取扱説明書

セキュリティガイドライン

IPC

バージョン　3.0
日付:　2019-06-19

BECKHOFF

目次

1 序文

1.1 取扱説明書に関する注記

この説明書は関連する国内規格を熟知した、制御およびオートメーションエンジニアリングの専門家の使用のみを目的としています。
本製品のインストールおよびコミッショニングの際は、必ず以下の注意事項と説明に従ってください。

本製品を使用するうえでの責任者は、本製品の用途および使用方法が、関連するすべての法律、法規、ガイドラインおよび規格を含む、安全に関するすべての要件を満たしていることを確認してください。

免責事項

この取扱説明書の記載内容は、 一般的な製品説明および性能を記載したものであり、場合により記載通りに動作しない場合があります。
製品の情報・仕様は予告なく変更されます。
製品の個別の特性に関する情報提供の義務は、契約条件において明示的に合意している 場合にのみ発生します。この説明書に記載されているデータ、図および説明に基づいて、すでに納品されている製品の変更を要求することはできません。掲載されている写真やイラストと、実際の製品は異なる場合があります。この説明書は最新でない可能性があります。必ずhttps://infosys.beckhoff.comに掲載された最新バージョンの説明書を参照してください。

商標

Beckhoff®、TwinCAT®、 EtherCAT®、 Safety over EtherCAT®、 TwinSAFE®、 XFC® およびXTS®は、Beckhoff Automation GmbHの登録商標です。
この取扱説明書で使用されているその他の名称は商標である可能性があり、第三者が独自の目的のために使用すると所有者の権利を侵害する可能性があります。

特許出願

EtherCATテクノロジについては、欧州特許
EP1590927 および EP1789857、 ドイツ特許 DE102004044764 および DE102007017835
に記載されていますが、これらに限定されるものではありません。

TwinCATテクノロジについては
EP0851348、US6167425、および各国の 対応する特許出願または登録に記載されていますが、これらに限定されるものではありません。

EtherCAT®は、Beckhoff Automation GmbH（ドイツ）がライセンスを受けた特許取得済み技術であり登録商標です。

著作権

1.2 安全に関する指示事項

安全に関する注意事項

この取扱説明書に記載された安全に関する指示や注意事項はよくお読みになり、必ず指示に従ってください。

納入仕様

すべての製品は、用途に適した特定のハードウェア構成およびソフトウェア構成を有する状態で供給されます。ハードウェアまたはソフトウェアに取扱説明書に記載されている以外の変更を加えることは許可されていません。許可されていない変更を加えると、Beckhoff Automation GmbH & Co. KGの保証の対象外となります。

使用者の資格

この説明書は関連する国内法規を熟知した、制御およびオートメーションエンジニアリングの専門家の使用を目的としています。

安全記号の説明

この取扱説明書では、安全に関する指示や注意事項とともに以下の安全記号を使用します。安全に関する指示事項はよくお読みになり、必ず指示に従ってください。

 危険	**重大な人的傷害の危険** この記号が付いた安全に関する注意事項に従わないと、人命および健康に直ちに危害を及ぼします。
 警告	**人的傷害の危険** この記号が付いた安全に関する注意事項に従わないと、人命および健康に危険を及ぼします。
 注意	**人的傷害の恐れ** この記号が付いた安全に関する注意事項に従わないと、人命および健康に危険を及ぼす恐れがあります。
 注意	**物的損害と環境汚染** この記号が付いた安全に関する注意事項に従わないと、物的損害と環境汚染をもたらす恐れがあります。
 注記	**ヒントまたはアドバイス** この記号が示す情報により、さらに理解が深まります。

2 概要

このガイドは、ベッコフ製品使用時のセキュリティリスク管理の支援を目的としています。

セキュリティリスクの管理は、オートメーションシステム全体のリスク管理の一部です。セキュリティリスク管理の目的は、セキュリティリスクの検出、分析、評価、監視、制御を通してオートメーションシステムの安全な状態を実現することです。ただし、完全にリスクのない安全な状態にすることは不可能です。

このガイドはリスク管理に関して記載し、ベッコフ製品をさまざまな脅威から保護する基本的な方法について説明しています。このガイドは定期的に改訂および補訂されます。

内容

ハザードおよびリスクアセスメント [▶ 9]	このセクションでは、オートメーションシステムのハザードおよびリスクアセスメントの概要について記載します。さまざまな攻撃者、攻撃の種類、および典型的な脅威のシナリオや保護原理について説明します。基本的な事項が、このガイドの付録内のセクション「セキュリティに関するプロパティ [▶ 28]」に記載されています。
対策 [▶ 14]	このセクションでは、物理的な対策、ユーザおよびプログラムの管理、OSのセキュリティ強化、および通信関連の事項を含む基本的なセキュリティ対策について記載します。 目的に合った対策を講じ、アプリケーションに応じて有効な対策を選択することを推奨します。
付録 [▶ 19]	対策の実施については、付録で順を追って説明します。加えて、セキュリティ関連のプロパティの概要、および参考資料やツールに関する記載があります。

個々の対策を単独で実施するだけでは、セキュリティの強化は実現できません。さまざまな支援プロセスを実施することで、初めてセキュリティを維持できます。このようなセキュリティプロセスは、例えばIEC 62443で説明されています。セキュリティプロセスには、資産管理、脅威の分析、パッチ管理が含まれます(「参考資料 [▶ 29]」を参照)。

セキュリティの問題に関するサポート

当社製品のセキュリティに関する事象を解決したい場合、またはセキュリティの問題をレポートする場合は、Eメール(product-securityincident@beckhoff.com)あてにご連絡ください。お客様からのご要望は、可能な限り迅速に処理いたします。

2.1 ベッコフの障害対応チームの連絡先

住所

Beckhoff Automation GmbH & Co. KG
Product management (Security)
Huelshorstweg 20
33415 Verl
Germany

Eメール

<product-securityincident@beckhoff.com>

このアドレス宛のEメールは、ベッコフの障害対応チームの対応可能なメンバーに送信されます。

公開鍵

ベッコフの障害対応チームに連絡する際に必要な鍵が2つあります。

- ID B4 F4 15 9A およびフィンガープリント C9 6F 56 5C 39 49 43 58 AE B5 07 93 80 95 E1 2D B4 F4 15 9A のPGP鍵
- ID 2e 9d 0d bf 0d ee b3 37 63 2f ae 96 およびフィンガープリント 90 69 af 0c 32 d6 ad 15 25 3d 84 60 ae c9 ca 48 75 b5 8a 91 のS/MIME証明書

鍵のダウンロード: https://download.beckhoff.com/download/document/product-security/Keys

受付時間

障害対応チームは、通常9:00から17:00まで受け付けています。NRW(ノルトライン＝ヴェストファーレン)州の祝日は受け付けていません。

タイムゾーン: CET（ヨーロッパ/ベルリン）

3 ハザードおよびリスクアセスメント

このセクションでは、オートメーションシステムのハザードおよびリスクアセスメントの概要について記載します。さまざまな攻撃者、攻撃の種類、および典型的な脅威のシナリオや保護原理について説明します。

3.1 攻撃者

攻撃者の場所による分類

システムへのアクセス方法に応じて、攻撃者は4つのクラスに分類できます。

クラス	説明
インサイダー攻撃者	オートメーションシステムに対して特定の操作を実行しようとする攻撃者。攻撃者は、許可されていない損傷を与える操作を実行することを意図しています。加えて、このような攻撃者には、不正操作の実行に必要なパスワードなどの秘密情報へのアクセスがあります。
ローカル攻撃者	オートメーションシステムのコンポーネントに直接アクセスする攻撃者。このクラスには、ハードウェアインターフェイス経由でコンポーネントに直接アクセスできる攻撃者、または別の場所でネットワークトポロジを変更できるローカル攻撃者も含まれます。
内部ネットワークの攻撃者	内部ネットワーク上でデバイスを制御する攻撃者。通常、これらの攻撃者はネットワークトポロジを変更できず、ネットワーク内の既存のサービスを使用します。
外部ネットワークからの攻撃者	例えば、インターネットに接続されているインターフェイス経由でしか操作を実行できない攻撃者。内部コンポーネントへの攻撃が成功すると、これらの攻撃者は内部ネットワークの攻撃者へとエスカレートすることがあります。

前提

すべての攻撃者について、以下の前提条件を仮定する必要があります。

- インターネットから、またはサービス呼び出しによってドキュメンテーションなどの公開情報を取得できる。
- 市販されているあらゆる製品を取得し、これらの製品を分析することで意図する攻撃の準備ができる。
- クラウドプロバイダから演算時間を借りるなどして、膨大な演算性能を自由に使用できる。

多くの場合、攻撃者の動機は仮定や推測でしか知ることができないため、攻撃者の動機を根拠にその都度、分類を変更することは適切ではありません。

3.2 攻撃の種類

攻撃者は、実行する攻撃の種類によって分類できます。どのような試みで攻撃が行われるかが分類のポイントです。

分類	説明
広範囲のウイルス攻撃	この攻撃はシステムの広域な脆弱性を悪用し、到達可能な近隣のシステムへと攻撃を拡大します。このような「無差別攻撃」は、攻撃者に利益をもたらすために、できるだけ多くの関係システムを攻撃することを目的としています。例えば、攻撃者はデータの復号とひきかえに金銭を恐喝する行為(ランサムウェア)や、攻撃対象者のリソースの使用(ボットネット)などから利益を享受します。多くの場合、これらの攻撃はパッチが適用されていない脆弱性や、弱いパスワードなど企業の一般的な不備を悪用します。

分類	説明
製品固有の攻撃	この攻撃は、あまり一般的ではない特定の製品の脆弱性を悪用します。この攻撃も自動的に広がる可能性はありますが、この脆弱性は特定の製品または設定に存在します。攻撃の目的は、ノウハウのスパイ行為など、業界固有である場合もあります。
インストール固有の攻撃	この攻撃は1つのシステムインストールのみを対象として実行されるため、標的型攻撃とも呼ばれます。攻撃者はこれらの攻撃を巧みに実行するため、これを検出することは困難です。攻撃の目的を達成するために、攻撃の標的となるシステムの設定が悪用されます。攻撃の標的は多種多様であり、一般に予測が困難とされています。

注記	このセキュリティガイドは、広範囲のウイルス攻撃および製品固有の攻撃に対する対策のみを記載しています。インストール固有の攻撃に対しては、アプリケーション固有の分析および対策が必要となります。

3.3 典型的な脅威のシナリオ

このセクションは典型的な脅威についての説明であり、対策がすべて網羅されている訳ではありません。

不正操作されたブートメディア

攻撃の種類/攻撃者	インサイダー	ローカル	内部ネットワーク	リモート
広範囲のウイルス攻撃	対象外	対象外	対象外	対象外
製品固有の攻撃	対象	対象	対象外	対象外

あらかじめ用意されたデータストレージデバイスがコンポーネントに接続され、このデバイスからコンポーネントが起動されます。UEFI/BIOSの起動順序が外部ディスクからの起動に設定されている場合、または攻撃者が起動順序を変更できる場合に、上記の操作が可能になります。

この攻撃によって、攻撃者はコンポーネントのすべてのデータ、特に設定やノウハウに関するデータへの読み取りおよび書き込みアクセス権を取得します。このようなアクセスが発生した後は、コンポーネント全体を安全ではないとみなす必要があります。

防御手段:

- BIOSパスワード(BIOS設定 [▶ 14])
- ブートメディアの設定(BIOS設定 [▶ 14])
- 制御盤のロック [▶ 14]

不正操作されたPXEブートサーバ

攻撃の種類/攻撃者	インサイダー	ローカル	内部ネットワーク	リモート
広範囲のウイルス攻撃	対象外	対象外	対象	対象外
製品固有の攻撃	対象外	対象外	対象	対象外

内部ネットワーク内の不正操作されたPXEブートサーバからの起動。この攻撃には、攻撃者によって制御されたコード実行が含まれます。

この攻撃によって、攻撃者はコンポーネントのすべてのデータ、特に設定やノウハウに関するデータへの読み取りおよび書き込みアクセス権を取得します。このようなアクセスが発生した後は、コンポーネント全体を安全ではないとみなす必要があります。

防御手段:

- PXEブートの無効化(BIOS設定 [▶ 14])

不正操作されたUSBデバイス

攻撃の種類/攻撃者	インサイダー	ローカル	内部ネットワーク	リモート
広範囲のウイルス攻撃	対象外	対象	対象外	対象外
製品固有の攻撃	対象	対象	対象外	対象外

不正操作されたUSBデバイスが接続されると、関係デバイス上で攻撃者が悪意のあるコードを実行する可能性があります。加えて、不正操作されたUSBデバイスがノウハウの盗み出しに使用される可能性もあります。例えば、自動起動を適切に設定すれば、あらゆるコードを実行できます。あらかじめ準備された入力デバイスによって、不正な入力が行われたりログに記録されたりする可能性があります。

このような攻撃によって、攻撃者はOS（特に設定やノウハウ）に関する多くのデータへの読み取りおよび書き込みアクセス権を取得します。このようなアクセスが発生した後は、コンポーネント全体を安全ではないとみなす必要があります。

防御手段:

- 自動起動の無効化（自動起動 [▶ 15]）
- USBデバイスのホワイトリスト化（グループポリシー - USBデバイス [▶ 15]）
- 制御盤のロック [▶ 14]
- BIOSでのインターフェイスの無効化（BIOS設定 [▶ 14]）
- プログラムのホワイトリスト化 [▶ 15]

ローカルインターフェイスを介した弱いパスワードの推測

攻撃の種類/攻撃者	インサイダー	ローカル	内部ネットワーク	リモート
広範囲のウイルス攻撃	対象外	対象外	対象外	対象外
製品固有の攻撃	対象	対象	対象外	対象外

初期パスワードや簡単に推測できるパスワードなど、弱いパスワードはローカルの攻撃者に悪用される可能性があります。攻撃者は未変更の初期パスワードを使用して、権限のあるローカルユーザ同様にログインできます。

このような攻撃によって、攻撃者はOS（特に設定やノウハウ）に関する多くのデータへの読み取りおよび書き込みアクセス権を取得します。このようなアクセスが発生した後は、コンポーネント全体を安全ではないとみなす必要があります。

防御手段:

- セキュアなパスワードの選択 [▶ 14]
- パーソナライズドユーザの設定

データストレージメディアの盗難

攻撃の種類/攻撃者	インサイダー	ローカル	内部ネットワーク	リモート
広範囲のウイルス攻撃	対象外	対象外	対象外	対象外
製品固有の攻撃	対象	対象	対象外	対象外

攻撃者がデータストレージデバイスを不正に取り外し、オートメーションシステム内のサービスのナレッジを取得し、それらのサービスにアクセスする可能性があります。

このような攻撃によって、攻撃者はOS、特にアクセスデータや、設定、ノウハウに関する多くのデータへの読み取りアクセス権を取得します。

防御手段:

- ハードディスクの暗号化 [▶ 16]
- 制御盤のロック [▶ 14]

迷惑メールの処理

攻撃の種類/攻撃者	インサイダー	ローカル	内部ネットワーク	リモート
広範囲のウイルス攻撃	対象外	対象外	対象外	対象
製品固有の攻撃	対象外	対象外	対象外	対象

迷惑メールは、マルウェアを拡散するための一般的な方法です。この攻撃は特に、受信者が最新ではないブラウザでハイパーリンクを開いたり、Eメールの添付ファイルを開いたりする操作を悪用します。Eメールが信頼できるメールに見えるように偽装されている場合もあります。

攻撃が成功すると、システム操作が可能なユーザ権限で不正な操作の実行が可能になります。

防御手段:

- Eメールの処理に制御用コンピュータを使用しない
- 定期的または自動的なソフトウェア更新(更新 [▶ 16])
- プログラムのホワイトリスト化 [▶ 15]

最新ではないソフトウェアの既知の脆弱性の悪用

攻撃の種類/攻撃者	インサイダー	ローカル	内部ネットワーク	リモート
広範囲のウイルス攻撃	対象	対象	対象	対象
製品固有の攻撃	対象	対象	対象	対象

メーカは既知の脆弱性を修正するためのソフトウェア更新をリリースします。使用中のソフトウェアが更新されていない場合、広範囲にわたるウイルス攻撃の対象となる可能性があります。

攻撃が成功すると、関連するソフトウェアの内容に影響を及ぼす不正な操作の実行が可能になります。

防御手段:

- Windowsアップデート(更新 [▶ 16])
- 定期的または自動的なソフトウェア更新(更新 [▶ 16])
- ネットワークベースの不正検知メカニズム(IDS/IPS)
- 不要なサービスの無効化
- 不要なコンポーネントの除外 [▶ 16]

不正操作されたWebサイト

攻撃の種類/攻撃者	インサイダー	ローカル	内部ネットワーク	リモート
広範囲のウイルス攻撃	対象外	対象外	対象外	対象
製品固有の攻撃	対象外	対象外	対象外	対象

ユーザが、不正なWebサイトを閲覧するように誘導されます。ブラウザの脆弱性を悪用して任意の悪意のあるコードを実行する場合や、ユーザがログインデータなど機密情報を開示するようにWebサイトが設計されている場合などがあります。

攻撃が成功すると、システム操作が可能なユーザ権限で不正な操作の実行が可能になります。

防御手段:

- 定期的または自動的なソフトウェア更新(更新 [▶ 16])
- ネットサーフィン行為に対する組織的な対策

中間者攻撃

攻撃の種類/攻撃者	インサイダー	ローカル	内部ネットワーク	リモート
広範囲のウイルス攻撃	対象	対象外	対象外	対象外
製品固有の攻撃	対象	対象	対象	対象

セキュリティで保護されていないネットワークプロトコルを使用すると、攻撃者はネットワーク内の正常なリモートステーションになりすますことができます。これにより、このプロトコル経由で送信される情報の不正操作や傍受が可能になります。

攻撃が成功すると、オートメーションシステム内でサービスの意図しない動作が発生する可能性があります。

防御手段:

- ネットワークセグメンテーション
- セキュリティで保護されたネットワークプロトコルの使用

ネットワークサービスの不正使用

攻撃の種類/攻撃者	インサイダー	ローカル	内部ネットワーク	リモート
広範囲のウイルス攻撃	対象外	対象外	対象	対象
製品固有の攻撃	対象外	対象外	対象	対象

攻撃者がアクセス可能なネットワークサービスが提供されていると、不正操作を招く恐れがあります。

攻撃が成功すると、オートメーションシステム内でサービスの意図しない動作が発生する可能性があります。

防御手段:

- ネットワークセグメンテーション
- ネットワークサービス認証の使用
- 不要なサービスの無効化
- 不要なコンポーネントの除外 [▶ 16]

4 対策

このセクションでは、物理的な対策、ユーザおよびプログラムの管理、OSのセキュリティ強化、および通信関連の事項を含む基本的なセキュリティ対策について記載します。

対策の実施については、付録で順を追って説明します。対策がすべて網羅されている訳ではありません。

4.1 物理的な対策

制御盤のロック

産業用PCを格納する制御盤は、基本的にロックする必要があります。産業用PCの特定のインターフェイスのみを制御盤の外に出すことで、攻撃対象領域を大幅に縮小できます。制御盤は、業務で必要な人のみがアクセスできるようにする必要があります。スマートカードなどの電子ロックシステムも使用できます。鍵で管理される他のシステムと同様に、制御盤へのアクセスが不要となった時点で、鍵を無効にする必要があります。

監視カメラ

監視カメラは、多くの人がコントローラへのアクセスを必要とする環境や、施設が地理的に分散している環境での交代勤務の場合などに適しています。ただし、監視カメラによって攻撃を検出することはできても、それを防ぐことはできません。このため、監視カメラは他の対策と組み合わせて使用する必要があります。

4.2 ユーザおよびプログラムの管理

4.2.1 セキュアなパスワードの選択

システムのセキュリティを保証する上で、強力なパスワードが重要な前提条件となります。

ベッコフは、Windowsのデフォルトユーザ名および初期パスワードでイメージを納入します。これらはお客様によって変更する必要があります。コントローラは、UEFI/BIOSのパスワードが設定されていない状態で納入されます。ここでも、パスワードを設定することを推奨します。

以下に注意してください。

- パスワードはユーザおよびサービスごとに設定する必要があります。
- これまでの推奨事項に反することですが、定期的なパスワードの変更は行わず、権限のない人物にパスワードが漏えいする事象が発生した後でのみパスワードを変更することを推奨します。(https://arstechnica.com/information-technology/2016/08/frequent-password-changes-are-the-enemy-of-security-ftc-technologist-says/ も参照)
- ログオンに失敗した後に、強制的に一定の待機時間を設けることは有用です。

参考資料:

- セキュアなパスワードの選択 [▶ 19]

4.2.2 BIOS設定

起動順序やCPUクロックなどの重要な設定を無許可で変更できないように、BIOSに対してパスワードを設定することを推奨します。起動順序を設定し、外部ディスクからの起動を防止することも有用です。

4.2.3 グループポリシー - USBデバイス

USBなどの外部インターフェイスをブロックするために、制御盤などによって物理的にセキュリティを強化できます。ただし、デバイスが制御盤に取り付けられている場合でも、USBポートが使用されている、または使用することが必要な場合があります。攻撃対象領域を縮小するため、OSでインターフェイスの使用を調整および制限する必要があります。

参考資料:

- 不要なコンポーネントの除外 [▶ 23]

4.2.4 監査ポリシー

ファイルやフォルダへのアクセス操作は、Windowsでログとして記録できます。選択したファイルまたはフォルダにユーザがアクセスするたびに、いわゆる監視イベントがWindowsログ内に記録されます。

参考資料:

- 監査ポリシー [▶ 21]

4.2.5 プログラムのホワイトリスト化

ホワイトリストを使用した対策により、システム上で実行可能なプログラムを明示的に指定できます。これらの対策によって、不正なコードからの保護が可能です。

Windows 7/10には、2つの異なるホワイトリストの方法が用意されています。

- ソフトウェア制限ポリシー(SRP)
- AppLocker

ソフトウェア制限ポリシーは、システム上で実行可能なプログラムを明示的に指定するためのスコープを定めます。これにより、他のすべてのプログラムが実行できなくなります。これらのポリシーは、ローカルセキュリティポリシーから使用できます。

Windows 7から採用されているAppLockerには、広範囲な機能をそなえています。AppLockerとSRPの違いはこちらで説明されています。

参考資料:

- プログラムのホワイトリスト化 [▶ 21]
- ベッコフソフトウェアのパス [▶ 28]（ベッコフ製品の概要および対応するプログラムのパス）

4.3 OSのセキュリティ強化

4.3.1 自動起動

外部デバイス(USBストレージメディアやキーボードなど)が接続されていると、自動起動のメカニズムによってコントローラが容易にウイルス感染してしまいます。自動起動が不要な場合は、無効にする必要があります。

参考資料:

- 自動起動 [▶ 22]

4.3.2 プログラムの非表示

特定のユーザグループのみアクセス可能な機能の使用を防止するために、これらをOSの機能によってブロックまたは非表示にすることが可能です。

プログラムおよびその実行は、ホワイトリスト化によっても制限できます。

参考資料:

- プログラムのホワイトリスト化 [▶ 21]
- プログラムの非表示 [▶ 22] (Windows 7/10の特定の機能をブロックする命令)

4.3.3 不要なコンポーネントの除外

攻撃対象領域を縮小するため、不要なプログラムおよびOSコンポーネントは削除する必要があります。

4.3.4 ライトフィルタ

Windows Embedded OSのライトフィルタ機能により、ストレージメディアで行われた変更を別のストレージメディアに保存することが可能です(オーバーレイ)。これは、例えばコンパクトフラッシュカードやSSDに対する書き込み操作をRAMオーバーレイに保存し、書き込みアクセス操作の影響を軽減して、寿命を延ばす場合などに便利です。ただし、システムの再起動時にデータ消失しないように、変更を明示的に適用する必要があります。

オペレータの視点からすれば、マルウェアによって行われた変更が再起動後に解消され、操作を再開できれば合理的です。ただしこの場合、繰り返し発生する可能性がある感染や攻撃に関する情報は、ほぼ収集できません。

また、ライトフィルタのオン/オフの切り替えは安全ではありません。攻撃が発生したコンテキストのユーザがライトフィルタ設定を変更できる場合、攻撃者もこれを変更できることになります。

参考資料:

-

4.3.5 ハードディスクの暗号化

ハードディスクの暗号化の目的は、保存されているデータへの不正アクセスを防止することです。

ストレージメディア上のデータを暗号化する方法には、特定のデータのみを暗号化する方法(Microsoft EFSなど)や、パーティション全体を暗号化する方法(Microsoft Bitlockerなど)があります。

重要なポイントは、鍵の管理です。

- 誰にアクセスを許可するか?
- どのような認証オプションがあるか? (USBトークン、TPM、PIN、パスワード、ユーザ名とパスワード...)

いずれの場合も、データを復号して使用すると保護されません。

参考資料:

- ハードディスクの暗号化 [▶ 23]

4.3.6 更新

OSおよびプログラムを最新に保つ方法は複数存在します。

- イメージ全体の更新

- 個々のプログラムの更新
- 内蔵OSの更新

コンピュータ、OS、および使用するプログラムに応じて、さまざまなオプションがサポートされています。

参考資料:

- 更新 [▶ 24]

4.4 通信

4.4.1 リモートメンテナンス

リモートメンテナンスは、工業設備において重要な役割を担います。サービスエンジニアやプログラマは誤作動発生時にリモートでメンテナンス作業を実行できます。

リモートメンテナンス用のアクセスルートは、誤作動発生時に迅速に対応できるよう常時使用できる状態にあり、多くの場合セキュリティ対策が手薄になっているため、攻撃のためにしばしば悪用されます。

システム操作を妨害する攻撃を防ぐため、ここでの対策は必要不可欠です。

参考資料:

- VPN [▶ 18]
- RDP [▶ 18]

4.4.2 ファイアウォール

ファイアウォールを使用して、通過するネットワークパケットをフィルタリングできます。使用するファイアウォールによっては、アドレス、ポート、通信関係の状態、パケットの内容などでフィルタルールを定義できます。このことから、ファイアウォールは攻撃対象領域を縮小するツールであるといえます。

ファイアウォールは、追加ソフトウェア、OSの一部、またはスタンドアロンアプリケーションとしてインストールできます。それぞれにメリットとデメリットがあります。例えば、OSの一部であるファイアウォールは外部のファイアウォールとは異なり、プログラムごとにルールを設定できますが、マルウェアがそのルールを変更、有効または無効にする可能性も高くなります。

ディープパケットインスペクション機能を持つファイアウォールは、データパケットのユーザデータも評価しますが、暗号化された接続のコンテンツは確認できません。Webアプリケーションなどのコンテンツの処理を可能にするために、ファイアウォールで暗号化を終了し、クライアント向けのデータを再度暗号化する方法がよく使用されます。これによって、ファイアウォールはコンテンツを確認できるようになりますが、エンドツーエンドの暗号化は中断されます。

参考資料:

- ファイアウォール [▶ 26]

4.4.3 ネットワークテクノロジ - 使用可能なプロトコル

このセクションでは、いくつかのプロトコルのセキュリティに関する特徴を説明します。

4.4.3.1 Modbus

Modbusプロトコルは、元々シリアル通信プロトコルとして1970年代後半に開発されました。その主な目的は、設定や管理が簡単で、情報モデルの構築を必要とせずにデータを転送する産業用アプリケーション向けの通信プロトコルを提供することでした。このシンプルさゆえ、30年にわたって高い支持を得ています。し

かし、このシンプルさが、セキュリティや情報モデルといった通信プロトコルに対してより複雑な要求を課す最新の産業用プラントでのModbusの使用を難しくしています。オリジナルのModbusプロトコルには、暗号化や認証といったセキュリティ対策は含まれていません。

ベッコフはModbus RTU用とModbus TCP用の2つのTwinCAT機能を提供していますが、セキュリティメカニズムを最初から実装しているOPC UAなどのより高度なプロトコルの使用を推奨します。

4.4.3.2 ADS

オートメーションデバイス仕様(Automation Device Specification - ADS)は、ベッコフが開発した独自の通信プロトコルです。このプロトコルは、他の転送プロトコル(TCPやシリアルなど)よりも高いスループットとポータビリティを実現するように設計されています。ADSはパフォーマンスやスループットを低下させないために、セキュリティを考慮しておらず、暗号化動作も行いません。

ADSはセキュリティで保護されている環境(セキュリティで保護されている転送チャンネルの使用など)でのみ使用することを推奨します。

ADSはセキュリティで保護されている転送チャンネル経由で転送可能です(ADS-over-MQTTを参照)。

4.4.3.3 OPC UA

OPC Unified Architecture (IEC 62541)は、製造レベルから生産計画、またはERPシステムに至るまで、ローデータや前処理済みの情報を安全、確実、かつメーカに依存せずに転送するためのOPC Foundationによる新しいテクノロジ仕様です。OPC UAを使用すれば、認証されたすべてのアプリケーションおよび認証されたすべてのユーザは、いつでもどこからでも必要なすべての情報を入手できます。

4.4.3.4 VPN

仮想プライベートネットワーク(VPN)を使用すると、パブリックネットワーク経由で異なるデバイス間に仮想LANを確立できます。通常、パブリックネットワーク上で伝送されるデータトラフィックは暗号化されます。VPNソリューションは、例えばセキュアな代替方法を使用できるようになるまで、セキュリティで保護されていないプロトコルを一時的にトンネルする場合などに使用できます。

4.4.3.5 RDP

リモートデスクトッププロトコル(RDP)は、グラフィカルなリモートアクセスを実現するMicrosoft独自のプロトコルです。

5 付録

5.1 対策の手順

このセクションでは、対策の具体的な実装方法について順を追って説明します。

5.1.1 ユーザおよびプログラムの管理

5.1.1.1 セキュアなパスワードの選択

プロパティ

- パスワードの複雑さ: パスワードには大文字と小文字、数字、句読点、および特殊文字を含めることを推奨します。
- パスワードの長さ: パスワードは10文字以上にすることを推奨します。

パスワードの生成

セキュアなパスワードを作成するには、さまざまな方法があります。以下の表には、パスワード生成方法の1つを記載します。この手順は、複雑なパスワードを忘れないためにも役立ちます。

手順	例
1. 1つまたは2つの文を用意します。	Complex passwords are more secure
2. スペースを削除します。	Complexpasswordsaremoresecure
3. 単語を略したり、スペルミスを追加したりします。	Complxpasswordsarmorescure
4. 数字や特殊文字を挿入して、パスワードを長くします。	Complxpasswordsarmorescure#529954#

問題のあるパスワード

サイバー犯罪者は、高精度でパスワード攻撃が可能な専用ツールを使用します。このため、以下を含むパスワードは避けることを推奨します。

- 辞書に含まれる単語
- スペルを逆にした単語、一般的なスペルミスや略語
- 12345678やabcdefghなどの反復文字列
- 誕生日、ID番号、電話番号などの個人情報

5.1.1.1.1 Windows CE

Windows CEでは、デフォルトで以下のユーザが用意されています。

ユーザ名	初期パスワード
system user	1
guest	1
webguest	1

Windows CEは、異なるユーザを区別できません。このため、設定が異なるユーザも同一と判断されます。

Windows CEでのパスワード設定

✓ Windows CEのユーザインターフェイスが動作している状態で、以下を実行します。

1. [Start|Control Panel|Password]を選択します。
2. パスワードを入力し、確認します。
3. [OK]でダイアログを終了します。
4. システムを再起動します。

⇨ ユーザーはパスワードを入力した場合にのみプログラムを起動できます。

RASサーバのパスワード変更

RASユーザは、コントローラをリモートで管理できます。デフォルトでは、RASサーバは無効になっていますが、サーバが有効になった際に初期パスワードでRASサーバにアクセスされることを防止するために、パスワードを変更する必要があります。

✓ Windows CEのユーザインターフェイスが動作している状態で、以下を実行します。

1. [Start|Control Panel|CX Configuration]を選択します。
2. [RAS Control]タブを選択します。

⇨ このタブの右側に、ユーザ管理セクションがあります。

5.1.1.1.2 Windows 7/10

パスワードポリシー

パスワードポリシーによって、ユーザアカウントのパスワード選択を制限し、ユーザにセキュアなパスワードを選択させることが可能になります。パスワードポリシーのメリットについては賛否両論あることに注意してください。

パスワードポリシーの作成

1. [Control Panel]を開き、[Administrative Tools|Local Security Policy]を選択します。
2. 開いたウィンドウ内で、[Account Policies|Password Policy]を選択します。
3. パスワードポリシーを設定します。

5.1.1.2 グループポリシー - USBデバイス

OSレベルでUSBデバイスを制限する方法は複数存在します。

- USBデバイスがまだ取り付けられていない場合は、以下のファイルへの現在のユーザおよびSYSTEMユーザのアクセスを拒否することで、USBデバイスの取り付けを防止できます。
  - %SystemRoot%¥Inf¥Usbstor.pnf
  - %SystemRoot%¥Inf¥Usbstor.inf
  - %SystemRoot%¥System32¥DriverStore¥Usbstor.inf*
- エントリ"ImagePath"を HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSer¥services¥USBSTOR下のレジストリで無効なパスに設定することで、USB大容量記憶デバイスの一般的な使用を防ぐことができます。
- ポリシー設定(グループポリシー)によってUSBデバイスの使用をより詳細に制限する方法は、こちらに記載されています。
- USBインターフェイスは、BIOSでもオフに切り替えられます。この方法でオフに切り替えられたインターフェイスに接続されたキーボードやマウスなどの入力デバイスは動作しなくなりますのでご注意ください。

5.1.1.3 監査ポリシー

5.1.1.3.1 Windows 7/10

監査ポリシーの作成

1. [Control Panel]を開き、[Administrative Tools|Local Security Policy]を選択します。
2. 開いたウィンドウ内で、[Local Policies|Audit Policy]を選択します。
3. オプション[Audit object access]を有効にします。

⇨ アクセスを監視するファイルやフォルダを個別に設定できます。

オブジェクトへのアクセス操作が監視されている場合、以下の手順でオブジェクトを選択できます。

1. 該当するファイルまたはフォルダを右クリックします。
2. [Security]タブを選択し、[Advanced]をクリックします。
3. [Auditing]タブを選択し、[Add]をクリックして、ログを設定します。

⇨ アクセス操作が、[Windows logs|Security]に記録されます。

注記! Windowsログの容量は、ログエントリが追加されるたびに増加します。ハードディスクの空き容量に注意してください。

5.1.1.4 プログラムのホワイトリスト化

5.1.1.4.1 Windows 7/10 (SRP)

セキュリティレベルをデフォルトとして設定できます。このデフォルトのレベルに対して、例外を定義できます。

セキュリティレベル	説明
Not permitted	プログラムを実行できません。
Default user	デフォルトユーザの権限でプログラムを実行できます。
Not restricted	各ユーザが制限なしでプログラムを実行できます。

特定のプログラムに対して、以下の例外ルールを定義できます。これらは追加ルールとして参照されます。

タイプ	説明
ハッシュ規則	変更されていない特定バージョンのプログラムファイルについて、ファイル名が無視されます。 **注記! 更新については、これらのハッシュ規則を更新する必要があります。**
Certificate Rule	発行者証明書が設定された、正しく署名されたプログラムファイルが対象。
Path Rule	特定パスのプログラムファイルが対象。パスには、プレースホルダや環境変数(%PROGRAMFILES% など)も含めることができます。
Internet zone Rule	Internet Explorerによって定義されたネットワークゾーン内にあるプログラム。

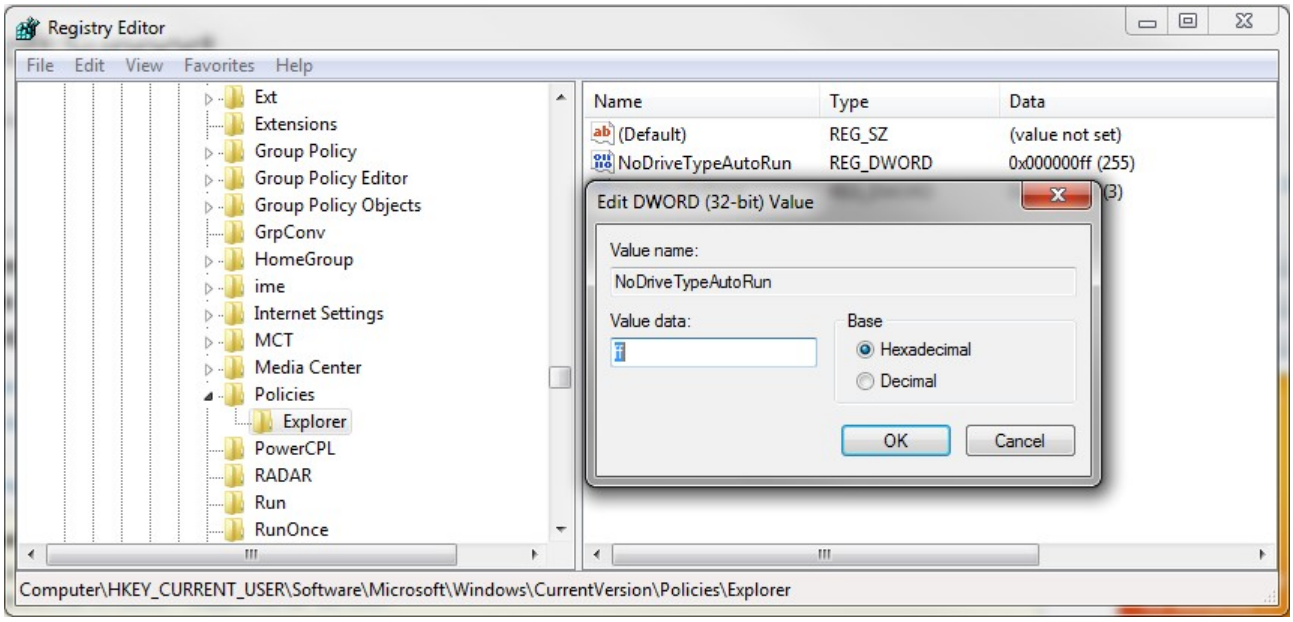
5.1.2 OSのセキュリティ強化

5.1.2.1 自動起動

5.1.2.1.1 Windows 7/10

新しいデバイスの接続時に動作する自動処理を無効にできます。これらはレジストリ「HKEY_CURRENT_USER¥Software¥Microsoft¥Windows¥CurrentVersion¥Policies¥Explorer」にあります。

デバイスの種類に応じて自動起動機能を設定するエントリの例:



「HKEY_LOCAL_MACHINE¥Software¥Microsoft¥Windows¥CurrentVersion¥Policies¥Explorer」にもエントリがあります。

詳細な説明は、こちらを参照してください。

5.1.2.2 プログラムの非表示

5.1.2.2.1 Windows 7/10

Windowsではレジストリに変更を加えることで、以下の機能を非表示にできます。

レジストリ

HKEY_CURRENT_USER¥Software¥Microsoft¥Windows¥CurrentVersion¥Policies¥System

名前が「DisableRegistryTool」のエントリの値を1にすると、ユーザはレジストリエディタを開始できなくなります。

コマンドプロンプト

HKEY_CURRENT_USER¥Software¥Microsoft¥Windows¥CurrentVersion¥Policies¥System

「DisableCMD」というエントリは、値によって効果が異なります。

- 0: コマンドラインアクセスが許可され、バッチファイルを実行できます。
- 1: コマンドラインアクセスが許可されず、バッチファイルを実行できません。

・ 2: コマンドラインアクセスが許可されませんが、バッチファイルを実行できます。

ネットワーク環境

HKEY_CURRENT_USER¥Software¥Microsoft¥Windows¥CurrentVersion¥Policies¥NonEum¥

名前が「{F02C1A0D-BE21-4350-88B0-7367FC96EF3C}」のDWORDエントリの値を1にすると、ネットワーク環境が非表示にされます。

個々のドライブ文字

HKEY_CURRENT_USER¥Software¥Microsoft¥Windows¥CurrentVersion¥Policies¥Explorer¥

名前が「NoViewOnDrive」および「NoDrives」のREG_DWORDエントリを使用して、どのドライブ文字を制限するかを設定できます。「NoViewOnDrives」は、ドライブへのアクセスを制限します。「NoDrives」は、単にドライブ文字を非表示にします。アクセスは可能です。入力値は、以下の表に記載された対応する文字のエントリの合計です。

A: 1	G: 64	M: 4096	S: 262144	Y: 16777216
B: 2	H: 128	N: 8192	T: 524288	Z: 33554432
C: 4	I: 256	O: 16384	U: 1048576	All: 67108863
D: 8	J: 512	P: 32768	V: 2097152	
E: 16	K: 1024	Q: 65536	W: 4194304	
F: 32	L: 2048	R: 131072	X: 8388608	

例えば、ドライブA、B、D、およびPへのアクセスを制限する場合は、入力値は32779 (1 + 2 + 8 + 32768) となります。値の設定後、設定を反映するためにOSを再起動する必要があります。

設定オプションの詳細は、こちらにまとめられています。

5.1.2.3 不要なコンポーネントの除外

5.1.2.3.1 Windows 7/10

[Control Panel]の[Programs and Features]で、不要なプログラムおよびWindowsコンポーネントをアンインストールできます。

この機能に直接アクセスするには、「control appwiz.cpl」を実行します。

5.1.2.4 ハードディスクの暗号化

EFSの有効化

1. フォルダまたはファイルを右クリックし、開いたコンテキストメニューから[Properties]を選択します。
2. [General]タブを開き、[Advanced]をクリックします。
3. フォルダまたはファイルを暗号化するには、[Encrypt contents to secure data]チェックボックスを選択します。

⇨ この方法で初めてデータを暗号化する場合は、Windowsがローカル証明書ストア内にEFS証明書を自動的に作成します。この証明書が保存されたことを確認してください。保存されていない場合、データを復元できなくなります(証明書の保存 [▶ 23]を参照)。

証明書の保存

1. certmgr.mscを起動します。
2. [Add]をクリックし、[My user account]を選択して[Finish]をクリックします。

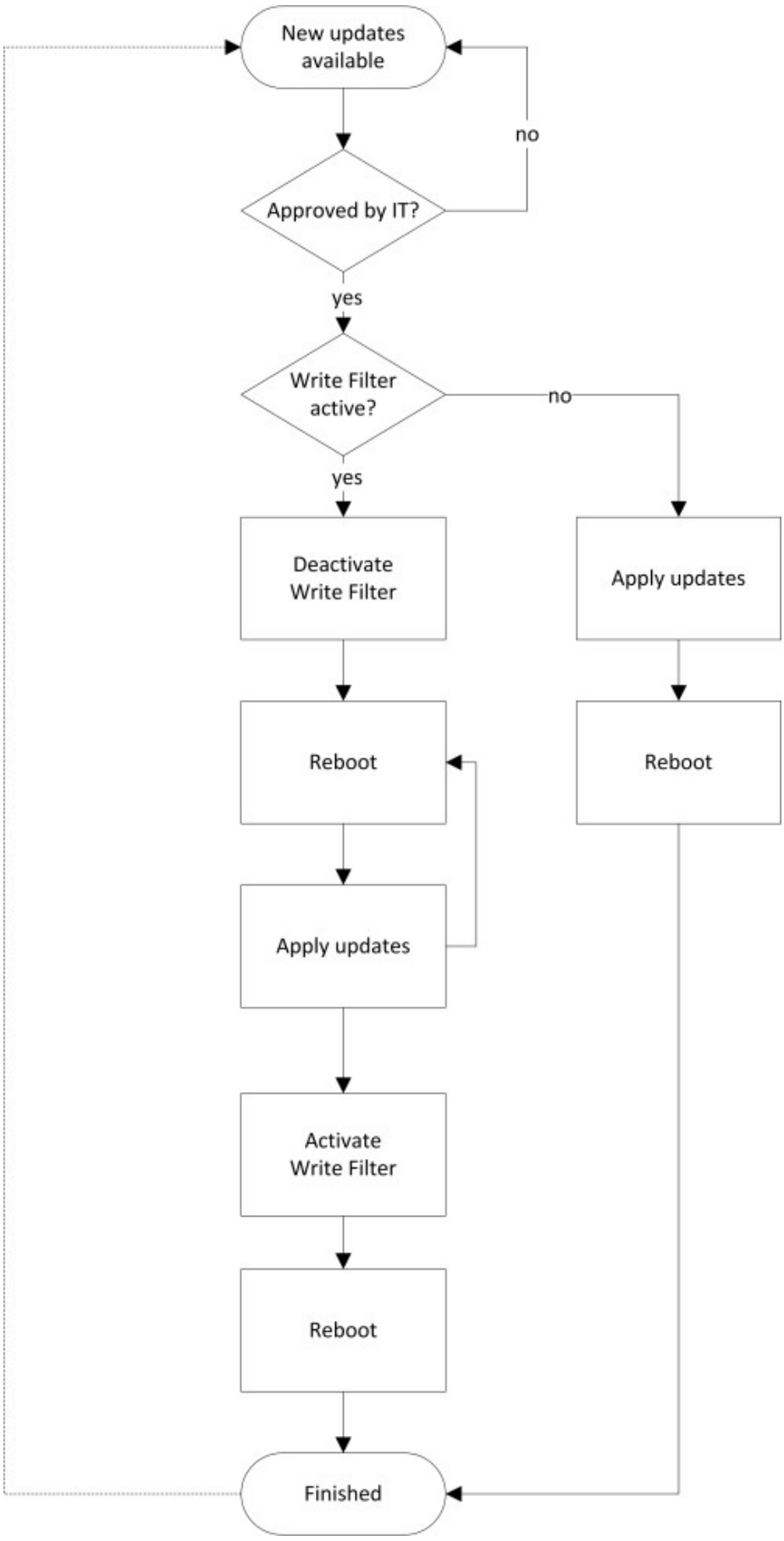
3. 「個人」フォルダを開き、[**Certificates**]をクリックします。
   ⇨ 証明書の「Intended Purpose(目的）」には「Encrypting File System（暗号化ファイル システム）」と表示されます。
4. 証明書を保存するには、証明書を右クリックして[**All Tasks** |**Export**]を選択します。
5. [**Export Private Key**]を選択します。
6. [**Personal Information Exchange**]、[**Include all certificates…**]、および[**Enable strong protection**]を選択します。
7. 証明書を保護するパスワードを指定します。この証明書は、インポートの際に必要になります。
8. 証明書を保存するパスを指定します。証明書は、他の安全な場所に保存してください。

注記! システムパーティション全体、Windowsシステムファイル、またはTwinCATフォルダを暗号化しないでください。これにより、誤作動が発生する可能性があります。

5.1.2.5 更新

5.1.2.5.1 Windows 7/10

Windows 7/10には、OS固有の更新機能が用意されています。開発用PCは、更新によって最新の状態を維持する必要がありますが、産業用環境ではこれが難しい場合があります。例えば、ライトフィルタを使用している場合、対策を講じずに実行された更新が、再起動時に破棄されてしまいます。これを回避するために、以下の方法を推奨します。



この操作を行った後、オペレータはシステムが正常に機能しているかを十分にテストする必要があります。ベッコフは、約半年に一度、Windows更新プログラムを含む更新済みかつテスト済みのイメージをお客様に提供可能です。

5.1.2.5.2 Windows CE

Windows CEには、OS固有の更新機能は用意されていません。このため、更新を行うには、イメージ全体を更新する以外にはありません。現在インストールされているイメージは、フォルダ ¥Hard Disk¥ 内のイメージ(バージョン含む)のファイル名から分かります。

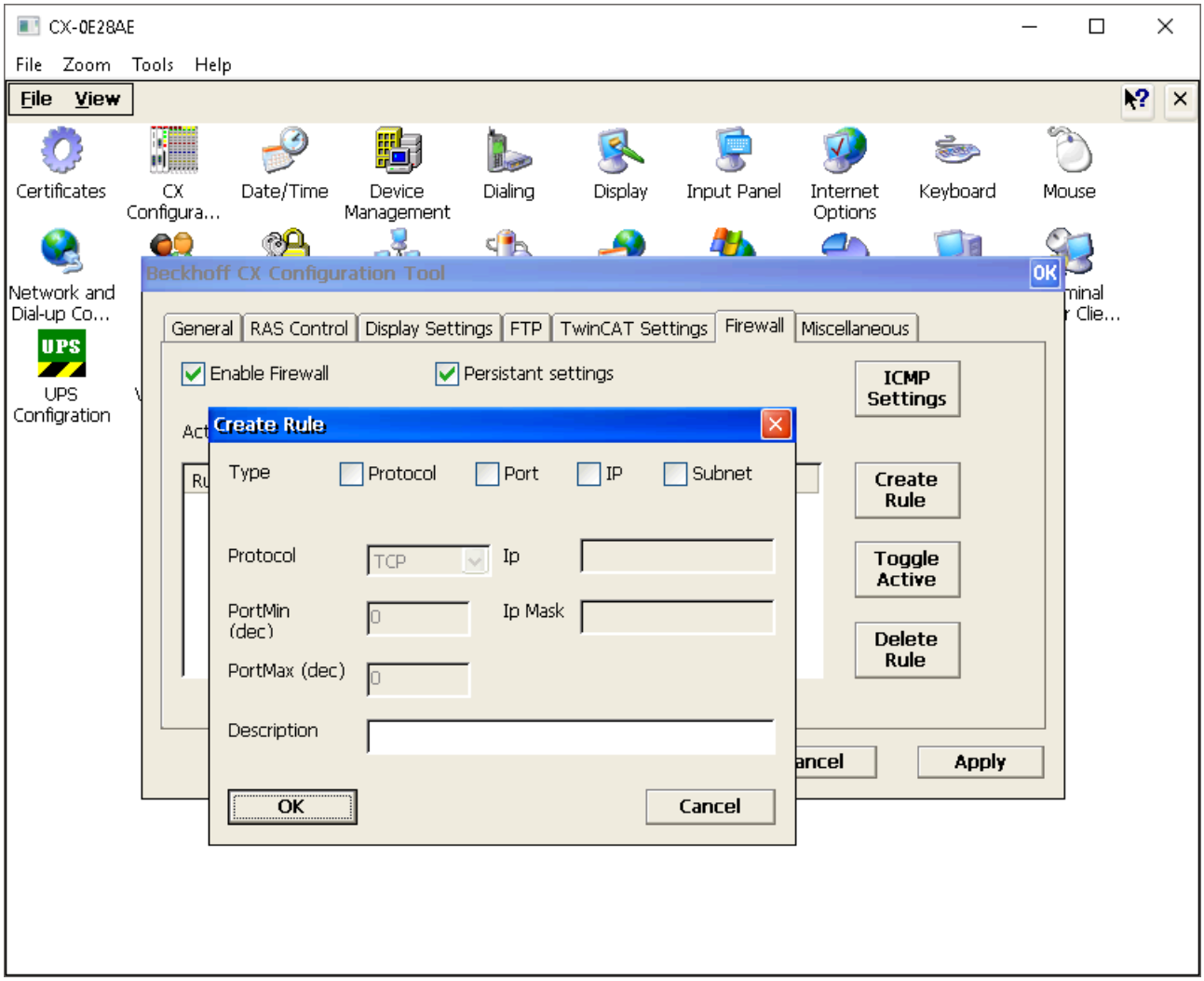
5.1.3 通信

5.1.3.1 ファイアウォール

5.1.3.1.1 Windows CE

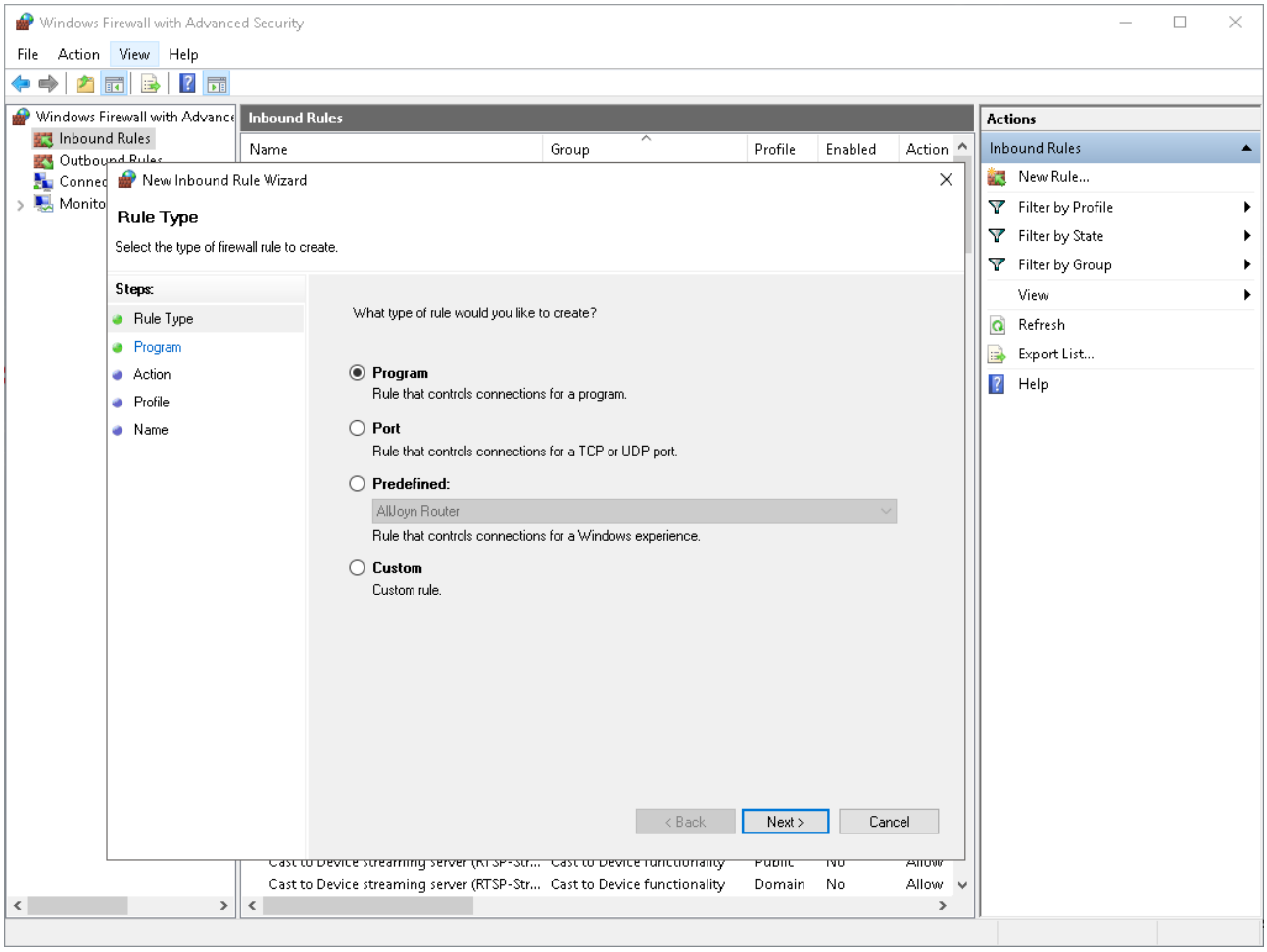
Windows CEのファイアウォールは、レジストリ内のエントリで設定します(https://msdn.microsoft.com/en-us/library/ee494503(v=winembedded.60).aspx などを参照)。

Beckhoff CX Configuration Tooの[**Firewall**]タブで、簡単に設定できます。



5.1.3.1.2 Windows 7/10

コマンド「**wf.msc**」でコマンドラインからMMCスナップイン[Windows Firewall with Advanced Security]を開き、ファイアウォールを設定できます。[**New Rule**]ボタンを使用して、ルールを追加できます。



5.1.3.2 プロトコルを実装したサーバ

5.1.3.2.1 Internet Information Services(IIS)

5.1.3.2.1. Windows CE 1

以下のレジストリエントリを変更して、Windows CEのWebサーバを無効にできます。

HKEY_LOCAL_MACHINE¥Services¥HTTPD¥Flags

このエントリが「DWORD 4」に設定されると、Webサーバが無効になります。

注記! このWebサーバによるすべてのWebページが動作しなくなります。

5.1.3.2.1. Windows 7/10 2

IIS Webサーバを無効にするには、サービス管理機能(「**services.msc**」または[**Control Panel | Management|Services**])を開き、「World Wide Web Publishing Service」を無効にします。このWebサーバによるサービス(ベッコフIPC診断ツール「Beckhoff IPC diagnostics」など)が動作しなくなるため、注意してください。

5.2 セキュリティに関するプロパティ

5.2.1 ベッコフのソフトウェアパス

TwinCATシステム

プログラム	パス
TwinCAT XAE	%PF%¥Microsoft Visual Studio 10.0¥Common7¥IDE¥devenv.exe
ベッコフFBWFマネージャ	%PF%¥FBWFMgr¥Beckhoff FBWF Manager.exe
TwinCAT ADSテストツール	%TC%¥Common32¥TcAdsTest.exe
TwinCATスコープビュー2	%TC%¥Functions¥TE130X-TC3-Scope-View¥TwinCatScopeView2.exe
TwinCATイベントバー	%TC3DIR%¥Components¥TcEventLogger¥TcEventBar.exe
TwinCAT SysUI	%TC3DIR%¥System¥TcSysUI.exe
TwinCAT AMSリモートマネージャ	%TC%¥ADS Api¥TcAdsDll¥TcAmsRemoteMgr.exe
ベッコフEWFマネージャ	%PF%¥BEWFMgr¥BEWFMgr.exe
TcSwitchRuntime	%TC%¥TcSwitchRuntime¥TcSwitchRuntime.exe

TwinCATファンクション

プログラム	パス
TF6100 コンフィグレータ	%TCFUN%¥TF6100-OPC-UA¥Win32¥Configurator¥TcOpcUaConfigurator.exe
TF6100 サンプルクライアント	%TCFUN%¥TF6100-OPC-UA¥Win32¥SampleClient¥UaSampleClient.exe
TF6120 コンフィグレータ	%TCFUN%¥TF6120-OPC-DA¥Win32¥Configurator¥TcOpcCfg.exe
TF6120 クライアント	%TCFUN%¥TF6120-OPC-DA¥Win32¥SampleClient¥TcOpcClient.exe
TF6250 コンフィグレータ	%TCFUN%¥TF6250-Modbus-TCP¥Win32¥Server¥TcModbusCfg.exe
TF6420 コンフィグレータ	%TCFUN%¥TF6420-DatabaseServer¥Win32¥Configurator ¥TcDatabaseSrv_Configfileeditor.exe

環境変数:

- %TC%: TwinCATフォルダ、*C:¥TwinCAT* など
- %TC3DIR%: TwinCAT 3フォルダ、*C:¥TwinCAT¥3.x* など
- %TCFUN%: TwinCATファンクションフォルダ、*C:¥TwinCAT¥Functions* など
- %PF%: プログラムファイルフォルダ、 *C:¥Program Files* など

注記! TwinCATのスタートメニューエントリをホワイトリストに追加しなければ、動作しない場合があります。

5.2.2 ベッコフのポート

標準サービス

アプリケーションによっては、物理的に安全なネットワークやVPNなどの下位レイヤで安全ではないサービスを保護する必要があります。

サービス	ポート
CerHost	987 / tcp (受信)
FTPサーバ	21 / tcp (受信)

サービス	ポート
IPC診断	4852 / tcp（受信） 80 / tcp（受信） 5120 / tcp（受信）
リモートデスクトップ(RDP)	3389 / tcp（受信）
SMB	137 / tcp（受信） 138 / tcp（受信） 139 / tcp（受信） 445 / tcp（受信）
TwinCAT ADS	48898 / tcp（受信、送信） 48899 / udp（受信、送信）

その他のサービス

サービス	ポート(デフォルト設定)
TF6100 OPC UA	4840 / tcp（受信）、可変
TF6120 OPC DA	1024～65535（受信）で可変(DCOMにより異なる)
TF6250 Modbus TCP	502 / tcp（受信）
TF6310 TCP-IP	可変 / tcp（受信、送信）
TF6300 FTP	20 / tcp（送信） 21 / tcp（送信） TF6300の取扱説明書も参照してください。
TF6420データベースサーバ	選択されたデータベースにより異なる TF6420の取扱説明書も参照してください。

5.3 参考資料

IEC 62443は、オートメーションシステムのセキュリティに関する一連の国際標準です。セクションによっては、現在も引き続き策定されています。すでに公開されているセクションでは、システムやコンポーネントの組織的および技術的な概念と対策について説明しています。URL: https://webstore.iec.ch/publication/7029

NIST SP800-82 産業制御システム(ICS)セキュリティガイドでは、工業設備に対する脅威の分析、およびその安全対策について具体的に記述されています。URL: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

BSI IT Basic Protection Compendiumは、リスク分析および対策の適用のための構造化されたファンクションブロックを提供します。この概要には、産業ITに関するファンクションブロックも含まれています。URL: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/itgrundschutzKompendium_node.html（ドイツ語のみ）

5.4 サポートとサービス

世界中のベッコフ支社と代理店は、包括的なサポートとサービスを提供し、ベッコフ製品とシステムソリューションに関するあらゆる質問に対して迅速かつ的確なサポートを提供しています。

ベッコフの支社と代理店

ベッコフ製品に対するローカルサポートおよびサービスについては、最寄りのベッコフ支社または代理店にお問い合わせください。

世界中のベッコフ支社と代理店の所在はベッコフウェブ(
http://www.beckhoff.co.jp)よりご確認いただけます。

また、このウェブページでベッコフ製品に関するドキュメンテーションも公開されています。

ベッコフ本社

Beckhoff Automation GmbH & Co. KG

Huelshorstweg 20
33415 Verl
Germany

電話:	+49(0)5246/963-0
ファックス:	+49(0)5246/963-198
電子メール:	info@beckhoff.com

ベッコフサポート

ベッコフサポートはベッコフ製品に関するお問い合わせだけではなく、その他のあらゆる包括的な技術サポートを提供しています。

- サポート
- 複雑なオートメーションシステムの設計、プログラミング、およびコミッショニング
- ベッコフシステムコンポーネントに関する広範なトレーニングプログラム

ホットライン:	+49(0)5246/963-157
ファックス:	+49(0)5246/963-9157
電子メール:	support@beckhoff.com

ベッコフのサービス

ベッコフサービスセンタは、すべてのアフターサービスでお客様をサポートいたします。

- オンサイトサービス
- 修理サービス
- スペアパーツサービス
- ホットラインサービス

ホットライン:	+49(0)5246/963-460
ファックス:	+49(0)5246/963-479
電子メール:	service@beckhoff.com