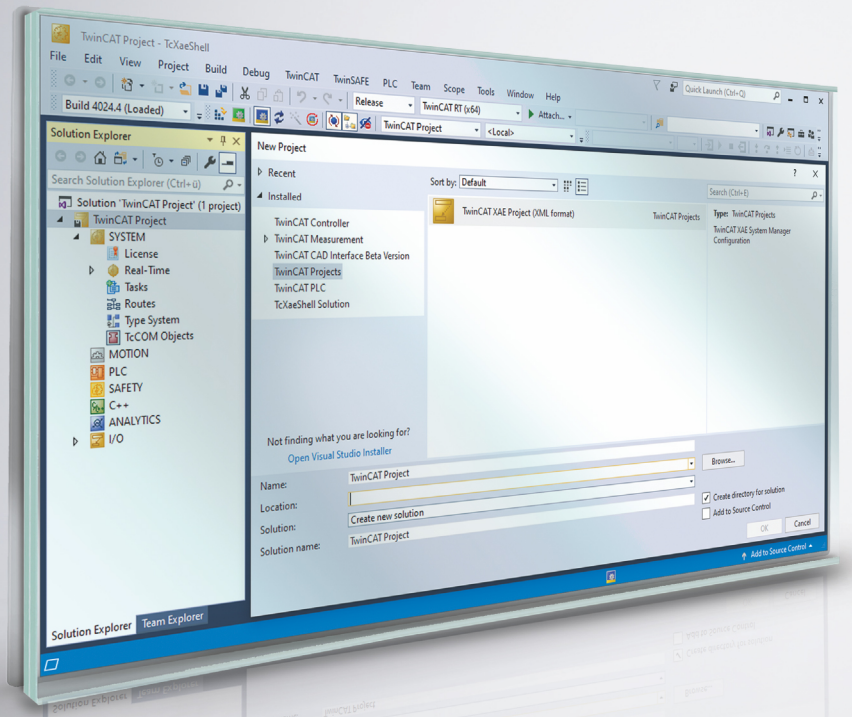
BECKHOFF New Automation Technology

取扱説明書 | JA

IPCセキュリティガイドライン

Windows 10



2025-04-22 | 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 [▶ 56]。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 [▶ 16]）
- ブートメディアの設定 (BIOS設定 [▶ 16])
- 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 [▶ 16])

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:

- 自動起動の無効化 (自動起動 [▶ 38])
- USBデバイスのホワイトリスト化 (USBフィルター [▶ 49])
- 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 [▶ 16])
- プログラムのホワイトリスト化 [▶ 32]

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 [▶ 21]
- 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:

- ファイルの暗号化 [▶ 20]
- 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:

- ファイルの暗号化 [▶ 20]
- 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 [▶ 17])
- プログラムのホワイトリスト化 [▶ 32]

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:

- Windows Update（アップデート [▶ 17]）
- 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 [▶ 17])
- 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 [▶ 37]

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 [▶ 17])
- 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 [▶ 37]

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。

完全なハードディスク上のデータは、特別なソフトウェアを使用して上書きすることにより、完全に復元不可能に消去できます。データは、指定された文字または乱数で1回または数回上書きされ、ほとんどの場合はこれで十分です。

Windowsは "低速 "フォーマット時には、パーティションをゼロで完全に上書きするようになりました。古いハードディスク（80GB未満）の場合は、データを7回上書きする必要があります。最近のハードディスクでは、ATA-"Enhanced Security Erase "コマンドを使用できます。ここでは、欠陥のあるメモリ領域を含むハードディスク全体を消去する、ベンダー固有のルーチンが開始されます。この消去方法は、SSD または SSHD で推奨されます。このコマンドは、前述の上書き手順と組み合わせる必要があります。データキャリアは上書き後も使用可能です。

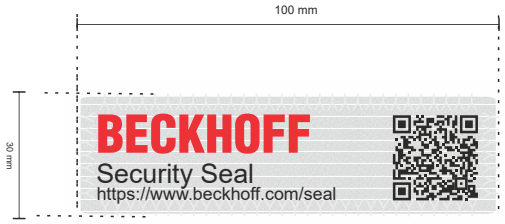
前述の上書き方法を実行するために、市場では無料と有料の両方のソフトウェアが提供されています。これらのツールのほとんどは、異なる上書き方法を提供しています。ブート可能なメディア（CDやUSBフラッシュドライブなど）から起動し、ハードディスク全体を上書きできるプログラムの使用をお勧めします。

物理的破壊

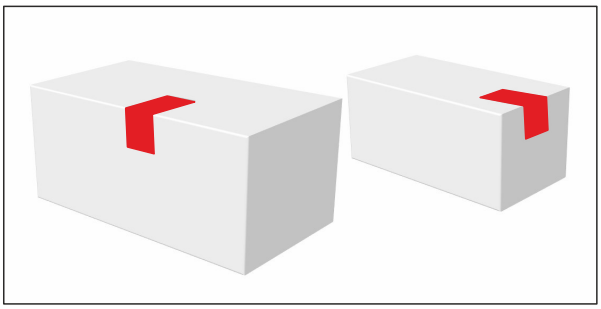
ハードディスクを上書きしたくない場合、あるいは欠陥のために上書きできない場合は、ハードディスクを物理的に損傷させるか破壊してください。

3.4 製品パッケージのセキュリティシール

2021年末からは、工場で産業用PCや組込み型PCの一部の製品パッケージにセキュリティ機能を備えたシールが貼付されます。



シールの貼付位置と性質により、商品をパッケージから取り出すと、パッケージおよびシールに不可逆的で明確な変化が生じるようになっています。そのため、パッケージ開封前に、目視で製品が未開封であることを確認できます。



シールは、梱包された製品を効率的にチェックするためのものです。絶対的な安全は不可能であるため、シールは以下を確認するための用途に限定されます：パッケージを開封することなく、梱包内の商品が無傷であること、完全な状態であること、純正であることを正しく証明する。シールまたは包装が破損している場合、受領者は、商品の受領または使用に際し、商品の状態に問題がないかを確認する必要があります。商品がITセキュリティに関わる用途を意図している場合、配送中のシールや包装の状態から製品に改ざんが疑われる場合、受領者は使用前に商品が改ざんされていないか確認するよう促すなど対策を講じてください。

ベッコフ製品の受領および使用に関する有意義なプロセスおよび、ルールの規定は、受領者の側の責任となります。

開封済みシール

ベッコフの製品は、多くの場合、複数の流通経路を経てユーザに届きます。製品の配送処理中にシールが開封される可能性があります。開封済みシールは保証請求の理由にはなりません。

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 バックアップ生成と復元

各デバイスごとにバックアップの生成と復元の対策を講じ、次のような事態から保護されるようにしてください：

- セキュリティインシデント
- 記憶媒体の欠陥によるデータの損失
- または不適切なシャットダウンによるデータの破損

最新のバックアップデータを最短時間で復元することにより、ダウンタイムを最小限に抑えることができます。バックアップ生成とは別に、復元手順を定義しておくことも重要です。

バックアップ生成と復元は、セキュリティに限った問題ではありませんが、セキュリティインシデントの際のダウンタイムを最小限に抑えるのに役立ちます。

安全なコピーを生成する手順と、それを復元する手順の両方を定義する必要があります。その際、セキュリティ面も考慮する必要があります。

完全に自動化されたバックアップソリューションを使用する場合、バックアップシステム自体がネットワーク上でアクセス可能であるため、脆弱性があります。このため、マニュアル作業（オフライン）によるバックアップがより良い選択肢となります。オフサイトのバックアップ、つまりローカルで隔離して保存されるバックアップデータは、機械自体に影響がないローカルインシデントの場合に復元できるメリットがあります。

このように、多種多様な実装方法を考慮できます。

TwinCATブートプロジェクトと全ての必要な情報は、各オペレーティングシステムのファイルシステム上に保存されるため、この場合はファイルベースのセキュリティで十分です。

ベッコフでは、Beckhoff Service Tool（BST）という形式でバックアップ生成と復元のためのソリューションを提供しています。BSTの詳細については、こちらを参照ください：Infosys Beckhoff Service Tool（BST)マニュアル

ご使用の産業用PCがシステムパーティションのBitLocker暗号化を有効にして出荷されている場合、自動ブート中にパーティションを復号化するキーは、デバイスのメインボード上のTrusted Platform Module (TPM)によって保護されます。初期起動プロセスの監視によって、既知のコンフィギュレーションを持つ以前に信頼されたソフトウェアが起動されたことを確認し、ソフトウェアも、コンフィギュレーションも、次に起動されるソフトウェア（つまりカーネル）も操作されていないことが確認された場合のみ、TPMモジュールがWindowsカーネルに復号化のためのキーを提供します。

完全なバックアップデータには、ブートパーティションとシステムパーティションを含める必要があります。ブートディスク全体をRAWデバイスとしてバックアップした場合、バックアップデータには暗号化されたシステムパーティションが含まれます。バックアップデータに加えて、回復キーも必ずエクスポートしてください。回復キーは、バックアップデータを別のハードウェアに復元して使用する場合に必要となります。回復キーは安全な場所に保管してください。また、初期起動プロセスを構成するソフトウェアやコンフィギュレーションに正当な変更が加えられた場合に備えて、回復キーを常に手元に置いておくことを強く推奨します。これは例えば、管理者によってファームウェア（BIOS）のブートシーケンスが変更された場合などに想定されます。

BitLocker 暗号化が有効な場合、暗号化されたシステムパーティションを含む完全なバックアップデータの代わりに、システムパーティションの暗号化を一時的に無効にして、通常通りオフラインのバックアップデータを作成する方法があります。バックアップ完了後、暗号化を再び有効化することを忘れないでください。

5.2 アップデート

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。

- イメージ全体のアップデート

- 個々のプログラムのアップデート
- 内蔵OSのアップデート

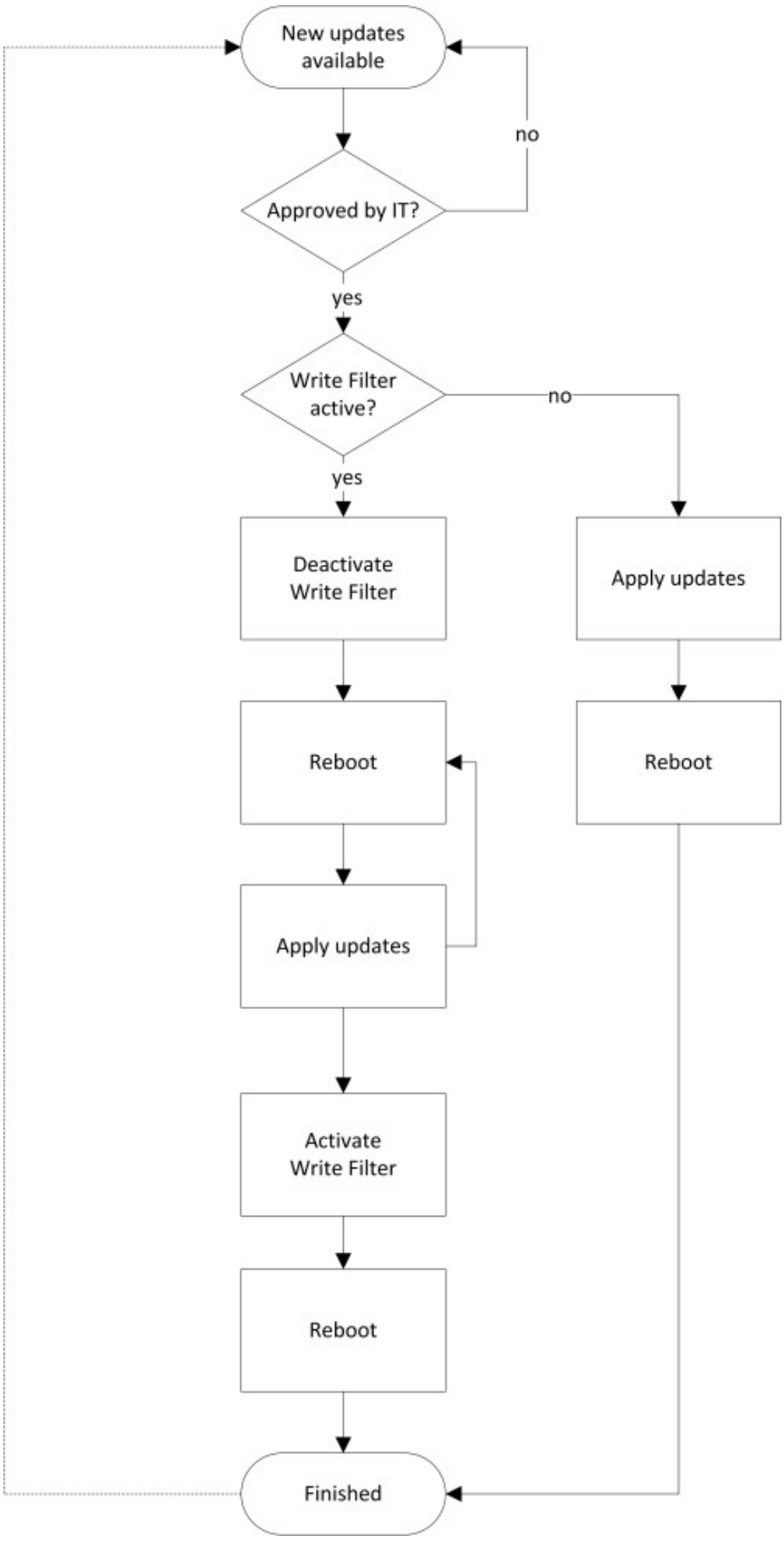
注記

データ損失の回避

アップデートを実行する前に、データをバックアップしてください。まず、BST（Beckhoff Service Tool）を使用してPCのバックアップイメージを作成します。https://www.beckhoff.de/default.asp?industrial_pc/bst.htm

Windows 7/10オペレーティングシステムには、Windows Updateサービスという独自のアップデートメカニズムがあります。システムに不用意に変更が加えられるのを防ぐため、ベッコフが提供するイメージではWindows Updateサービスは無効になっています。Windows Updateは、マイクロソフトからダウンロードして手動でインストールすることもできます。Windows アップデートサービスが有効になっている場合、アップデートプログラムはMicrosoft Windows Updateサーバーから標準設定で取得されます。サーバーとの通信は、暗号化され署名された接続を介して行われます。取得されたアップデートはマイクロソフトの公式証明書で署名され、その信憑性をチェックできます。

開発用PCは、アップデート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、Writeフィルターを使用している場合、対策を講じずに実行されたアップデートが、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。ベッコフのデバイスは、半年ごとにアップデートされ、Windows Updateを含む互換性のあるテスト済みイメージとともに提供されます。

これらWindows 7/10のイメージは、ベッコフサービスにリクエストできます。これには、デバイスのシリアル番号が必要です。

以下も参照してください。

- https://www.beckhoff.de/default.asp?industrial_pc/bst.htm

5.3 ファイルの暗号化

注記

誤動作

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、誤動作が発生する可能性があります。

原則としては、機密性の高いファイルやディレクトリを不正アクセスから保護するには、アクセスの制御を確立することで十分です。しかし、データキャリアを紛失した場合には、これらデータの保護は保証されなくなり、個々のファイルやディレクトリの暗号化による追加の保護が必要になります。

Windowsは、EFS（暗号化ファイルシステム）により、個々のファイルやディレクトリ全体を暗号化する機能を提供します。これにより、追加のセキュリティレベルと暗号化による保護が利用できます。

暗号化した場合には、キーの管理と以下の点を明確にしておくことが重要です：

- アクセス権を誰に付与すべきか
- どのような認証オプションがあるか (USBトークン、PIN、パスワード、ユーザ名とパスワード、など)
- キーの管理方法

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。

それと比較して、BitLockerはデータキャリアの完全な暗号化をサポートします。さらに、BitLocker はTPM(Trusted Platform Module) と併用することで、最大限の保護を提供します。詳細は以下に記載されています。TPM documentation

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 [▶ 20]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。

5.4 ユーザおよび権限管理

5.4.1 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#

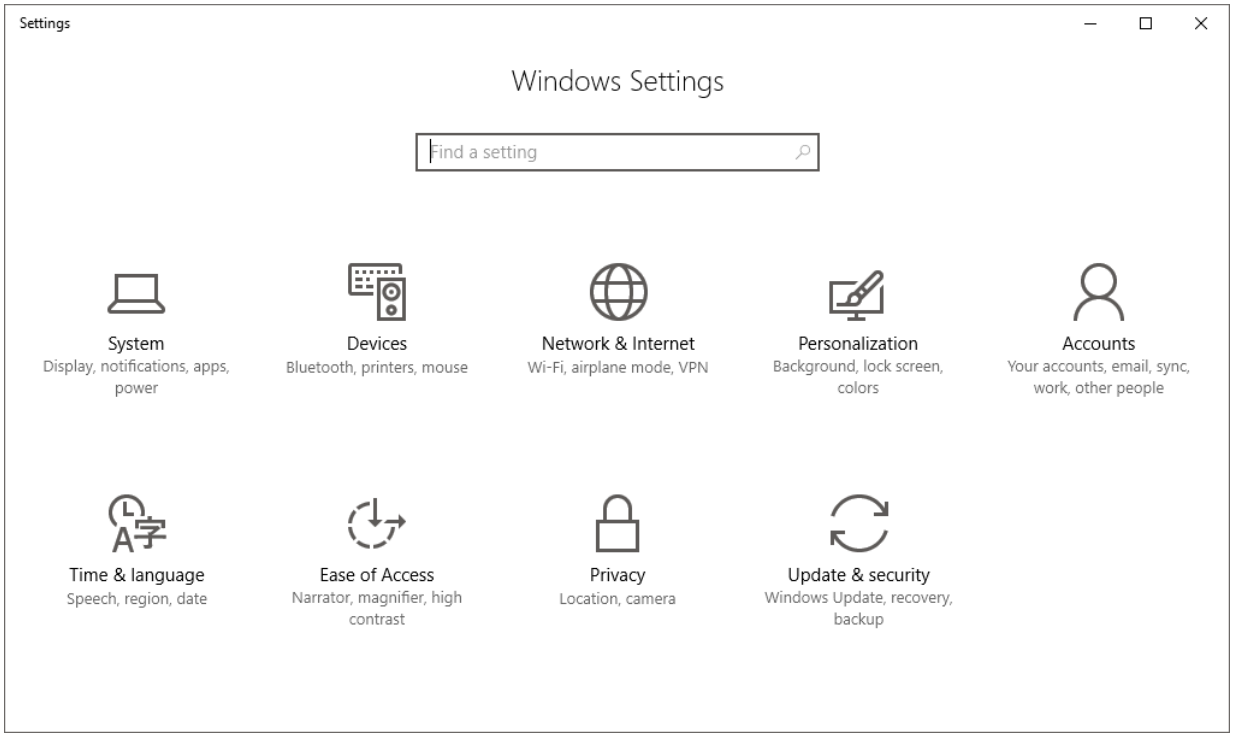
問題のあるパスワード

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。

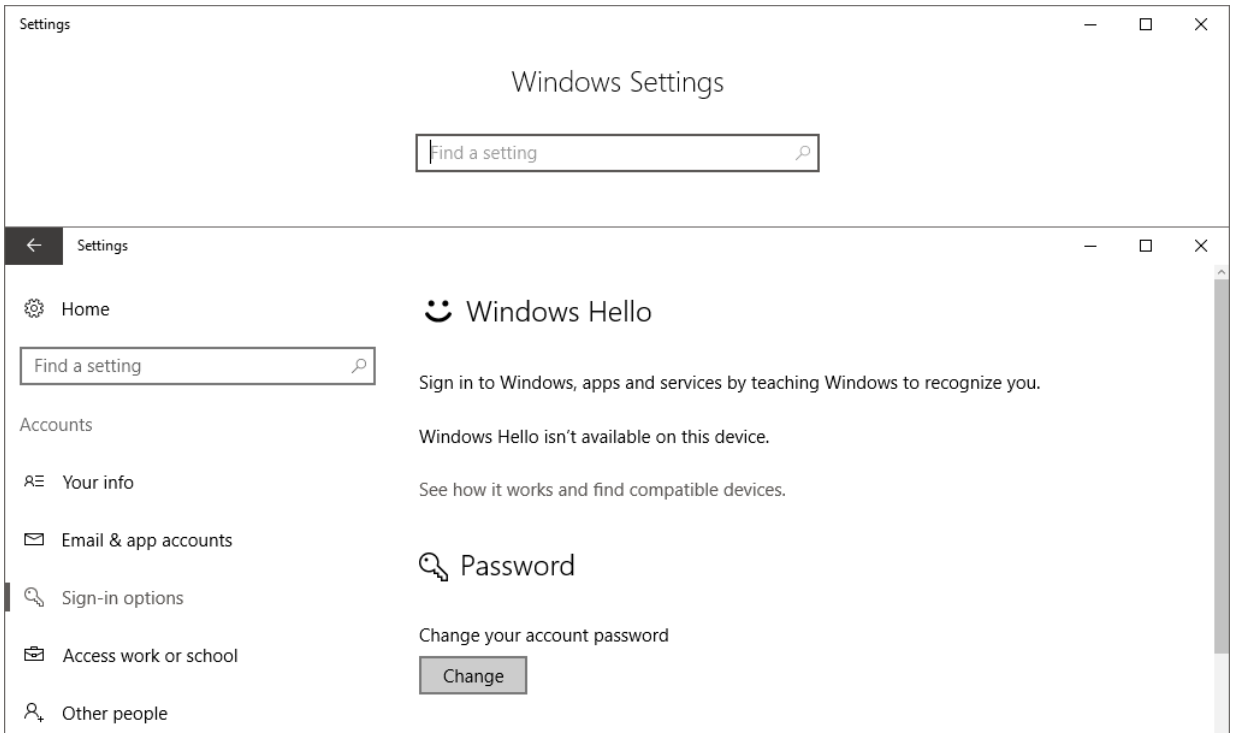
- 辞書に含まれる単語
- スペルを逆にした単語、一般的なスペルミスや略語
- 12345678やabcdefghなどの反復文字列
- 誕生日、ID番号、電話番号などの個人情報

5.4.1.1 パスワードを変更する

1. 設定を開き**Accounts**をクリックします。



2. **Sign-in options**を選択し、パスワードエリアで**Change**をクリックします。



3. 現在のパスワードを入力してください。

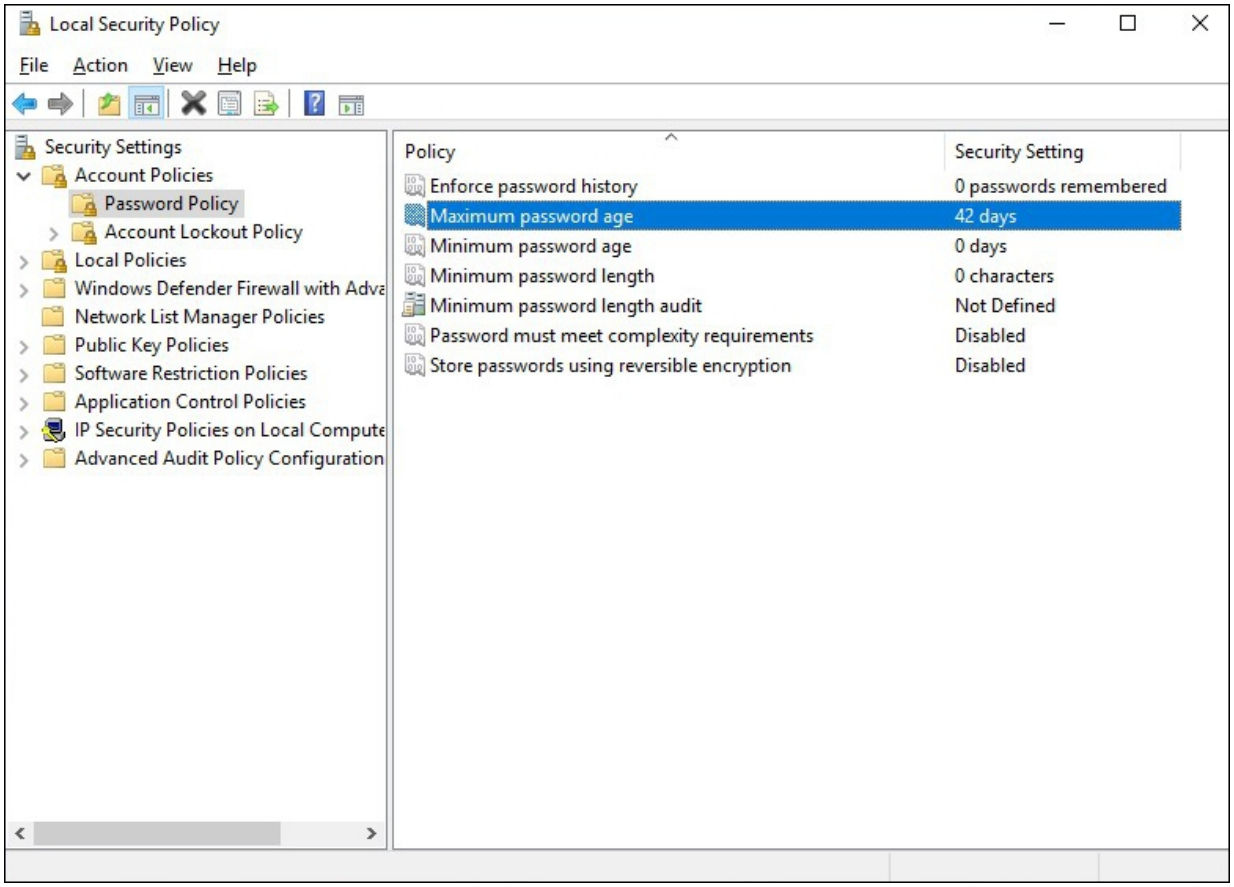
4. 新しいパスワードを入力してください。

⇨ パスワードはリセットされました。

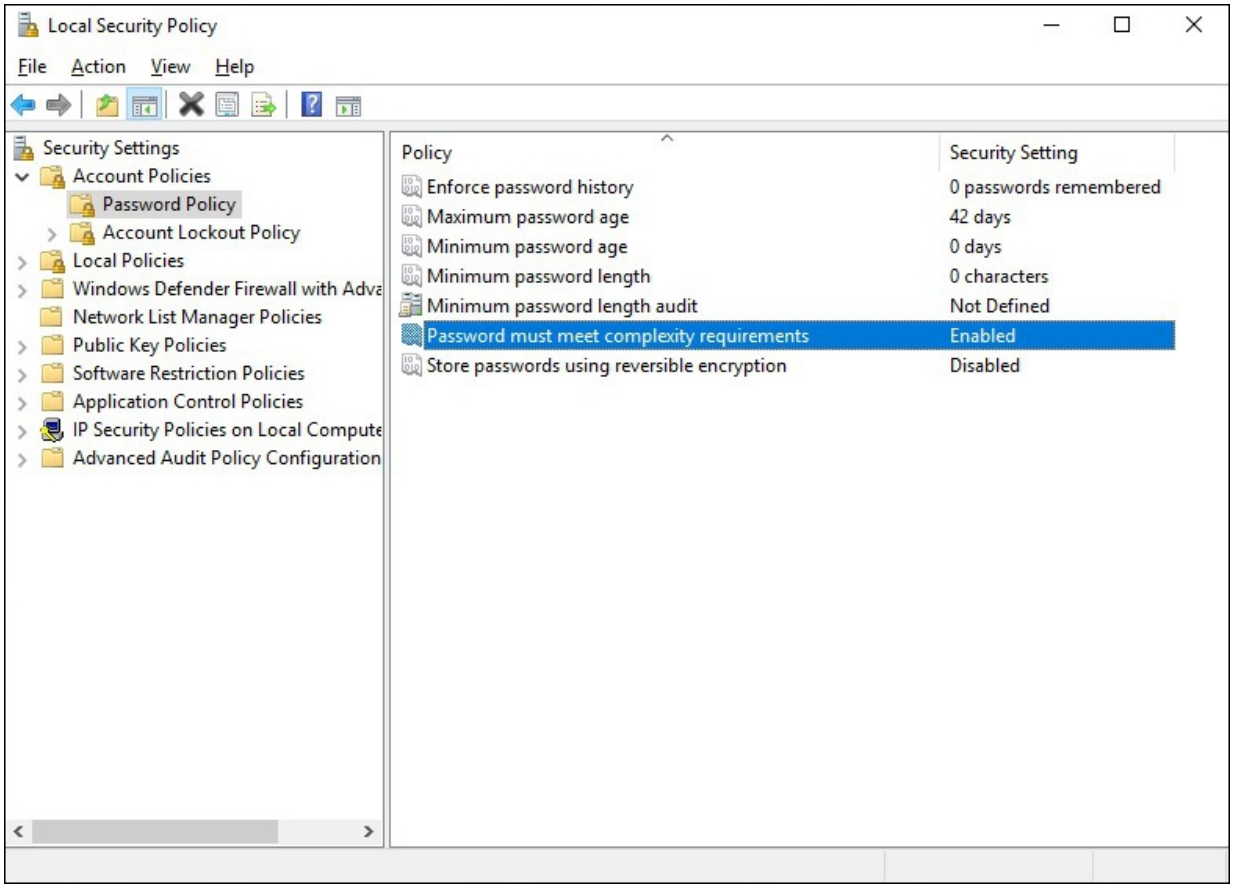
5.4.1.2 パスワードポリシー

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、ユーザに安全なパスワードを選択させることが可能になります。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ます。

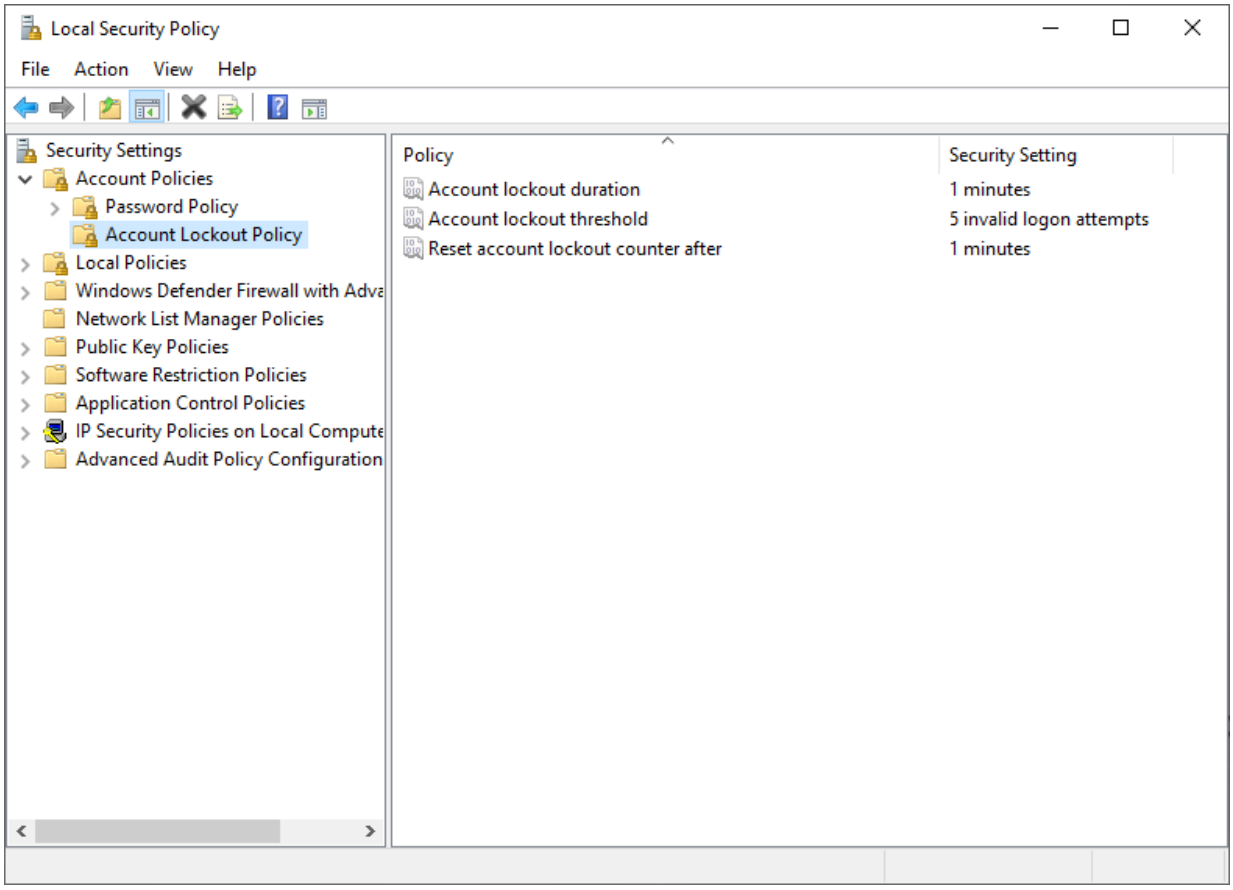
1. **Control Panel**を開き、**Administrative Tools > Local Security Policy**を選択します。
2. 開いたウィンドウ内で、**Account Policies > Password Policy**を選択します。
3. パスワードポリシーを設定します。
4. 最大のパスワード有効期限を設定するには、システムがユーザにパスワードの変更を促すまでの期間（日単位）をポリシーの**Maximum password age**から定義します。



5. パスワードの複雑さを要求するために、**Password must meet complexity requirements**のポリシーを設定できます。このポリシーを有効にすると、以降設定されるパスワードは、少なくとも大文字、小文字、数字、特殊文字を含む必要があります。



6. ユーザ認証データを推測する攻撃を防ぐために、**Account Lockout Policy**から設定を行うことができます。ログインに失敗した回数に応じてユーザアカウントをロックアウトする設定をします。**Account lockout duration**ポリシーを使用して、ロックされたアカウントが自動的にロック解除されるまでの期間を分単位で設定できます。



⇨ パスワードポリシーの定義

5.4.1.3 IPCセキュリティウィザード

ユーザパスワードは、IPC診断のウェブページから設定できます。httpsのPort443からアクセスできます。

初期納入状態では、ユーザが httpsから接続するか、デバイスでローカル作業する場合にIPCセキュリティウィザードが起動します。

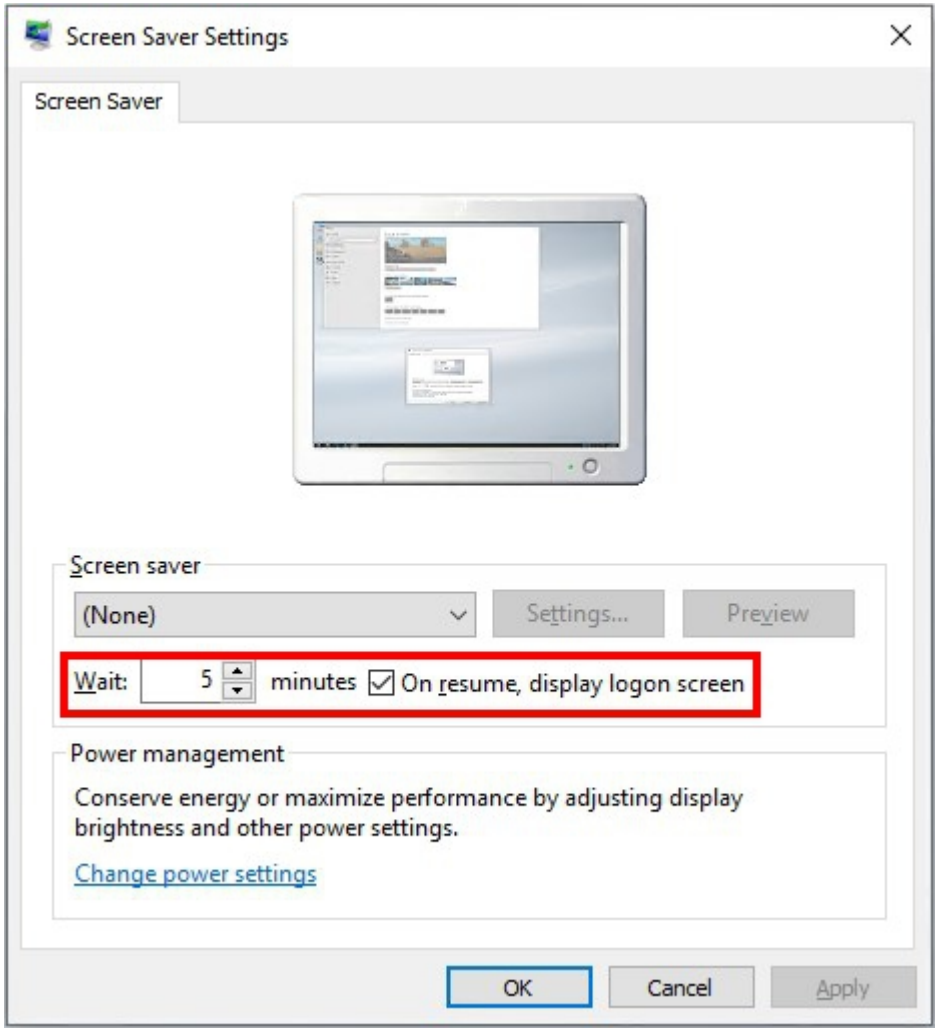
IPCセキュリティウィザードは、デフォルトのパスワードを変更するようユーザに促します。

以下も参照してください。

- Information SystemのIPC診断マニュアル

5.4.2 自動ログアウト

すでにログオンしているユーザがしばらく使用していないときにシステムが悪用されないように、ユーザの自動ログアウトを設定できます。これを行うには、スクリーンセーバーの設定で時間を定義します。設定した時間が経過すると、未使用のシステムはロックされ、ユーザは再度認証する必要があります。



5.4.3 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。

マイクロソフトは、関連する設定とベストプラクティスを掲載したWindowsのセキュリティ監査ガイドを発表しました。基本的な監査ポリシーには以下のカテゴリがあります。これらはデフォルトでは無効になっていますが有効化できます：

- アカウントのログオンイベントの監査 [▶ 27]
- ディレクトリサービスへのアクセスを監査 [▶ 28]
- ログオンイベントの監査
- オブジェクトへのアクセスを監査

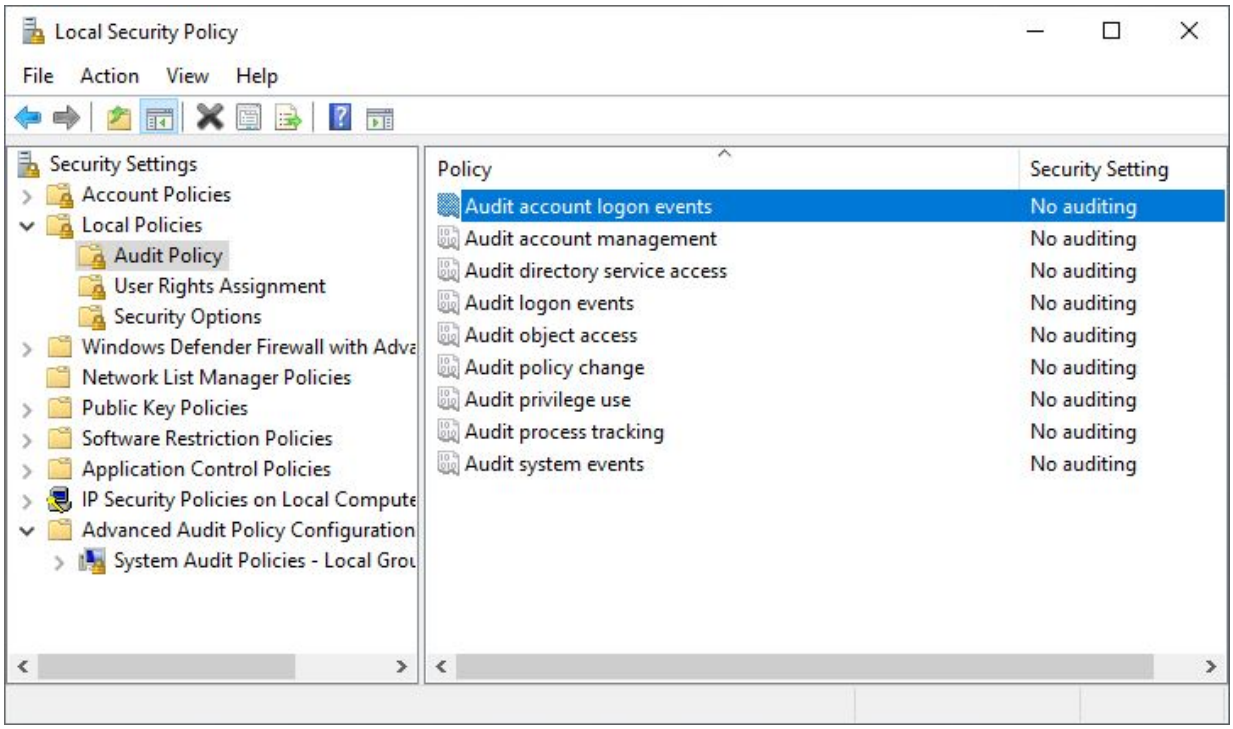
- ポリシーの変更を監査
- 特権使用の監査
- 監査プロセスの追跡
- システムイベントの監査

5.4.3.1 アカウントのログオンイベントの監査

誰がどのIPアドレスからWebインターフェースにログオンしたかを確認したい場合などに、Beckhoff Device Managerでログオンイベントを監査し、適切なポリシーを有効にします。

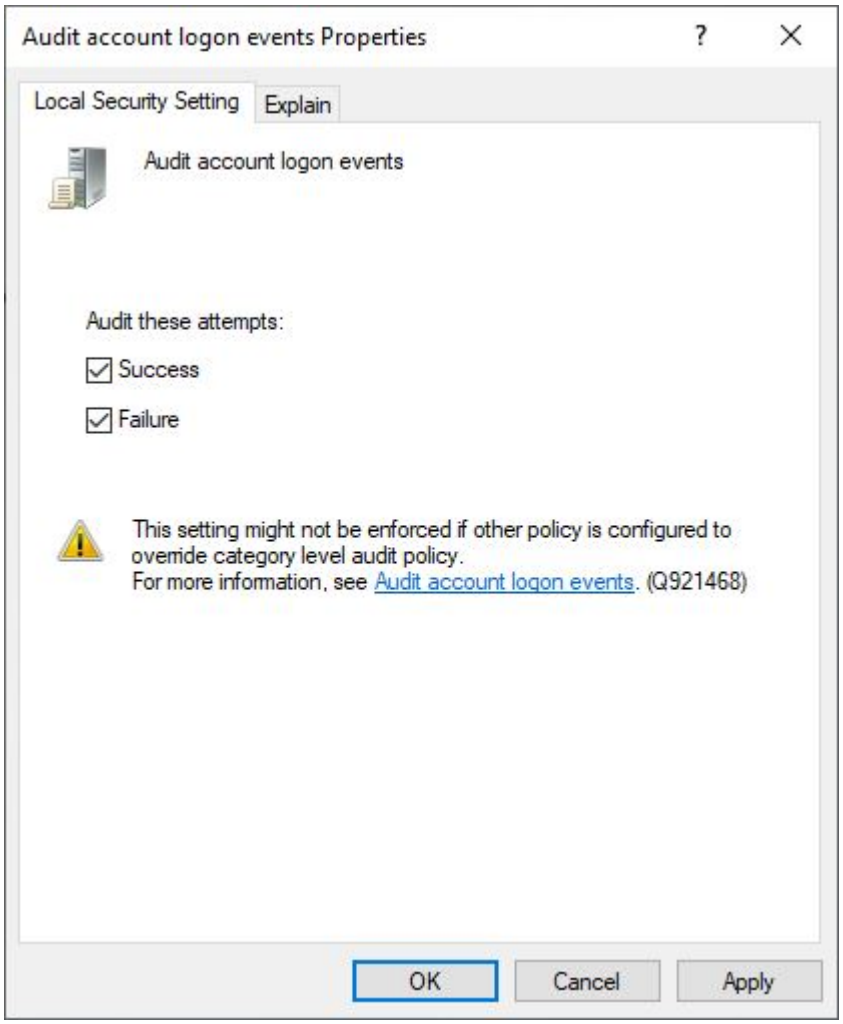
以下の手順に従ってください。

1. ショートカット**[Windows キー] + [R]**で実行ダイアログを呼び出し、**secpol.msc** と入力します。**Local Security Policy**のウィンドウが表示されます。



2. 左側の構造ツリーで、**Local Policies > Audit Policy**をクリックし、**Audit account logon events**のポリシーを選択します。

3. 失敗した試行のログのみを記録する場合は、**Failure**のチェックボックスを選択します。成功した試行もログに記録したい場合は、**Success**のチェックボックスも選択します。



⇨ **[Windowsキー] + [R]**でダイアログを呼び出し、**eventvwr**と入力すると、**Event Viewer**からログに記録されたエントリを表示できます。このエントリーは、**Windowsログ > Security**から確認できます。

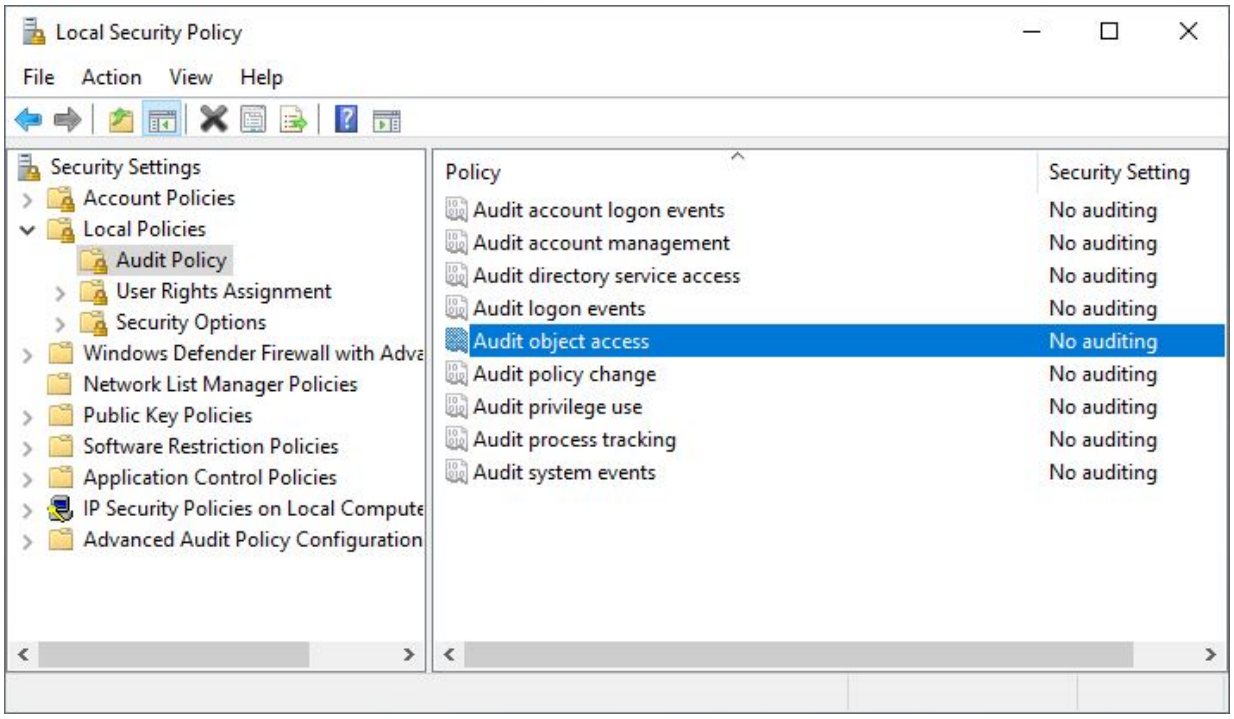
5.4.3.2 ディレクトリサービスへのアクセスを監査

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。

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。

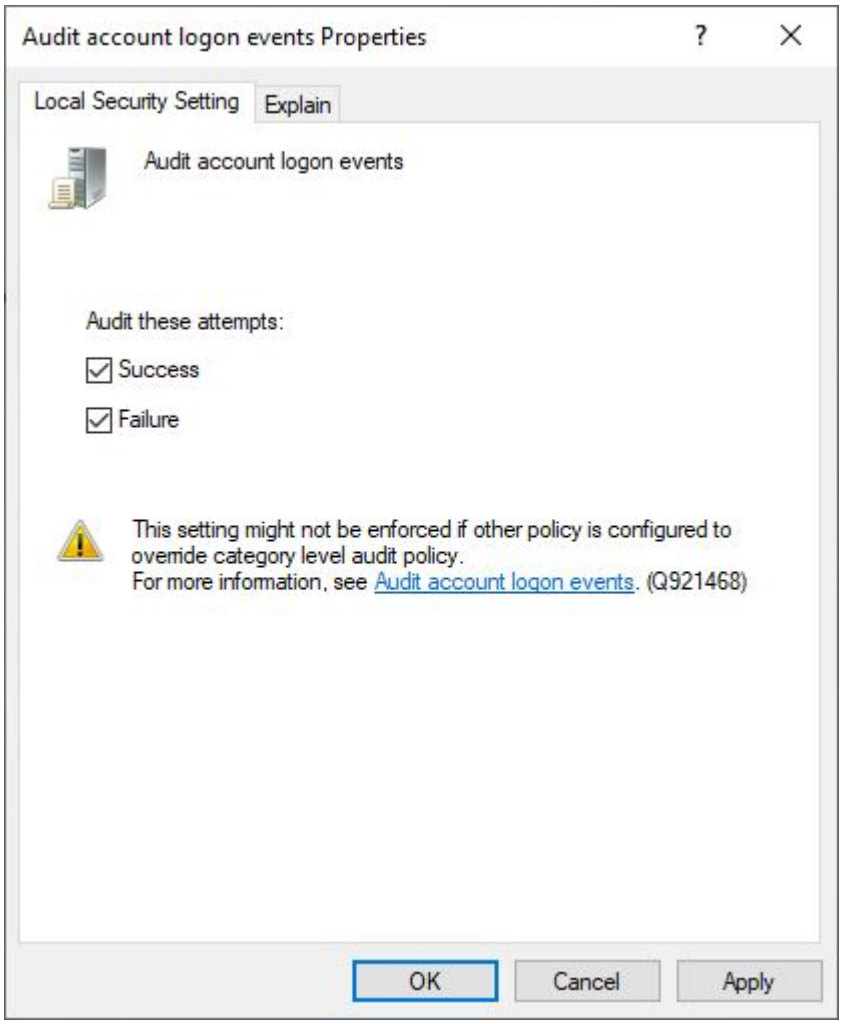
ファイルとフォルダアクセスの監査ポリシーを作成：

1. ショートカット**[Windows キー] + [R]**で実行ダイアログを呼び出し、**secpol.msc** と入力します。**Local Security Policy**のウィンドウが表示されます。



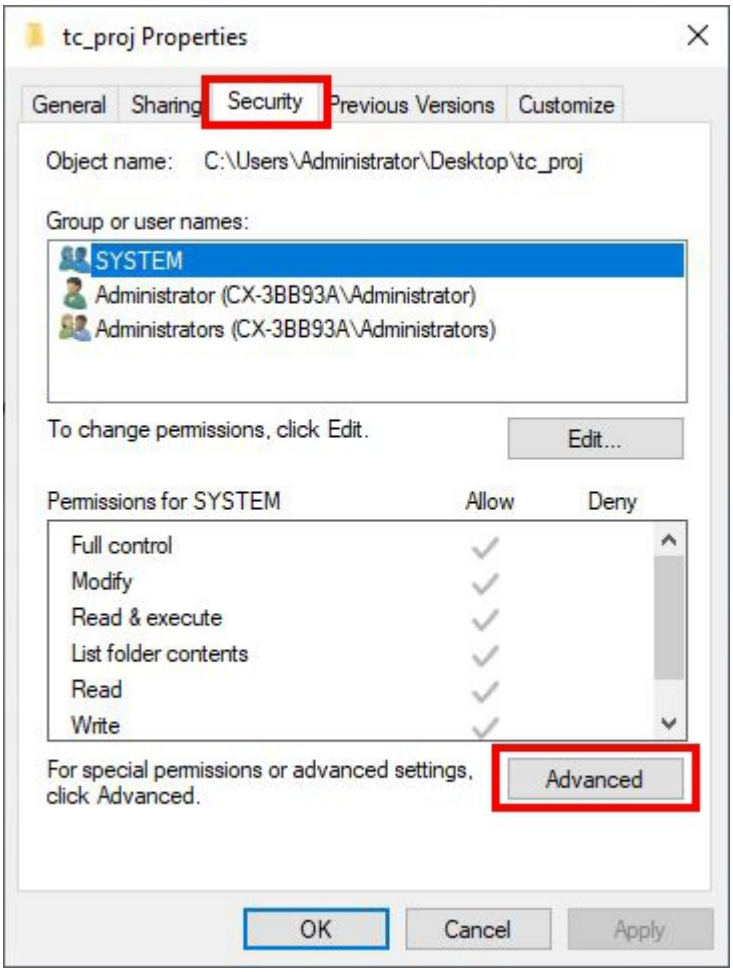
2. 左側の構造ツリーで **Local Policies > Audit Policy**をクリックし、**Audit object access**のポリシーを選択します。

3. 失敗したアクセスのみを記録する場合は、**Failure**のチェックボックスを選択します。成功したアクセスも記録したい場合は、**Success**のチェックボックスも選択します。

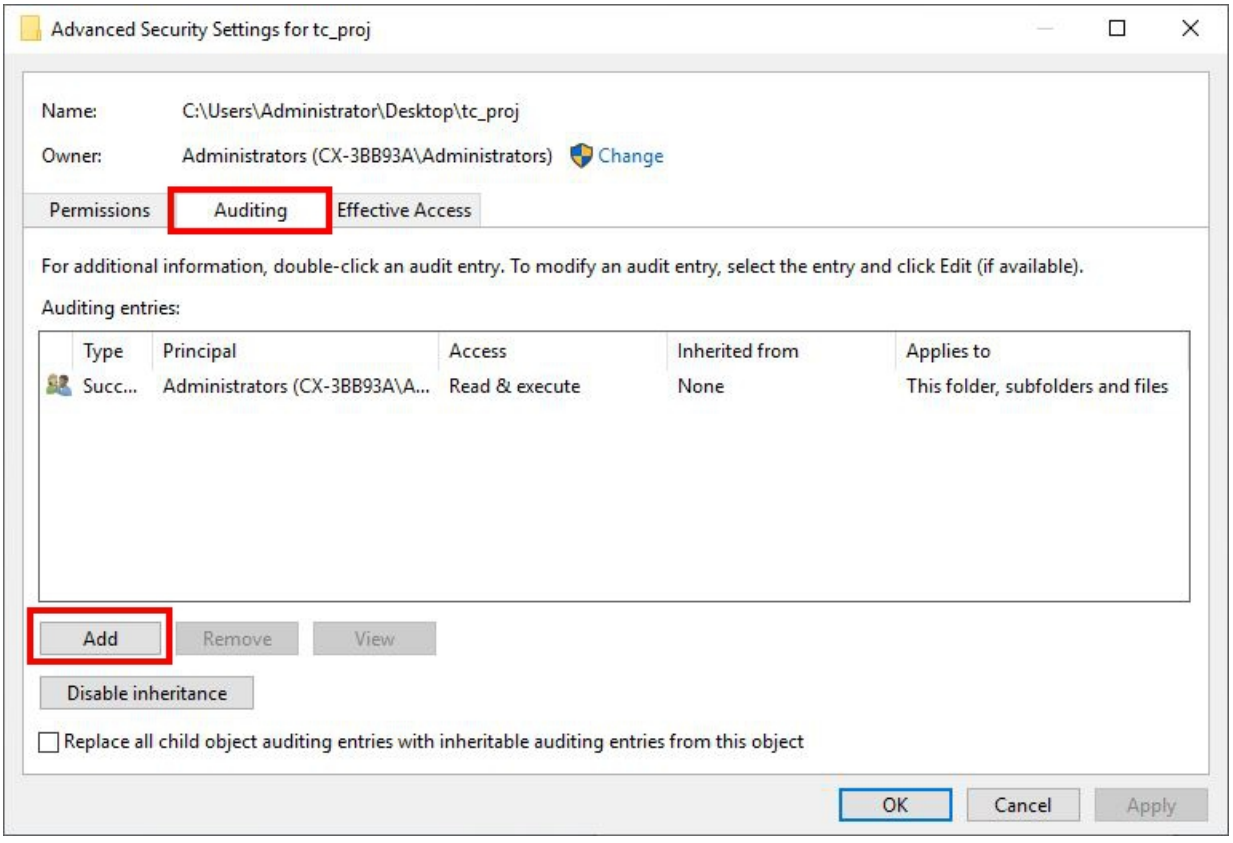


4. 該当するファイルまたはフォルダを右クリックし、**Properties**を選択します。

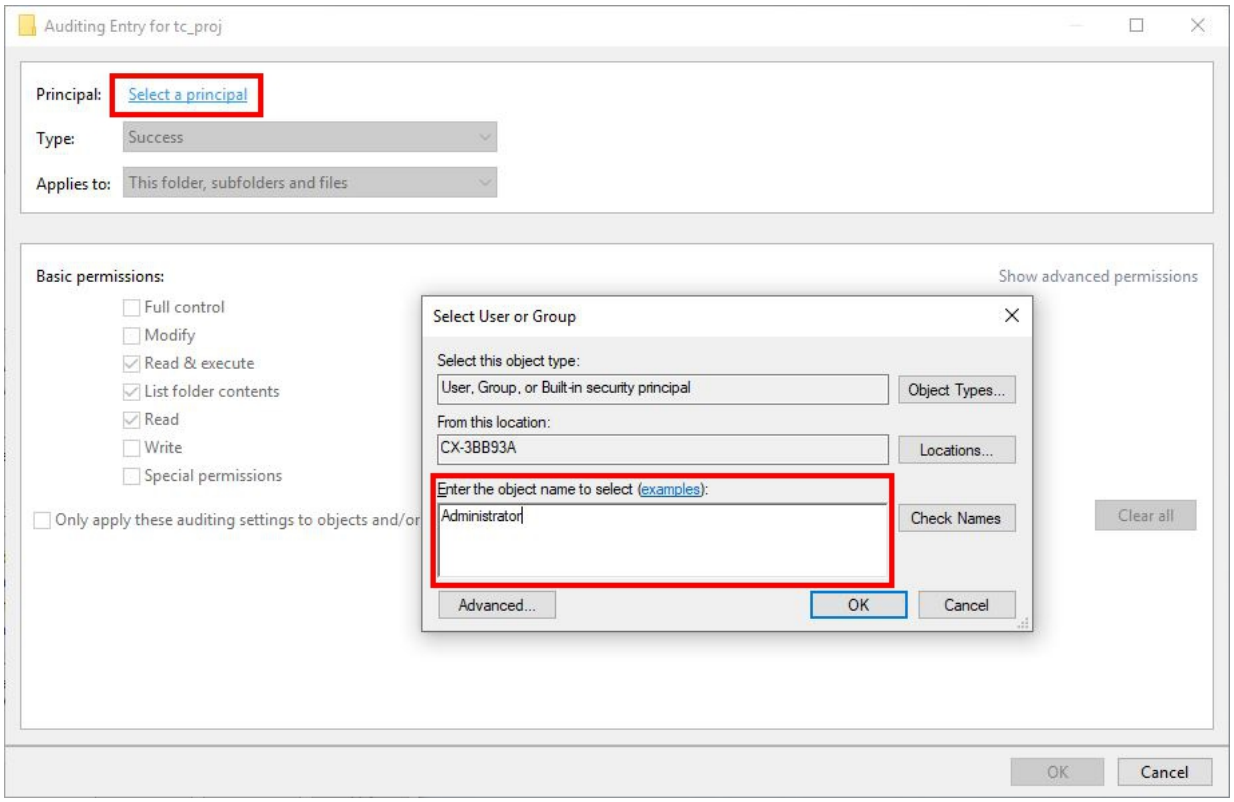
5. **Security**タブを選択し、**Advanced**をクリックします。



6. **Auditing**タブを選択し、**Add**をクリックして監査用の新しいエントリを作成します。



7. ユーザまたはグループの監査を設定するには、希望するユーザまたはグループの名前を入力し、**OKを**選択します。



8. **[Windowsキー] + [R]**でダイアログを呼び出し、**eventvwr**と入力すると、**Event Viewer**からログに記録されたエントリを表示できます。このエントリーは、**Windowsログ > Security**から確認できます。

5.5 プログラム

5.5.1 プログラムのホワイトリスト化

アプリケーションのホワイトリストは、システムで承認されていない全てのプログラムの実行を防止します。ホワイトリストにより、管理者はシステムが実行を許可する承認済みアプリケーションのリストを作成します。ウイルス対策ソフトウェアとは異なり、現在のセキュリティホールを塞ぐための継続的なアップデートは必要ありません。新しいアプリケーションが追加されたときだけ、リストを拡張する必要があります。産業界では、このリストの方がウイルス対策ソフトよりも多くの場合、保守しやすいとされています。Windows10に内蔵されている機能はAppLockerと呼ばれます。

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では、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。

5.5.1.1 ソフトウェア制限ポリシー(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。

ルールの種類	説明
Hash Rule	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 アップデートについては、これらのハッシュ規則をアップデート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。

以下の手順は、Windows 10のキオスクモードを設定するのに役立ちます：

https://docs.microsoft.com/en-us/windows/configuration/lock-down-windows-10-applocker

マイクロソフト社による一般的な導入ガイドは、こちらをご覧ください：

https://docs.microsoft.com/de-de/windows/security/threat-protection/windows-defender-application-control/applocker/applocker-policies-deployment-guide

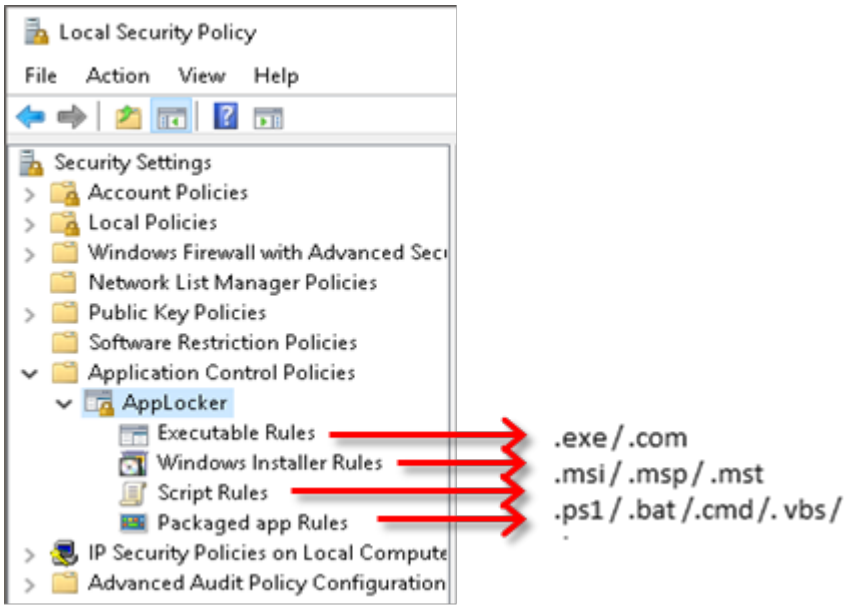
以下も参照してください。

- AppLocker [▶ 33]

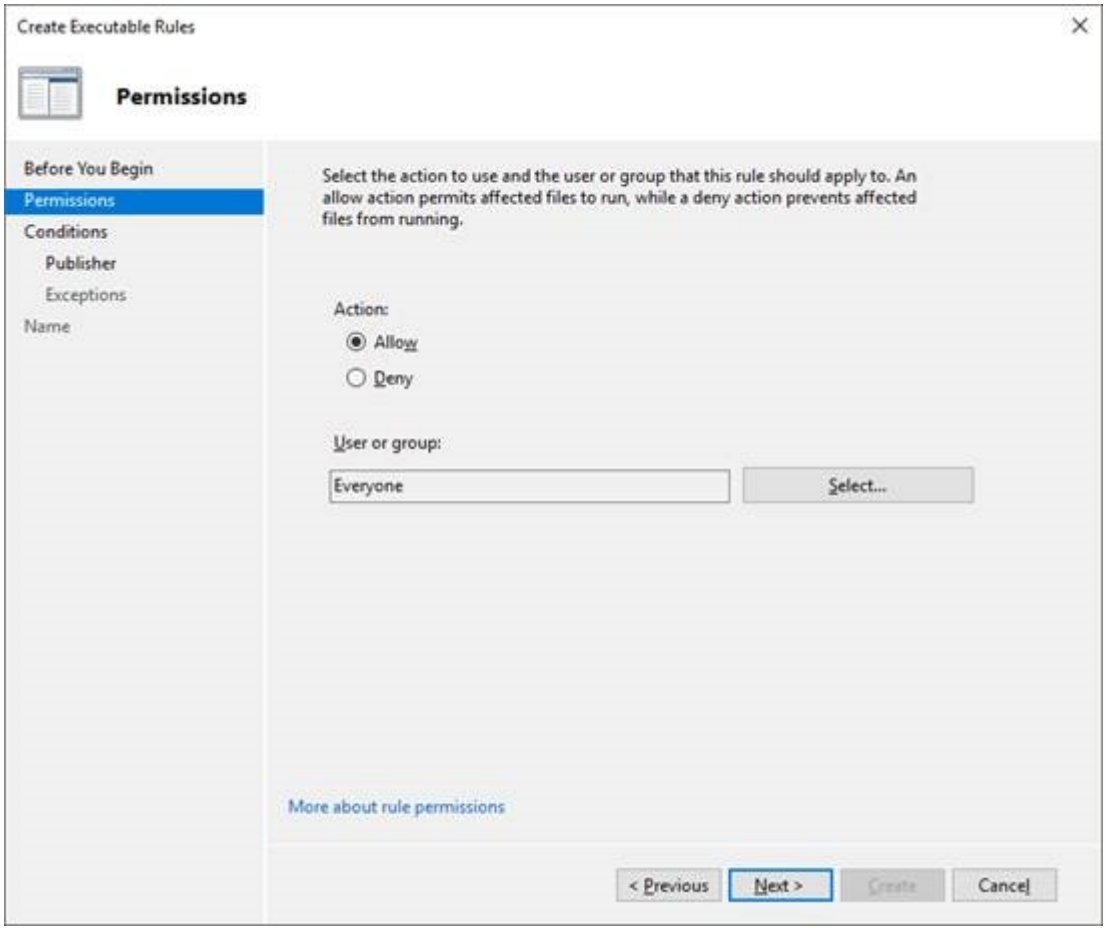
5.5.1.2 AppLocker

AppLockerは、プログラムの実行を制限するために使用できます。

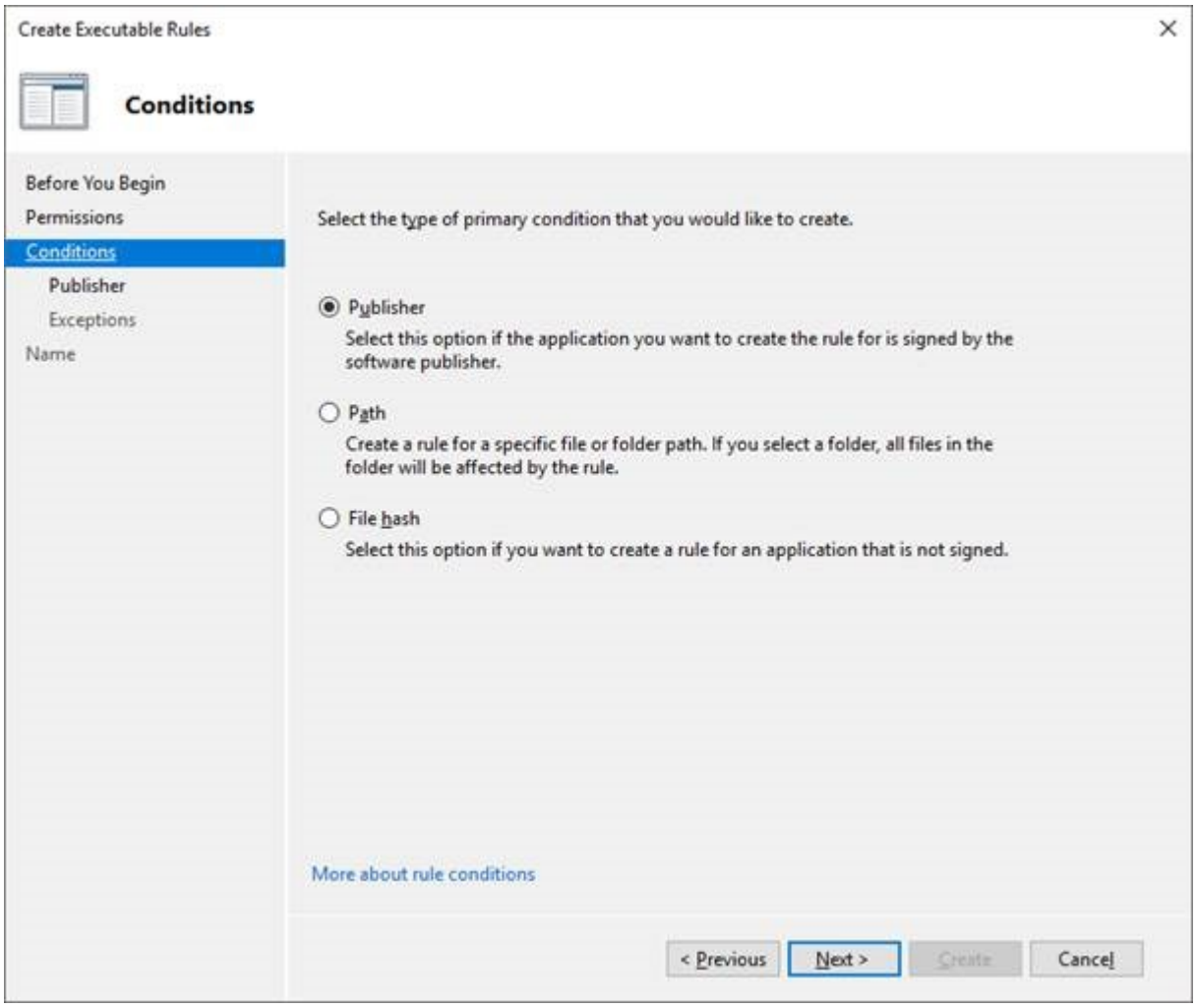
1. **secpol.mscを**実行してセキュリティポリシーを開きます。**Application control policies**を選択し、その下の**AppLockerを**選択します。様々な種類のデータをルール対象にできます：



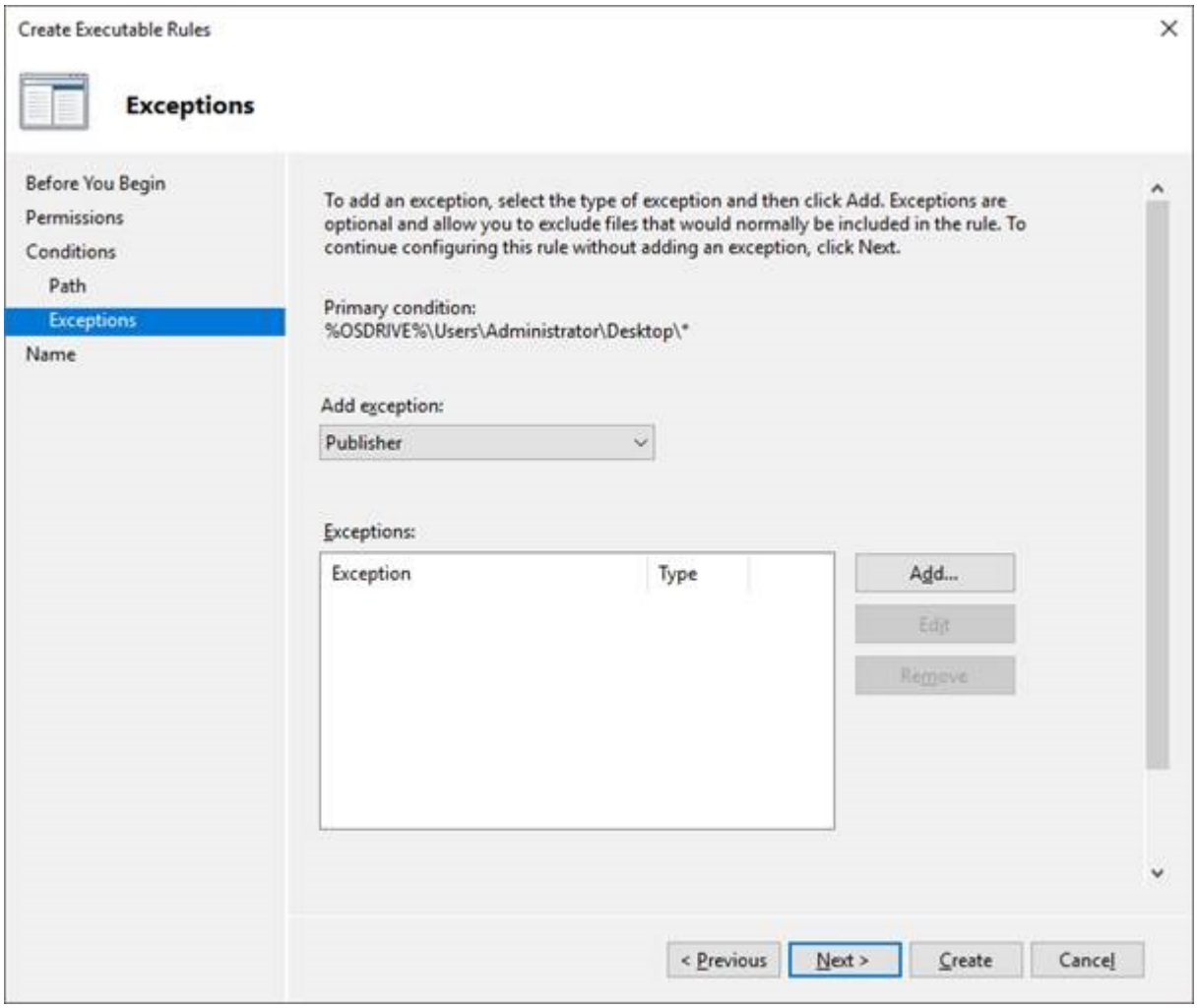
2. ルールのいずれかを右クリックして、**Create new rule**を選択できます。
3. **Allow**または**Refuse**を選択して、ルールを適用する**User**または**Group**を選択します：



4. 新しいルールに適用する第一条件の種類を選択します：



5. **Publisher**、**Path** 、または**File hash**を指定することで、より正確にルールを指定できます。加えて、Publishers、Paths および File hashesをそれぞれルールから除外できます：



⇨ これで設定は完了です。

注記：

- AppLockerはデフォルトでは「Allow list（許可リスト）」として機能します。
  - AppLockerはまず、アクションを拒否するルールがあるかどうかをチェックします。
  - アクションを拒否するルールは、アクションを許可するルールよりも優先されます。
- 全てのWindowsシステムファイルを許可してください。
- いわゆる「標準ルール」（Windowsシステムファイル用のルール）を作成できます。
- AppLockerを使用すると、自身のシステムから自分を締め出すこともできます。

追記：

- ルールは機械間でインポート/エクスポートできます。
- ルールは、HLKM¥Software¥Policies¥Microsoft¥Windows¥SrpV2に保存されます。
- ファイル識別のために、アプリケーション認証サービス（Appidsvc）を開始してください。

詳しくはマイクロソフトのドキュメントを参照ください：

- https://docs.microsoft.com/de-de/windows/security/threat-protection/windows-defender-application-control/applocker/using-software-restriction-policies-and-applocker-policies

5.5.2 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。

以下も参照してください。

プログラムのホワイトリスト化 [▶ 32]

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。

5.5.3 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。

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。

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。

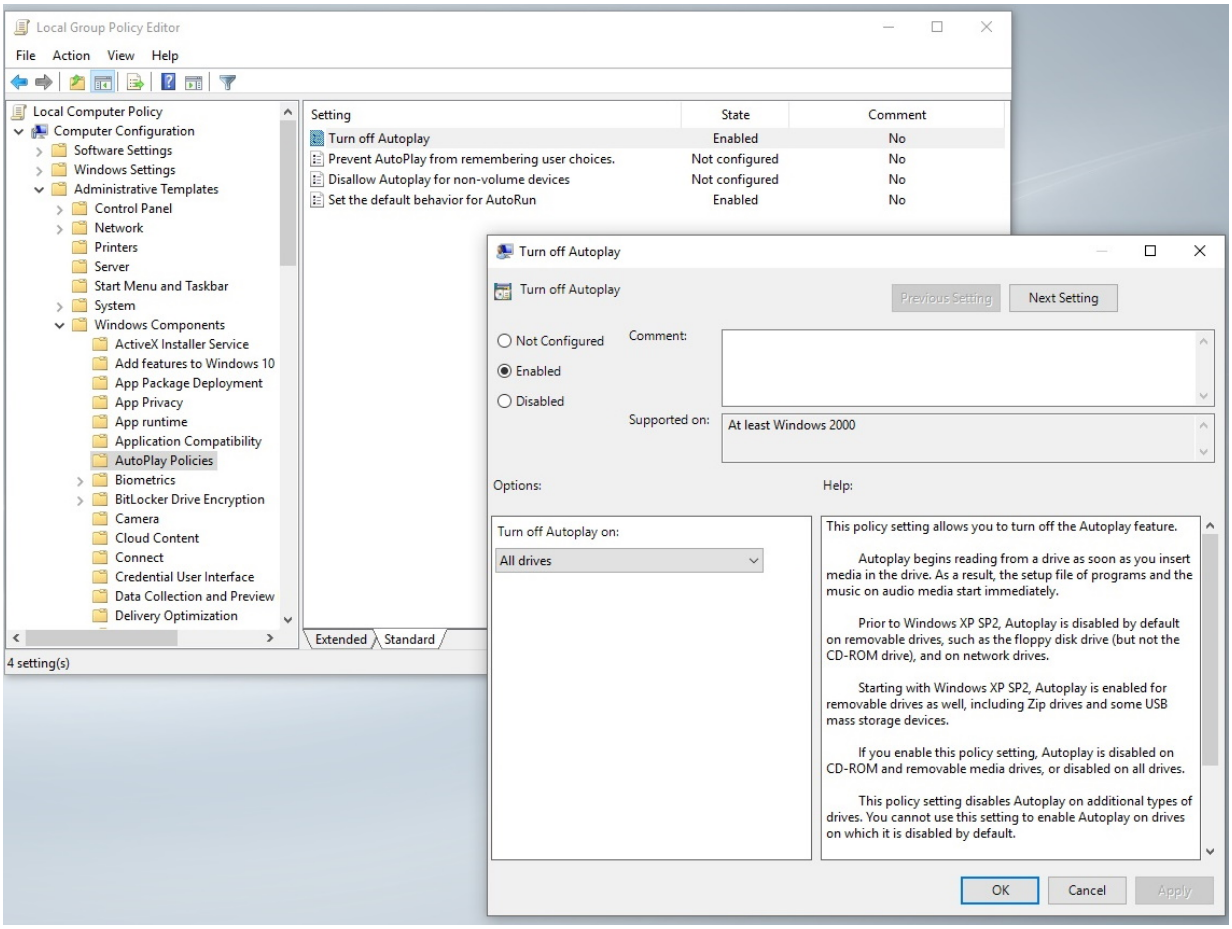
5.5.4 自動起動

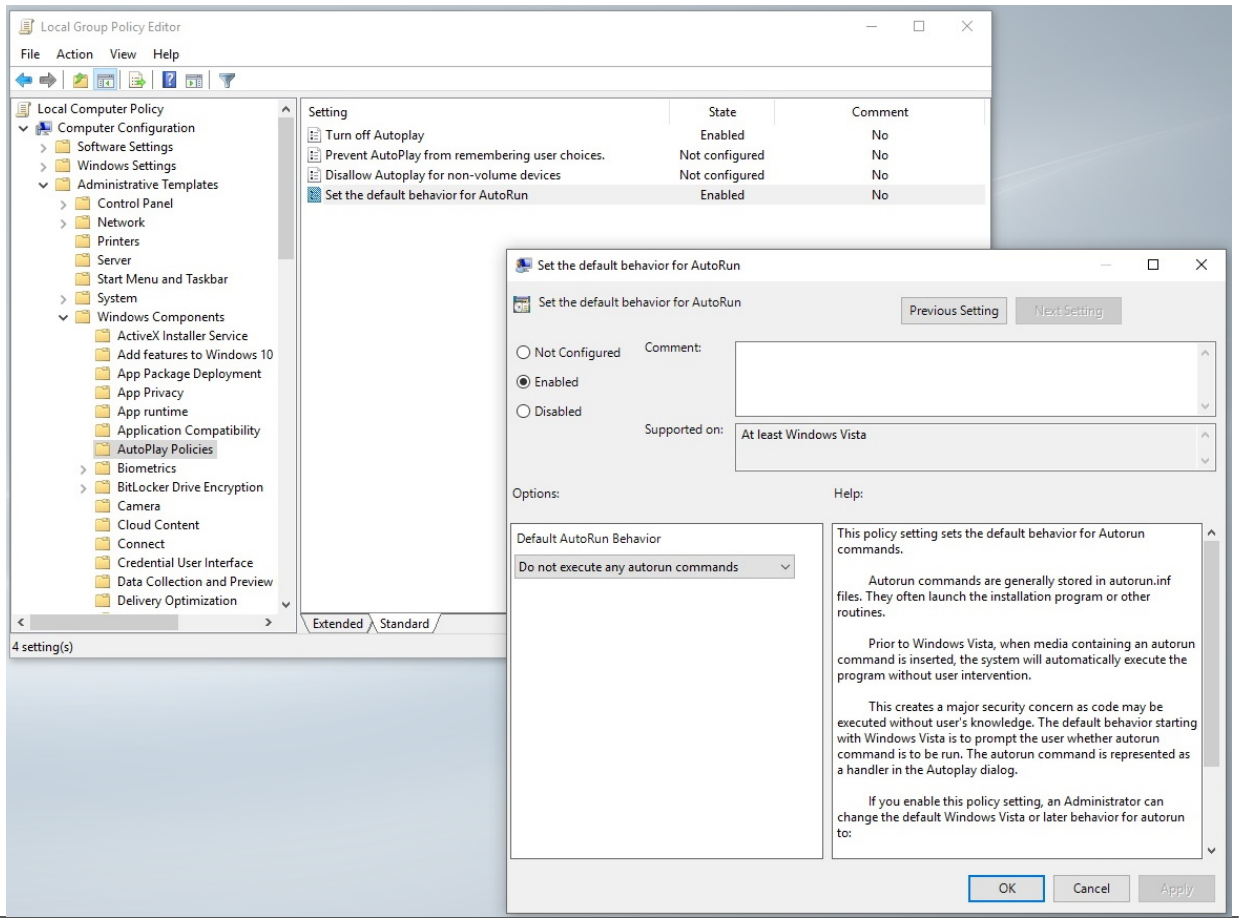
外部デバイス(USBストレージメディアやキーボードなど)が接続されていると、自動起動のメカニズムによってコントローラが容易にウイルス感染してしまいます。これは特に、USBメディアが接続されるとすぐにオペレーティングシステムが自動的にアクションを実行する場合に当てはまります。

自動起動が不要な場合は、無効にする必要があります。ここでは、AutoPlay（すでにインストールされているソフトウェアによるメディアの再生）とAutoRun（プログラムの起動）を区別します。

グループポリシーによってAutoRunとAutoPlayを完全に無効にするには、以下の手順を踏む必要があります。

1. gpedit.mscを実行してグループポリシーを開き、Computer Configuration > Administrative Templates > Windows Components > **AutoPlay Policies**に移動します。そこで、以下のように**Turn off AutoPlay**と**Set the default behavior for AutoRun**のポリシーを設定します。





⇨ 再起動後、設定が完了します。

5.5.5 ウイルス対策プログラム

ウイルス対策ソフトウェアは、データキャリアやネットワークを介してシステムに侵入するマルウェアからシステムを保護します。これは既知のマルウェアのブラックリストです。マルウェアを認識できるように、ウイルス対策ソフトは常に最新の状態に保つ必要があります。これにはデメリットもあります。

ウイルス対策プログラムは、すでに知られているマルウェア（ブラックリスト）を認識し、マルウェアコードの実行を阻止しようとします。

しかし、このブラックリスト（マルウェアパターン）の必要なアップデートを通じて、ウイルス対策プログラムはシステムに対する危険性も高めています。

特定の機械で常に同じプログラムを実行する場合は、先に説明したホワイトリスト方式を使用すべきです。どのような場合でも、ウイルス対策プログラムのようなブラックリスト方式が全体としてメリットかあるかどうかを吟味する必要があります。全体として、ホワイトリスト方式の設定に要する多くの手間と、常にアップデートを要するウイルス対策プログラムを比較する必要があります。

Windows Defenderは、信頼性が高く、TwinCATと互換性があることが証明されています。しかし、最新のセキュリティホールを塞ぐためには、常に最新バージョンにアップデートする必要があります。

特にTwinCATに関しては、ウイルス対策プログラムの使用を正しく評価する必要があります。これはウイルス対策プログラムが、オペレーティングシステムの奥深くで動作するため、TwinCATのリアルタイム統合を阻害する可能性があるためです。

TwinCATには、ウイルス対策プログラムとの互換性に関する独自の説明があります：

ウイルス対策プログラムの互換性

詳しくは、マイクロソフトのドキュメントを参照ください。https://support.microsoft.com/en-us/help/4013263/windows-10-stay-protected-with-windows-security

5.6 Writeフィルター

WindowsのWriteフィルターは、書き込みアクセスからパーティションを保護するためにMicrosoft Windowsが特別に開発したツールです。書き込みアクセスはRAMにリダイレクトされ、その結果、パーティションはあらかじめ設定された状態で保護されます。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。

ユースケースに合わせてWriteフィルターを設定できます。このようにして、予期しない書き込みアクセスからシステムを保護します。除外設定により、書き込みアクセスを許可するフォルダを定義します。

ITセキュリティの意義

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。しかし、その結果、感染や攻撃について収集できる情報は少なくなり、再び発生する可能性があります。

また、Writeフィルターのオン/オフ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Writeフィルター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。

注記

オーバーフィルRAMのオーバーレイおよびディスクオーバーレイ

UWFは、継続的なモニタリングとデフォルト設定なしでの連続運転（24時間365日）には適していません。RAMオーバーレイまたはディスクオーバーレイは、（除外された領域であっても）書き込みアクセスで事前に設定した最大サイズまで、アクセスが失敗するまで継続的に生成されます。そうなると、オペレーティングシステムは動作できなくなります。

UWF（Unified Write Filter）は、Windows10にのみインストールされたWriteフィルターです。ユーザは、Beckhoff Unified Write Filter Managerのグラフィカルなユーザインタフェースから UWFを制御できます。このソフトウェアは、簡単な設定オプションを提供します。Windowsのコマンドラインから全ての機能が利用可能で、マイクロソフトのドキュメントに詳細が記載されています。
https://docs.microsoft.com/de-de/windows-hardware/customize/enterprise/unified-write-filter

UWF Managerの概要

UWFモード、ステータスおよびオーバーレイのサイズは**General**タブで設定できます。ここでWriteフィルターの有効／無効を設定します。

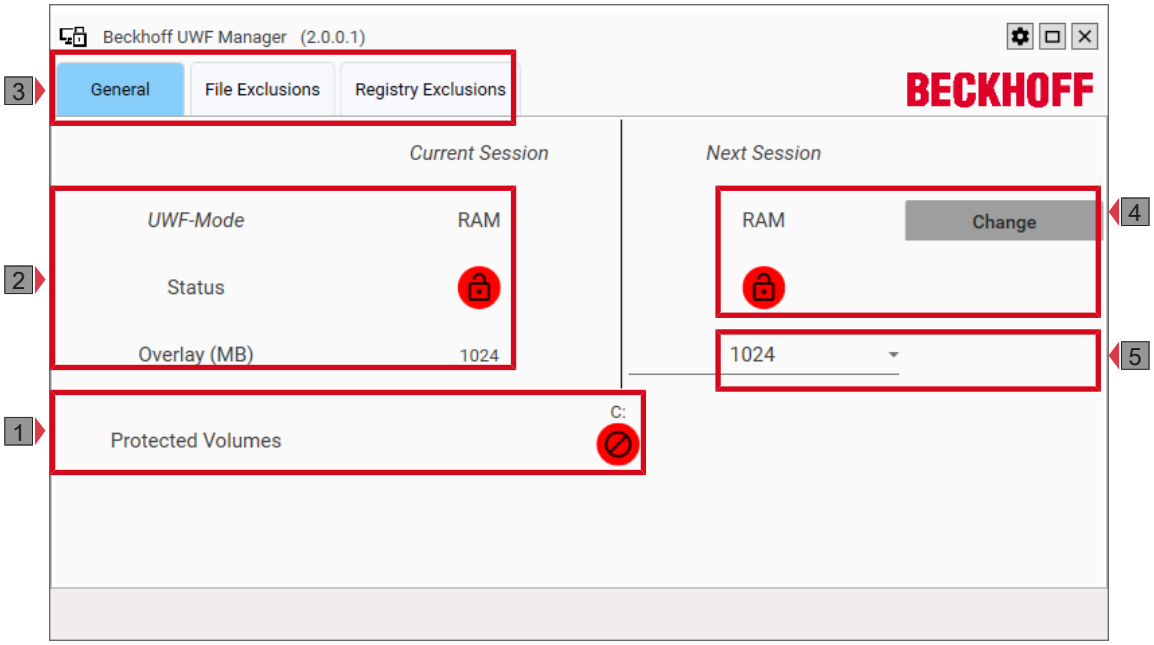


図 1: UWF ManagerはRAMモードで、パーティションC:は保護なし

表 *1: UWF Managerの凡例*

番号	説明
1	個々のパーティションはこのボタンで保護できます。
2	現在のUWFモード、ステータス、オーバーレイのサイズがここに表示されます。
3	ファイルとレジストリの除外は、これらのタブで定義できます。
4	UWFが変更された場合の将来のステータスがここに表示されます。**Change**ボタンでRAMモードとディスクモードを切り替えます。
5	オーバーレイのサイズはこのボックスで設定できます。

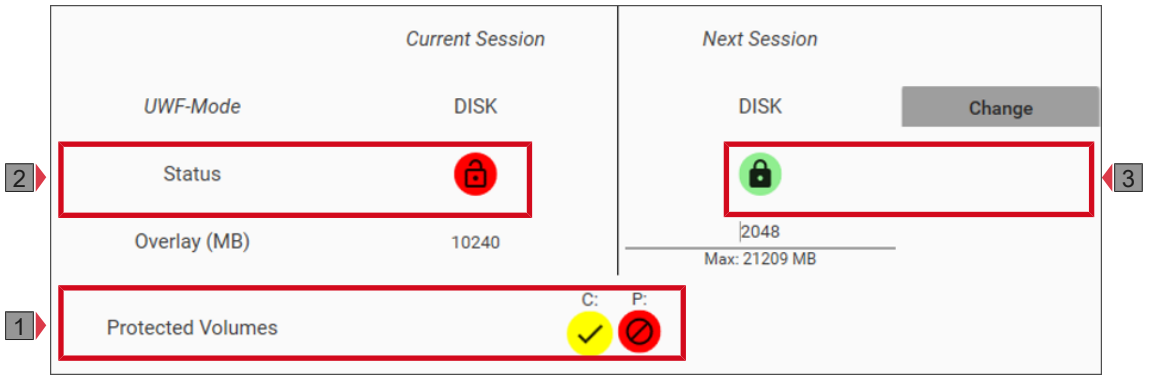


図 2: UWF Managerはディスクモードで、パーティションC:は次の再起動から保護

表 *2: UWF Managerの色の凡例*

番号	説明
1	赤 = スイッチオフ、保護されていない
2	緑 = スイッチオン、保護されている
3	黄色 = スイッチが入り、次の再起動後に保護される。

ファイルの除外

File Exclusionsタブでは、例外を定義し、個々のファイルやフォルダへの書き込みアクセスを許可できます。

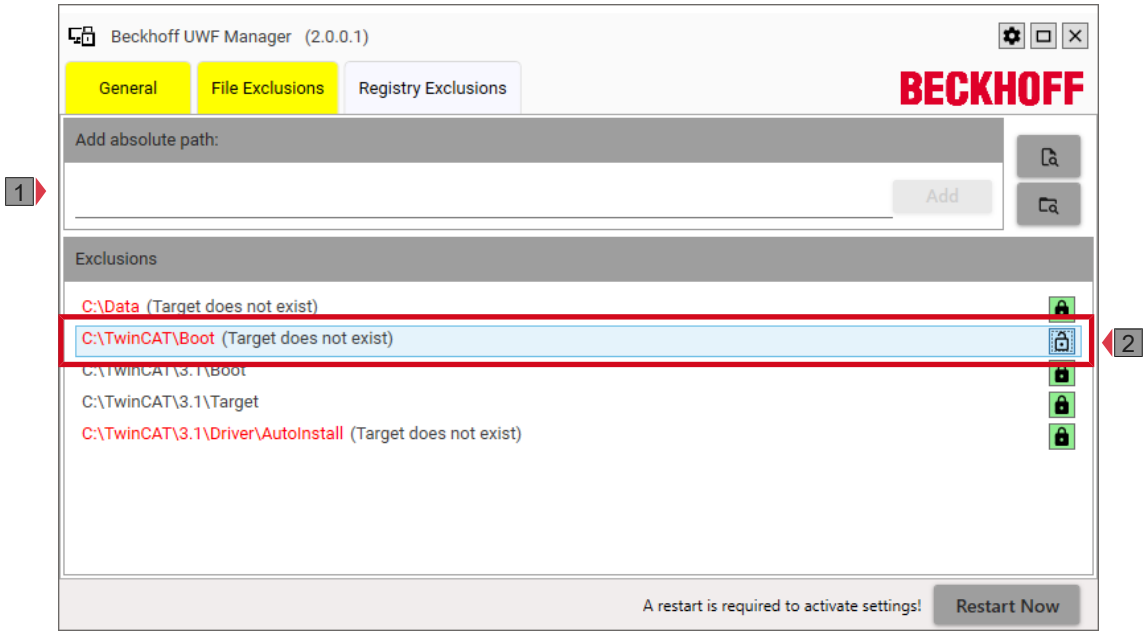


図 3: UWF Managerのファイル除外

表 *3: UWF Managerの凡例（ファイル除外）*

番号	説明
1	このボックスを使って、新しいフォルダを除外対象に追加できます。
2	既存の除外項目は、このボタンでオン/オフを切り替えることができます。

レジストリの除外

Registry Exclusionsタブから、例外を定義し、個々のレジストリキーへの書き込みアクセスを許可できます。

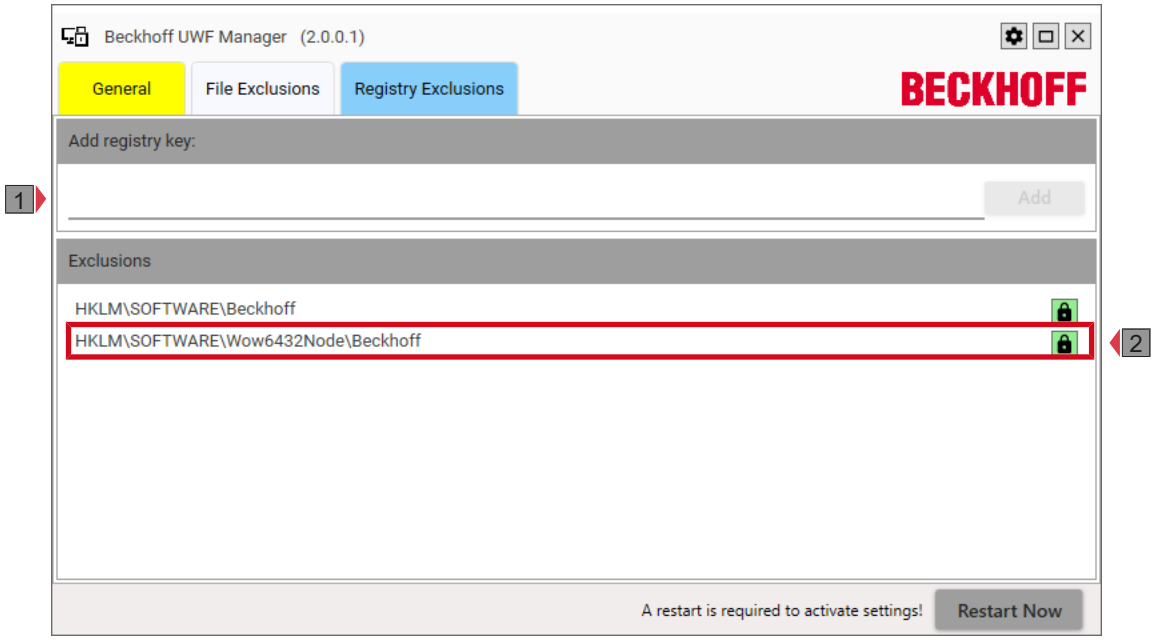


図 4: UWF Managerのレジストリ除外

表 *4: UWF Managerの凡例（レジストリの除外）*

番号	説明
1	このボックスを使って、新しいレジストリキーを除外対象に追加できます。
2	既存の除外項目は、このボタンでオン/オフを切り替えることができます。

UWFが有効な場合、メインメモリ（RAMオーバーレイ）またはディスクオーバーレイそれぞれへの書き込みアクセスは全て迂回され、パーティションへのアクセスは読み込みのみになります。再起動後、Windowsは再び最初に定義された状態で起動します。

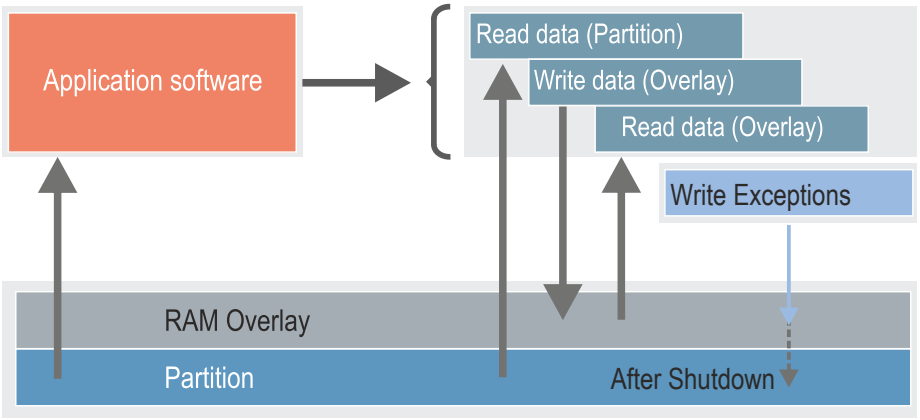


図 5: Windows Write Filter、RAMモードでのアプリケーションソフト動作モード

さらに、UWFで例外を定義し、その結果、個々のファイル、フォルダー、レジストリキーへの書き込みアクセスを許可できます。例外は再起動後にのみパーティションに書き込まれ、それまではRAMオーバーレイまたはディスクオーバーレイにバッファリングされることに注意してください。

システムによってオーバーレイに大量のデータが書き込まれる場合、このデータはUWFで例外として定義する必要があります。オーバーレイメモリとその中に含まれるファイルは、ベッコフUWF Managerを使用して解析し、メモリ占有率を特定できます。このためには、ベッコフUWF Managerの設定で「Enable Overlay tracing（オーバーレイトレースを有効にする）」のチェックボックスをオンにする必要があります。

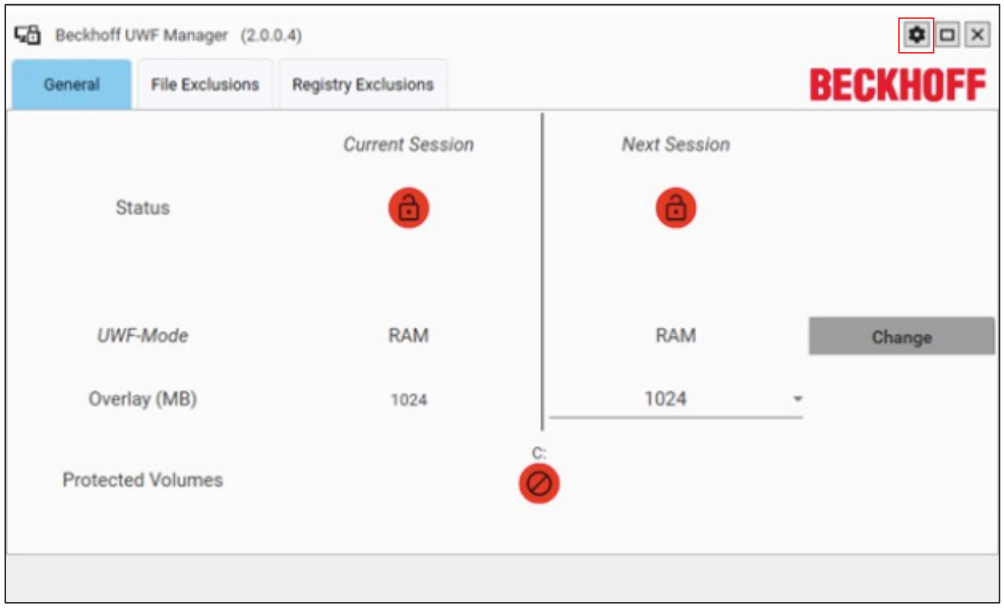


図 6: UWF Managerの設定

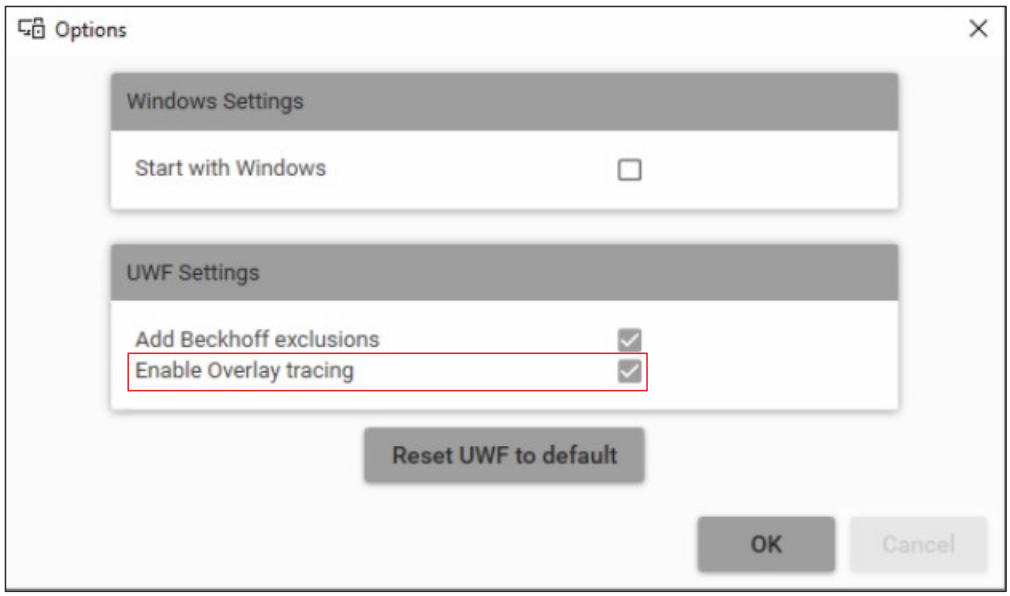


図 7: UWF Manager「Enable Overlay tracing（オーバーレイトレースを有効にする）」チェックボックス

enabled UWFを有効にしてWindowsを再起動すると、ベッコフUWF Managerに追加のタブが表示され、オーバーレイ内のファイルと関連するファイルサイズが一覧表示されます。

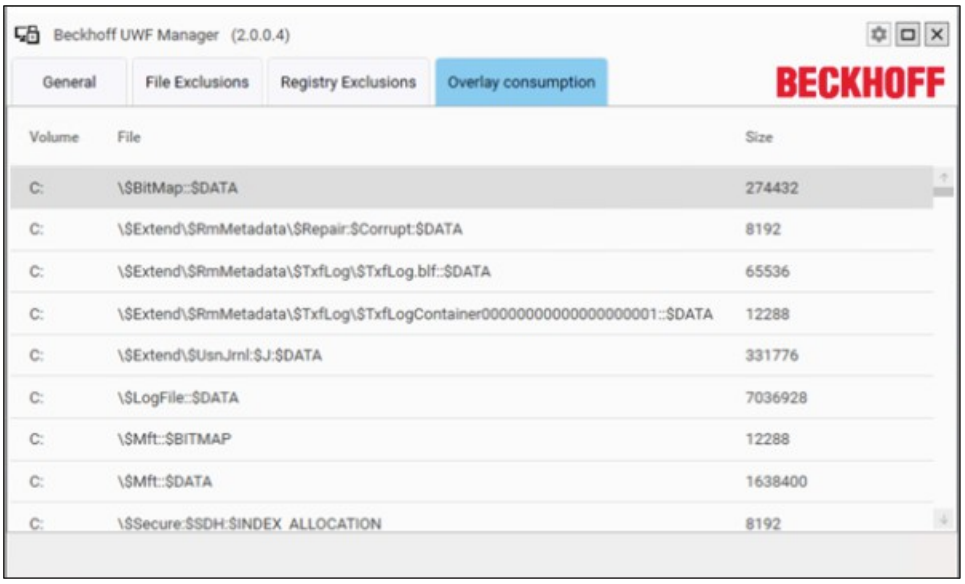


図 8: UWF Manager オーバーレイ消費

UWFは、デフォルト設定での連続運転には適していません。

UWFは、デフォルト設定での連続運転（24時間365日）には適していません。RAMオーバーレイまたはディスクオーバーレイは、（除外された領域であっても）書き込みアクセスで事前に設定した最大サイズまで、アクセスが失敗するまで継続的に生成されます。オーバーレイは再起動後にのみ有効になります。

RAMオーバーレイやディスクオーバーレイをいかに大きく設定しても、再起動しない限り、いずれ上限に達する可能性があります。RAMオーバーレイは、メインメモリ全体の最大50%を占めることがあるため、特に危険です。RAMまたはディスクオーバーレイがいっぱいの場合、それ以上の書き込みは失敗します。この状態になると、デバイスが反応しなくなり、動作が重くなることがあります。ディスクオーバーレイは、十分な空き容量があれば大きなオーバーレイを生成できるので、解決策になる可能性があります。

マイクロソフトのドキュメントを参照してください：
https://docs.microsoft.com/en-us/windows-hardware/customize/enterprise/uwfoverlay

使用率が高い場合の警告

オーバーレイの負荷を正確に予測することはできません。新しいUWF Managerは、UWFの使用のためにオペレーティングシステムを最適化しますが、例外なく24時間365日トラブルなく作動することを保証するものではありません。警告メッセージは、オーバーレイの使用率が50%と70%のときにユーザに表示されます。これらの警告には必ず対処してください。

UWFによるバックアップ生成と復元

システムのバックアップを生成する前に、UWFをオフにする必要があります。そうしないと、復元したシステムでUWFが正しく設定されません。バックアップが復元された後、新しく作成された容量に対してUWFを再び有効化できます。

一般的な推薦事項

1. RAMオーバーレイを使用したUWFは、連続運転（24時間365日運転）では使用しないでください。
2. システム内で連続的にスイッチを入れる前に、UWFの動作を正確に分析する必要があります。

様々なアプリケーションシナリオに対する推奨事項

- データが少ない、RAMが十分、ディスクの空き容量が少ない→RAMモード
- ディスクに十分な空き容量があり、データ量が多い可能性がある→ディスクモード
- データ量が多い→データ用にセカンドボリュームを作成し、UWFでC:だけを保護する

5.7 キーボードフィルター

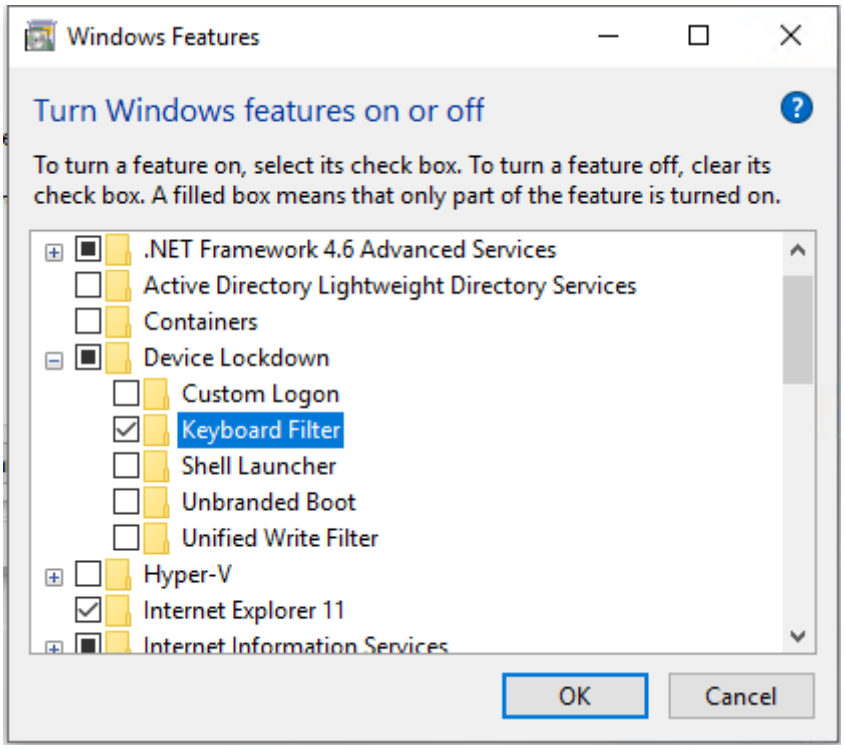
キーボードフィルターは、予期しないアクセスからシステムを保護します。例えば、アプリケーションの終了につながるショートカットをブロックできます。アプリケーションの操作に必要なキーボード入力のみを有効にします。さらに、キーボードフィルターを無効にするショートカットを指定することもできます。管理者用のフィルタを無効にするオプションも便利です。

キーボードフィルターは、ユーザのオペレーティングシステムに対する操作を制限し、攻撃の可能性を最小化するためのオプションを提供します。

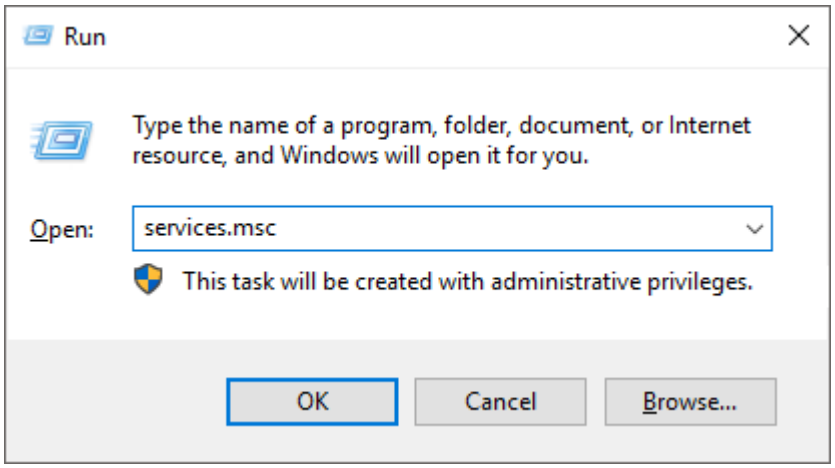
通常、「キオスクモード」が設定され、例えば、ログインに成功したユーザがHMIアプリケーションのみを起動できるようにします。ユーザは、他のプログラムを起動したり、IPCにシャットダウンなどのコマンドを送信することができなくなります。

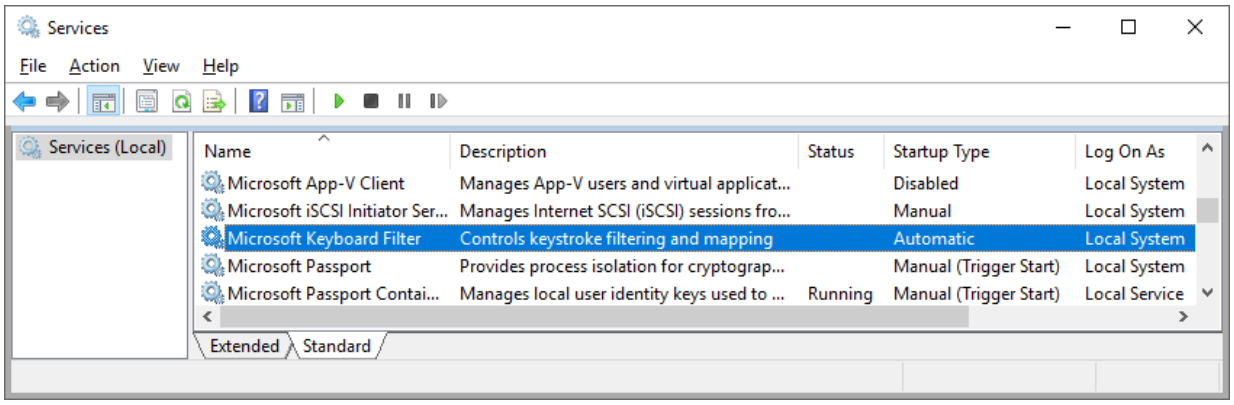
Windows10はこのためのサービスを提供します。ここでは、その起動方法と設定方法について説明します。

まず、サービスを利用するためにWindows 10の内部機能をオンにします。これを行うには、ダイアログ **Turn Windows features on or off**を開き、メニュー項目**Device Lockdown**の下にある**Keyboard Filter**の機能を選択します。その後、PCを再起動します。

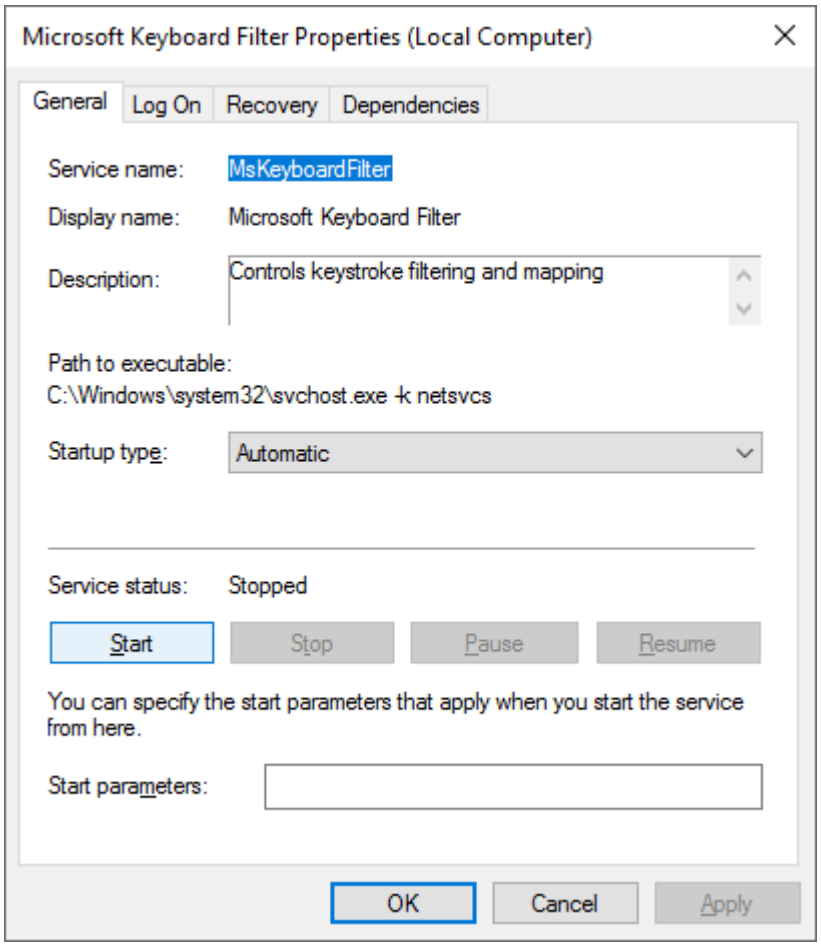


1. **Microsoft Keyboard Filter**のサービスを開始します。

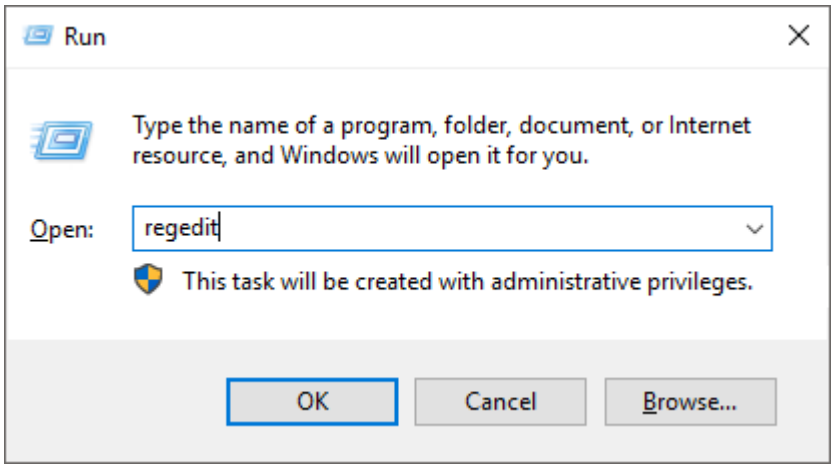




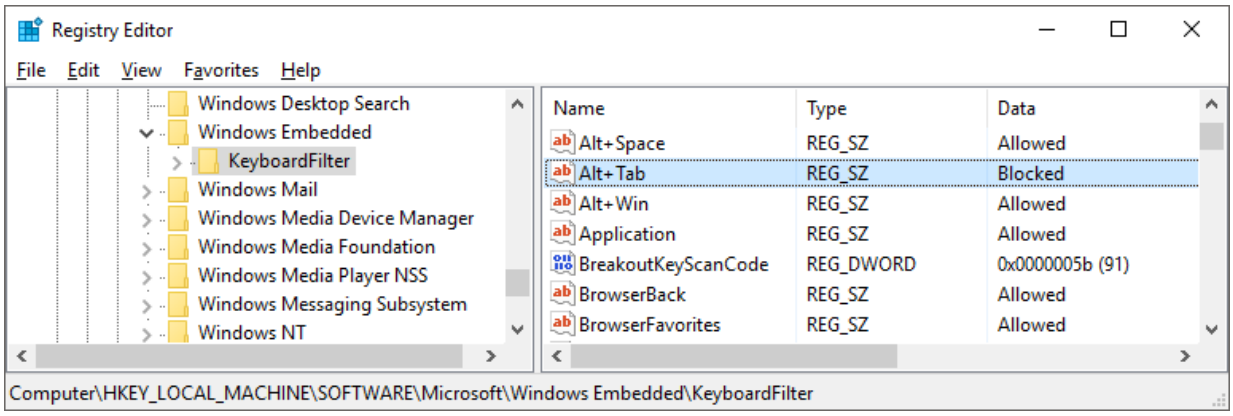
2. 起動タイプを**automatic**設定します：



3. **Registry Editor**を開きます



4. **KeyboardFilter**に移動します：**HKEY_LOCAL_MACHINE>SOFTWARE>Microsoft>Windows Embedded**



5. 値とよく使われるショートカットを以下の表に示します。

⇨ キーボードフィルターが有効になりました。

以下の値は個々のショートカットを表しています：

値	説明
"Allowed"	ショートカットを許可する
"Blocked"	ショートカットをブロックする
DisableKeyboardFilterForAdministrator を "1" にする	管理者にはキーボードフィルターが無効
BreakoutKeyScanCodeを "01 "にする	ESCのスキャンコードをブレイクアウト

以下のショートカットは通常ブロックされています：

値	説明
CTRL-SHIFT-ESCキー	タスクマネージャーを開く
CTRL-ALT-DELキー	以下のオプションでメニューを開く： ロックシステム タスクマネージャーを開く パスワードを変更する システムをシャットダウンする ユーザを切り替える

詳しくはマイクロソフトのドキュメントをご参照ください： https://docs.microsoft.com/en-us/windows-hardware/customize/enterprise/keyboardfilter

5.8 USBフィルター

アプリケーションのホワイトリストと同様に、USBデバイスも信頼済みとしてリストアップできます。承認リストにないUSBデバイスは、オペレーティングシステムが受け付けません。したがって、機器のメンテナンスのために、承認されたアプリケーションのみを含む、定期的にチェックされた単一のUSBフラッシュドライブを定義できます。そのため、アプリケーションに特化していない（プライベート用などの）USBフラッシュドライブが害を及ぼすことはありません。USBフィルターは、USBで接続された全てのデバイスに対応しています。これらには、例えば、マウス/キーボードなどのHIDデバイスや、USBフラッシュドライブ、ハードディスク、カードリーダーなどの全ての大容量記憶デバイスが含まれます。

しかし、オペレーティングシステムのUSBフィルターは、USB内のベンダーIDとプロダクトID（ベンダーID[VID]/プロダクトID[PID]）を参照しており、暗号的なセキュリティはなく、偽造される可能性があります。

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。

しかし、USBフィルターで使用されるIDは暗号的に保護されていないため、用意されたUSBデバイスを使った悪意のある攻撃によって、USBフィルターを回避できます。

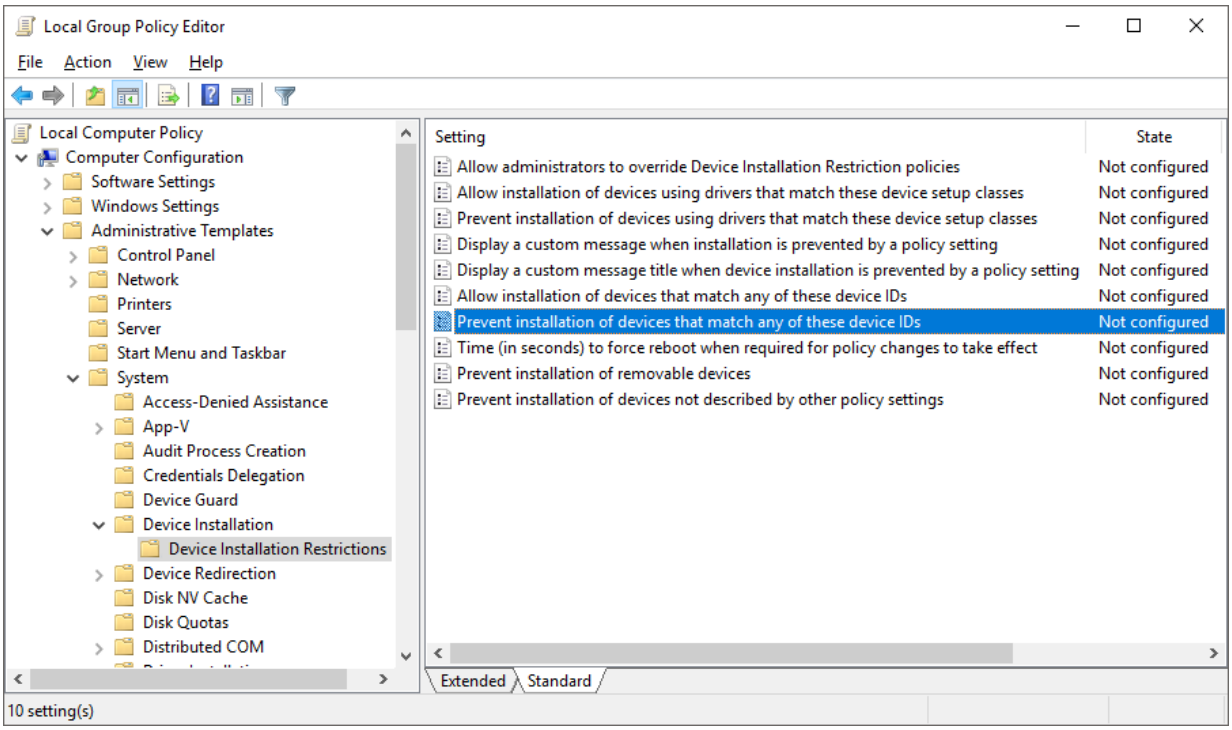
OSレベルでUSBデバイスを制限する方法は複数存在します。

- 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。

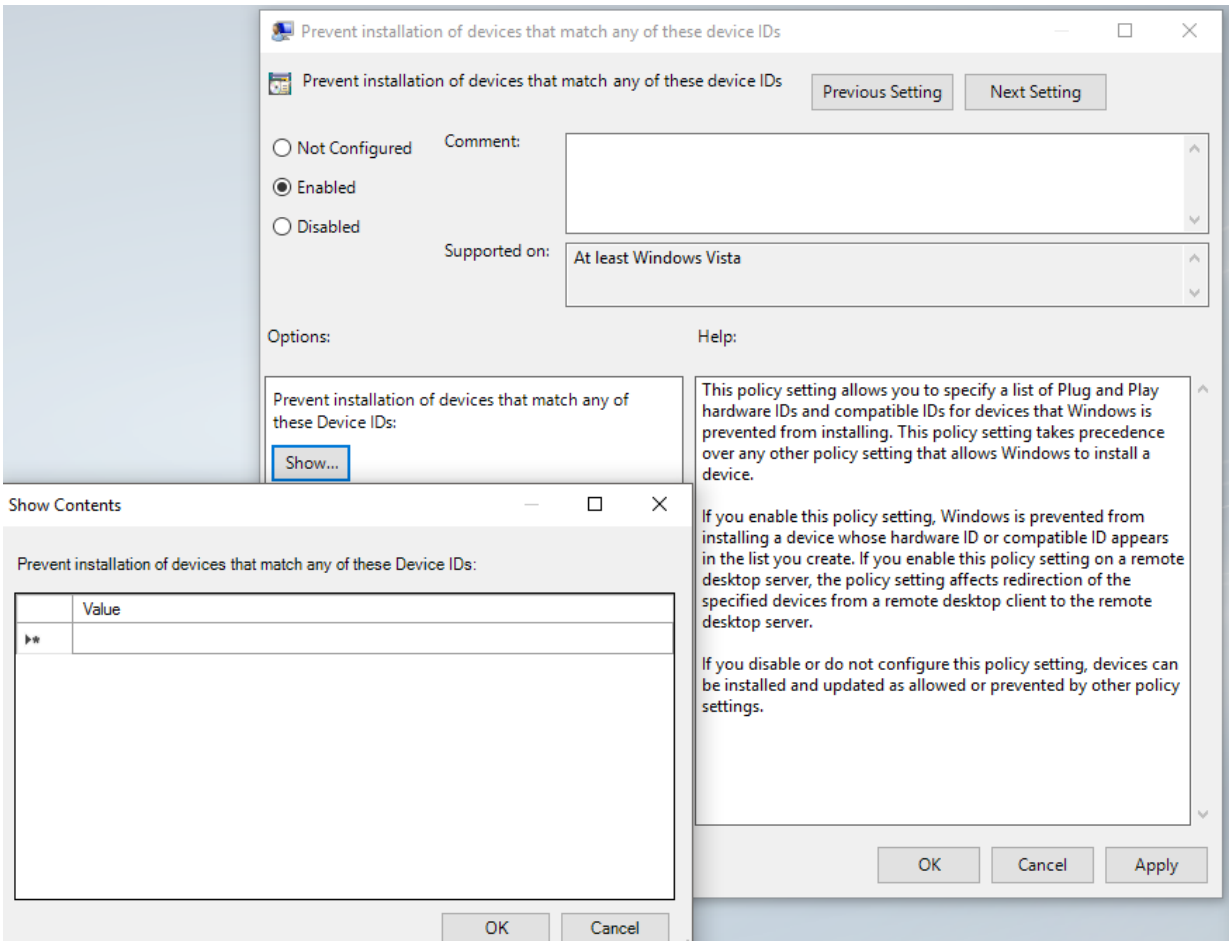
レジストリを介して設定された値は、グループポリシーで設定された値と自動的に同期されないことに注意してください。グループポリシーのみで設定することをお勧めします。

Windows10では、USBデバイスの取り扱いに関するオプションを設定できます。

1. 実行ウィンドウで**gpedit.msc**と入力し、グループポリシーエディターを開きます。アプリケーションに応じて、**Prevent/Allow Installation of devices that match any of those device IDs（これらのデバイスIDのいずれかに一致するデバイスのインストールを防止/許可する）**を選択します。



2. グループポリシーを有効にし、許可またはブロックするデバイスを入力します：



⇨ これでUSBフィルターの設定は完了です。

詳しくは、マイクロソフトのドキュメントを参照してください。http://msdn.microsoft.com/en-us/library/bb530324.aspx

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 [▶ 56] 。

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 [▶ 55]
- RDP [▶ 55]

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。

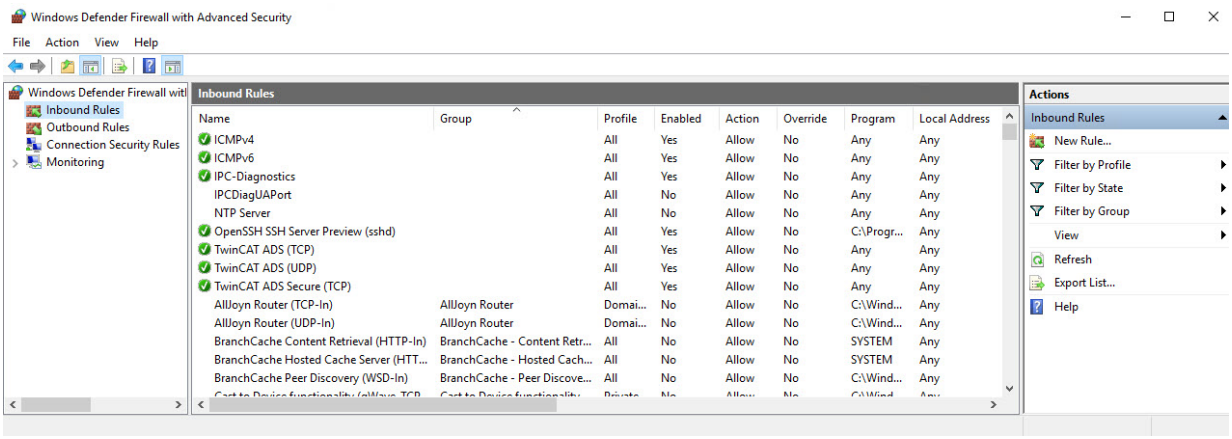
ファイアウォール経由の通信を制限的に明示的に設定することは、必要な範囲に限定してネットワークアクセスを許可するために重要な対策です。

重要なTCP/UDPポート [▶ 56] 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。

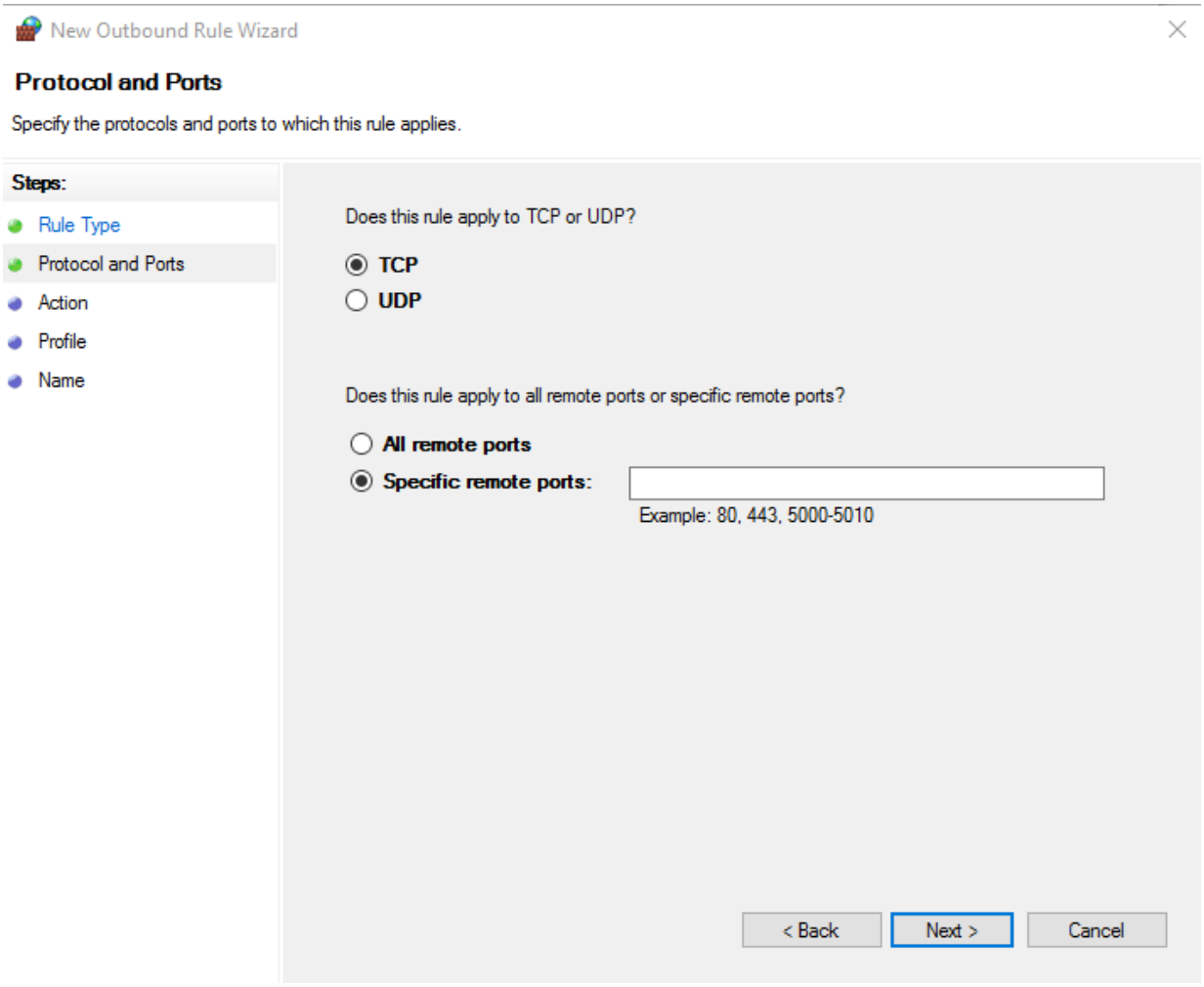
コマンド**wf.msc**で、コマンドラインからMMCスナップイン**Windows Firewall with Advanced Security**を開き、ファイアウォールを設定できます。**New Rule**ボタンを使用して、ルールを追加できます。

選択されたポートまたはサービスの開放ルールは、再び閉じることができます。ルールを右クリックすると、**Disable Rule**でルールを無効化したり、**Delete**で削除したりできます。

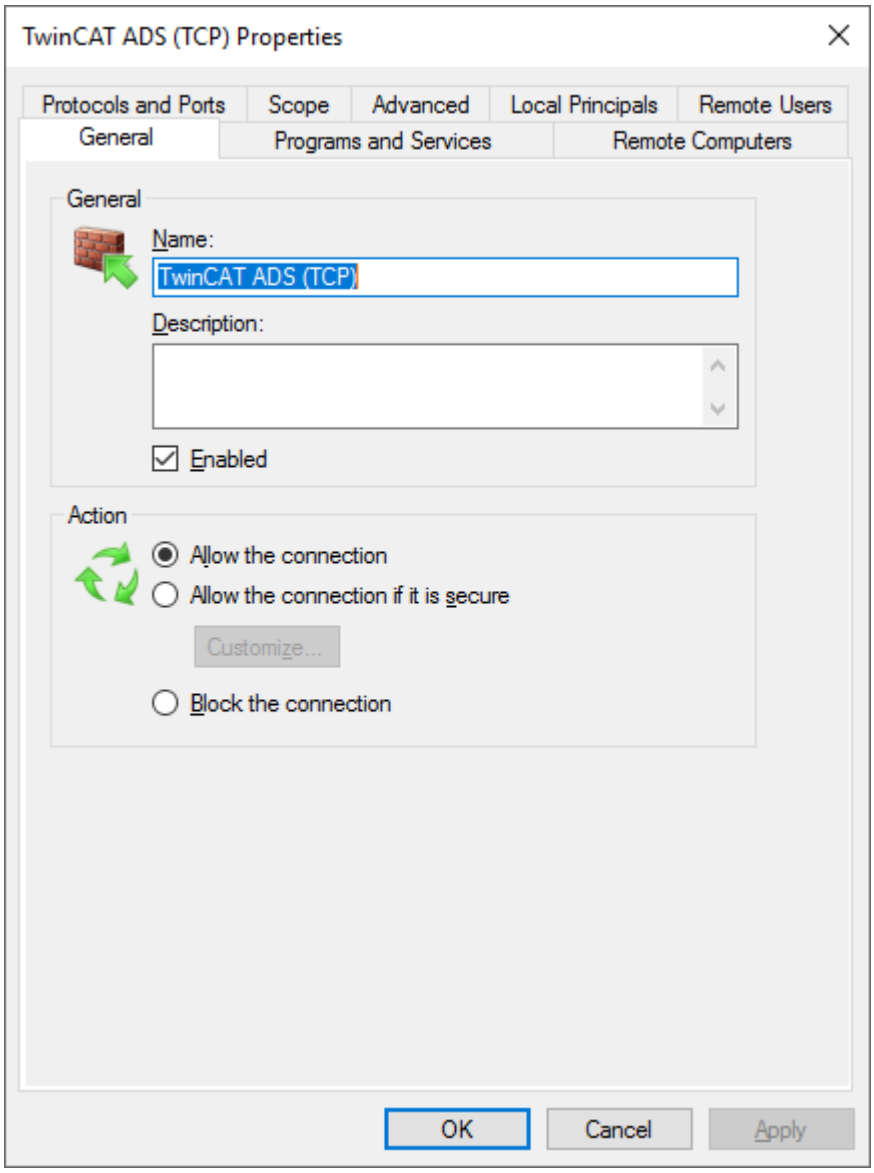
1. ファイアウォール設定を開きます。



2. ルールをダブルクリックすると、接続の許可またはブロックなど、既存のルールを変更できます。新しいルールは**New Rule**を使って作成します。
オプションを案内するウィザードが起動します：



3. これらのルールのオプションは、後から変更することもできます：



⇨ ファイアウォールの新しいルールが作成できました。

詳しくはマイクロソフトのドキュメントを参照ください：

https://docs.microsoft.com/en-us/previous-versions/windows/desktop/ics/windows-firewall-integration-and-best-practices

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。

6.3.5 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。

6.3.6 CerHost

CerHostは、Windows CEベースのオペレーティングシステムにグラフィック・リモート・アクセスするための、マイクロソフト社独自の非暗号化プロトコルです。

CerHostは安全な環境（例えば安全なトランスポートチャネル経由）でのみ使用することが推奨されています。

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 IIS Webサーバー

デフォルトでは、WindowsでIIS Webサーバーは有効で、Beckhoff Device ManagerやPLC HMIなどに使用されます。システムの安全性をさらに高め、Webサーバー経由のアクセスを制限するには、以下の方法があります：

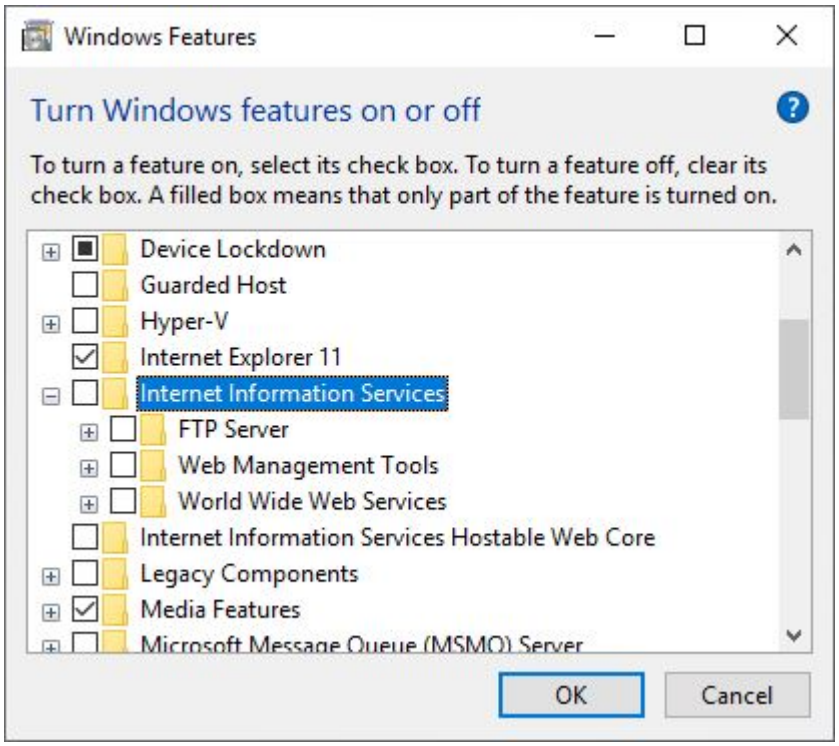
- IIS Webサーバーを無効にする
- または外部からのアクセスを制限する。

この2つの選択肢のどちらが合っているかは、使用条件によって決まります。完全に無効化した場合、IIS Webサーバーにアクセスする全てのアプリケーションが影響を受け、動作しなくなりますのでご注意ください。アクセスが制限された場合、Beckhoff Device Managerにアクセスできなくなります。無効化しても、Beckhoff Device Managerのローカルアクセスは引き続き使用でき、他の全てのアプリケーションは影響を受けません。

IIS Webサーバーの停止：

1. ショートカット **[Windowsキー] + [R]**で実行ダイアログを呼び出し、**optionalfeatures**と入力します。
   Windows Featuresのウィンドウが開きます。

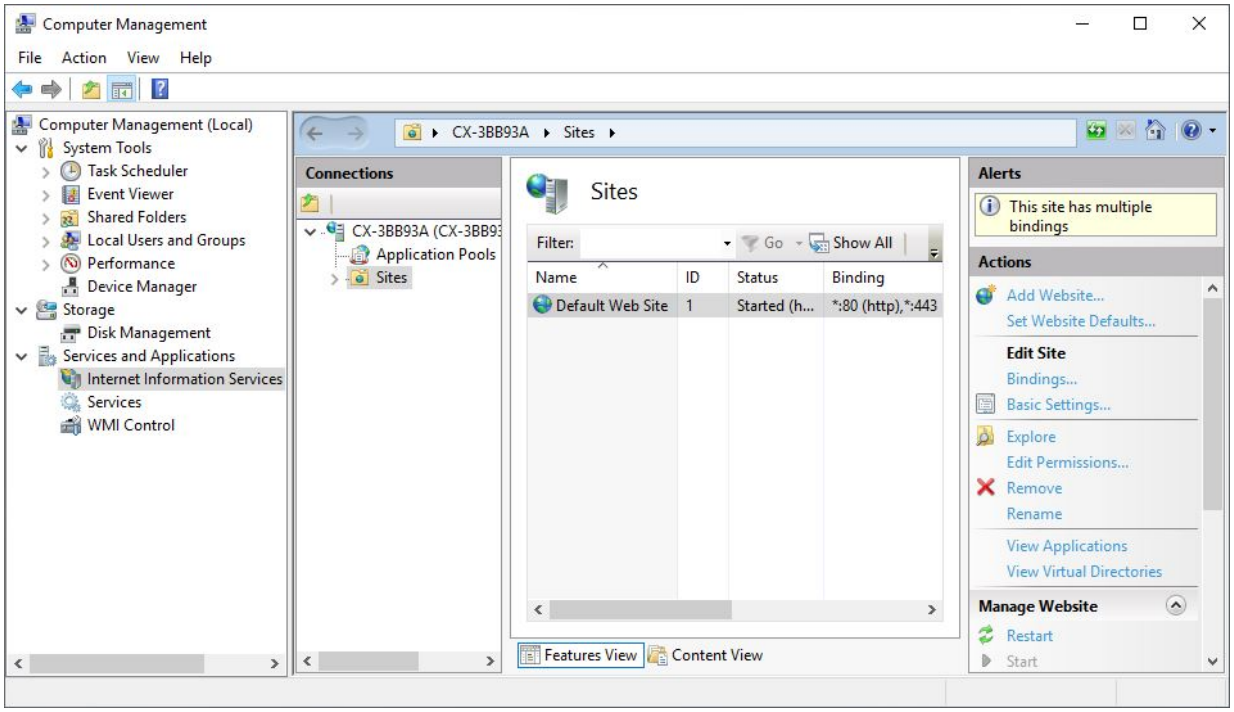
2. **Internet Information Service**のオプションを無効にします。



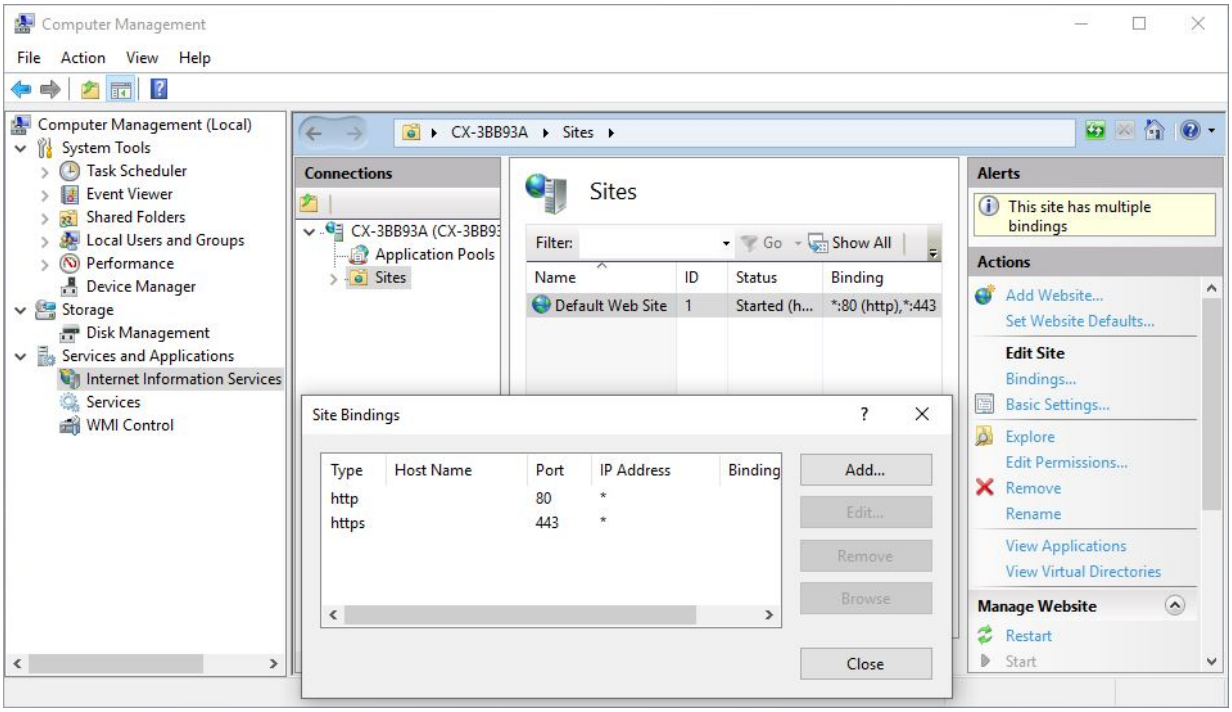
3. IIS Webサーバーが無効になりました。IIS Webサーバーにアクセスする全てのアプリケーションが、この変更の影響を受けます。

外部からのアクセスを制限する：

1. 外部からのアクセスを無効にするには、**[Windowsキー] + [R]**ショートカットで実行ダイアログを呼び出し、**compmgmt.msc**と入力します。
2. 左側の構造ツリーで、**Internet Information Services**のエントリーを選択し、**Connections**の下にある**Sites**というフォルダーを選択します。

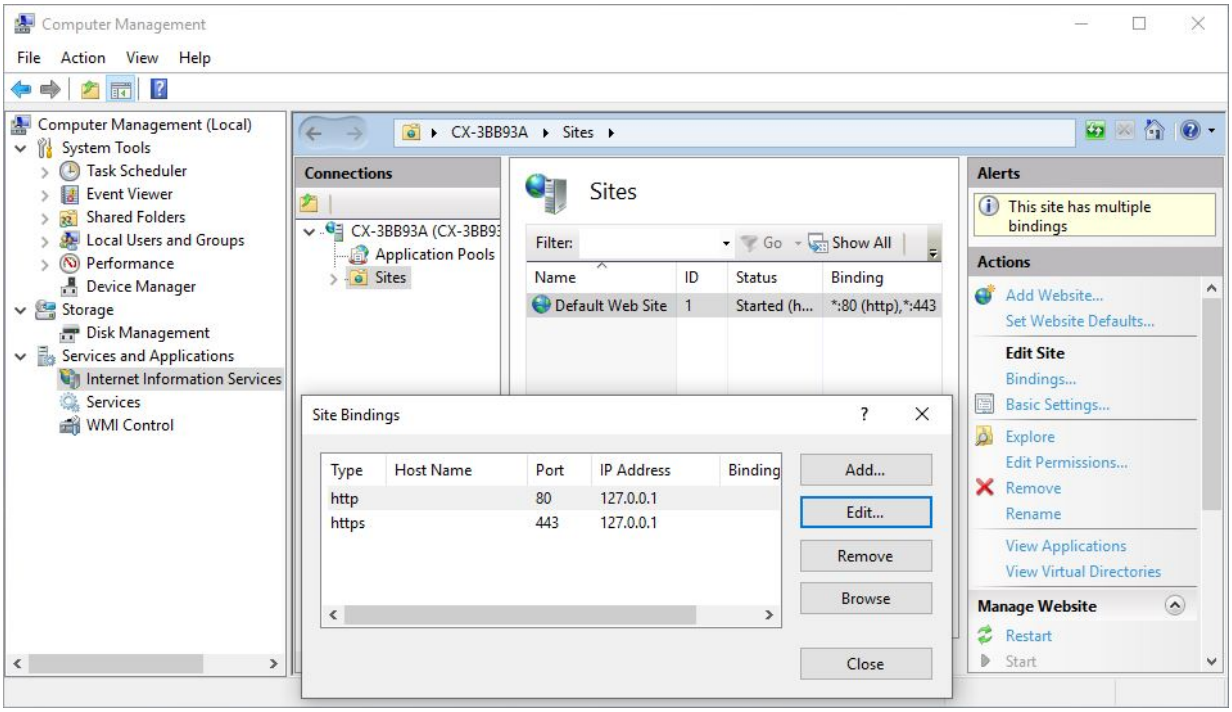


3. 右側のActionsの下にある**Bindings**をクリックします。**Site Bindings**ウィンドウでは、httpとhttpsの**IP Address**列にアスタリスク(*)が表示されます。



これで、外部からのアクセスは全て許可されます。

4. httpまたはhttpsのエントリを編集し、**127.0.0.1**のローカルアクセスのみを許可します。



⇨ 以降、外部からのBeckhoff Device Managerへのアクセスは制限されます。ローカルアクセスは、**127.0.0.1/config**で可能であり、他の全てのアプリケーションは、完全無効化の影響を受けません。

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

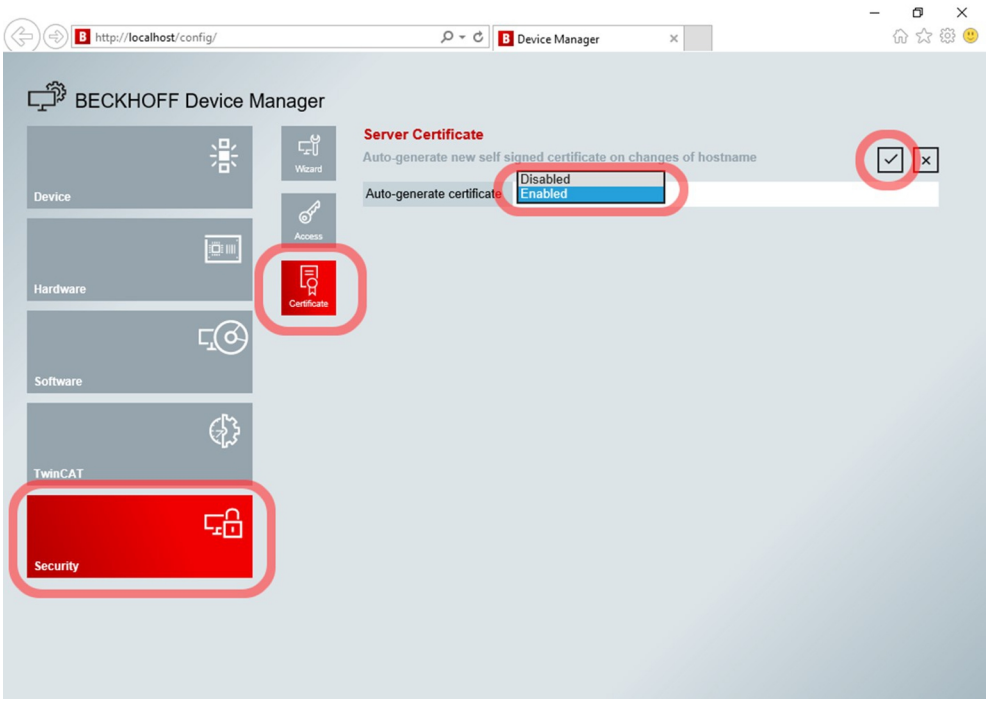
正確な手順と必要なステップについては、本章で説明します。

6.7.1 証明書の自動生成を無効にする

まず、証明書の自動生成を無効にして、独自の証明書がインストールされるようにする必要があります。設定は、Beckhoff Device Managerを使用して行います。Beckhoff Device Managerは、産業用PCのローカルまたはリモートから呼び出します。

以下の手順に従ってください。

1. 産業用PCのローカルで作業している場合は、ブラウザの検索ボックスにURLhttp://localhost/config を入力して、Beckhoff Device Managerを起動します。リモート接続の場合は、https://<IP-Adresse>/config を入力してください。
2. 左側の**Security**タイルをクリックし、次に**Certificate**をクリックします。



3. **Auto-generate certificate**で、**Disabled**を選択します。
4. 右上のチェックマークをクリックして変更を適用します。

⇨ 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 [▶ 61]）。

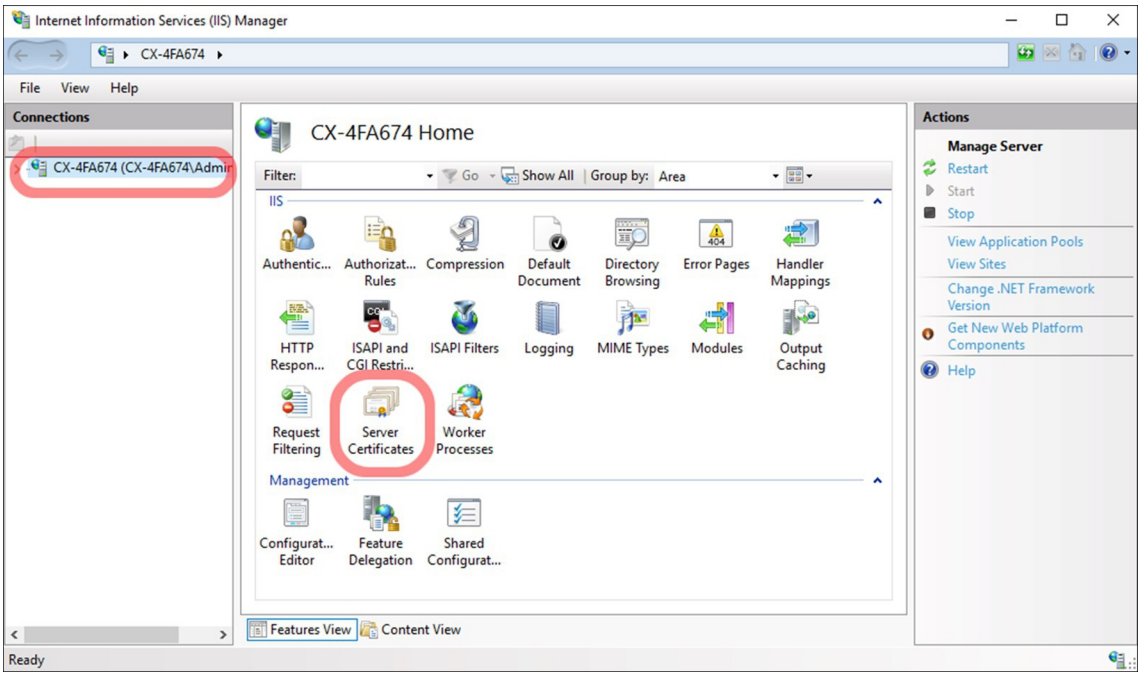
6.7.2 HTTPS証明書のリクエスト

ベッコフの産業用PCで使用されるHTTPSサーバーは、Windowsに付属するインターネットインフォメーションサービス（IIS）サーバーです。通常、IISサーバーの場合、認証局（CA）が発行した証明書をインストールする方法について、インストール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。これは、認証のために自分のWindowsドメイン内のソフトウェアインスタンスを使用する場合に特に当てはまります。それ以外の場合は、以下のステップで説明します。

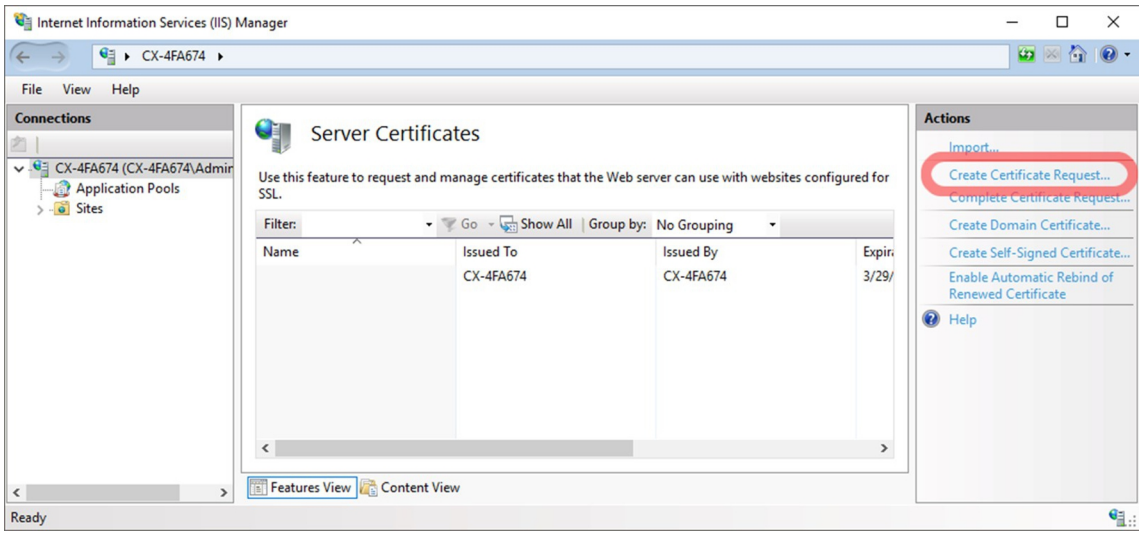
まず、産業用PCのIIS Managerを使用して証明書署名要求（CSR）を作成し、その指示に従ってリクエストを認証局に転送します。その後、認証局からサーバー証明書と中間証明書が提供され、証明書署名要求が作成されます。

以下の手順に従ってください。

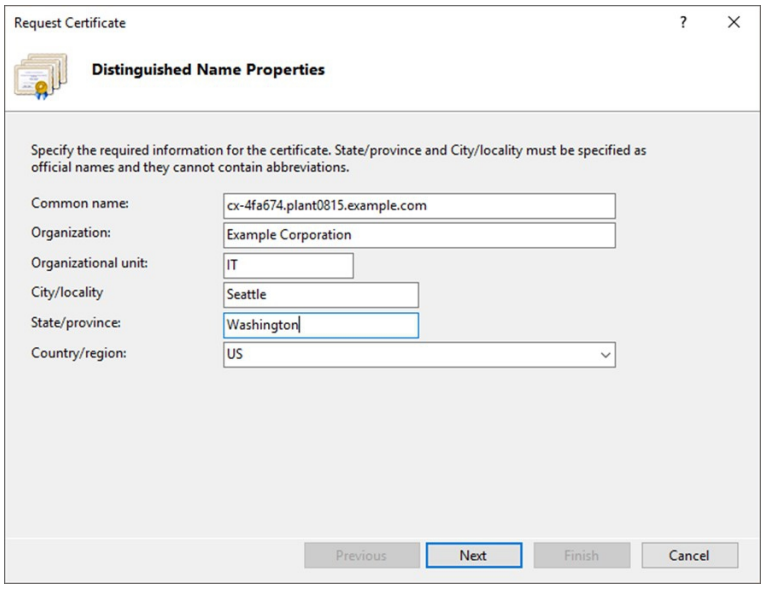
1. 産業用PCのInternet Information Services(IIS)Managerを管理者として開きます。
2. 左側の**Connections**メニューからWebサーバーを選択し、**Server Certificates**をダブルクリックします。



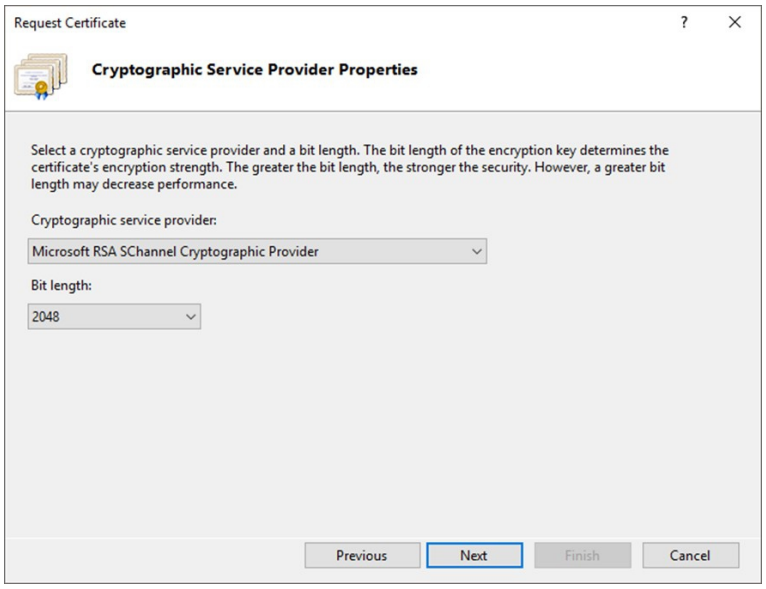
3. **Actions**セクションで**Create Certificate Request**を選択し、要件に従ってフォームに記入します。



4. 互換性の理由から、クライアントから産業用PCに到達できる完全修飾ドメイン名（DNS名）を**Common name**のフィールドに入力する必要があります。DNS名がない場合は、IPアドレスを使用することもできます。一般的には、顧客がURLでリクエストを行う際にアプリケーションで使用する名前またはIPアドレスでなければなりません。代替IPアドレスまたはDNS名を指定する必要がある場合は、認証局に依頼して、発行した証明書の拡張子（サブジェクト代替名）として入力してもらいます。このような追加の要求は、CSRの場合とは異なる方法で行われます。



5. 必要に応じて強力なキーを作成することを検討してください。1024ビットのRSAはもはや強力とはみなされません。



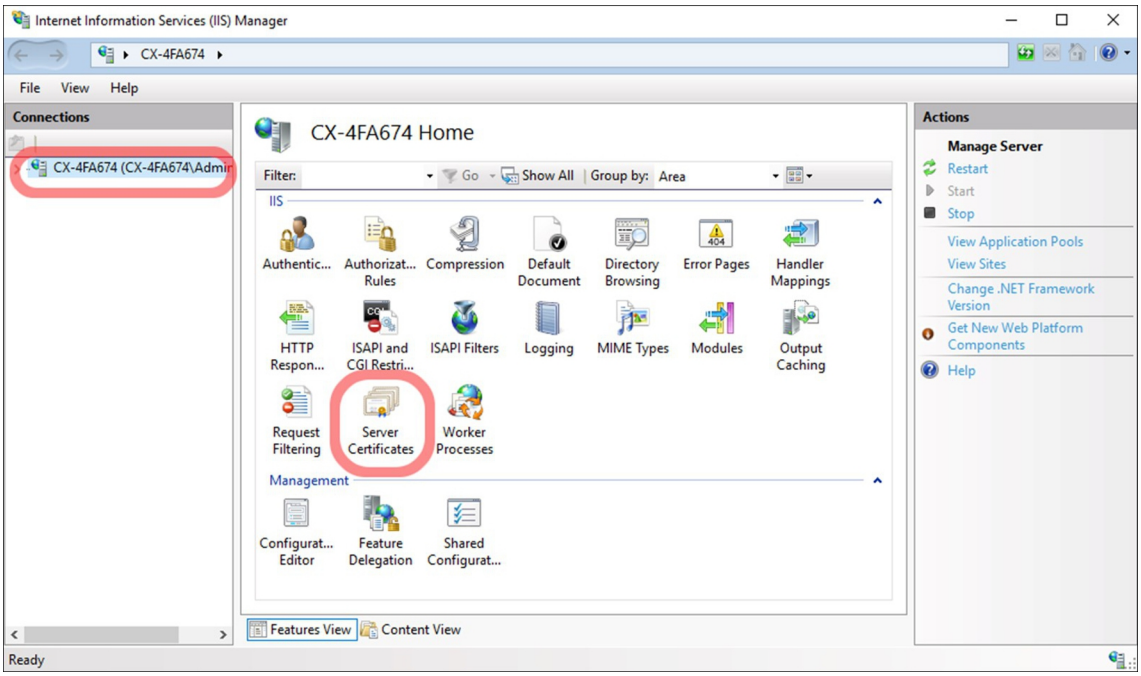
⇨ CSRファイルを保存し、認証局に送信します。認証局から応答を受け取ったら、次のステップは証明書をインポートすることです（以下を参照：証明書のインポート [▶ 64]）。

6.7.3 証明書のインポート

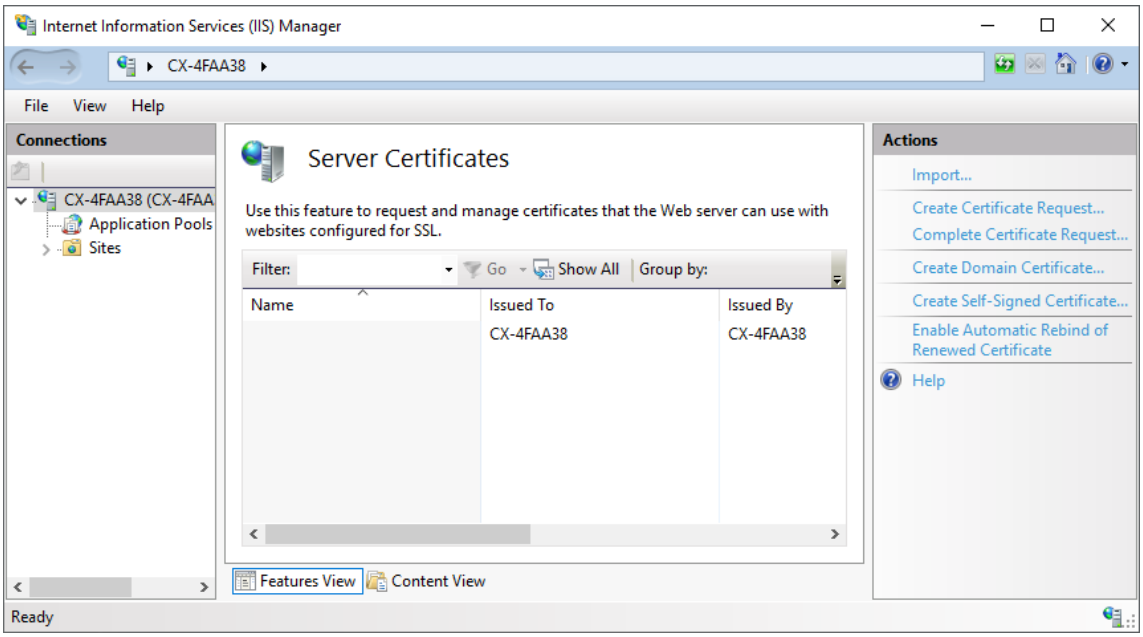
証明書署名要求(CSR)を認証局(CA)に送信すると、応答ファイルが送られてきます。応答ファイルを産業用PCにコピーし、以下の手順を実行してください。複数のファイルを受け取った場合は、証明書チェーン全体を含む拡張子 *.p7b のファイルを使用するのが望ましいです。

以下の手順に従ってください。

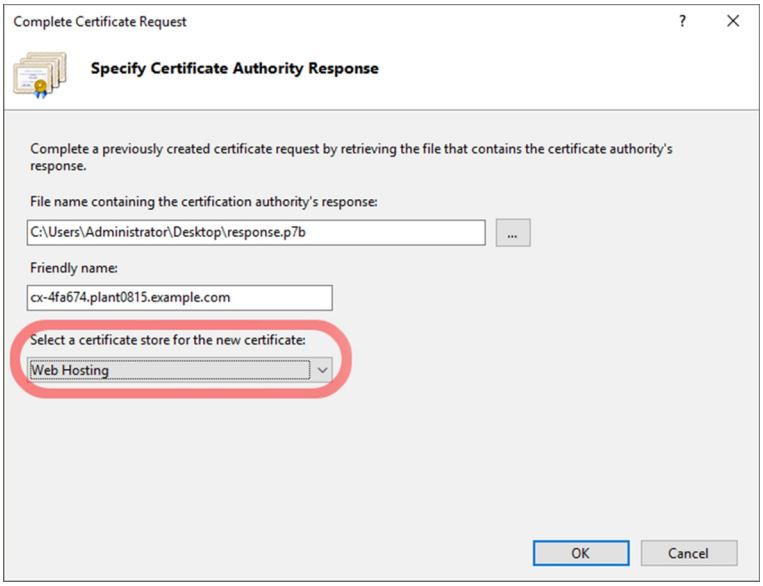
1. 産業用PCのInternet Information Services(IIS)Managerを管理者として開きます。
2. 左側の**Connections**メニューからWebサーバーを選択し、**Server Certificates**をダブルクリックします。



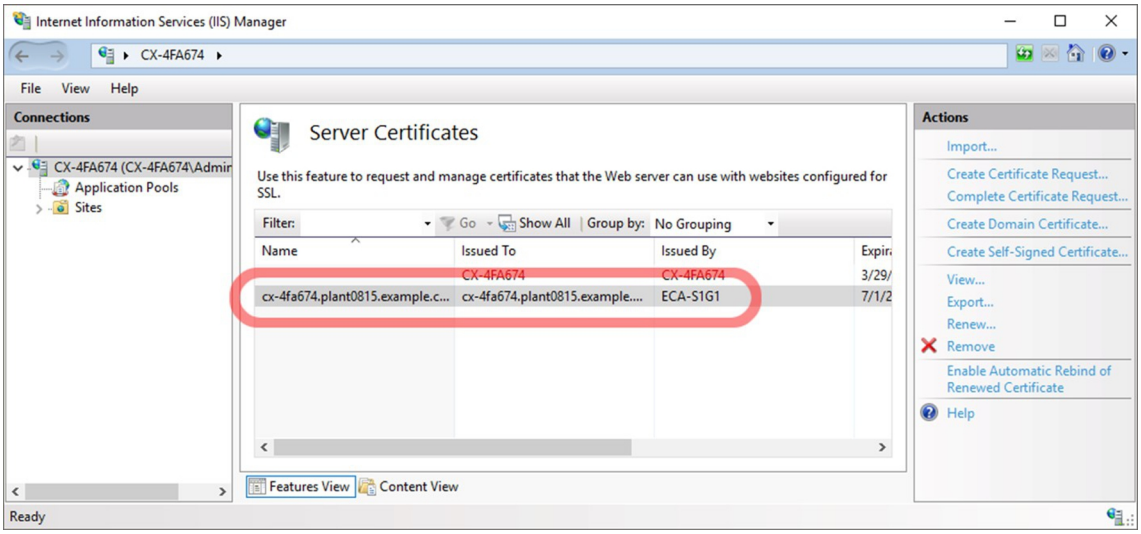
3. **Actions**セクションで、**Complete Certificate Request**オプションをクリックし、インポートする*.p7bファイル拡張子の証明書をロードします。



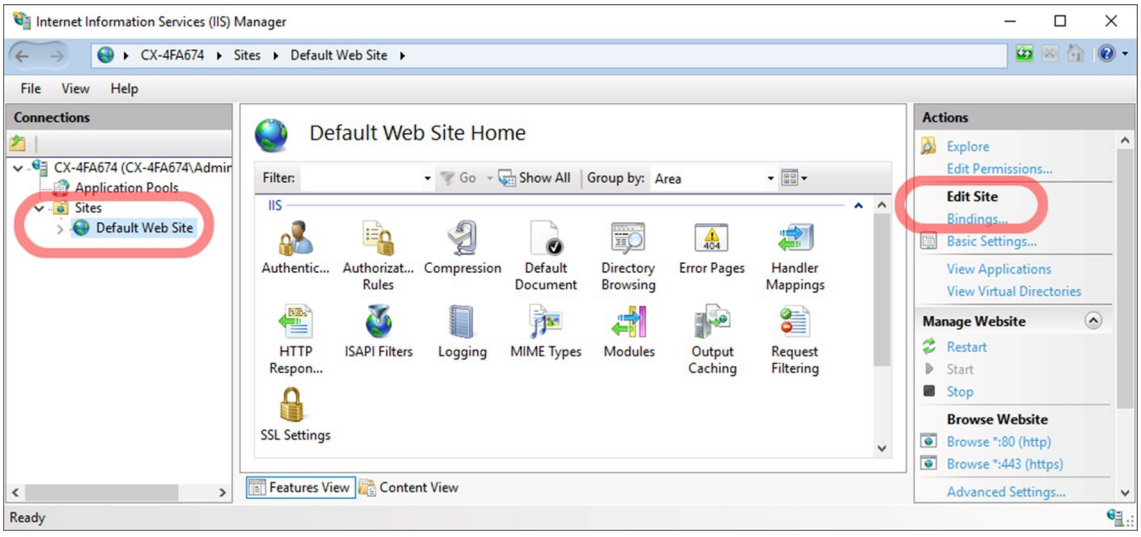
4. **Specify Certificate Authority Response**ウィンドウが表示されます。証明書に名前を付けて、証明書ストアに保存すします。理想的には、証明書署名要求（CSR）の際に**Common Name**フィールドで選択したのと同じ値を選択します。証明書ストアの**Web Hosting**オプションを選択することを忘れないでください。



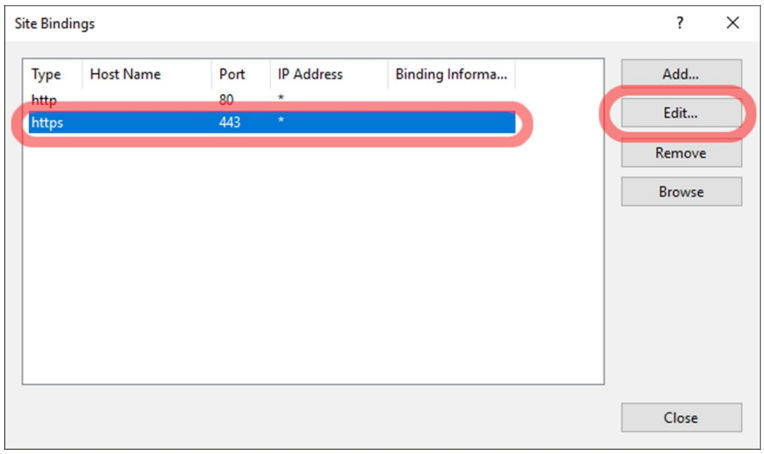
5. インポート後、証明書は利用可能なサーバー証明書のリストに表示されます。



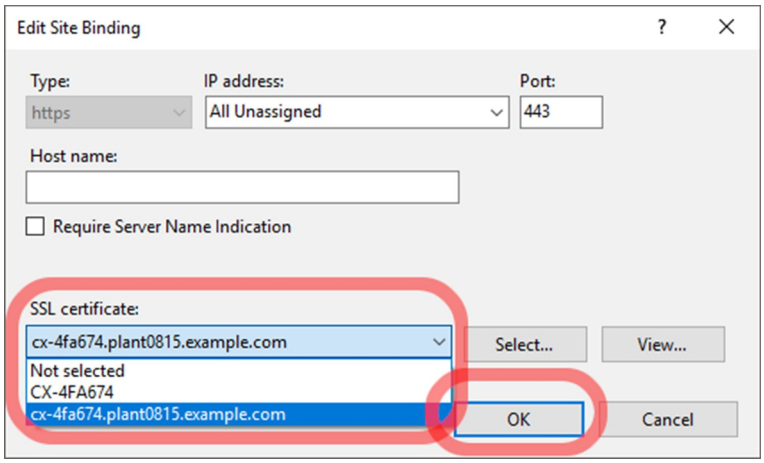
6. 左側の**Default Web Site**をクリックし、**Edit Site**メニューの**Bindings**をクリックします。



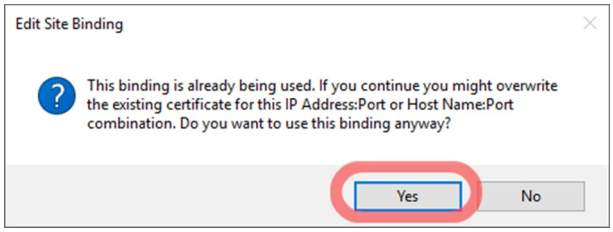
7. **https**をクリックし、**Edit**をクリックします。



8. **SSL certificate**でインポートした証明書を選択し、**OK**で受け入れます。



9. 以前の証明書を置き換え、代わりに新しく作成した証明書を使用する設定を確定します。



⇨ 設定後、産業用PCは直ちに新しい証明書を使用します。Webブラウザなどのクライアントから確認できます。接続するには、Webブラウザを再起動するか、キャッシュをクリアする必要があるかもしれません。

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 *5:* 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 *6:* 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 *7: 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 *8: 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.

Microsoft, Microsoft Azure, Microsoft Edge, PowerShell, Visual Studio, Windows and Xbox are trademarks of the Microsoft group of companies.

詳細はこちら:
www.beckhoff.com

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