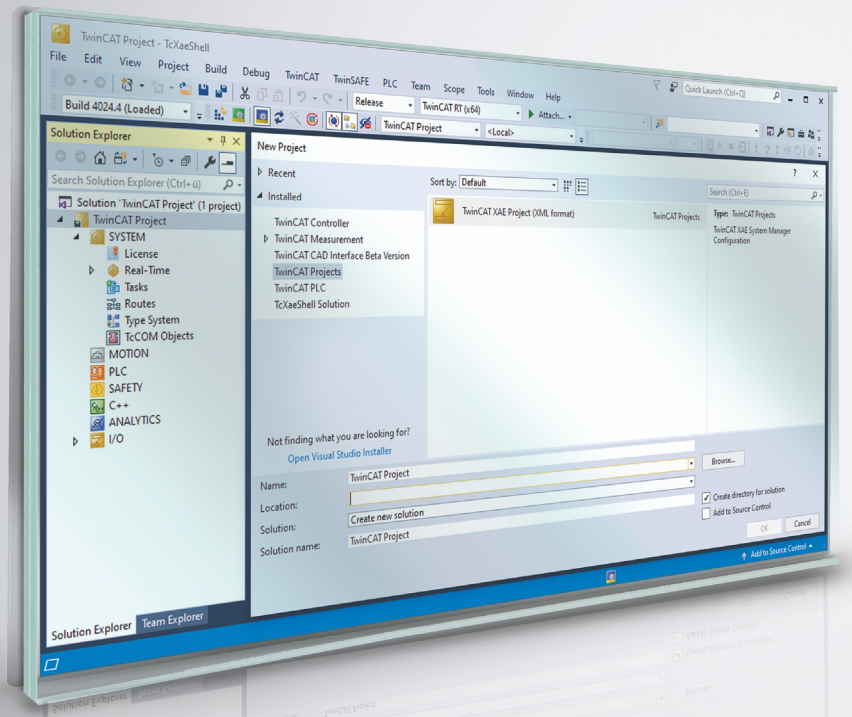
BECKHOFF New Automation Technology

取扱説明書 | JA

IPCセキュリティガイドライン

TwinCAT/BSD



2025-06-10 | バージョン: 1.3

目次

1 取扱説明書に関する注記

この説明書は対応する国内規格を熟知した、トレーニングを受けた制御、オートメーションエンジニアリングの有資格者のみの使用を対象としています。
本製品の設置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。
有資格者は、常に最新版のドキュメントを参照してください。

本製品を使用する上での責任者は、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ことがあります。製品の情報・仕様は予告なく変更されます。
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、既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。必ず最新バージョンの説明書を参照してください。

商標

Beckhoff®, TwinCAT®, TwinCAT/BSD®, TC/BSD®, EtherCAT®, EtherCAT G®, EtherCAT G10®, EtherCAT P®, Safety over EtherCAT®, TwinSAFE®, XFC®, XTS®, XPlanar® 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。

EtherCAT®は、Beckhoff Automation GmbHの登録商標および特許技術です。

著作権

第三者商標

本書では、他社の商標が使用される場合があります。商標に関する詳細は以下を参照してください。
https://www.beckhoff.com/trademarks

1.1 脆弱性の報告

セキュリティアナリストの皆様には、セキュリティホールを塞ぐための解決策を開発するために、公表前に十分な時間をいただけますようお願いします。情報開示を調整することによって、顧客はセキュリティホール対策に関する最新情報を得ることができ、アップデート開発中に不必要に危険にさらされることはありません。顧客の安全が保護されれば、セキュリティホールに関するオープンな議論は、業界全体の製品およびソリューションの改善に役立ちます。

ベッコフの製品に脆弱性が疑われる場合、セキュリティホールの発見者およびコーディネータは、product-securityincident@beckhoff.com まで、できるだけ英語またはドイツ語で脆弱性レポートをお送りください。守秘義務を遵守してください。暗号化されたメッセージを送信する手段については、ベッコフの障害対応チームの連絡先 に記載されています。

発見者は、連絡がつくように脆弱性レポートに必要な連絡先情報をすべて記載するようお願いします。しかしながら、匿名の脆弱性レポートにも対応します。現象を再現できるよう、できるだけ詳細な情報を提供してください。発見者が公開を希望する場合、ベッコフは30日以内に適切な速報リリース日を調整するよう努めます。発見者には、リリース日より前に対策の可用性が通知され、関連するBeckhoff Advisory（ベッコフによる勧告）が送付されます。ベッコフは、発見者の公開予定（該当する場合は要求されたCVEを含む）を受け取ります。その後、最終的なリリース日が合意されます。この日に、発見者の発表とBeckhoff Advisoryの両方がリリースされます。発見者が希望し、上記の手続きを遵守する場合は、発見者への謝辞と、発見者の発表への参照、参考になる場合には発見者の発表に関する情報をBeckhoff Advisoryに追記します。

1.2 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)
Hülshorstweg 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暗号化鍵が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 0a 0e 85 68 56 18 0f 5c 8a 5c 4e 83 およびフィンガープリント のS/MIME証明書4c b4 d0 99 d4 a0 6c f0 af 69 ee 7a 8f 81 a1 c3 42 eb 17 da

暗号化鍵のダウンロード: 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)

1.3 情報セキュリティに関する注記

Beckhoff Automation GmbH & Co. KG（ベッコフ）の製品は、オンラインアクセスが可能であれば、プラント、システム、機械、ネットワークの安全な運用をサポートするセキュリティ機能を備えています。セキュリティ機能にもかかわらず、プラント、システム、機械、ネットワークをサイバー脅威から守るためには、運用のための全体的なセキュリティ コンセプトの作成、実施、継続的な更新が必要です。ベッコフが販売する製品は、全体的なセキュリティ コンセプトの一部に過ぎません。お客様は、プラント、システム、機械、ネットワークへの第三者による不正アクセスを防止する責任を負います。ネットワークは、適切な保護措置が講じられている場合にのみ、社内ネットワークまたはインターネットに接続すべきです。

また、ベッコフが推奨する適切な保護対策も遵守してください。情報セキュリティと産業セキュリティに関する詳細は、https://www.beckhoff.com/secguide を参照してください。

ベッコフの製品とソリューションは常に進化し続けています。これはセキュリティ機能にも当てはまります。継続的な開発により、ベッコフでは、製品を常に最新の状態に保ち、アップデートが提供され次第、製品にインストールすることを明示的に推奨しています。古いバージョンやサポートが終了した製品の使用は、サイバー脅威のリスクを高めるおそれがあります。

ベッコフ製品の情報セキュリティ情報については、RSSフィードをご購読ください https://www.beckhoff.com/secinfo。

1.4 セキュリティ設計の目的

ベッコフの産業用PC(IPC)ハードウェアは、オフィス環境の一般的なPCと同様に使えるように設計されていますが、産業環境での使用のために堅牢性が大幅に強化されています。完全なPC基板は、このような環境下で信頼性が高く、高度に時間確定的な動作をするよう設計されています。ハードウェアは、Windows®やFreeBSDベースのTwinCAT/BSDなどの汎用オペレーティングシステムをサポートしています。その結果、ハードウェアは、オペレーティングシステムが提供する従来型およびオフィスITグレードのセキュリティメカニズムをサポートするように設計されています。これらのセキュリティ機能を特定の環境に合わせて適切に設定することは、IPCを運用環境に統合する担当者の義務です。また、担当者はオペレーターに安全な使用方法を指導する必要があります。このような設定および使用に関するガイドラインは、特定の環境に対する包括的なセキュリティコンセプトから作成されるべきで、その環境に適合したものでなければなりません。

ベッコフのIPCは、オペレーティングシステム有りでも無しでもご購入いただけます。オペレーティングシステムは、Windows 10とTwinCAT/BSDが利用可能です。これらは、特別な要求がない限り、「Secure By Default（デフォルトで安全）」と呼ばれる方法で提供されます。つまり、デバイスへのすべてのアクセスは認証され、事前に設定されたユーザのみが管理者アクセスできるようなデフォルト設定のサービスのみ有効になっている状態です。歴史的な理由から、事前に設定されたユーザが「Administrator（管理者）」になります。ベッコフでは、IPCにプリインストールされた名前付きのオペレーティングシステムイメージを2つの方法で提供しています。1つは、デバイスのラベルに記載された「Administrator」用のランダムパスワードがあらかじめ設定されているものです。2つ目は、ドキュメントにあるように、よく知られたパスワードがあらかじめ設定されているものです。注意：後者は、ある環境要件では 「デフォルトで安全」ではないが、その他の環境ではうまく機能する。

これらのOSはベッコフが開発したものではありません。ベッコフのWindows 10イメージの基盤は、マイクロソフト社によって開発・保守されています。TwinCAT/BSDの基盤は、"The FreeBSD Project"によって開発・保守されています。どちらの基盤も、数十年来、オフィスやサーバー環境での使用において、そのセキュリティ機能は定評があります。最先端のセキュリティ機能を搭載し、提供しています。特定の環境とアプリケーションには、特定のセキュリティ機能設定および使用に関するニーズがあります。ベッコフが提供するオペレーティングシステムは汎用的なものであり、アプリケーションの実装を制限するものではありませんが、ベッコフは特定のアプリケーションや統合から生じる特殊なセキュリティニーズを予測することはできません。したがって、安全な設定と使用に関するガイドラインは、オペレーティングシステムを特定の用途の環境に統合する担当者が作成する必要があります。しかしながら、ベッコフでは、IPCとそのオペレーティングシステムを安全に使用するためのガイドラインを当ガイドに記載しています。このようなガイドラインは、一般的なヒントとして考慮されるものであり、完全かつ十分な参考資料ではありません。オペレーティングシステムの開発者が、オペレーティングシステムのセキュリティ機能に関する完全な文書を提供しています。

ベッコフは、これらのオペレーティングシステムの拡張機能を開発し、特に自動化業界のリアルタイムアプリケーションで使用するために、オペレーティングシステムの時間確定的動作を最適化しました。拡張機能は、ベッコフが配布するオペレーティングシステムのイメージに統合されています。これらの拡張機能は、堅牢性と時間確定的な動作が設計の主な目的です。ただし、ベッコフでは、特に断りのない限り、これらの拡張機能がオペレーティングシステムの基本的なセキュリティ機能を損なうことがないよう配慮しています。

ベッコフでは、多種多様なソフトウェア製品を販売しています。その一例が「TwinCAT 3.1 - eXtended Automation Runtime (XAR)」で、略してTwinCAT 3.1 XARと呼ばれる製品です。IPCによっては、オペレーティングシステム内にプリインストールされているものもあります。この特定のソフトウェアの主な目的は、自動化の用途で時間確定的で堅牢、かつ高度にカスタマイズ可能な実行環境を提供することです。これがIPCにインストールされると、デバイスがプログラマブルなロジックコントローラ（PLC）に変わります。このソフトウェアは、堅牢性と時間確定性による可用性に加えて、開発時に周辺セキュリティを追加できます。つまり、TwinCAT 3.1 XARで実装されているプロトコルを使用して、アクセスを安全に認証するように設定し、使用できます。この周辺セキュリティの観点は、IPCのネットワークインターフェースにより境界線を引くということです。ベッコフがこの種のセキュリティリスクとして認識しているのは、TwinCAT 3.1 XARで実装されたプロトコルを介して、権限のないユーザがIPCにアクセスすることです。歴史的な理由と後方互換性のため、TwinCAT 3.1 XARは、このようなアクセスの前に認証を行わないプロトコルを提供しています。TwinCAT 3.1 XARがプリインストールされたIPCの中には、デフォルトで安全な設定を持つものがあります。つまり、このデフォルト設定では、TwinCAT 3.1 XARの安全なプロトコルのみが有効です。TwinCAT 3.1 XARがプリインストールされたIPCの多くは、後方互換性のためにデフォルトで安全な設定になっていないことに注意してください。このセキュリティガイドには、TwinCAT 3.1 XARでサポートされるプロトコルのリストと、どのプロトコルが安全であるかについてのアドバイスが含まれています。以下を参照：重要なTCP/UDPポート [▶ 32]。その他のソフトウェア製品には、独自のドキュメントやガイドが付属しています。注意：後者は、TwinCAT 3.1 XARに別のインストーラで追加できるTwinCATファンクションについても当てはまります。

2 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。

2.1 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、またはサービスコール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。

この分類は、セキュリティ分析を行う際に役立ちますが、実際の攻撃者は、複数のカテゴリーにまたがる様々な能力を保持することに留意する必要があります。

2.2 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。

カテゴリ	説明
広範囲のウイルス攻撃	この攻撃はシステムの広域的脆弱性を悪用し、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。

カテゴリ	説明
ベンダーやインテグレーターを狙った攻撃	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。このような攻撃は自動的に広がる可能性はありますが、脆弱性として特殊な製品や設定をターゲットにしています（ベッコフやインテグレーターの設定および拡張機能など）。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。
ユーザを狙った攻撃	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。

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。ユーザを狙った特殊な攻撃には、ユーザ側の分析と対策が必要です。

2.3 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
ベンダーやインテグレーターを狙った攻撃	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 [▶ 15]）
- ブートメディアの設定 (BIOS設定 [▶ 15])
- 制御盤の施錠 [▶ 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
ベンダーやインテグレーターを狙った攻撃	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 [▶ 15])

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
ベンダーやインテグレーターを狙った攻撃	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:

- USBデバイスのホワイトリスト化 (USBフィルター [▶ 29])
- 制御盤の施錠 [▶ 14]
- BIOSでのインターフェースの無効化(BIOS設定 [▶ 15])
- プログラムのホワイトリスト化 [▶ 27]

ローカルインターフェー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
ベンダーやインテグレーターを狙った攻撃	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:

- 安全なパスワード [▶ 22]
- 共有アカウントではなく、個々のユーザを設定する。
- ユーザ権利の最小化し（最小特権の原則）、特に必要でない場合は管理者権限を与えない。

データキャリアの盗難

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
広範なウイルス攻撃	対象外	対象外	対象外	対象外
ベンダーやインテグレーターを狙った攻撃	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およびアクセス情報を取得する可能性があります。

このような攻撃により、攻撃者はオペレーティングシステムに関連する大量のデータ、特にアクセスデータ、設定、ノウハウ、その他機密性の高い個人情報への読み取りアクセスを取得します。

攻撃者はまた、廃棄された後の記憶媒体を盗難することで、機密データへのアクセスを試みる可能性もあります。

防御手段:

- 制御盤の施錠 [▶ 14]
- 安全なデータ廃棄 [▶ 14]

廃棄物から機密データを抽出

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
広範なウイルス攻撃	対象外	対象外	対象外	対象外
ベンダーやインテグレーターを狙った攻撃	対象	対象	対象外	対象外

攻撃者は、機密データを含む記憶媒体などの廃棄物にアクセスする可能性があります。

このような攻撃により、攻撃者はオペレーティングシステムに関連する大量のデータ、特にアクセスデータ、設定、ノウハウ、その他機密性の高い個人情報への読み取りアクセスを取得します。

防御手段:

- 安全なデータ廃棄 [▶ 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	対象
ベンダーやインテグレーターを狙った攻撃	対象外	対象外	対象	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アップデート(アップデート [▶ 21])
- プログラムのホワイトリスト化 [▶ 27]

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
ベンダーやインテグレーターを狙った攻撃	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アップデートをリリースします。使用中のソフトウェアがアップデートされていない場合、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:

- 定期的または自動的なソフトウェアアップデート(アップデート [▶ 21])
- 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 [▶ 28]

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
ベンダーやインテグレーターを狙った攻撃	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アップデート(アップデート [▶ 21])
- 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
ベンダーやインテグレーターを狙った攻撃	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
ベンダーやインテグレーターを狙った攻撃	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 [▶ 28]

3 一般的な対策

3.1 従業員のトレーニング

トレーニングを受けた人員は、システムを守る重要な要素になります。デバイスにアクセスできる従業員は、操作方法を習得している必要があります。これには、パスワードやUSBメモリなどのデータキャリアの責任ある取り扱いといった一般的な対策が含まれます。すべての従業員は、システムに介入することで起こりうる事象について認識すべきです。

3.2 物理的な対策

最も簡単で安全なセキュリティ対策のひとつは、物理的な保護です。管理者と技術者のみがデバイスにアクセスできるようにしてください。最大のリスクのひとつであるUSBメモリーやその他のデータキャリアなどの物理的アクセスによる攻撃は、この方法でリスク低減できます。装置の物理的な保護は、施錠可能な制御盤などにより実現できます。

制御盤の施錠

産業用PCを格納する制御盤は、基本的に施錠する必要があります。産業用PCの特定のインターフェー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。導出されたインターフェースも、施錠可能にするなど、さらに保護すべきです。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。

3.3 安全なデータ廃棄

廃棄部品の場合、データを確実に消去することが重要です。データキャリアの複数回の上書きは、適切で信頼できる手段です。

廃棄または取り外し部品のデータを安全に破棄するには、データキャリアの上書きを推奨します。これを行うには、TwinCAT/BSDインストーラスティックからデバイスを起動します。デバイスが自動的にスティックからブートしない場合は、ブートプロセス中にF7を押してUSBフラッシュドライブを選択します。インストーラスティックのメニューで、"Shell "メニューからTwinCAT/BSDシェルにアクセスできるようになりました。ここで、

```
ls /dev
```

を入力すると、検出されたデバイスノードまたはデータキャリアを表示します。データキャリアは通常ada0またはda0で示され、adaはSataデータキャリア、daはSCSIデータキャリアを表します。したがって、CFastカードは "ada"、USBフラッシュドライブは "da "と表示されます。

デバイスのCFastカード上のデータを復元不可能に破壊する場合は、以下の手順でデータキャリアをゼロで上書きしてください：

```
dd if=/dev/null of=/dev/ada0 bs=100m
```

物理的破壊

ハードディスクを上書きしたくない場合、あるいは欠陥のために上書きできない場合は、ハードディスクを物理的に損傷させるか破壊してください。

4 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。BIOSの設定は熟練者のみが行ってください。未知のパラメータを変更すると、システムの機能に悪影響を及ぼす可能性があります。

5 オペレーティングシステム

5.1 復元オプション

データ損失や記憶媒体の故障時にTwinCAT/BSD を短時間で復元するために、TwinCAT/BSD システムのバックアップ作成と復元の対策をあらかじめ定義してください。バックアップ作成は、ダウンタイムを最小限に抑え、生産に大きな損失を与えることなく作業を継続するのに役立ちます。バックアップコピーの作成手順と、それを復元する手段の両方を定義する必要があります。セキュリティー面も考慮し、バックアップデータの保管場所なども決めておく必要があります。

ベッコフでは、TwinCAT/BSD インストーラスティックによるシンプルなバックアップソリューションを提供しています。さらに、restorepoint プログラムは、TwinCAT/BSD の復元ポイントを設定できます。これらの復元ポイントはシステムの現在の状態を保存し、必要に応じて復元します。このため、様々な実装方法が可能です。バックアップ作成と復元の対策の厳密な定義はユーザに委ねられています。

以下のようなシナリオが想定されます。これは、様々な動作モードを理解するためのものです。しかしながら、これらがベッコフが推奨する唯一の手段ではありません。

シナリオ1：工場出荷時の設定

TwinCAT/BSD 搭載の産業用PCを、問題発生時に工場出荷時の設定にリセットします。

- ユーザは、TwinCAT/BSD 搭載の産業用PCでテストおよび開発を行います。
- テストや開発の段階で、例えば基本設定が変更されたために問題が発生することがあります。
- ユーザは、TwinCAT/BSD を工場出荷時の設定にリセットすることで問題を解決します（参照：工場出荷時設定へのリセット [▶ 17] ）。

シナリオ2：量産

テストおよび開発段階は成功裏に終了しました。機械メーカは量産を開始したいと考えています。

- 機械メーカは、エラー発生時にシステムを復元できるよう、復元ポイント（OEM納入状態）を作成します（参照：復元ポイントの作成 [▶ 17] 。機械メーカのエンドユーザは、問題が発生した場合にこの復元ポイントを使用できます。
- その後、機械メーカはWriteフィルターを有効にします。これは、TwinCAT/BSD を事前に設定された状態で保護し、エンドユーザでの設定ミスを防ぐためです（参照：Writeフィルター [▶ 28] ）。
- 最終段階では、機械メーカがバックアップを作成し、マスターイメージとして保存して、量産に使用します（参照：バックアップの作成 [▶ 19] ）。

シナリオ3：エンドユーザでの試運転

機械はエンドユーザに到着し、試運転後にバックアップが作成されます。

- 機械をパラメータ化した後、エンドユーザは"Commissioning"という名前で復元ポイントを作成します（参照：復元ポイントの作成 [▶ 17] ）。
- その後、偶発的な設定ミスを避けるため、エンドユーザでWriteフィルターライトを有効にします（参照：Writeフィルター [▶ 28] ）。
- 例えば、データキャリアに欠陥がある場合（参照：バックアップからの復旧 [▶ 20] ）などにシステムを復元できるように、エンドユーザーが自身でバックアップを作成します（参照：バックアップの作成 [▶ 19] ）。

5.1.1 復元ポイント

復元ポイントは、大規模なシステム変更または設定ミスの後に、TwinCAT/BSD が望ましくない動作を示した場合、修正が容易でない場合に旧システムの状態を復元するために使用します。復元ポイントの利点は、TwinCAT/BSD を再インストールすることなく、これらの設定エラーを簡単かつ迅速に元に戻すことができることです。

復元ポイントを作成するタイミングは、大規模なシステム変更や、他社製プログラムのインストール時などに設定します。しかし、復元ポイントはフルバックアップの代わりではなく、データ損失を防ぐものではありません。定期的なバックアップ作成は、ストレージメディアの欠陥などによるデータ損失から身を守るためのもうひとつの保護手段です（参照：バックアップの作成 [▶ 19]）。

復元ポイントは、restorepoint プログラムを使ってコンソールで作成・管理します。プログラムでは、以下のモードをサポートしています：

- status:利用可能なすべての復元ポイントを一覧表示します。納品時には、factoryreset （ベッコフの工場出荷時設定）という復元ポイントが利用できます。
- create:新しい復元ポイントを作成します。復元ポイントの名前を引数として設定できます。名前を指定しない場合は、自動生成された名前が使用されます。
- rollback:特定の復元ポイントに戻ります。復元ポイント以降に作成されたデータはすべて破棄されることに注意してください。引数として復元ポイントが指定されていない場合、対話型のダイアログでユーザに質問します。
- destroy:指定された復元ポイントは破棄されます。このモードでは、既存のデータはすべて保存されますが、復元ポイント自体は削除されます。

TwinCAT/BSDの復元ポイントは、ZFSスナップショットに基づいています。その結果、作成時に消費するメモリはほとんどありません。ユーザが現在作業している本番システム用に保存された復元ポイントの変更は、復元ポイント用のメモリ領域に反映されます。すべてのシステムスナップショットを表示するには、zfs list -t snap を使用します。

USED列は、スナップショットによって使用される実際のスペースを示し、REFER列は、スナップショットによって参照されるが、実際には他のデータセットに格納されているスペースを示しています。したがって、システムに変更を加える前に、復元ポイントを作成することをお勧めします。これにはシステムリソースをほとんど使用しないためです。時間が経過し、本番システムの復元ポイントで多くの変更が行われた後、使用されるメモリ領域が増加するため、不要になった復元ポイントを削除することをお勧めします。

5.1.1.1 工場出荷時設定へのリセット

TwinCAT/BSD はいつでも工場出荷時の設定にリセットできます。例えば、設定ミスによりシステムが正常に動作しなくなった場合、納入時の状態を復元できます。

復元ポイントは、restorepoint プログラムを使ってコンソールで作成・管理します。このセクションでは、TwinCAT/BSD を工場出荷時の設定にリセットする方法を説明します。

以下の手順に従ってください。

1. コンソールでコマンドdoas restorepoint rollback factoryresetを入力します 。
2. システムがリセットされたすべてのスナップショットが表示されます。
3. **[y]**で復元を確定します。

⇨ システムは工場出荷時の設定にリセットされました。再起動後、TwinCAT/BSD は再び納入時の状態になります。

5.1.1.2 復元ポイントの作成

復元ポイントによるメモリ消費

復元ポイントは、var/crash にあるカーネルダンプを含め、システム全体がバックアップされるため、ストレージ容量を消費します。復元ポイントを作成する前にシステムをクリーンアップするか、古い復元ポイントを削除してください。

復元ポイントは、大規模なシステム変更や設定ミスの後、TwinCAT/BSD が正常に動作しなくなった場合に、古いシステム状態を復元するために使用します。システムの大きな変更、プログラムのインストール、テストを実行する場合には、復元ポイントを作成してください。

復元ポイントは、restorepoint プログラムを使ってコンソールで作成・管理します。このセクションでは、TwinCAT/BSD で復元ポイントを作成する方法を説明します。

以下の手順に従ってください。

1. コンソールでコマンドdoas restorepoint create を入力します。
2. 復元ポイントは自動生成された名前で作成されます。
3. restorepoint status コマンドで作成した復元ポイントを確認し、すべての復元ポイントを表示させます。

```
Administrator@CX-4FAA38$ restorepoint status
last BE: zroot/ROOT/default
factoryreset
2020-08-28T08:56:14Z
2020-08-28T09:03:05Z
```

4. または、doas restorepoint create your-restorepoint というコマンドを使用して、復元ポイントに独自の名前を設定することもできます。

⇨ 復元ポイントは、システムをリセットするためにいつでも作成、使用できます（参照：復元ポイントにリセットした場合 [▶ 18]）。

```
Administrator@CX-4FAA38$ restorepoint status
last BE: zroot/ROOT/default
factoryreset
2020-08-28T08:56:14Z
2020-08-28T09:03:05Z
your-restorepoint
```

5.1.1.3 復元ポイントにリセットした場合

注記

データの喪失

特定の復元ポイント以降に作成されたデータや復元ポイントは、それ以前の復元ポイントにリセットする際に削除されます。

TwinCAT/BSD が設定ミスで正常に動作しなくなった場合、TwinCAT/BSD を再インストールすることなく、復元ポイントを使用してこれらの設定エラーを簡単に元に戻すことができます。

以下の手順に従ってください。

1. コンソールでコマンドrestorepoint status を入力すると、使用可能な復元ポイントがすべて表示されます。

```
Administrator@CX-4FAA38$ restorepoint status
last BE: zroot/ROOT/default
factoryreset
2020-08-28T08:56:14Z
2020-08-28T09:03:05Z
your-restorepoint
```

2. コンソールでコマンドdoas restorepoint rollback を入力すると、既存の復元ポイントがすべて表示されます。
3. 特定の復元ポイントにシステムをリセットするためのメニュー項目を選択します。

```
Administrator@CX-4FAA38~ $ doas restorepoint rollback
Password:
   1 factoryreset
   2 2020-08-28T08:56:14Z
   3 2020-08-28T09:03:05Z
   4 your-restorepoint
```

4. システムがリセットされたすべてのスナップショットが表示されます。
5. **[y]**で復元を確定します。

⇨ TwinCAT/BSD は復元ポイントにリセットされ、再起動されます。選択した復元ポイント以降に作成されたデータと復元ポイントは、リセット中に削除されることに注意してください。

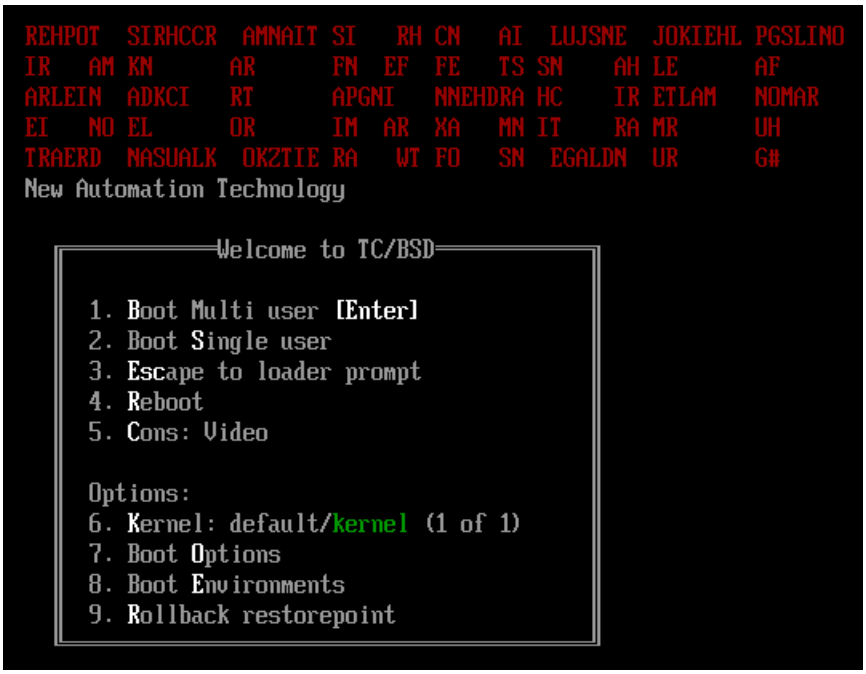
5.1.1.4 復元ブート環境の使用

TwinCAT/BSD が起動しなくなり、その結果コンソールにアクセスできなくなった場合、復元ブート環境から復元ポイントを復元できます。これを行うには、ブートプロセス中にブートメニューを起動し、復元ブート環境に切り替えます。

以下の手順に従ってください。

1. 産業用PCを起動します。

2. 起動中に**[Space bar]**を長押しします。ブートメニューが表示されます。



3. **Rollback restorepoint**オプションを選択します。

⇨ TwinCAT/BSD は復元ブート環境で起動します。工場出荷時の設定に戻すには、restorepoint rollback factoryreset コマンドを使用するか、別途作成した復元ポイントを使用します（復元ポイントにリセットした場合 [▶ 18] 参照）。

5.1.2 バックアップ作成と復旧

復元ポイントとは異なり、TwinCAT/BSD は、バックアップによって外部記憶デバイスにバックアップコピーとして保存・管理できます。

このバックアップコピーは、システム障害やデータ損失の際にシステムを復旧するために使用できます。産業用PCをバックアップ時の状態に復旧するために、システムから定期的にバックアップを作成してください。

5.1.2.1 バックアップの作成

TwinCAT/BSD インストーラースティックを使ってバックアップを作成し、復旧できます。すべてのバックアップはUSBメモリ上のFAT32パーティションに保存されます。FAT32はWindowsやFreeBSDと相互運用可能です。これにより、作成したバックアップをTwinCAT/BSDシステムとWindowsシステムの両方で管理できます。

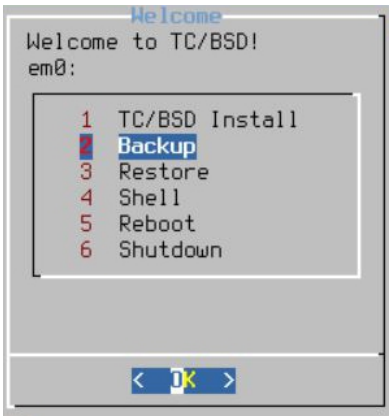
要件:

- TwinCAT/BSD インストーラースティック（参照）

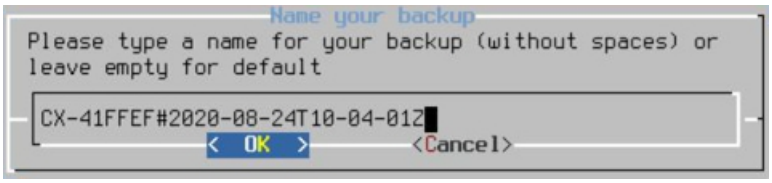
以下の手順でバックアップを作成します：

1. TwinCAT/BSD インストーラースティックを産業用 PC に接続します。
2. TwinCAT/BSD インストーラスティックから産業用 PC を起動します。
3. 産業用PCがUSBスティックから自動的に起動しない場合は、**[F7]**でブートメニューを開きます。
4. USBスティックのUEFIエントリーを選択し、**[Enter]**で確定します。USBメモリから産業用PCが起動し、Beckhoff TwinCAT/BSDインストーラが実行されます。

5. **Backup**オプションを選択します。



6. バックアップにファイル名を割り当てるか、ホスト名とタイムスタンプからなるデフォルト名を承認します。



7. バックアップが完了したら、再起動するために**Reboot**オプションを選択します。

⇨ バックアップは設定したファイル名でUSBスティックに保存されます。USBメモリにバックアップをアーカイブします。また、バックアップを外部記憶媒体にコピーしたり、ネットワーク上にアーカイブすることもできます。

5.1.2.2 バックアップからの復旧

適切なバックアップを使用して復旧してください

バックアップは、CX51x0、CX20x3、C6015など、同一シリーズ内の1つのデバイスにのみリストアできます。バックアップを異なるシリーズのデバイスにリストアすると、非互換のため不具合が発生する可能性があります。

TwinCAT/BSD インストーラースティックを使ってバックアップを復旧できます。これを行うには、産業用PCをTwinCAT/BSD インストーラースティックから起動する必要があります。

要件:

- TwinCAT/BSD インストーラースティック（参照）

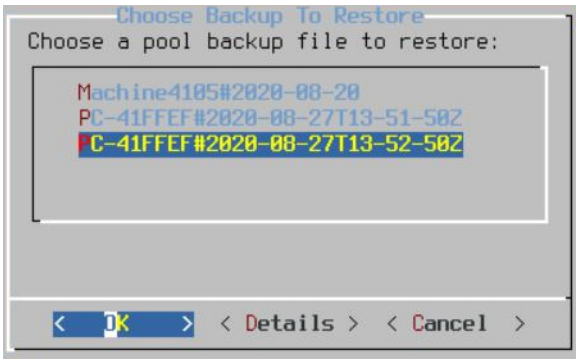
以下の手順に従ってください。

1. TwinCAT/BSD インストーラースティックを産業用PCに接続してください。
2. TwinCAT/BSD インストーラスティックから産業用 PC を起動します。

産業用PCがUSBスティックから自動的に起動しない場合は、[F7]でブートメニューを開きます。

3. USBスティックのUEFIエントリーを選択し、**[Enter]**で確定します。産業用PCがUSBスティックから起動し、Beckhoff TwinCAT/BSDインストーラが実行されます。
Restoreオプションを選択します。

4. 産業用PCに復元するバックアップを選択します。



⇨ 復旧後、産業用PCを再起動してください。産業用PCはバックアップ時の状態に戻りました。

5.1.2.3 本番システムからのバックアップ作成と復旧

アプリケーションで必要な場合には、TwinCAT/BSDインストーラを使用せずに、本番システムからバックアップを作成し、リストアすることもできます。このために、スクリプトTcBackupとTcRestoreを使用します。

システムがディスクに書き込みを行っている場合は、実行中のシステムからバックアップを作成しないでください。バックアップ中にシステムがディスクに書き込みアクセスすると、バックアップデータが破損する可能性があります。他にデータを持続的にバックアップするプロセスが実行されていないことと、バックアップを作成するディスクに十分な空き容量があることを確認してください。

TcBackupとTcRestoreの実行と、バックアップ元およびバックアップ先ファイルの書き込みは、root権限で行う必要があります。つまり、あらかじめroot権限でシェルを実行し、その中で作業するか、root権限のシェルで文字列としてコマンドを1つ実行してください。後者のオプションは以下の例で説明します。

以下の手順に従ってください。

1. コマンドdoas sh -c "TcBackup.sh --disk /dev/ada0 > backup.tcbkp00" を入力して、ada0ディスクからBackup.tcbkp00ファイルへのバックアップを作成します。
2. コマンドdoas sh -c "TcRestore.sh --disk /dev/ada1 < backup.tcbkp00" を入力して、ada1ディスク上のBackup.tcbkp00ファイルからバックアップを復旧します。

⇨ この2つのコマンドは、以下のように組み合わせできます。コマンドdoas sh -c "TcBackup.sh --disk /dev/ada0 | TcRestore.sh --disk /dev/ada1" は、ada0ディスクからバックアップを作成し、直ちにada1ディスクに復旧します。

5.2 アップデート

定期的なアップデートは、特に危険なセキュリティホールを塞ぐために重要です。オープンソースコミュニティは通常、既知のセキュリティホールを非常に迅速に塞ぎます。この利点を生かし、速やかにパッチを適用してください。ベッコフでは、各システムにプリセットされたパブリックパッケージサーバーを通じて、基本システムおよび多くのプログラムのアップデートを提供しています。

システムアップデートは、以下の手順で進めてください：

1. 可能であれば、まず、テスト用ハードウェア上で自身のプログラムとの相互作用環境でアップデートをテストしてください。
2. 不測の事態に備え、システムのバックアップ作成するか、復元ポイントを作成して古いシステム状態を復旧できるようにしてください（参照：復元オプション [▶ 16]）。
3. まず、doas pkg upgrade -n でアップデート可能なパッケージを表示し、doas pkg upgrade <packagename> でアップデートを実行します。

5.3 ユーザおよび権限管理

5.3.1 安全なパスワード

システムのセキュリティを保証する上で、安全なパスワードが重要な前提条件となります。ベッコフでは、デバイスのOSイメージ用に、標準ユーザ名とパスワードを設定しています。これらはお客様で必ず変更してください。変更しない場合、お客様のデバイスは、ネットワーク経由の攻撃や、権限のない者によるアクセスに対して脆弱になります。

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。

セキュリティウィザードはシステムに統合されています。これは、ローカルアクセス中にデバイスを起動した直後に開始します。このウィザードはユーザにパスワードの変更を要求します。パスワードはOSのツールを使ってローカルで変更することもできます。

以下に注意してください。

- ユーザおよびサービスごとに異なるパスワードを設定してください。
- 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。
- 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。以下も参照してください。https://arstechnica.com/information-technology/2016/08/frequent-password-changes-are-the-enemy-of-security-ftc-technologist-says/
- 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。

安全なパスワードの作成

安全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

5.3.1.1 パスワードを変更する

現在ログインしているユーザのパスワードは、コマンドpasswd で変更できます。doas passwd を使用する場合、root権限でコマンドを実行し、ログインユーザのパスワードではなく、スーパーユーザ・アカウント（root ）のパスワードを変更することに注意してください。root権限でpasswdを実行しないでください 。

TwinCAT/BSDの納入時には、コンソールにログインできるユーザ（Administrator ）がデフォルトで設定されています。このユーザは、Windowsシステムのような通常の管理者権限を持たないが、特定の目的のためにroot権限を取得する権限を持っています。

ログインデータ：

- ログイン：Administrator
- パスワード：1

以下の手順に従ってください。

1. 産業用PCを起動します。
2. ユーザ名Administrator とパスワード1 でログインします。
3. ログインに成功すると、産業用 PC のユーザ名とホスト名が表示されます。例：CX-1D7BD4
4. TwinCAT/BSDの新しいパスワードを設定するには、コマンド passwd を入力します。指示に従ってください。

⇨ TwinCAT/BSDの新しいパスワードの設定が完了しました。

5.3.1.2 パスワードポリシー

別のパスワードポリシーは、弱いパスワードの使用からシステムを保護します。使用するユーザパスワードの長さと複雑さを設定し、以下の推奨事項に従ってください：

パスワードポリシーを定義するには、/etc/pam.d/passwd を以下のように編集します：

```
doas ee /etc/pam.d/passwd
```

行頭の "#"を削除し

```
password requisite pam_passwdqc.so enforce=users
```

必要に応じてpam_passwdqcモジュールのエントリーを追加します：

```
password requisite pam_passwdqc.so min=disabled,disabled,disabled,disabled,10 similar=deny retry=3
en-force=users
```

このモジュールには5つのパスワードカテゴリーがあらかじめ定義されているため、pam_passwdqc の後ろに5つの値を設定できます。カテゴリーには、特殊文字、小文字、大文字、数字の組み合わせなど、パスワードの複雑さの要件が含まれます。pam_passwdqc.s 以降の各桁は、無効にするか、必要なパスワードの長さを数字で表し、以下のパスワードカテゴリのいずれかを表します：

- 1文字クラスのパスワードが許可されています（数字、小文字、大文字のみからなるパスワード）
- 2文字クラスのパスワードが許可されています（小文字と大文字で構成されたパスワード）
- パスフレーズが許可されています（スペースで区切られた文字列）
- 小文字、大文字、数字など、3つのパスワードカテゴリーで構成されるパスワード
- 小文字、大文字、数字、特殊文字など、4つのパスワードカテゴリーで構成されるパスワード

この例では、4つのパスワードカテゴリーを使用した10文字で構成されるパスワードのみ許可しています。"similiar"は、新しいパスワードが古いパスワードに似ているかどうかも定義します。"retry "は、ユーザがパスワードポリシーに従って新しいパスワードを選択できなかったときに、pam_passwdqc プロンプトが新しいパスワードの入力を求める頻度を示します。

パスワードポリシーの設定についての詳しい情報は、https://www.freebsd.org/cgi/man.cgi?query=pam_passwdqcを参照してください。

5.3.2 自動ログアウト

自動ログアウトを設定すると、コマンドラインを操作しない時間が一定時間経過すると、自動的にログアウトされます。これは、IPCが無人状態でユーザがログアウトを忘れた場合に、コマンドラインへの不正アクセスを防ぐために使用します。デフォルトでは、自動ログアウトは有効ではありませんが、試運転の際にはオンにする必要があります。

自動ログアウトを有効にするには、ユーザのシェルをshからtcshに変更してください。tcshシェルはすでに自動ログアウトを実装しており、後で設定できるようになっています。

```
chsh -s tcsh
```

```
ee ~/.login
```

以下の行を追加し、自動ログアウトが実行されるまでのアイドル時間を指定します：

```
set -r autologout=1
```

変更を有効にするには、login で再ログインしてください。

5.3.3 グループとファイルの許可

TwinCAT/BSDは、Unixのような他のシステムでも使用されているアクセス制御リストを使用しています。一般的に、許可できるユーザには、ファイルの所有者、所有者のグループ、その他の全てのユーザ（所有者/グループ/その他）の3種類があります。各ユーザタイプに対して、ファイルへの書き込み、読み取り、実行権限を設定できます。

ls –lで、ファイルやディレクトリの許可を表示できます。

```
Administrator@CX-0C8440$ ls -l
total 10
-rw-r--r--  1 root           Administrator   5 Dec  4 12:31 file
-rw-r--r--  2 Administrator  Administrator  10 Dec  4 15:29 test
drwxr-xr-x  3 Administrator  Administrator   6 Dec  7 10:44 testdir
```

最初の列には許可スキームがあり、その後にファイルの所有者と所有者のグループが続きます。許可スキームは4つの部分に分けられます。最初の記号はファイルの種類を示します。ファイル（-）かディレクトリ（d）かを示します。次の3つの記号は所有者の権利、次の3つの記号はグループの権利、最後の3つの記号はその他の全てのユーザの権利を示しています。これら3つの記号のうち、最初の記号は読み取り許可が付与されているかどうか（r）、2番目の記号は書き込み許可が付与されているかどうか（w）、3番目の記号はファイルの実行またはディレクトリへのアクセスが可能かどうか（x）を示します。ls –l で出力された上記の許可スキームは以下のように読み解けます：

タイプ	所有者	グループ	その他
-file（ファイル）	rw-read write（読み取り・書き込み）	r-read（読み取り）	r-read（読み取り）
-file（ファイル）	rw-read write（読み取り・書き込み）	r-read（読み取り）	r-read（読み取り）
d directory（ディレクトリ）	rwx read write execute（読み取り・書き込み・実行）	r-x read execute（読み取り・実行）	r-x read execute（読み取り・実行）

デフォルトでは、新しいファイルには–rw–r––r–– という権限が与えられ、新しいスクリプトはまず実行可能の状態にします。デフォルトの許可では、スーパーユーザのrootでもスクリプトを実行できません。

開発用コンピュータからリモートで許可を変更するには、TwinCAT/BSDドキュメントの「Managing files with WinSCP client（WinSCPクライアントによるファイル管理）」の章で説明されているWinSCPを使用します。ローカルでは、許可はプログラムchmodで変更できます。ローカルのマニュアルはman chmodを入力してください。

非特権ユーザの作成

HMIユーザや保守ユーザのように、タスクごとにユーザを使い分けることをお勧めします。各ユーザには、それぞれのタスクを実行するために必要な権限を与え、責任あるユーザのみにroot権限が与えられるようにします。ユーザアカウントを作成するには、以下のコマンドを使用します：

```
doas adduser
```

ウィザードが起動し、ユーザ作成プロセスを案内します。ユーザを編集するにはdoas chpass <Benutzer>を使用します。

すでにベースシステムに含まれているユーザもいます。管理者ユーザのほかに、いわゆるシステムアカウントがあります。これらのアカウントは対話型のアカウントとして設定されておらず、統合プログラムの管理と実行にのみ使用されます。

グループ

ユーザは1つまたは複数のグループに分けられます。新しいユーザが作成されると、デフォルトでは同じ名前のグループが作成されます。さらに、同様のタスクを持つユーザを共通のグループに割り当て、同様の権限を持たせることもできます。これらの許可には、特定フォルダやファイルへのアクセス、実行中のプログラムへのアクセスなどがあります。

"Wheel"グループに割り当てられたユーザには、root権限を付与できます。事前に"Administrator"に設定されたユーザは "Wheel"メンバーであり、プログラムの前にコマンドdoasを置き、パスワードで再度認証することでroot権限を取得できます。

doas ee /etc/groupで/etc/groupを編集することで、グループメンバーシップを変更し、新しいグループを作成できます。

このファイルには、利用可能な全てのグループが表示されています。表示されているグループのほとんどはデフォルトのグループで、Unixに由来します。セキュリティ上の理由から、これらのグループは特定のタスクを持つシステムユーザに割り当てられます。そうしないと、これらのプログラムは制限なしにroot権限で実行されてしまいます。

システムの使用を制限する

いわゆるログオンクラスを使用して、ユーザが利用できるシステムリソースや情報を定義できます。

5.3.4 ファイルフラグ

FreeBSD は基本的なファイル許可に加えて、ファイルフラグを提供し、ファイルの制御にもう 1 つのセキュリティレベルを追加します。Securelevel [▶ 26] の章で説明されているセキュリティーレベルによって、ファイルフラグの効果は異なります。以下は、システムを保護するための一般的なファイルフラグです。ファイルフラグの完全なリストは、各マニュアルに記載されています。

sappnd : このフラグが付いたファイルは編集や削除はできないが、内容を追加することはできます。これは、例えば、増大する可能性のあるログファイルで、攻撃者による削除が不可で侵入をより困難にするために有効です。Sappndはroot権限でのみ設定可能で、Securelevel 1以上では削除できません。

uppnd : sappndと同様ですが、root権限以外にファイルの所有者もこのフラグを設定したり削除したりできます。誤ってファイルを削除したり変更したりするのを防ぐのに便利です。

schg : このフラグが付いたファイルは、編集、削除、別の場所への移動ができません。Schgはroot権限でのみ設定可能で、セキュリティレベル1以上では削除できません。

uchg : schgと同様ですが、root権限以外にファイル所有者もこのフラグを設定したり削除したりできます。

ファイルフラグを設定するにはコマンドchflagsを使用し、その後に各ファイルフラグと保護したいファイルを続けます：doas chflags sappnd /pfad/zu/datei

ファイルフラグ名の前に "no "を付けて、ファイルフラグを削除します：doas chflags nosappnd /pfad/zu/datei

システムをより安全にするためにファイルフラグを使用する一例として、ファイルシステムカーネルを改ざんから保護する方法があります：doas chflags schg /boot/kernel/kernel

システムアップデートの場合は、ファイルフラグをクリアしなければならないことに注意してください。

-R オプションを使用すると、指定したフォルダ内のディレクトリとファイルに対して、ファイルフラグが冗長設定されます。以下のコマンドですべてのログファイルを削除することはできませんが、システムはログを付帯できます：doas chflags -R schg /var/log

ファイルフラグを簡単に削除できない場合は、システムのセキュリティレベルが高い可能性があります。TwinCAT/BSDはデフォルトでは、セキュリティレベル-1になっており、システムに対して追加のセキュリティは提供されず、ファイルフラグを変更できます。より高いセキュリティレベルの場合、ファイルフラグを変更できません。

5.3.5 Securelevel

Securelevelは、カーネルで設定されるセキュリティ設定です。Securelevelを変更することで、システム変更に対してどの程度、制約が課されるべきかが定義されます。

ブート時にSecurelevelを有効にするには、以下の行を追加します：/etc/rc.conf

```
kern_securelevel_enable="YES"
```

切り替え可能なSecurelevelは5段階です。システムのSecurelevelが高いほど、より多くのセキュリティ機能が追加されます。c.conf にkern_securelevel=2 を追加して、Securelevelを定義します。ここでは、Securelevel2に設定されています。システムの再起動後、変更が有効になります。

以下は、各Securelevelのシステムへの影響について説明しています：

-1: デフォルト、追加のカーネルセキュリティなし。

0：Securelevel「0」に設定されたシステムは、Securelevel「-1」のみで起動し、マルチユーザモード（標準操作モード）になると自動的にSecurelevel「1」に切り替わる。これは、Securelevel1では実行が禁止されている自動起動スクリプトを使用する場合に推奨される。

1：基本的なセキュリティ機能を提供する：

- ファイルフラグは単純にオフにすることはできない（参照：ファイルフラグ [▶ 25]）
- ユーザはカーネルモジュールのロードとアンロードができない
- プログラムは、デバイスノード（/dev/mem および/dev/kmem ）を経由してメモリに書き込みできない
- デバイスノード/dev/io には対応不可
- sysctl プログラムによるシステムのデバッグとパニックは無効
- RAWディスクデバイスへの書き込みは禁止されている

2：「1」のプロパティに追加プロパティを加えたもの：

- ユーザはデバイスノード経由でRAWディスクデバイスに書き込みできない
- システム時間を1秒以上変更することは禁止されている

3：セキュリティレベル1と2の機能を含み、さらにネットワークセキュリティを提供する：

- ファイアウォールルールの編集はできない

適切なSecurelevelの選択

Securelevelの選択は、要件次第です。常に変更を加え、柔軟なシステムが必要な場合は、何も変更せずデフォルトのSecurelevel（-1）のままにしておいてください。システムをほとんど設定する必要がなく、システムを生産環境で使用する場合は、Securelevelを高く設定することをお勧めします。これ以上のシステム変更が必要ない本番環境のシステムには、セキュリティレベル2を推奨しています。すでにネットワークも設定されており、これ以上ファイアウォールの変更が必要ない場合は、Securelevelを3に上げることができます。

5.3.6 監査ポリシー

デバイスをネットワークに統合するためのセキュリティ対策の一環として、潜在的な攻撃を検知するために、どのレベルのセキュリティ監査が適しているかを特定する必要があります。セキュリティ監査とは、産業用PCとデバイスとの相互作用が発生するとすぐ、産業用PCがイベントの監査ログを作成することを意味します。例えば、ユーザが選択したファイルやフォルダにアクセスするたびに、アクセスログを記録できます。

これらのログは、攻撃を示す可能性のある通常使用からの逸脱を検出するための評価、または攻撃に関する詳細を再構築するための情報収集を目的とします。チェックは、自動化されたメカニズムまたは手動で、即座にあるいは一定の間隔で実施できます。どのような逸脱に対応するかは、環境やアプリケーションによって異なります。したがって、どのアクションがログに記録されるかを記述するルールは、通常、監査ポリシーを使って設定します。

しかし、あまりに多くのルールを設定しすぎると、一種の盲目になりかねません。ログは無関係なエントリーで溢れかえり、関連するエントリーが簡単に見落とされたり、自動監視メカニズムによって迅速に処理されなかったりする可能性があります。限られたログ容量の超過を避けるために、ログを中央の保存場所に転送し、自動的に評価したり、アーカイブしたりするのが良い方法である場合もあります。

TwinCAT/BSDでは、ファイルやフォルダへのアクセス、およびユーザエントリをログに記録できます。ユーザが特定のアクションを実行するたびに、イベントがログに記録されます。これらのイベントログは、システムを監視し、不正アクセスを検知し、セキュリティインシデント発生後に分析するために特に重要です。

システム起動後に監査デーモンを自動的に起動させます：

```
doas ee /etc/rc.conf
auditd_enable="YES"
```

現在のセッションの監査デーモンを起動します：

```
doas service auditd start
```

/etc/security には、監査デーモンの設定ファイルがあり、監査の微調整に使用できます。ここで特に重要なのは2つのファイルです：

/etc/security/audit_control:一般的なシステム全体の監査設定

デフォルト設定では、監査ログは/var/audit に保存されます。メモリの5%が監査ファイルに使用されると、警告メッセージが表示され、10ヶ月後に監査ログが削除されます。

zroot/var/auditでは 、すでに監査ログ用に別のZFSデータセットが用意されています。このデータセットにはクォータ、つまり容量制限を設定することをお勧めします。標準的な監査設定でも、大量のデータが生成されます。10カ月後に監査ログが自動的に削除されることを考慮してもです。このデータセットの保存容量を制限し、他の重要なデータセットのための容量を確保するために、次のコマンドを使って監査ログの保存容量を、例えば2GBに制限できます：

```
doas zfs set quota=2G zroot/var/audit
```

あるいは、この対策に加えて、/etc/security/audit_controlで、監査ログが削除されるまでの期間を短くすることもできます。

```
doas ee /etc/security/audit_control
expire-after:10M □ expire-after:2M
```

/etc/security/audit_user:各ユーザの監査設定

ここでは、各ユーザに対して個別の監査ルールを定義できます。監査ルールの詳細な説明と、ユーザの監査ルールを定義するためのオプション一覧は、 FreeBSD ハンドブックhttps://docs.freebsd.org/en/books/handbook/audit/に記載されています。

5.4 プログラム

5.4.1 プログラムのホワイトリスト化

WindowsのApplockerやいわゆるソフトウェア制限ポリシー（SRP）のようなアプリケーションのホワイトリストは、TwinCAT/BSDでは使用できません。Unixシステムでは、アプリケーションのホワイトリスト化を実現するために、さまざまなアプローチがあります。これらはWindowsと比較して一般的ではありません。その理由は、Windowsではほとんどがグラフィカルな入力であるのに対し、Unixではコマンドラインやスクリプトによる複雑さが増すからです。代わりに、パッケージのソースに細心の注意を払い、どのパッケージがシステムにインストールされているかをチェックしてください（参照：不要なコンポーネントの除外 [▶ 28]）。

5.4.2 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。

システムコンポーネントの取り外しは、熟練者のみが行ってください。副作用が発生し、プログラムが正常に実行できなくなる可能性があります。

pkg info を使えば、システムにインストールされているすべてのパッケージを表示できます。ここに掲載されているパッケージは、基本システムまたはベッコフソフトウェアに関連するものです。TCで始まるTwinCAT用パッケージ、ベッコフIPC診断、および "os-generic "で始まる基本システム用パッケージに加えて、依存関係にあるプログラム（他のプログラムで必要とされるプログラム）もここに表示されます。

他のパッケージと依存関係にあるパッケージを削除する場合、システムは関連するパッケージも削除するかどうかを尋ねます。これにより、どのパッケージが、インストールされている他のパッケージと依存関係にあるか判断できます。不要になったパッケージはdoas pkg delete <pkg-name> で削除できます。その後、doas pkg autoremove というコマンドを使って、不要になった依存関係をすべて削除できます。これにより、不要になったパッケージがシステム上に残りません。

5.4.3 パッケージ監査

TwinCAT/BSDのソフトウェアのインストールとアップデートに使用されるパッケージツールには、インストールされたソフトウェアの既知の脆弱性をチェックする監査機能があります。

```
doas pkg audit -F
```

このコマンドは、既知の脆弱性のリストをダウンロードし、ローカルのパッケージと比較します。CVE番号（Common Vulnerabilities and Exposures）と、脆弱性に関する詳細情報へのリンクが表示されます。

5.4.4 ウイルス対策プログラム

一般的には、TwinCAT/BSDおよびUNIXシステムには、ウイルス対策プログラムは必要とされていません。なぜなら、UNIXシステム用の悪意のあるソフトウェアはまれである傾向があるためです。Unixシステム向けのウイルスはまだ非常にまれです。主な理由は、WindowsやMac OSに比べてシステムの普及が進んでいないためです。

さらに、ユーザアカウントとその権利が明確に分けられているためです。TwinCAT/BSDでは、Administratorユーザであっても、システム関連ファイルの変更やプログラムの実行には、パスワードを入力してroot権限を取得する必要があります。スクリプトの実行には、実行可能な状態への変更が要求されます。誤ってダウンロードされたウイルスは、最初はログインしているユーザのファイルにのみ感染します。厳重な権利管理のため、システム上には容易には拡散しません。

しかしながら、セキュリティホールは定期的なアップデートによって塞がなければなりません。大規模なオープンソースコミュニティがあるため、セキュリティホールは通常すぐに特定され、塞がれます。アップデートは、各システムにプリセットされたBeckhoffパッケージサーバーから入手できます。

Unixシステム用のウイルス対策プログラムもありますが、主にメールサーバーやファイルサーバーに有効で、Windowsクライアントでも使用できます。もちろん、ウイルス対策プログラムは、システムに別のセキュリティレベルを追加するために使用することもできます。TwinCAT/BSDでは、いくつかの専用アプリケーションに加えて、無償のLinuxアンチウイルスプログラムClam Antivirusが利用可能です。このプログラムはGPLライセンスにあたり、その条項に従う必要があることに注意してください。

5.5 Writeフィルター

TwinCAT/BSDには、特定のデータセットを書き込みアクセスから保護するためのWriteフィルターがあります。Writeフィルターの利点は、ユーザがあらかじめ設定した状態でシステムを保護できることです。再起動後、システムは自動的に最初に定義された状態にリセットされます。

データセットzroot/ROOT/default は、システムおよびTwinCATの大部分を含み、Writeフィルターが有効な場合に書き込みアクセスから保護されます。他のデータセットはWriteフィルターの対象ではありません。例えば、システムの他の部分が再起動後にリセットされても、ユーザファイルは/home に、ログファイルは/var/log に、永続的に保存できます。

5.5.1 Writeフィルターの有効化および無効化

このステップでは、TwinCAT/BSDでWriteフィルターを有効または無効にする方法を示します。Writeフィルターの変更は、再起動後にのみ有効になることに注意してください。

以下の手順に従ってください。

1. コンソールでコマンドdoas service bwf enable を入力し、Writeフィルターを有効にします。
2. 管理者パスワードでコマンドを確定します。

```
Administrator@CX-3D6912:~ $ doas service bwf enable
Password:
bwf_enable: NO -> YES
writefilter enabled, please reboot to make your changes take effect.
```

3. shutdown -r now で産業用PCを再起動し、設定を適用します。

⇨ Writeフィルターは再起動後も有効です。Writeフィルターは、コマンドdoas service bwf disable で再び無効化できます。

5.5.2 例外の定義

Writeフィルターの例外は、新しいデータセットを作成することで定義できます。zroot/ROOT/default のデータセットのみが書き込みアクセスから保護されるためです。新しく作成されたデータセットを含め、他のすべてのシステムデータセットは保護対象から除外されます。

本章では、TwinCATブートディレクトリ用に別のデータセットを作成し、このディレクトリをWriteフィルター保護から除外する例を示します。

要件:

- この例に従う場合は、TwinCATブートディレクトリを事前に保存してください。
- Writeフィルターを無効にしてください（Writeフィルターの有効化および無効化 [▶ 29] を参照）。

以下の手順に従ってください。

1. コマンドdoas rm -rf /usr/local/etc/TwinCAT/3.1/Boot/* を入力します。
2. ディレクトリusr/local/etc/TwinCAT/3.1/Boot はファイル階層から切り離されます。
3. コマンドdoas zfs create -o mountpoint=/usr/local/etc/TwinCAT/3.1/Boot zroot/usr/TwinCAT-Boot を入力して、新しいデータセットzroot/usr/TwinCAT-Boot をマウントします。

⇨ TwinCATブートディレクトリに新しいデータセットが作成されました。新しいデータセットzroot/usr/TwinCAT-Boot を含め、マウントされているすべてのデータセットを表示するには、zfs mount を使用します。今後、このディレクトリ以下のすべてのディレクトリは、有効なWriteフィルターによる書き込みアクセスから保護されなくなります。

5.6 USBフィルター

セキュリティ上の理由から、USBストレージデバイスは自動的にマウントされません。セッションごとに手動でリンクするか、自動リンクを設定する必要があります。どちらの方法もTwinCAT/BSDのドキュメントに記載されています。

6 ネットワーク通信

ここでは、通信に関する措置の概要を説明します。ネットワークのセグメンテーションなど、実際のIPC以外のトピックは扱っていません。

TwinCAT製品に使用されるポートの一覧は、以下を参照ください 重要なTCP/UDPポート [▶ 32] 。

6.1 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動作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、誤動作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。

以下も参照してください。

- VPN [▶ 31]

6.2 ファイアウォール

ファイアウォールの設定は、ネットワーク攻撃からシステムを保護する手段です。不要な受信ポートはブロックすべきです。それ以上に推奨されるのは、これらのポート開通のサービスを一切起動しないことです。関与する全員で連携し使用するポートの一覧を設定する必要があります。

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、ソフトウェア、オペレーティングシステムの一部、または自己完結型のデバイスのいずれかとして追加で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解除し、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。この結果、コンテンツはファイアウォールから見え、エンドツーエンドの暗号化は（ファイアウォール内で）途切れます。

ファイアウォール経由の通信を制限的に明示的に設定することは、必要な範囲に限定してネットワークアクセスを許可するために重要な対策です。

重要なTCP/UDPポート [▶ 32] には、ファイアウォールを設定するために考慮する必要のあるTCP/UDPポートのリストが含まれています。

TwinCAT/BSDは、ファイアウォールとしてパケットフィルタ（PF）を使用します。これは FreeBSD の基本システムの一部で、 TCP/IP ネットワークトラフィックをフィルタリングするシステムです。さらに、NATやポートフォワーディングなど、ネットワーク関連の設定も可能です。

デフォルトでは、システムは事前に強化設定されており、暗号化された接続はわずかしか許可されていません。例えば、ADSポート48898は工場出荷時にブロックされており、ADS Secureのみがポート8016で許可されています。TwinCAT機能やその他のベッコフアプリケーションが必要となるポートは、ファイアウォールで動的にオープンになります。さらに、SSH、HTTPS、Pingはファイアウォールを通して許可されます。

cat /etc/pf.confで 、一般的なファイアウォールルールが出力されます。

cat /etc/pf.conf.d/bhf は、ベッコフアプリケーションに関連するファイアウォールルールを出力するために使用します。

6.3 各種ネットワーク技術

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。

6.3.1 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。

6.3.2 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た環境でのみ使用するか、適切にセキュリティ保護されたトランスポートチャネルを使用することが推奨されています。

ADSには現在、暗号化をサポートする2つのTCPトランスポートチャネルがあります：

- ADS-over-MQTT
- Secure ADS

6.3.3 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、認証された全てのアプリケーションおよび認証された全てのユーザは、いつでもどこからでも必要な全ての情報を入手できます。

詳しくは以下のドキュメントを参照ください：TF6100 TC3 OPC UA

6.3.4 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。

6.4 セキュリティゲートウェイ

ネットワークの影響からシステムを保護するその他のオプションは、セキュリティゲートウェイの使用です。このハードウェアソリューションは、IPCの前のネットワークに設置できます。こうすることで、特定のネットワークセグメントやすべてのPCを保護できます。

デバイスは、ネットワークの保護機能に加えて、例えば、アンチウイルスソフトウェアを実行し、制御コンピュータのリアルタイム機能を制限することなく、ローカルのクリップボード経由で実行されるファイル転送を監視するオプションも提供します。

6.5 重要なTCP/UDPポート

アプリケーションによっては、安全でないプロトコルは無効にするか、物理的に安全なネットワークやVPNなど、より下位レベルのレイヤーで保護する必要があります。

セキュリティで保護されたプロトコルの場合、製品マニュアルに従ってセキュリティの試運転を実施してください。

標準サービス

以下の表は、納入時のイメージで、通常オープンな受信ポートの概要です。

サービス	ポート（受信）
IPC診断	https: 443 / tcp
リモートデスクトップ - RDP（Windows 7/10のみ）	3389/tcp
TwinCAT ADS	Discovery: 48899/udp（送信も含む） Not secured : 48898 / tcp (送信も含む)。TwinCAT/BSD®のポートはクローズ。 Secure ADS: 8016/tcp（送信も含む）

その他のサービス

以下の表は、追加で開くことができる、頻繁に使用されるサービスの概要です。

サービス	ポート（受信）
SMB	137-139/tcp 445/tcp OPC-UA:4852/tcp
Cerhost (Windows CE)	987/tcp
FTP	21/tcp

TwinCATサービス

以下の表は、TwinCAT製品で一般的に使用されるポートの概要を示しています：

サービス	ポート(デフォルト設定)
TF1810 TwinCAT PLC HMI Web	80/tcp(受信) TF1810のドキュメントも参照してください。
TF2000 TwinCAT HMI	1010/tcp（ローカル） 1020/tcp(受信) TF2000のドキュメントも参照してください。
TF6100 OPC UA	4840/tcp（UAサーバー、受信）、変更可能 48050/tcp（UAゲートウェイ、受信）、変更可能 TF6100のドキュメントも参照してください。
TF6100 OPC DA	1024～65535(受信)で可変(DCOMにより異なる) TF6120のドキュメントも参照してください。
TF6250 Modbus TCP	502/tcp（受信）、変更可能 TF6250のドキュメントも参照してください。

サービス	ポート(デフォルト設定)
TF6310 TCP-IP	可変/tcp (受信、送信) TF6310のドキュメントも参照してください。
TF6311 TCP/UDP Realtime	可変/tcp (受信、送信) OSのファイアウォールによって通信が影響を受けることはない。 TF6311のドキュメントも参照してください。
TF6300 FTP	20/tcp (送信) 21/tcp (送信) TF6300のドキュメントも参照してください。
TF6420 Database Server	データベースによって変更可能 / tcp (送信) TF6420のドキュメントも参照してください。
TF67xx IoT TF35xx Analytics	ブローカーによって変更可能 / tcp (送信) こちらも参照ください：TF670xおよびTF35xxに関するドキュメント
TwinCAT EAP	34980/udp（受信）、UDP経由でEAPを使用する場合。 OSのファイアウォールによって通信が影響を受けることはない。 EAPのドキュメントも参照してください。
TwinCAT ADS-over-MQTT	ブローカーによって変更可能 / tcp (送信) 以下も参照ください：ADS-over-MQTTに関するドキュメント

6.6 Nginx Webサーバー

デフォルトでは、TwinCAT/BSDでNginx Webサーバーは有効で、Beckhoff Device ManagerやPLC HMI Webなどに使用されます。

システムの安全性を高め、Webサーバー経由のアクセスを制限するために、例えば、ファイル IPCDiagnostics.conf でBeckhoff Device Managerへの転送を無効にすることができます。そのためには、合計3項目をコメントアウトする必要があります。

1. /usr/local/etc/nginx以下のファイルIPCDiagnostics.confを開きます。
2. location/ 、 location /config 、 location /console 以下のエントリを完全にコメントアウトします。

```
---snipped---
include errorpages.conf;
include authelia.conf;

# location / {
# add_header ServerHostname $hostname;
# root /usr/local/www/default;
# index index.html index.htm;
# }

# location /config/ {
# include errorpages.conf;
# include auth.conf;
# include proxy.conf;
# proxy_pass http://127.0.0.1:42340/;
# }

# location /console/ {
# include errorpages.conf;
# include auth.conf;
# include proxy.conf;
# proxy_set_header Upgrade $http_upgrade;
# proxy_set_header Connection "upgrade";
# proxy_pass "http://127.0.0.1:7681/";
# }

location /Tc3PlcHmiWeb {
include proxy.conf;
---snipped---
```

3. 変更内容を保存します。

⇨ コマンドshutdown -r now でTwinCAT/BSD を再起動するか、doas service nginx restartでNginx サービスを再起動します。以降、Beckhoff Device Managerにリクエストが転送されることはありません。

6.7 HTTPS 証明書

この章では、ベッコフがデフォルトで提供するWebインターフェース（Device Manager）用の証明書がアプリケーションに適していない場合に、独自のHTTPS証明書を作成してインポートする方法について説明します。

証明書は、ITにおいて身元を安全に証明するために使用されます。これにより、メッセージや文書を暗号化し、意図した受信者だけが再び内容を解読できるようになります。この技術は特に、HTTPSプロトコルを介してページを取得する際に、全てのWebブラウザで使用されます。

ネットワーク加入者は、通信接続を確立する際、他の加入者の証明書を要求します。証明書と、相手が関連するキーを使用して自身を認証しているかどうかがチェックされます。いったん身元が証明されれば、その後の接続を介したメッセージ交換は、不正な操作から保護され、オプションとして不正な閲覧からも保護されます。

特別に生成されたHTTPS証明書を使用するためには以下が必要です：

- 産業用PCの証明書の自動生成を無効にする
- 証明書は認証局(CA)に要求する
- その後、HTTPS証明書をインポートする

正確な手順と必要なステップについては、本章で説明します。

6.7.1 証明書の自動生成を無効にする

一部のユースケースでは、ユーザーがTwinCAT/BSD®によって生成された証明書をWebサーバーで再利用することは適切ではありません。このユースケースでは、自動同期を無効にし、TwinCAT/BSD® Webサーバ（nginx）用の独自の証明書を使用します。

これを行うには、まず証明書の自動作成を無効にし、独自の証明書をインストールします。さらに、デフォルトのベッコフ証明書で上書きされないようにする必要があります。

以下の手順に従ってください。

1. 証明書がデフォルトのベッコフ証明書で上書きされないように、サービスIPCDiagnostics を無効にしてください。
2. これを行うには、コンソールでコマンドdoas service IPCDiagnostics disable を入力します。

⇨ 証明書の自動生成は無効になりました。次のステップでは、証明書を認証局（CA）に要求します（以下を参照：HTTPS証明書のリクエストまたは生成 [▶ 34]）。

6.7.2 HTTPS証明書のリクエストまたは生成

通常、認証局（CA）は、発行した証明書のインストール方法について手順を提供しています。認証局は、証明書の申請方法についても提供しています。認証局の指示を優先して、それに従ってください。

まず、証明書署名要求（CSR）を作成し、その指示に従って認証局に証明書要求を提出します。その後、認証局からサーバー証明書と中間証明書が提供され、証明書署名要求が作成されます。

正式な認証局（CA）からの証明書がない場合、テスト目的で自己署名証明書を作成することができます。

以下の手順に従ってください。

1. 以下のコマンドで、テスト用に自己署名証明書を作成します：

```
doas openssl req -x509 -newkey rsa:4096 -nodes -sha256 -days 3650 ¥
        -keyout IPCDiagnostics.key ¥
        -out IPCDiagnostics.crt ¥
        -subj '/CN=<hostname>' ¥
        -addext 'subjectAltName=DNS:<hostname>,IP:<ipaddress>'
```

2. このコマンドは、秘密鍵IPCDiagnostics.key と自己署名証明書IPCDiagnostics.crt を作成します。

   openssl req: コマンドreqの部分は、証明書署名要求（CSR）の作成と処理を行います。-x509 では、代わりに自己署名証明書が作成されます。

-newkey rsa:4096：RSAアルゴリズムと4096ビットの鍵長で新しい鍵ペアを作成します。

-nodes：「no DES（DESなし）」を意味します。秘密鍵は暗号化された形式では保存されません。すなわち、鍵の使用にパスワードは不要です。

-sha256：安全なハッシュアルゴリズムSHA-256を使用して証明書署名を作成します。

-keyout IPCDiagnostics.key：秘密鍵を IPCDiagnostics.key ファイルに格納します。

-out IPCDiagnostics.crt：作成された証明書をIPCDiagnostics.crt ファイルに格納します。

-subj '/CN=<hostname>':対話型のリクエストなしで証明書のデータを指定します。/CN=<hostname> はコモンネーム（CN）を指定します。コモンネームは通常、証明書で保護されるホスト名またはドメイン名です。

-addext 'subjectAltName=DNS:<hostname>,IP:<ipaddress>':証明書に拡張子を追加します。subjectAltName (SAN) を使用すると、証明書で追加の名前やIPアドレスをカバーできます。

3. <hostname> をホスト名に、<ipaddress> をTwinCAT/BSDデバイスのIPアドレスに置き換えてください。

⇨ 次のステップで、証明書をインポートできます（参照：証明書のインポート [▶ 35]）。

6.7.3 証明書のインポート

公式な認証局（CA）から証明書を受け取ったら、すぐにTwinCAT/BSDシステムにインポートできます。また、テスト用に作成した自己署名証明書を使用することもできます。

以下の手順に従ってください。

1. nginxの既存の秘密鍵を、自身の秘密鍵で置き換えます：

```
doas cp IPCDiagnostics.key /usr/local/etc/TwinCAT/3.1/Target/PrivateKeys/IPCDiagnostics.key
```

2. nginxの既存の証明書を、自身の証明書で置き換えます：

```
doas cp IPCDiagnostics.crt /usr/local/etc/TwinCAT/3.1/Target/Certificates/IPCDiagnostics.crt
```

3. nginx Webサーバーを再起動します：

```
doas service nginx restart
```

4. サービスを再起動すると証明書が使用できるようになります。

⇨ 正式な認証局（CA）の証明書を使用していない場合、ブラウザにセキュリティ警告が表示されます。サーバー証明書をブラウザの証明書ストアにインポートすることで、ブラウザが証明書を自動的に受け入れるように設定できます。詳細は、以下を参照してください：https接続用の自己署名証明書

一部のブラウザ（Mozilla Firefoxなど）は独自の証明書ストアを使用しているため、ブラウザで証明書を直接インポートする必要があります。

7 TwinCAT

eXtended Automation Engineering（XAE）とeXtended Automation Runtime（XAR）にとっての脅威は、プラントのセキュリティコンセプトから考慮すべきです。IEC 62433 規格は、特に重要な脅威分析について説明しており、セキュリテ ィコンセプトの策定に役立ちます。さらに、VDMAのガイドを参考にすることで、セキュリティやサイバー攻撃に対する業務プロセスや製品耐性を高めることができます。
https://www.vdma.org/viewer/-/v2article/render/16110956

この章では、XAEとXARに関連する脅威の例をいくつか列挙します。

7.1 eXtended Automation Engineering (XAE)

表 *1:* ソースコードの不正操作

対策	説明
技術的な対策	• 権限を定義し、ソフトウェア保護で実装する • バージョン管理システムを使用して、変更を追跡可能にする • バージョン管理システムに個別のアクセス制御を付与する
組織的な対策	• ITセキュリティマネジメントシステム（ISO27001など）を使用する • バージョン管理システムを使用する（参照：ソース管理）： • ステージングの手法を使用する： ◦ 最初に開発用ソース管理リポジトリにチェックインする ◦ アルファ版、ベータ版、RC版、リリース版をビルドするには、別の（リリース前の）ビルド・リポジトリを使用する ◦ 例えば、プロジェクト比較ツール（参照：プロジェクト比較ツール）などを使用して、レビュー後にのみ開発リポジトリを（リリース前の）ビルドリポジトリに転送する

表 *2:* ソースコードへの不正アクセス

対策	説明
技術的な対策	• ソフトウェア保護を使用してソースコードを暗号化して保存する（参照：ソフトウェア保護）
組織的な対策	• ITセキュリティ管理システム（ISO27001など）を使用する。 • 保管場所への安全なアクセス。 • 暗号化されたストレージを使用する。

7.2 eXtended Automation Runtime (XAR)

表 *3: ADS* または *Secure ADS* を介した不正アクセス

対策	説明
技術的な対策	Secure ADS を使用する（参照：Secure ADS）： • 定義されたリモートステーションのみオープン • ファイアウォールの制限 • 静的ルート • リモートステーションを不正操作から保護
組織的な対策	• Secure ADS経由のアクセスをOPC UA経由のアクセスに置き換える。

表 *4: ADS / Secure ADS*を介したリアルタイム制御

対策	説明
技術的な対策	Secure ADS を使用する（参照：Secure ADS）：

対策	説明
	• 定義されたリモートステーションのみオープン • ファイアウォールの制限 • 静的ルート • リモートステーションを不正操作から保護
組織的な対策	• Secure ADS経由のアクセスをOPC UA経由のアクセスに置き換える。

7.3 技術情報の詳細

本章では、TwinCATのセキュリティに関するリンク集をまとめています。各項目について詳しく説明したベッコフのドキュメントへのリンクです。選択されたドキュメントはガイドです。これは、最初に確認することを意図されたものであり、完全なものではありません。

TwinCAT全般	詳細情報
TwinCAT 3 Software Protection	https://infosys.beckhoff.com/english.php?content=../content/1033/tc3_security_management/index.html&id=355557539833111233
ADS	https://infosys.beckhoff.com/english.php?content=../content/1033/tc3_ads_intro/index.html&id=7262890787652929099
ADSの無効化	https://infosys.beckhoff.com/english.php?content=../content/1033/secure_ads/6917981195.html&id=5745105416081707706
Secure ADS	https://infosys.beckhoff.com/english.php?content=../content/1033/secure_ads/index.html&id=2501949194726739202
ADS over MQTT	https://infosys.beckhoff.com/english.php?content=../content/1033/tc3_ads_over_mqtt/index.html&id=120186874503837909

OPC UA	詳細情報
サーバーセキュリティ	https://infosys.beckhoff.com/english.php?content=../content/1033/tf6100_tc3_opcua/1448394251.html&id=2325029100913163478
IOクライアントセキュリティ	https://infosys.beckhoff.com/english.php?content=../content/1033/tf6100_tc3_opcua/1452984075.html&id=
PLCLib クライアントセキュリティ	https://infosys.beckhoff.com/english.php?content=../content/1033/tf6100_tc3_opcua/1452984075.html&id=7305736008379229744
ゲートウェイセキュリティ	https://infosys.beckhoff.com/english.php?content=../content/1033/tf6100_tc3_opcua/1452984075.html&id=954414165455750259

8 付録

8.1 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

8.2 注意事項

当社のSecurity Advisory（セキュリティ勧告）は、お客様がベッコフ産業用PCおよび組込み型PCを特定の影響から保護することを目的としています。以下の表は、セキュリティの脆弱性に関する勧告の概要と、ドキュメントをダウンロードするためのリンクです。

これらのセキュリティ勧告は、 RSSフィードとしても提供されています。また、ベッコフでは、他のメーカとともに、CERT@VDE の一環としてこれらの勧告を公開しています：https://cert.vde.com/de/advisories/vendor/beckhoff/

当社製品にセキュリティ上の脆弱性があると思われる場合は、に記載されている手順で当社までお知らせください。

番号	タイトル	バージョン	言語	ダウンロード	外部 CNA
2024-005	Local command injection via TwinCAT Package Manager	1.0	英語	PDF	HTML、CSAF
2024-004	Local Denial of Service issue in TwinCAT/BSD "MDP" package	1.0	英語	PDF	HTML、CSAF
2024-003	Local Denial of Service issue in TwinCAT/BSD package "IPC-Diagnostics"	1.0	英語	PDF	HTML、CSAF
2024-002	Improper neutralization of input in TwinCAT/BSD package "IPC-Diagnostics-www"	1.0	英語	PDF	HTML、CSAF
2024-001	Local authentication bypass in TwinCAT/BSD package "IPC-Diagnostics"	1.0	英語	PDF	HTML、CSAF
2023-001	Open redirect in TwinCAT/BSD package "authelia-bhf"	1.0	英語	PDF	HTML
2022-001	Null Pointer Dereference vulnerability in products with OPC UA technology	1.0	英語	PDF	HTML
2021-003	Relative path traversal vulnerability through TwinCAT OPC UA Server	1.0	英語	PDF	HTML
2021-002	Stack Overflow and XXE vulnerability in various OPC UA products	1.0	英語	PDF	HTML
2021-001	DoS Vulnerability for TwinCAT OPC UA Server and IPC Diagnostics UA Server	1.2	英語	PDF	HTML

番号	タイトル	バージョン	言語	ダウンロード	外部 CNA
2020-003	Privilege Escalation through TwinCAT System Tray (TcSysUI.exe)	1.1	英語	PDF	HTML
2020-002	EtherLeak in TwinCAT RT network driver	1.1	英語	PDF	HTML
2020-01	BK9000 couplers – Denial of service inhibits function	1.0	英語	PDF	HTML
2019-07	Denial-of-Service on TwinCAT using Profinet protocol	1.1	英語	PDF	HTML
2019-06	CE Remote Display behaves incorrectly with wrong credentials	1.2	英語	PDF	
2019-05	Remote Code Execution in Remote Desktop Service ("Dejablue")	1.0	英語	PDF	
2019-04	ADS Discovery	1.1	英語	PDF	
2019-03	Remote Code Execution in Remote Desktop Service	1.4	英語	PDF	
2019-02	Microarchitectural Data Sampling (MDS) vulnerabilities	1.2	英語	PDF	
2019-01	Spectre-V2 and impact on application performance as well as TwinCAT compatibility	1.4	英語	PDF	
2018-02	Updates for OPC-UA components (Several Vulnerabilities)	1.0	英語	PDF	
2018-01	TwinCAT 2 and 3.1 Kernel Driver Privilege Escalation	1.1	英語	PDF	
2017-02	Add Route using "Encrypted Password" bases on fixed key	1.3	英語	PDF	
2017-01	ADS is only designed for use in protected environments	1.4	英語	PDF	
2015-001	Potential misuse of IPC Diagnostics version < 1.8 backend	1.1	英語	PDF	
2014-003	Recommendation to change default passwords	1.1	英語	PDF	
2014-002	ADS communication port allows password bruteforce	1.1	英語	PDF	
2014-001	Potential misuse of several administrative services	1.1	英語	PDF	

8.3 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。

ダウンロード検索

ダウンロード検索 から当社が提供する各種ファイルをダウンロードいただけます。アプリケーションレポート、技術マニュアル、図面、Configurationファイルなど、必要なファイルを検索してダウンロードできます。

様々なファイル形式でダウンロードできます。

ベッコフの支社と代理店

ベッコフ製品に関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。

各国のベッコフ支社および代理店の所在はベッコフWebサイト(http://www.beckhoff.com/ja-jp)よりご確認いただけます。

また、Webサイトではベッコフ製品マニュアルも公開されています。

ベッコフのサポート

ベッコフのサポート部門はベッコフ製品に関するお問い合わせの他、各種の技術サポートを提供しています。

- サポート
- 複雑な自動化システムの設計、プログラミングおよびコミッショニング
- およびベッコフの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 5246 963-157
Eメール: support@beckhoff.co.jp

ベッコフのサービス

ベッコフのサービスセンターは、各種のアフターサービスを提供することでお客様をサポートします。

- オンサイトサービス
- 修理サービス
- 部品交換サービス
- 緊急サービス

ホットライン: +49 5246 963-460
Eメール: service@beckhoff.co.jp

ベッコフ本社

Beckhoff Automation GmbH & Co. KG

Huelshorstweg 20
33415 Verl
Germany

電話: +49 5246 963-0
Eメール: info@beckhoff.com
Webサイト: www.beckhoff.com

表の一覧

図の一覧

Trademark statements

Beckhoff®, TwinCAT®, TwinCAT/BSD®, TC/BSD®, EtherCAT®, EtherCAT G®, EtherCAT G10®, EtherCAT P®, Safety over EtherCAT®, TwinSAFE®, XFC®, XTS® and XPlanar® are registered trademarks of and licensed by Beckhoff Automation GmbH.

Third-party trademark statements

FreeBSD is a registered trademark of The FreeBSD Foundation and is used by Beckhoff with the permission of The FreeBSD Foundation.

The registered trademark Linux® is used pursuant to a sublicense from the Linux Foundation, the exclusive licensee of Linus Torvalds, owner of the mark on a worldwide basis.

UNIX is a registered trademark in the United States and other countries, licensed exclusively through X/Open Company Limited.

詳細はこちら:
www.beckhoff.com/TwinCAT-BSD

Beckhoff Automation GmbH & Co. KG
Hülshorstweg 20
33415 Verl
Germany
+49 5246 9630
info@beckhoff.com
www.beckhoff.com