を盛り込んだ機械規則も 2027 年に適用される。わが国でも OT サイバーセキュリティがより大きな問題になっていくのは必至である。

サイバーセキュリティ関連の法律と完全に一致するわけではないが、現時点での OT セキュリティ対策としては現状カバー範囲のもっとも広い IEC 62443 に適合するのが最善と考えられる。多層防御(Defense in depth)、最小権限の原則（Principle of least privilege)、セキュリティロギング、状態監視、常に新しい状態に保つ、定期的な脅威の見直しといった必須事項は IEC 62443 に記載されている。

弊社では、IEC 62443-2-4 に則ったサービス提供、IEC 62443-3-3 に則ったソリューション提供の認証を取得すると共に IEC 62443-4-1(ML3)によるコンポーネント開発プロセスの認証を受け、IT/OT の融合を可能にするリアルタイム Linux ベースのコントローラ PLCnext Control の 3 機種が、IEC 62443-4-2 SL2 に準拠した世界初の PLC として 2021 年に TÜV SÜD により認定された。

その後同規格に適合した製品を順次増やし、セーフティコントローラでも認証を取得している。さらに IEC 62351-3 という IEC 62443 の電力業界用に特化した規格にも適合、認証取得している。IEC 62443-4-2 に適合したセキュリティルータも発売予定である。それら IEC 62443-4-2 に適合したコンポーネント製品を利用することで IEC 62443 に適合したシステム開発がしやすくなり、サイバーセキュリティ関連法への対応も見通しが立てやすくなる。

図 1 PLCnext Control 各機種

② 適用技術概要(注力・強化機能等) 以下 PLCnext Control が実装している主なセキュリティ機能を説明する。

● ファイアウォール、セグメンテーション、ネットワーク負荷低減

ネットワークのセグメンテーションとファイアウォールの設定が多層防御のための第一歩となる。

PLCnext Control の一機種 AXC F 2152 はモジュール追加によって 2 つのイーサネットインタフェースを持つことができる。別の機種 AXC F 3152 は本体にイーサネットインタフェースが 3 つあり、3 つのセグメント化が可能。コントローラからの送受信、セグメント間の通信

をコントローラに組込まれたファイアウォールの設定で制限できる。各インタフェースで、ICMP、TCP、UDP、UDPLITE に関して制限をかけられる。指定 IP アドレス、指定ポートからの流入、指定 IP アドレス、指定ポートへの送出を制御できる。

Netload limiter によって、パケットかつまたはバイト単位の時間当たり流入量を制限できる。

●役割で制限されるアクセス　(RBAC)

PLCnext Control にアクセスするユーザーを登録できる。個々のユーザーに複数個の役割(User Role)を割り当てられる。役割は 28 種類あり、49 種類の作業に対して各役割が実行可能か決まっている(※1)(表 1)。

コントローラにユーザーとしてログインしアクセスする場合(eHMI, OPC UA, REST API、PLCnext Engineer、SSH など)、ユーザーが可能な操作は割り当てられた役割で限定される。役割の適用により Read Only のアクセスも実現できる。個別データ毎に、OPC UA、eHMI(Web)、IoT(MQTT)経路別に外部公開するかも選択できる。

eHMI（コントローラ組込み Web サーバー）の画面に配置するオブジェクト毎に、読み出しで必要なユーザーレベルと書き込みで必要なユーザーレベル(1～10)をそれぞれ指定できる。各ユーザーに対して読み出し可能な役割、書き換え可能な役割、ユーザーレベル役割(1～10)から必要な役割を設定すると、ログイン画面からログインしたユーザー毎に個別画面オブジェクトの読み書き制限が変わる。

PLCnext Engineer(専用エンジニアリングツール)からのコントローラアクセスも、ログインする役割で機能が制限される。SSH のような Linux 標準のコマンドでもユーザーに割り当てられる役割でアクセスが制限される。

その他ユーザー認証や証明書認証のしくみをサポートしていないプロトコルを使用するとセキュリティレベルが 2 は得られないが、例えば MODBUS TCP では、指定変数にのみアクセスできる。

表 1. PLCnext Control 役割表の一部

		User role																	
Application or service	Access permission for:	Admin	SecurityAdmin	SecurityAuditor	CertificateManager	UserManager	Engineer	Commissioner	Service	DataViewer	DataChanger	Viewer	FileReader	FileWriter	EHmiLevel1 → EHmiLevel10	EHmiViewer	EHmiChanger	SoftwareUpdate	SafetyEngineer	SafetyFirmwareUpdater
SD card, parameterization memory	SFTP access to the file system with an SFTP client note↳	√																		
Shell	SSH access to the shell note↳	√																		
PLCnext Engineer	View values in the cockpit (e.g., utilization)	√	√				√	√	√	√	√	√								
	Transfer a project to the controller	√					√	√												
	Start (cold/warm restart) or stop the controller	√					√	√	√											
	Restart the controller (reboot)	√																		
	Reset the controller to default setting type 1	√																		
	View online variable values	√	√				√		√	√	√	√								
	Overwrite variables	√					√		√											
	Set and delete breakpoints	√					√		√											
	Download safety-related programs to the controller	√					√ note↳												√ note↳	
	Start or stop safety-related programs	√					√ note↳												√ note↳	
	Debug safety-related programs	√					√ note↳												√ note↳	
By means of dedicated tools	Update safety-related firmware on the controller	√																		√
PLCnext Engineer HMI application	View online variable values	√	√													√	√			
	Overwrite variables	√															√			
OPC UA access by means of a	View online variable values	√	√				√		√	√	√	√								
	Overwrite variables	√					√		√		√									

●ローカルおよび集中ユーザー管理

正しい相手と接続しているか、真正性の確認はセキュリティ上重要である。
PLCnext Control はユーザー認証をサポートしている接続方法(Web アクセス、OPC UA SSH など)はパスワードでユーザー認証を行う。パスワードの設定には複雑な文字タイプの組み合わせや有効期間を設定可能である。

同一のアカウントの共有は、担当者の離職後にユーザーとパスワードが前のままであればセキュリティリスクとなる。アカウントをユーザー毎に作成し、担当を外れた場合にはそのユーザーを削除することでリスクを削減できる。ただし、複数台数で機器毎にユーザー管理すると、一部の機器で削除もれが起こり得るので、アカウントの集中管理が望まれる。一箇所での管理となり、アカウントの削除もれリスクも減少する。

PLCnext Control では、Microsoft Active Directory など LDAP サーバーとなるディレクトリサービスでアカウントの集中管理が可能である。最大 10 個までの LDAP サーバーに問い合わせできる。LDAP のユーザーが所属する Group に対応する役割を設定可能であり、LDAP 管理下のユーザーも役割によって権限が制限できる。

ローカル、集中管理にかかわらずユーザー毎の接続はセッションとして管理されていて、
無操作時のセッションタイムアウト時間や認証失敗時の再ログインに関するペナルティも設定可能である。同時に接続できるユーザーセッション数も設定できる。

●鍵管理と証明書管理

真正性の確認はデバイス、ソフトウエアに関しても重要である。
PLCnext Control では TPM を実装しており、機器の ID、秘密鍵、シリアル番号、初期パスワード、MAC アドレスなど製造時に IEC 62443-4-1 のプロセスに従ってセキュアに保管している。これによって確かに当社が製造したデバイスであることが確認でき、設定ツール PLCnext Engineer とのセキュアな接続にも使用される。また TPM に格納されている情報を使い、プログラムが想定した機器個体で動作しているか確証できるファンクションブロックがある。

PKI(公開鍵基盤)に対応し、秘密鍵で署名された自己証明書、自身の証明書チェインを Identity Store で管理し、外部エンティティの証明書チェイン、証明書失効リスト(CRL)を Trust Store で管理する。

PLCnext Control は内蔵ストレージの暗号化の他、暗号化可能な SD カードの中身を本体 TPM を利用して暗号化し、その本体か、リカバリーパスワードが設定された同タイプのコントローラとの組み合わせ以外では動作不可にできる。

集中ユーザー管理のための LDAP サーバーの真正性は、Trust Store に格納したサーバー証明書で検証可能である。

PLCnext Control では各種 OPC UA 通信機能が利用できるが、OPC UA クライアント機能、OPC UA サーバー機能では、接続の相互認証が可能である。クライアント側でサーバー証明書を検証し、OPC UA サーバーとしての真正性を確認できると共に、サーバー側でクライアント証明書を検証し、クライアント機器の真正性も確認できる。内蔵 OPC UA サーバーの証明書は OPC UA の Global Discovery Service (GDS)によって配布できる。

IPSec VPN、OpenVPN 機能を利用する場合も証明書で相互接続の真正性を確認できる。

● TLS によるセキュアな通信

PLCnext Control のファームウエアは入稿時点の最新長期サポート版である OpenSSL 3.0 を使用している。OPC UA、MQTT、LDAP、eHMI/REST API(http)も TLS に対応している。
PKI と TLS の仕組みによって、通信の真正性、完全性、機密性が担保される。

PLCnext Engineer からのプロジェクトダウンロード時にコントローラ本体ではハッシュコードにより完全性の確認を行う。

IEC 言語でも TLS_SOCKET_2 ファクションブロックにより TLS で双方向のセキュアな通信が可能（真正性、完全性、機密性)。また、集中ユーザー管理で使用する LDAP サーバーとの接続は LDAPS 及び STARTTLS での TLS 通信ができる。

●ローカルまたは集中セキュリティロギング

ローカルまたは集中ロギングが可能である。特定の役割のみがアクセスできる。

集中ロギングではプロトコルに TLS を選択できる syslog-ng を使用している。syslog サーバーのサーバー証明書を Trust Store にインポートし真正性を確認できる。

●バックアップ、リストア、 デバイスの更新管理 (DaUM)

OPC UA のファイル転送機能をサポートし、Windows または PC タイプの PLCnext Contol 上で動作する DaUM 機能から、集中管理でファームウエア、プロジェクトの更新、バックアップ、復旧も可能である。これにより可用性の向上にも貢献できるようになる。

③ 現場適用法と留意点

図 2 は、IEC 62443-4-2 要求に基づき OT セキュリティに焦点を当てた PLCnext の汎用セキュリティコンテキストを示している。

図 2 汎用セキュリティコンテキスト

本セキュリティコンテキストは図 2、表 2 で示す 6 層のセキュリティ層(ゾーン・コンジット)からなる多層防御コンセプトと対策に基づく。

より頑強な多層防御のため、製品はこのようなセキュリティコンテキストの中で使用されるべきである。

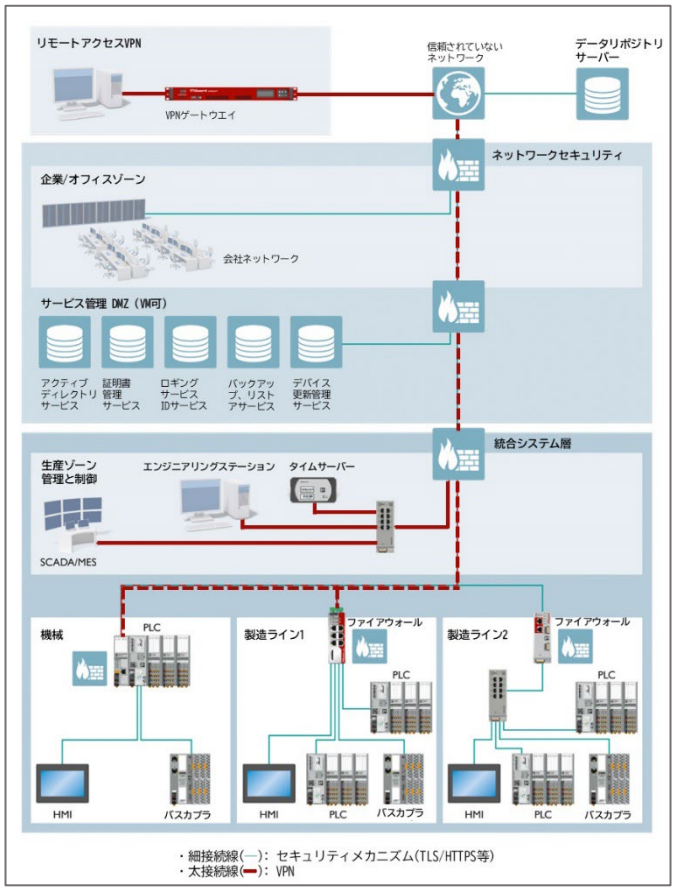

図 1: 汎用セキュリティコンテキスト

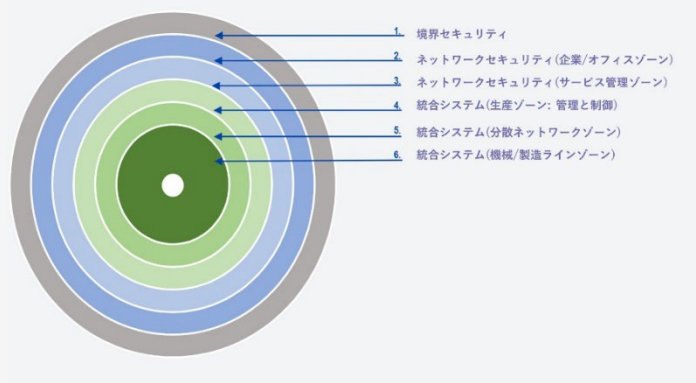

図 2: 6 層のセキュリティ層(ゾーン・コンジット)からなる多層防御コンセプト

2024 年 9 月現在のファームウエア(※1)では、Security Profile というフラグを有効にすると、セキュアでない設定は自動的に無効化され、IEC 62443-4-2 SL2 を満たす機能の設定ができるようになる。

表 2: セキュリティ層と対策

基本防御層	セキュリティ層	保護対策
境界セキュリティ(外側の層)	企業ネットワークのアクセス	物理的な分離
		ネットワークのセグメント化によるデジタル的分離
		論理的なアクセス制御
		ファイアウォール(認識された脅威と脆弱性に対応)
		リモートアクセス用にVPN他のセキュリティ手段
		すべてのリモートアクセスポイントのドキュメント化
ネットワークセキュリティ層	企業ネットワークゾーンと非武装地帯 (DMZ) と見なされるサービス管理ゾーンで構成される工場ネットワーク保護層	すべてのネットワークデバイスとホストの識別
		プロトコル/トラフィックの分析
		ワイヤレス通信/トラフィックの監査
		スイッチ/ルーター構成の分析
	DMZ	OSの脆弱性チェック
		OSパッチ管理
		USB、リムーバブルデバイスの制御室内での使用禁止
		外部コンピューターの接続を制限
統合システム層(内部層)	生産ゾーン・管理と制御(SCADAアプリケーション)	クリアテキスト転送のネットワーク監視、暗号化
		個々のユーザーアカウント使用
		デスクトップへのアクセス制限
	分散ネットワーク(フィールドコントローラ)	イーサネット接続デバイスかシリアル接続デバイスか
		脆弱性ラボテスト済イーサネットデバイス
		ベンダーデフォルトパスワードの削除
	マシン/製造ラインレベルの制御サブネットワーク層(メインプロセスとサブプロセス)	有線通信かワイヤレス通信か
		イーサネット通信かシリアル通信か
		イーサネット接続でのトラフィックのキャプチャ

結果 IEC 62443 に適合したシステム構築が出来上がったとしても、ソフトウエアには必ず不具合や欠陥がつきものであり後に脆弱性が顕在化しうる。弊社では、Product Incident Response Team (PSIRT)という組織において、報告された製品の脆弱性に対して IEC 62443 に記載のとおりセキュリティパッチの準備、発行を含む適切な対応をしている。

④　導入メリットと今後の課題・開発方向

OT デジタル化の促進とともにセキュリティリスクも高くなるが、PLCnext Control は、IT で広く使用されている技術で OT との融合化を図るだけでなく IEC 62443-4-2 に記載されている項目の多くを実装し、セキュアなシステムを構築するのに必要な多層防御、最小権限の原則を実現可能にしている。

現時点では Security Profile 設定によって有効となる IEC 62443-4-2 適合のセキュリティ機能が、近日中に Security By Default として初期設定になる予定である。

オープン性、利便性、緊急性などはセキュリティとは相反することがある。機能の多くは Web 画面でグラフィカルに設定できるが、セキュリティを保つ作業が、本来の目的の作業よりも多くなったり、緊急操作の妨害となったら本末転倒である。

機械可読できるセキュリティレポートのフォーマット CSAF（Common Security Advisory Format）に対応予定である。セキュリティパッチ適用までの時間短縮化が進み、セキュアなシステム維持の効率化が期待されている。OPC UA のサーバー証明書で実現している証明書配布の効率化も要求事項の一つである。

多層防御、最小権限の原則をより進め、真正性、完全性、機密性を確保する範囲もさらに広げて行く予定である。可用性及び他の要求との適切なバランスを保ちながら進めるのも重要なポイントである。

注）※1 ファームウエアバージョン 2024.0.6 LTS

《本記事は『計装』2024 年 11・12 月号掲載の内容です》

本資料に関するお問い合わせ：フエニックス・コンタクト株式会社

Website: www.phoenixcontact.co.jp Mailto:jp-info@phoenixcontact.co.jp