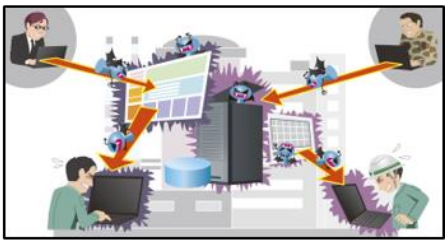
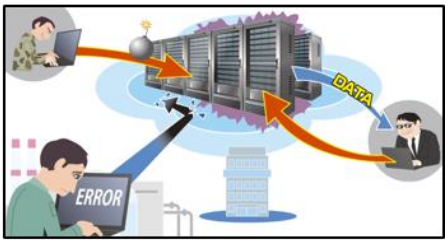
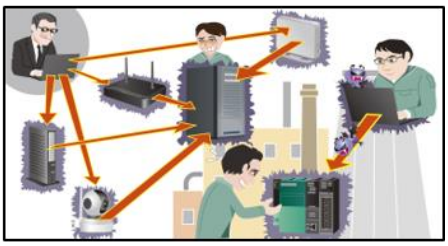
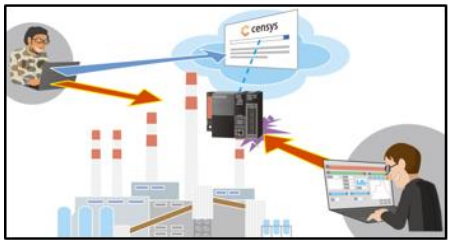
ドイツ連邦政府　情報セキュリティ庁（BSI）

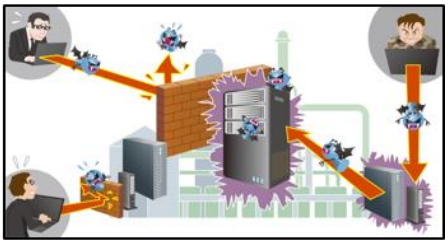
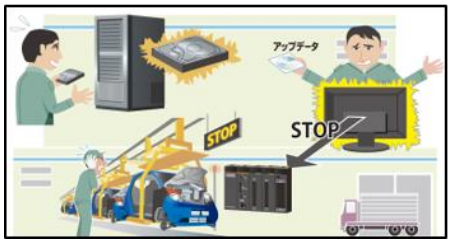
産業用制御システム（ICS）のセキュリティ

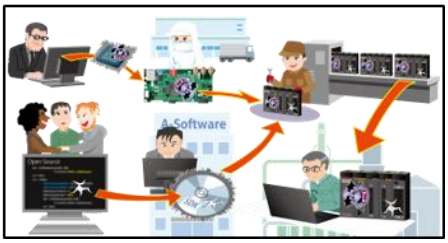
10大脅威と対策　2022





2022 年 12 月

IPA 独立行政法人**情報処理推進機構**
セキュリティセンター

2022 年 12 月 5 日
独立行政法人情報処理推進機構（IPA）

ドイツ連邦政府 情報セキュリティ庁（BSI）
「産業用制御システム（ICS）のセキュリティ - 10 大脅威と対策 2022」

This is a translation undertaken by IPA and therefore is not official translation of BSI.
The official version is in English and on the BSI site
https://www.bsi.bund.de/

本文書は、ドイツ連邦政府 情報セキュリティ庁（BSI）の文書 “Industrial Control System Security - Top 10 Threats and Countermeasures 2022”（英語版：2022 年 5 月 31 日発行）を独立行政法人 情報処理推進機構（IPA）が翻訳し、脅威の概要を示すイラストを追加したものであり、BSI による公式の翻訳ではありません。日本語へ翻訳した本文書の著作権は、IPA に帰属します。

本文書は、原文にできるだけ忠実に翻訳するよう努めていますが、完全性、正確性を保証するものではありません。翻訳監修主体である IPA は、本翻訳文書に記載されている情報より生じる損失または損害に対して、いかなる人物あるいは団体にも責任を負うものではありません。原文のありのままの内容を理解する必要のある場合は、BSI ウェブサイトに掲載されている原文をお読み下さい。

Industrial Control System Security :
Top 10 threats and countermeasures 2022 [English] v1.5
https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_005E.html

目次

推奨事項：稼働中の IT

産業用制御システム（ICS）のセキュリティ

10 大脅威と対策 2022

総称して産業用制御システム（ICS、IACS）と呼ばれる製造システムやプロセスオートメーションシステムは、物理的なプロセスを扱う、ほぼすべてのインフラで使用されている。その用途は、エネルギーの発電・送電、ガス・水の供給から産業オートメーション、交通管制技術、最新のビル管理まで多岐にわたる。これら ICS は、益々従来の IT システムと同様のサイバー脅威にさらされている。ICS のオペレータは、インシデントの頻度の増加と新たに発見される脆弱性といった問題に早急に対応する必要があり、したがって標的型／非標的型マルウェアおよび高度な技術を駆使した ICS インフラへの攻撃のリスクと被害の可能性を考慮しなければならない。これは直接インターネットに接続されたシステムおよび間接的にサイバー攻撃を受けるシステムにあてはまる。

BSI は、サイバーセキュリティに関する分析と産業界との協力の一環として、現在 ICS がさらされている最も危険度の高い現在の脅威のリストをまとめた。特定された脅威は下記の構成で表されている。

1. 問題および原因の説明：脆弱性または脅威の状況の存在に寄与する原因や基礎となる条件。
2. 想定される脅威のシナリオ：上記 1.で説明した問題が攻撃に悪用される可能性の説明。
3. 対策：脅威を軽減するため、あるいは残留リスクを最小化するために、現時点で適切と考えられる対策の特定。

本文書は、脅威のシナリオと対策の完全なリストではない。むしろ本文書に記載されているシナリオは、それぞれの脅威のスコープの範囲を説明することを目的としている。記載されている対策は、それぞれの脅威に対抗するための出発点であり、それぞれの脅威を防御するために必要な、全体的な対策の最初の評価を可能とするものである。具体的にどの対策が適しているか、どの代替案が必要かは、最終的にはそれぞれの用途で検討し、リスク分析の枠内で評価しなければならない。その際、特に有効性と経済効率に留意しなければならない。すべてのケースにおいて、運用、リアルタイム要件、安全要件との適合性が確保されなければならない。さらに、セキュリティ対策の実施が、保証やサポートサービスの喪失を招いてはならない。

はじめの一歩として、この 10 大脅威には、結果として生じるリスクの簡単な評価と、各自のセキュリティレベルの最初の個別評価のためのセルフチェックが含まれている。

脅威とその被害

ICS のリスクは、脆弱性が存在することによって、ICS、ひいては企業に被害をもたらす脅威から生じる。ICS にとって最も危険で頻繁に発生する脅威を、次の表にまとめている。

最初の攻撃と二次攻撃は区別されている。最初の攻撃は、攻撃者が産業用システムや企業に侵入することに焦点が当てられており、二次攻撃は、他の内部システムへのアクセスを可能とすることに焦点が当てられている。

10 大脅威	2019 年からの傾向
リムーバブルメディアやモバイルシステム経由のマルウェア感染	→
インターネットやイントラネット経由のマルウェア感染	↑
ヒューマンエラーと妨害行為	→
外部ネットワークやクラウドコンポーネントへの攻撃	↗
ソーシャルエンジニアリングとフィッシング	→
DoS/DDoS 攻撃	→
インターネットに接続された制御コンポーネント	↗
リモートメンテナンスアクセスからの侵入	↗
技術的な不具合と不可抗力	→
サプライチェーンにおけるソフトウェアおよびハードウェアの脆弱性	↑

このような最初の攻撃の多くを起点として、攻撃者は後続の攻撃によって次々と標的の企業全体に攻撃を拡散することができる。次の図は、そのつながりを表している。

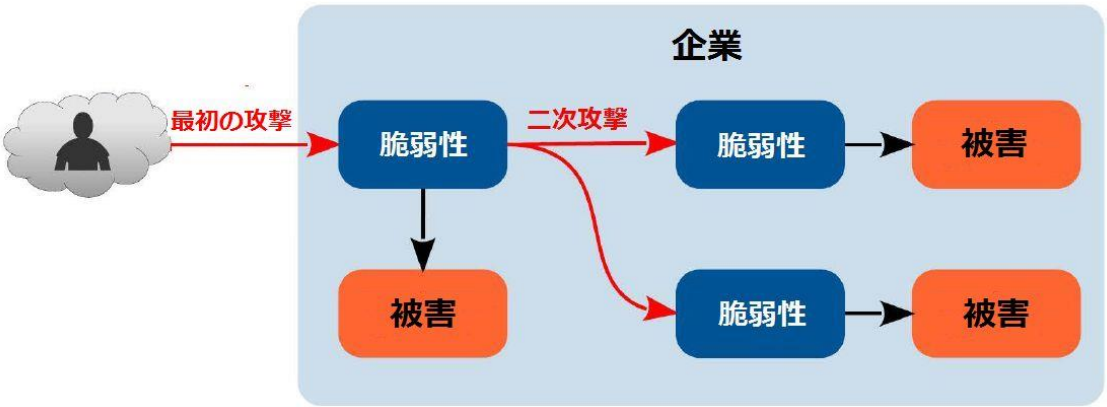


図 1 ：最初の攻撃、二次攻撃、および被害の結果のシーケンス

二次攻撃には、特に下記が含まれる。

・権限昇格：産業環境における、OS、アプリケーションサーバ、データベースなどの既存の標準の IT コンポーネントには、しばしば攻撃者が悪用できるバグと脆弱性が含まれている。

・他の内部システムへの不正アクセス：特に、企業ネットワークや制御ネットワークのサービスおよびコンポーネントが認証および認可に十分な方法を使用していない場合、または基本的な強化対策がとられていない場合、内部の不正行為者による攻撃や後続の攻撃が容易となる。

・フィールドバス通信の不正操作：現在、ほとんどの制御コンポーネントがプレーンテキストプロトコルを介して通信しており保護されていないため、制御コマンドの読み取り、改ざん、または不正発行が容易となる。

・ネットワークコンポーネントの不正操作：ルータやファイアウォールなどのコンポーネントは、セキュリティメカニズムを無効化したり、データトラフィックを再ルーティングしたりするために、攻撃者に不正操作される。

・ランサムウェアの展開：ランサムウェアはデータやシステムを暗号化することが多い。バックアップがない場合、身代金の支払いは推奨されないので、多くの場合、復旧が不可能となる。

このような後続の攻撃に対抗する対策の実装は、いわゆる多層防御の概念の観点において、最初の攻撃に対する基本的な防御を確立した後に行う必要がある 。[1]

組織的な欠陥、知識不足、またはヒューマンエラーは攻撃を助長し、後続の攻撃を容易にする。さらに、攻撃の検出と、攻撃成功後のシステムのクリーンアップと復旧も困難になる。潜在的な関連する被害は、様々な形で発生する可能性があり、かなり重大であると評価せざるを得ない。

・セーフティ手順またはセーフティシステムの発動、不正操作
　→人や環境への被害、生産の損失
　→機器への物理的被害
・ICS の一部または全体の可用性の途絶
　→生産の損失
・データ漏洩
　→ノウハウ（知的財産）の損失
・システムやパラメータの不正操作

[1] https://us-cert.cisa.gov/ics/Recommended-Practices

→製品の品質低下

以降にリストされている対策は、最初の防衛線を形成する。これらの実装には最高の優先度が割り当てられることが望ましい。

アセスメントの基準

実際のセキュリティインシデントからの経験、脅威、産業界からのフィードバックを評価の基礎として、最も頻度の高い 10 の脅威を示している。傾向の指標は現在の推移を示しており、傾向が変わらない、あるいは減少傾向である場合でも、IT セキュリティに対する脅威は依然として存在するため、企業の全体像を把握する必要がある。

リスクの評価には脅威の普及度という評価基準が不可欠と考えられるため、過去 2014 年と 2016 年の評価基準とは異なっている。これは主に、以前使用された他の評価基準（露呈度（訳注：脅威に対する脆弱性が存在する箇所の特定がどれくらい容易か）、悪用度（訳注：脅威に対する脆弱性の悪用が技術的・工数的にどのくらい容易か）、および検出度（訳注：攻撃の検知がどのくらい容易か）の変化がわずかであるのに対し、脅威の普及度は犯罪グループの活動によって大きく変化し得るという事実による。したがって、本文書における脅威の順序は、順位を表しているものではない。

結果として生じる自社にとっての脅威とリスクを評価するために、特定された脅威に対する技術的または組織的な実現可能性に基づいて、それぞれの対策を判断することが望ましい。また、この評価は各対策のコストの見積もりと一緒に行うことが望ましい。そして、このコストの見積もりは、それぞれのケースにおける事業被害、すなわち企業にとっての経済的な影響と比較し、判断することが望ましい。原則として、これは一般的な条件と起こり得る後続の攻撃を考慮して、事業者自身によってのみ実施することができる。

変更点の概要

「10 大脅威と対策 2019」と比較すると、悪用に関して多くの脅威に変化は見られない。しかしこれは、これらの脅威が減少し、そのため注意を払う必要がなくなったことを意味するものではない。全体として、リストアップされたすべての脅威について高い危険度が想定される。

スマートデバイスの脅威は、単独の章ではなく、リムーバブルメディアとモバイルシステムの脅威の一部となり、重要なポイントはそこに統合されている。

新たに追加されたのは、サプライチェーンにおけるソフトウェアとハードウェアの脆弱性がもたらす脅威である。今後、この点についてさらに注意を払う必要がある。

リムーバブルメディアや外部機器経由のマルウェア感染

問題と原因の説明

ICS コンポーネントの設定・メンテナンスや ICS とオフィスネットワーク間のデータ転送のために、ノート PC、スマートフォンやタブレットなどのスマートデバイス、プログラミング機器や USB メモリなどのリムーバルメディアが使われることがよくある。これらの機器の場合、使用される場所が明確に規定されていなかったり、オペレータにはわからなかったりすることがある。例えば、ノート PC やスマートフォンは私的利用が可能であり、社外の人間が自分の機器を持ち歩いているのが普通である。また、社外のメンテナンス担当者が別の会社で使用する可能性のある、外部のデータやメンテナンス用ソフトが入ったノート PC の使用にも、リスクが伴う。

想定される脅威のシナリオ

1. リムーバルメディアは、例えば社内ネットワークまたはプライベート環境で感染している可能性がある。そのような方法によって、マルウェアは ICS ネットワークに直接侵入することができる。
2. メンテナンスに使用されるノート PC やスマートデバイスは、インターネット、社内ネットワーク、または社外サービスプロバイダのそれぞれのインフラにアクセスする際に感染している可能性がある。これらが ICS ネットワークで使用されるとすぐに、システムとコンポーネントが悪意のあるコードに感染する。
3. プロジェクトファイルや実行可能アプリケーションには、感染またはデータ漏洩につながる悪意のあるコードが含まれている場合がある。
4. モバイルシステム（スマートフォンなど）や機密情報（パスワードや設定された ICS ネットワークへのリモートアクセスなど）を含む機器の盗難や紛失。

対策

1. リムーバブルメディアに関する厳格な組織ポリシーと技術的管理策の確立：
   a. 承認されたリムーバルメディアのインベントリ（一覧表）の作成とホワイトリストへの登録。
   b. モバイル機器のセキュリティ境界（メンテナンス機器とは異なる OS を使用するマシンに導入されるウイルス対策およびファイルのホワイトリスト）。
   c. 会社所有の専用の、できれば個別のリムーバルメディアの使用。
   d. ICS ネットワーク専用のリムーバブルメディアの使用。
   e. 樹脂封止、USB ロック、またはポートの取り外しなどによる、USB 機器の（不正な）接続に対する物理的障壁。
   f. データ記憶媒体の完全な暗号化。
2. メンテナンスに使用される外部機器、スマートフォン、タブレットなどのスマートデバイスに対する厳格な組織ポリシーと技術的管理策の確立：
   a. アクセス制限または使用制限。
   b. 前述の管理策の対象となるリムーバルメディアのみを介したデータ交換。
   c. 外部サービスプロバイダからのアクセスに対する検疫ネットワークの構築。
   d. 実際のシステムにアクセスする前に、持ち込まれた機器のウイルススキャンの実施。
   e. オペレータが保管するメンテナンス用ノート PC の完全な暗号化。
   f. ソフトウェア/アプリの制限と管理。

インターネットやイントラネット経由のマルウェア感染

問題と原因の説明

企業のネットワークでは OS、ウェブサーバやデータベースなど標準的なコンポーネントが使用されている。また、通常、ブラウザや電子メールクライアントはインターネットに接続されている。これらコンポーネントにおいては、ほぼ毎日、新たな脆弱性が発見されている。攻撃者はそれらの脆弱性を、イントラネットに侵入してマルウェアを展開するために悪用する。このマルウェアは、例えば、内部の不正行為者によって、イントラネットに置かれることもある。

ICS 環境でのイーサネットベースのネットワークとプロトコルの普及、社内ネットワーク（ファイルサーバ、ERP、MES 等）との接続も、マルウェアの展開を容易にしている。攻撃者が社内ネットワークへの侵入に成功した場合、または既にイントラネットに侵入している場合、直接または後続の攻撃によって、ICS ネットワークに侵入することが多い。このような接続に従業員が必ずしも気付くとは限らない。

ICS ネットワークまたは ICS に近いネットワークから他のネットワーク（特にインターネット）にアクセスすると、システムが直接マルウェアに感染する可能性もある。

想定される脅威のシナリオ

1. 電子メールの添付ファイルや細工されたオフィス文書など、オフィスコミュニケーションソフトウェア経由のシステムの感染。
2. 細工された外部ウェブサイト（例えば、ドライブバイダウンロードを実行するために、ユーザが介在することなく、すなわちウェブサイトにアクセスするだけで被害者が感染するよう、細工されたウェブサイト）。一例として、コントロールルームまたは他の操作コントロールの一部であるシステムでのインターネットの閲覧が挙げられる。

3. 社内ネットワークと ICS ネットワーク間の、文書化されていない、または保護されていない接続。
4. 企業ウェブページへの攻撃の実施（SQL インジェクション、クロスサイトスクリプティングなど）。
5. ICS コンポーネントに含まれる、マルウェアによる操作によって悪用される可能性がある既知の脆弱性。
6. マルウェアに感染している、あるいは感染経路となり得る私物のハードウェア（スマートフォン用 Wi-Fi ルータ、ゲーム用 PC、ゲーム機など）を職員が設置すること（「ヒューマンエラーと妨害行為」も参照）。

対策

1. ICS ネットワークへの攻撃経路を大幅に排除するために、ファイアウォールや VPN ソリューションで、異なるネットワークを最大限分離（セグメンテーション）する。保護されていないシステム、パッチが適用できないシステムを封鎖する（いわゆる"secure islands"）。
2. 境界における従来の予防策（ファイアウォール、ウイルス対策ソフト、侵入検知システムなど）または ICS での従来の予防策（ファイウォール、アプリケーション許可リストなど）の使用。
3. 重要な情報の漏洩を防ぐために、企業内（ファイルサーバ上またはデータベース内など）で利用可能な情報を制限する（need to know の原則）。
4. オフィスおよびバックエンドネットワーク、可能であれば ICS ネットワークの OS およびアプリケーションに定期的かつタイムリーにパッチを適用する。
5. ネットワークベースおよびホストベースの IDS によって、異常な接続、転送量、接続試行、活動を監視する。
6. オフィスや ICS で使用されるすべての IT コンポーネント（サービス、コンピュータ）を可能な限り堅牢にする。

ヒューマンエラーと妨害行為

問題と原因の説明

ICS 環境で働く人は、安全とセキュリティに関して特別な立場にある。これは、システムにアクセスできるか、またはリモートで作業するかに関係なく、社内スタッフおよびメンテナンスや建築などのすべての外部要員も同様である。セキュリティは技術的対策だけでは保証できないため、組織的な規則が必要となる。

想定される脅威のシナリオ

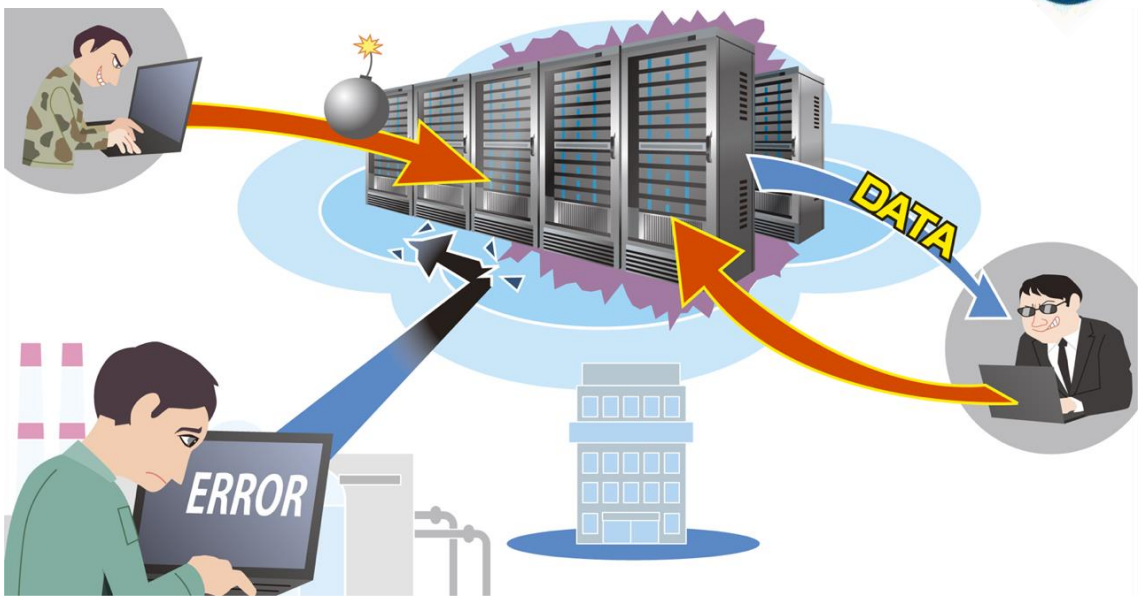
1. セキュリティ関連コンポーネント（ファイアウォールなど）、ネットワークコンポーネント、ICS コンポーネントの設定ミス。
2. 特に、計画立てて行われていないアップデートまたはパッチのインストールは、個々のコンポーネントの機能性とそれらの相互作用の問題につながる可能性がある。
3. 意図的な行動の副作用を考慮する（機器や設備の損傷、盗聴器の設置など）。
4. 未許可のソフトウェアまたはハードウェアによるシステムの侵害。ハードウェアの場合、ゲーム機、デジタルカメラ、スマートフォン、無線 LAN ルータ、またはスタッフが所有するその他の USB 機器が含まれる。
5. インフラおよびセキュリティコンポーネントに、承認されていない設定を作成する（モバイル機器からの不正な外部アクセスを許可するファイアウォール・ルールの追加など）。

上記のシナリオは、原則としてスパイ行為と妨害行為によって引き起こされるが、不注意、その他のヒューマンエラー、不正行為によっても引き起こされる可能性がある。特に、これらのインシデントは、組織上の欠陥によって可用性が著しく損なわれることにつながる。多くの侵害は、そのような欠陥によってのみ起こる。

対策

1. 情報は知る必要のある者に対してのみ与え、知る必要のない者には与えないという原則（need to know）を確立する：システムの詳細やパスワード等についての知識、機密データへのアクセスは可能な限り制限することが望ましい。
2. 機能コンポーネントおよび安全に特化したコンポーネントの操作と管理能力を確保するために、献身的で、資格があり、他の人と関わりを持つ従業員に適した状況を作り出す。資格やトレーニングプログラム、意識向上策は、長期的に設計し、義務化するべきである。
3. 制御システムおよび生産関連システムのインターネットアクセスを無効にする。また、オペレータが使用できる非 ICS タスク用コンポーネント（Microsoft Office、電子メール、ERP など）の提供は、十分に保護した上で、別のネットワークに統合する。
4. 新規雇用者、退職者、外部請負業者（メーカやサービスプロバイダなど）向けの標準化されたプロセスの確立。
5. 従業員による技術システムの取り扱いに関する適切なガイドライン（ポリシーと手順）（リムーバブルデータ記憶媒体の取り扱い、電子メールや SNS でのコミュニケーションにおける振る舞い、パスワードのガイドライン、個人用のソフトウェアのインストールなど）
6. 特に ICS ネットワークの重要なプロセスについて、適切なポリシーを確立する。例えば、セキュリティおよび構成管理に関する仕様で、セキュリティ専門家やその他の関連する役割の関与を規定し、変更またはアップデートが彼らと調整した後にのみ行われるようにする。すべての仕様を文書化し、可能であれば付随する予防策（「dual control の原則」など）を講じることが重要である。
7. システムの状態と設定の自動監視。
8. 事業（計画/企画）の内容やシステム構成情報のセキュアな保管。

外部ネットワークやクラウドコンポーネントの攻撃



問題と原因の説明

IT コンポーネントまたはアプリケーションのアウトソーシング（外部委託）という従来の IT で広まっている傾向は、ICS でも見られる。多くの場合、これらは実際のプロセスを直接制御するコンポーネントではない。しかし、ヒストリアンでのデータ取得や処理、マシンの設定や製造プロセスの最適化のための複雑なモデルの計算（ビッグデータ、デジタルツイン）の分野では、外部から操作するソフトウェアコンポーネントを提供するプロバイダが増えてきている。また、セキュリティに特化したコンポーネントが、クラウドベースのソリューションとして提供されることもある。例えば、リモートメンテナンスソリューションのプロバイダは、メンテナンス技術者が各コンポーネントへアクセスできるクラウド上に、リモートアクセス用のクライアントシステムを配置している。

現在、このようなソリューションは、特に中小企業（SME: Small and Medium Enterprise）にとって興味深いものである。一企業が自社で運用することは多くの場合不経済であるが、クラウドではスケーラビリティ、冗長性、従量制などの費用対効果に優れた利点があるからである。しかし、このようなクラウドソリューションでは、システムオペレータがこれらのコンポーネントのセキュリティとそれに関連する侵害の検出能力に対して非常に限定的な制御しかできないことになる。さらに、これらのコンポーネントは、生産設備に直接接続できる場合がある。

想定される脅威のシナリオ

1. DoS 攻撃などによる、生産設備とアウトソース（クラウド）コンポーネント間の通信の中断または遮断。カスケード効果によって、生産が損なわれる可能性がある。
2. クラウドサービスに一方的に依存し過ぎると、障害の影響で、拠点間のインフラや生産設備

が危険にさらされる可能性がある。
3. 外部に保存されたデータにアクセス（データの盗難、削除）するための、実装上の誤りや不十分なセキュリティメカニズムの悪用。
4. クラウドサービスの提供者が、各顧客の環境を十分に分離していない場合、クラウドサービスへの攻撃が、侵害（巻き添え被害）につながる可能性がある。

対策

1. 外部コンポーネントのオペレータが、たとえばサービスレベル合意書（SLA: Service Level Agreement）などにより、十分なセキュリティレベルに対する契約上の義務を負う。
2. 信頼できる、可能であれば認定されたサービスプロバイダの使用。
3. 制御を維持し、プロセスのノウハウを保護するためにプライベートクラウドを運用する。
4. クラウドに保存されているデータを保護するために、十分に強力な暗号メカニズム（暗号化、完全性保護）を使用する。
5. ローカルの生産設備と外部コンポーネント間の接続をセキュアにするために、仮想プライベートネットワーク（VPN）を使用する。

ソーシャルエンジニアリングとフィッシング

問題と原因の説明

ソーシャルエンジニアリングは、主に非技術的な行為によって情報または IT システムへ不正にアクセスする方法で、好奇心、親切心、信頼、恐れ、権威の尊重などの人間の特性を悪用する。これらの特性は、攻撃者が従業員に軽率な、または不注意な行動をとるよう誘導するための戦略として機能することが多い。典型的な例が、詐欺メール（フィッシングメール）で、従業員に、マルウェアが仕込まれた添付ファイルを開くよう仕向けたり、細工されたウェブサイトへのリンクをクリックするよう仕向けたりする。この脅威は、インターネットやイントラネットを介したマルウェア感染と密接に関連している。

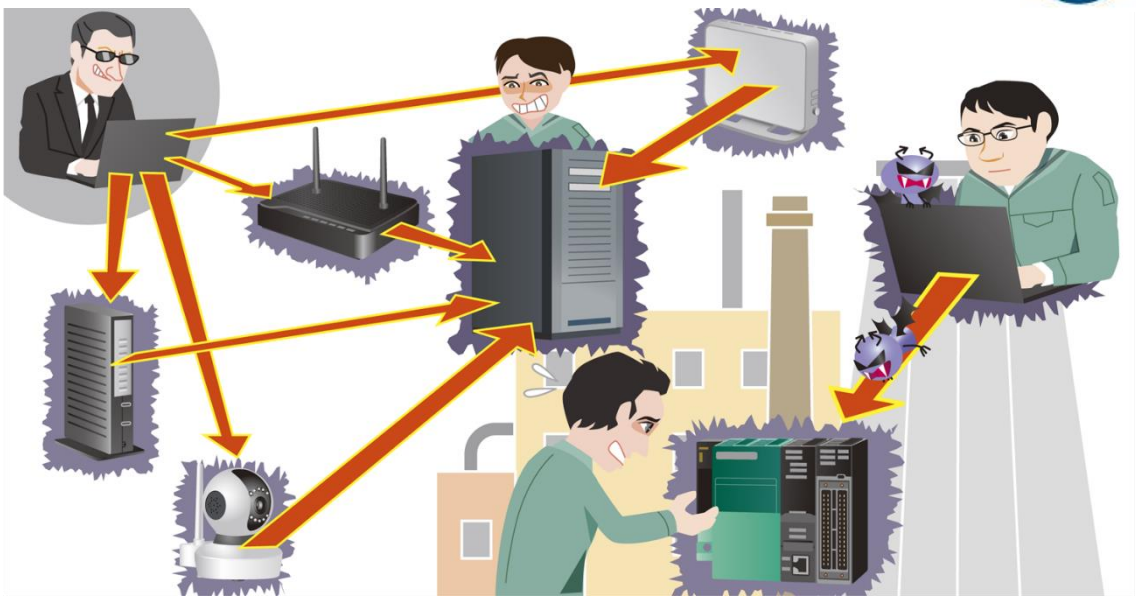
想定される脅威のシナリオ

1. 攻撃者が偽のメッセージを使用して、被害者のアクセス情報を取得したり、マルウェアを配布したりするフィッシング攻撃。
2. 一見無害に見えるリンクをクリックしたり、添付ファイルを開いたりすると、トロイの木馬やランサムウェアなどのマルウェアをインストールするメッセージ。
3. 攻撃者が、通常、少人数に対する攻撃で使用するが、各攻撃対象者に合わせた電子メールを送信するスピアフィッシング攻撃。企業のウェブサイトまたはソーシャルネットワークなどの他の情報源から取得した公開情報が使用される。
4. 攻撃者は、自信ありげで友好的なふりをしたり、他人になりすましたりする（例えば、技術者のふりをする）ことで、建物に不正アクセスすることができる。

対策

1. 特定の攻撃対象グループに対して、セキュリティ意識向上トレーニングを定期的に実施する。
2. 組織的な対策：セキュリティポリシーを策定し、実施する。
   a. 事業にとって価値のある情報を識別し、分類する。
   b. データバックアップのコンセプトを確立する。
   c. 自社の従業員だけでなく、パートナーやサービスプロバイダに対しても、機密保持やデータ保護の宣言を導入する。
   d. 紙に印刷された情報の廃棄に関するガイドライン（例：シュレッダー）。
   e. デジタルデータ記憶媒体の安全な廃棄。
   f. モバイル機器の取り扱いに関する規制（プライバシーフィルム、金庫での保管など）
3. インシデントが発生した場合および発生した疑いがある場合に危険を知らせる手段を確立する。これらの手段は定義され、伝達することが必要である。また、報告する従業員にマイナスの結果をもたらしてはならない。
4. 適用される規制を実施するために、また、不正行為や攻撃を自動検出するために、技術的なセキュリティメカニズム（機器制御、ネットワークのセグメンテーション、アクセス制御など）を使用する。
5. データとアプリケーションを復元するための定期的なバックアップ。

DoS/DDoS 攻撃



問題と原因の説明

サービス拒否（DoS）攻撃を受けると、通信リンクが過負荷になったり、中断されたり、受信サーバが多くのリクエストによって過負荷になったりする。その結果、データ交換ができなくなったり、遅延したりする。このリスクは、特にインターネットに接続したシステムに存在する。リモートアクセスの場合、このインタフェースが過負荷になり、監視や制御ができなくなる可能性がある。そうすると、測定および制御データの送信ができなくなる。

また、無線インタフェースでは、無線周波数に干渉することで、このような事態が発生する可能性がある。

DoS/DDoS 攻撃の観測頻度と帯域幅は年々増加している。その傾向は、高い帯域幅を持つ単純な亜種から、アプリケーションに合わせた大掛かりで高度な形態へと移行している。攻撃者は、アプリケーションとインフラを考慮に入れ、対策にも対抗している。

想定される脅威のシナリオ

1. 重要なコンポーネントまたはリモートコンポーネントのインターネット接続に対する DoS/DDoS 攻撃。これは特に、攻撃者がレンタルできるボットネットなどを介して実行できる。
2. 個々のコンポーネントのインタフェースに対する DoS 攻撃：この場合、コンポーネントの処理ロジックが、特定のメッセージによって妨害され、クラッシュする。これは、制御デバイスまたは重要なコンポーネント（データベースやアプリケーションサーバなど）に影響を及ぼす可能性がある。

3. 無線接続（WLAN、LoRaWAN など）またはモバイルネットワーク（GSM、LTE、5 G など）への攻撃。これは、たとえば次の方法で実行できる。
   a. 対応する周波数範囲をカバーする妨害電波送信装置の使用。
   b. 偽の基地局、すなわち、攻撃されたシステムを偽の無線ネットワークに接続させる偽の基地局（訳注：通信機能抑止装置）の使用。
   c. 既存の接続を終了させる、特殊なデータパケットの送信。
4. ランサムウェア（Trickbot など[2]）を使用した DoS 攻撃。

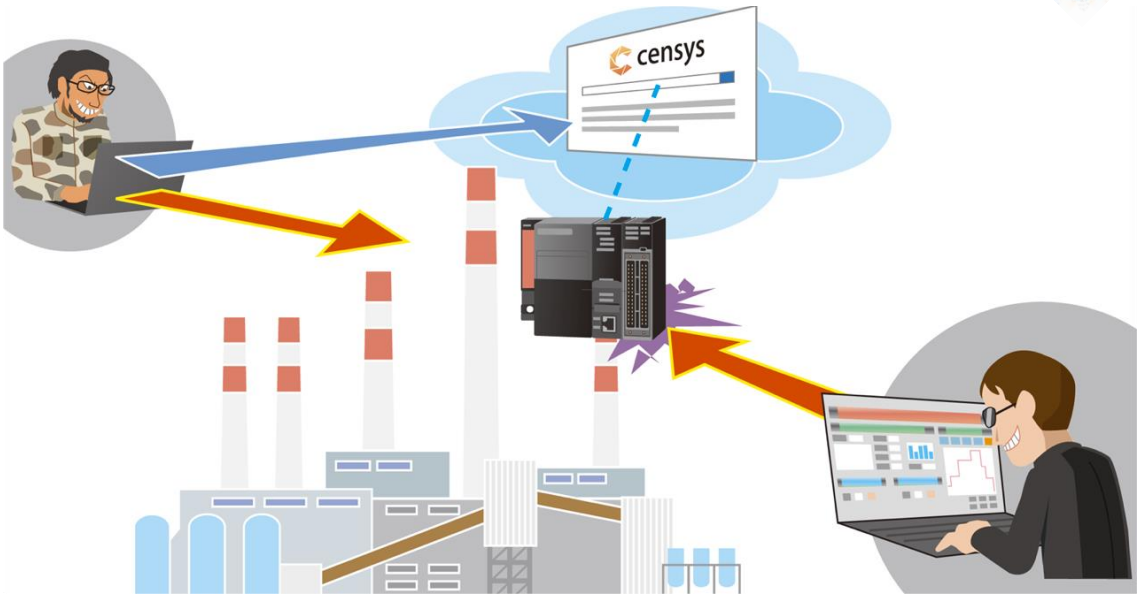
対策

1. ネットワーク接続と通信チャネルの厳密な設定と強化。
2. 重要な機能に専用の有線接続を使用する。
3. 該当する場合：侵入検知システム（IDS）を導入して、攻撃を検知し、代替チャネル経由で警告する。
4. 異なるプロトコルまたは通信パスを使用したコンポーネントの冗長接続。

上記対策に加えて、BSI は 「Allianz für Cyber-Sicherheit（訳注：サイバーセキュリティのためのアライアンス）」のウェブページで DDoS 緩和に関する文書を提供している[3]。自組織の対策と比較してみることが望ましい。

[2] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2020.pdf
[3] https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_002.html

インターネットに接続された制御コンポーネント



問題と原因の説明

製品ベンダからの勧告にもかかわらず、プログラマブルロジックコントローラ(PLC)などの ICS コンポーネントは、多くの場合、インターネットに直接接続されている。その結果、検索エンジンによって容易に検出される。さらに、これらのコンポーネントは、標準的な IT のような十分なセキュリティレベルを提供していないことが多い。また、これらのコンポーネントに脆弱性が発見された場合、パッチを（タイムリーに）インストールすることができない。したがって、追加のセキュリティメカニズムを実装することが早急に必要である。

想定される脅威のシナリオ

1. 一般的な検索エンジン（Google ハッキング）や Shodan[4]などの特殊な検索エンジン、または独自のインターネットスキャンによる制御コンポーネントの検索。
2. 保護されていないコンポーネントへの直接アクセス、または一般に公開されている標準的なパスワードを使用した、不正操作。
3. コンポーネントへのアクセス、または可用性を損なうことを目的としたウェブインタフェース（WWW）、FTP、SNMP、または TELNET などの利用可能なサービスの脆弱性の悪用。ICS のプロトコル（Modbus、BACnet など）にも直接アクセスされる場合が多い。これらのプロトコルには通常認証機能がないか、あっても弱いため、攻撃者は下流のコンポーネントに直接制御コマンドを送信することができる。

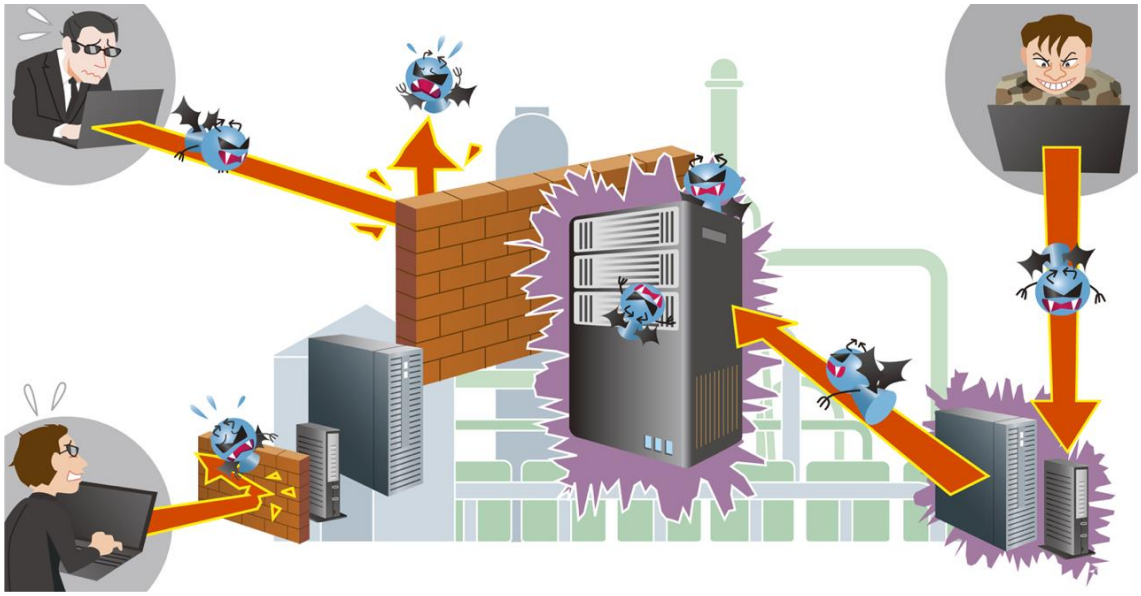
対策

1. 制御コンポーネントをインターネットに直接接続しない。

[4] https://www.shodan.io/

2. 不要なサービスの無効化、デフォルトパスワード（訳注：標準的なパスワードが用いられていることが多い）からの変更など、制御コンポーネントの設定の強化。
3. ファイアウォールや VPN ソリューションなどの追加管理策の使用。
4. 可能であれば、アップデートまたはパッチによる脆弱性を有する製品のタイムリーな更新。

リモートメンテナンスアクセスからの侵入



問題と原因の説明

ICS では、メンテナンス目的での外部からのアクセスが広く行われている。多くの場合、標準的なパスワードや、場合によってはハードコードされたパスワードが使用されている。仮想プライベートネットワーク（VPN）を介した外部アクセスは、アクセス可能なシステムに関して制限されていない場合がある。すなわち、特定のシステムへのメンテナンス用アクセスを介して、他のシステムにアクセスすることができる。認証や認可が不適切または欠如していたり、ネットワーク階層がフラットであったりすると、侵入が容易になる。

コンポーネントのメンテナンスやプログラミングには、各メーカや外部サービスプロバイダが利用されることが多い。これにより、複数の関係者のセキュリティ概念を一致させることが必要となるため、セキュリティマネジメントにさらなる課題をもたらしている。

想定される脅威のシナリオ

1. メンテナンス用アクセスへの直接攻撃。
   例えば、下記の手段による。
   a. パスワードで保護されたアクセスに対するブルートフォース攻撃。
   b. 以前に記録されたトークンの再利用。
   c. メンテナンス目的で使用されるアクセスポイントへのウェブ固有の攻撃（インジェクションや CSRF（訳注：クロスサイトリクエストフォージェリ）など）。
2. 外部からのアクセスが許可されているサービスプロバイダの IT システムを介した間接攻撃。
   例：

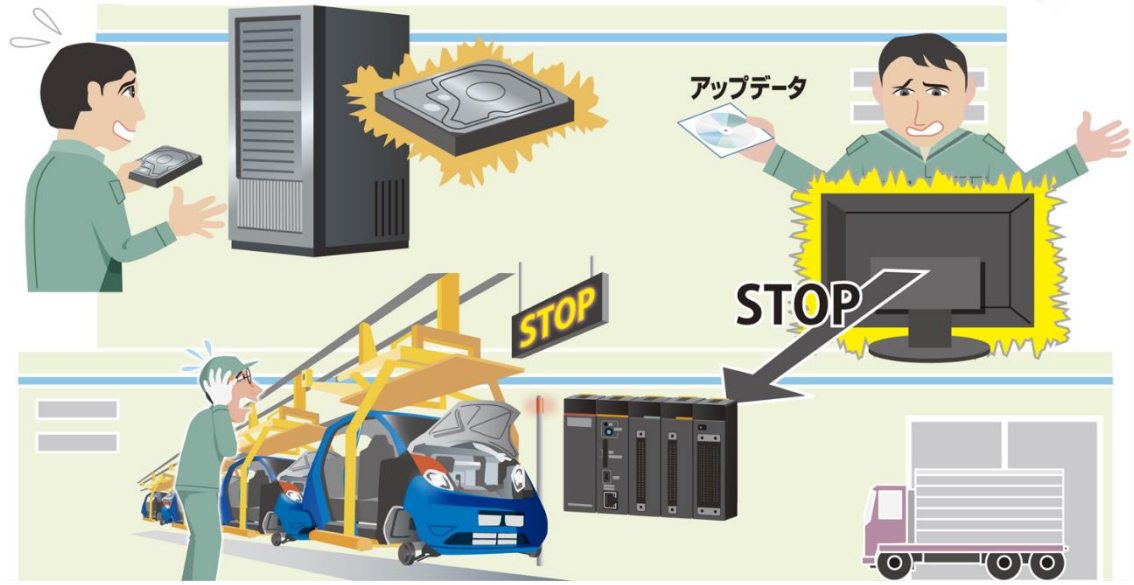
a. 外部のメンテナンス用コンピュータの直接アクセスを悪用するトロイの木馬。
b. パスワード、証明書、その他のトークンの盗難、または必要なアクセスデータの取得。例えば、権限を持つ従業員または内部の加害者の贈賄／恐喝などによるもの。
c. 外部アクセス用に設定されたソフトウェアがインストールされた、盗品ノート PC の使用。

対策

1. メーカによる標準的なユーザ名／パスワード（製品出荷時の状態）は、（製品受け入れ手順や規定にしたがって）ブロック／削除する 。
2. 事前共有鍵、証明書、ハードウェアトークン、ワンタイムパスワード、および所有と知識による多要素認証など、十分にセキュアな認証方法を使用する。
3. TLS[5]などの暗号化による伝送経路の保護。
4. リモートアクセスの「リーチ」（訳注：アクセスできる範囲）を最小限に抑えるための、十分にきめ細かな、ネットワークのセグメント化。
5. 非武装地帯（DMZ）にリモートメンテナンス用のアクセスポイントをセットアップし、サービスプロバイダが最初に ICS ネットワークではなく DMZ に接続し、そこから目的のシステムへのみアクセスできるようにする。
6. リモートアクセスは、常に目的のシステムへのアクセスを許可および監視するファイアウォールを介してルーティングしなければならない。メンテナンスに必要な IP アドレス、ポート、システムのみを解放する。
7. 内部担当者によるリモートアクセスの有効化は、リモートメンテナンス目的、およびメンテナンス期間に限定する。
8. 追跡可能性を確保するために、リモートアクセスのログを記録する。追加のプロセスで、このログデータを評価およびアーカイブできるようにする。
9. すべてのアクセスを、個人用とする。つまり、複数の人が使用する便利なアカウントを使用しない。ユーザごとに 1 つのログインのみを許可する。
10. このようなシステム／アクセスに対して監査を実施する。

[5] https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Mindeststandards/TLS-Protokoll/TLS-Protokoll_node.html

技術的な不具合と不可抗力



問題と原因の説明

セーフティ専用コンポーネント（訳注：セーフティコンポーネント）や ICS コンポーネントのソフトウェアエラーは、予期しない誤動作、およびハードウェアの不具合やネットワーク障害につながる可能性がある。特にハードウェアの不具合は、（汚れや温度などの）運用環境を考慮すると、いくつかのアプリケーションシナリオで発生する可能性が高くなる。

想定される脅威のシナリオ

1. ハードディスクまたはスイッチの故障、ケーブルの破損などの、即障害につながるコンポーネントの不具合。
2. ハードウェアの不具合とソフトウェアコンポーネントのエラーは、長期間気付かれないことがあり、例えばシステムの再起動や特定の境界条件が発生したときにのみ問題となる可能性がある。
3. ソフトウェアエラーは、システムの障害につながる可能性がある。例えば、中核のセキュリティコンポーネントの OS を更新すると、必要な再起動後にシステムが正しく機能しなくなる可能性がある。
4. 気候変動や、熱波や洪水などの異常気象が発生した場合、これまでの防護策や計画（冷却など）が適切でなくなり、機能停止につながる可能性がある。

特に、このようなインシデントは、組織的な欠陥により、可用性が著しく損なわれる可能性がある。

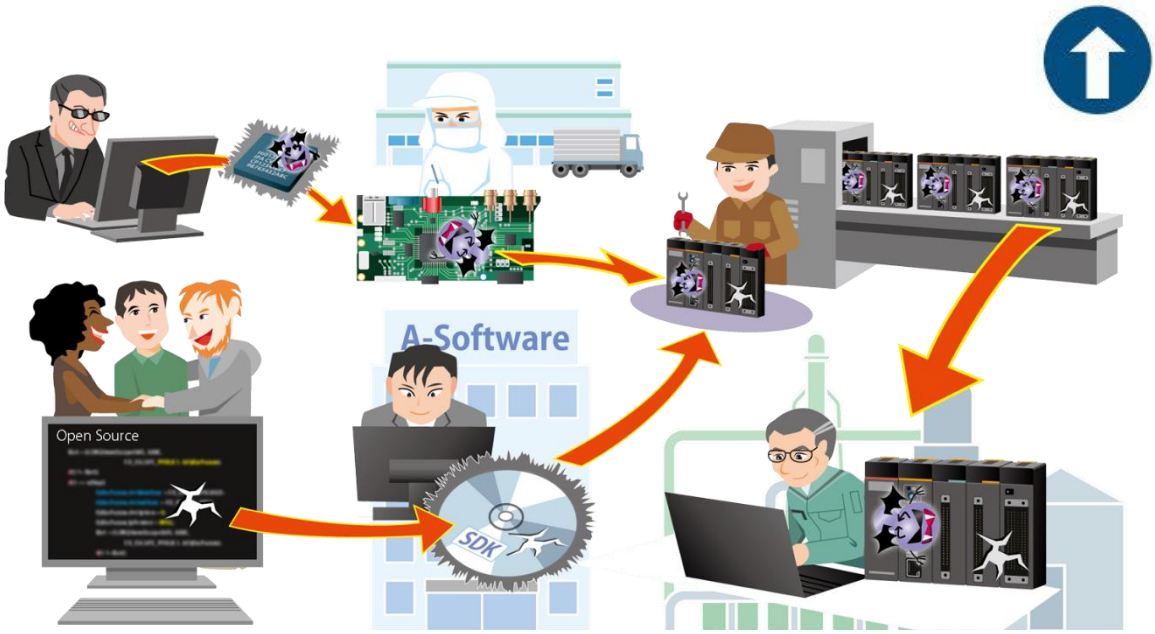
対策

1. 実施可能な対策、システム復旧の手順、代替通信オプション、訓練の実施などの側面を含む緊急時の管理体制を確立する。
2. 代替機器または予備機器を常備しておく。
3. テストシステム（訳注：テスト環境）およびステージングシステム（訳注：ステージング環境）を維持しておき、パッチ、アップデートおよび新しいソフトウェアコンポーネントを、本番システムにインストールする前に徹底的にテストするために使用する。
4. 単一ベンダが独自に開発したものではない、標準化され、開示されたインタフェースを使用する。これにより、検出されないギャップのリスクが軽減される。
5. 重要なコンポーネントの冗長設計。
6. 使用するシステムとコンポーネントを選択する際には、特定された保護の必要性に応じて、十分な最小要件を定義および実施する必要がある。これに関する重要な側面は次のとおり。
   a. メーカの信用性と信頼性。
   b. 製品の堅牢性。
   c. 適切なセキュリティメカニズムの存在（セキュアな認証など）。
   d. スペアパーツ、アップデート、メンテナンスの長期的な利用可能性。
   e. タイムリーなパッチの入手可能性。
   f. オープンな環境／製品への移行。
   g. 不要な製品機能を使用しない。
7. 適合性およびフレームワーク条件に関する対策の定期的なレビュー。

これらの側面およびその他の側面のための確固たる基盤は、たとえば BDEW のホワイトペーパー[6]などで提供されている。

[6] https://www.bdew.de/service/anwendungshilfen/whitepaper-anforderungen-sichere-steuerungs-telekommunikationssysteme/

サプライチェーンにおけるソフトウェアおよびハードウェアの脆弱性



問題と原因の説明

サプライチェーンは、時に相互の関連性が高い非常に複雑な構造をしており、その中ではメーカはしばしば顧客でもある。したがって、脆弱性は、サプライチェーンのすべての部分に影響を及ぼす可能性がある。ハードウェアとソフトウェアの脆弱性、および設定ミスは、多くのセキュリティの問題（本文書で言及されているものを含む）の出発点となっている。（サードパーティベンダ製の）ライブラリまたは外部のソースコードの統合は、異なるベンダ間の依存関係を増大させる。

脆弱性に対応するためのアップデートは、サプライチェーンに関わる全ての関係者が自社製品に反映しなければならない。サプライチェーンの長さによっては、全ての関係者が脆弱性情報を入手し、対策を講じて顧客に通知するまでに時間を要することがある。

想定される脅威のシナリオ

1. 脅威は、サプライチェーンのどこからでも発生する可能性がある。サプライチェーンの早い段階で脆弱なコードが存在すればするほど、より多くの製品が影響を受け、自身の脆弱性を特定することが難しくなる。また、攻撃者によって意図的に悪意のある機能や脆弱性が組み込まれている例もある。
2. 結果として生じるエラーは、様々な影響を及ぼす可能性がある。これらは、計算ミスから、広範囲のアクセス権、任意のコードを実行する可能性まで、多岐にわたる。これは、最初の攻撃に影響するだけでなく、二次攻撃にもしばしば不可欠なものである。
3. すべてのベンダが脆弱性の通知に対応するわけではない。これは、メーカが顧客に脆弱性、アップデート、回避策を通知する情報チャネルにも当てはまる。攻撃者は、パッチに関する情報を装ったフィッシングメールを使って、悪質なコードを配布する。

4. 外部ライブラリには、アップデートが入手できなくなったものや、製造業者が市場から撤退したものがある。

対策

1. 資産管理を実施することが望ましい。セキュリティアドバイザリやアップデートに関する情報を提供する情報源も明確化しておくことが望ましい。これにはメーカ、インテグレータ、その他関係するサービスプロバイダも含まれる。
2. アップデートやライブラリの入手には、信頼できるソースを使用することが望ましい。また、使用する前には、完全性を検証することが望ましい。
3. 脆弱性管理プロセスを確立することが望ましい[7]。このプロセスは、受け取ったセキュリティレポートを調査・評価し、コンポーネントやシステムにおけるアップデートの統合を計画・実行する。

[7] https://www.bsi.bund.de/csaf（訳注：共通セキュリティアドバイザリフレームワーク）

追加のセキュリティ対策

基本的な対策

ここで説明しているベストプラクティスは、ICS または企業全体で、秩序ある IT セキュリティプロセスの導入を紹介することだけを意図としているということを、強調しておきたい。一般的な IT セキュリティと特定の ICS セキュリティの両方を含めて確立された標準に基づいて、機能的な情報セキュリティマネジメントシステムを確立することが望ましい。下記はその標準の例である。

•BSI IT-Grundschutz（「IT ベースライン保護」）[8]
•ISO/IEC 27000 シリーズ[9]
•VDI/VDE 2182[10]
•IEC 62443[11]

これらの標準に基づいて、ICS 運用のための情報セキュリティマネジメントシステム（ISMS）は、企業の上位のマネジメントシステムの一部として理解することが望ましい。また ISMS は、ICS の特定のリスクを考慮し、情報セキュリティを永続的に管理、点検、維持、および継続的に改善することを目的としている。

最も重要なのは、ISMS を導入する際に、下記の基本的な管理策を検討することが望ましい 。これらは、責任を明確化し、既存のリスクを認識するために、現在のシステムとそのインフラの概要を提供するのに役立つ。この目的のために、今後の計画を可能な限り包括的で費用対効果の高いものにするには、できるだけ早く管理策を実装することが有効である。

•セキュリティ組織のセットアップ：この包括的なタスクは、セキュリティに関連する役割を定義し、ICS コンポーネントのセキュリティに関連する責任を明確化するのに役立つ。セキュリティに対するこの責任は、これらの役割を遂行する個人だけに関係するものではない。企業のスタッフ全員がこの責任を認識し、それを実践する必要がある。ICS のセキュリティは組織に関する概念において当然のことであることが望ましい。

•ドキュメントの作成とメンテナンス：リスクと脆弱性の分析、ネットワーク計画、ネットワーク管理、構成またはセキュリティプログラム、組織などの ICS コンポーネントのセキュリティに関するドキュメントと情報を作成・維持すると共に、不正アクセスから十分に保護することが望ましい。該当する場合には、サービスプロバイダと製品サプライヤの標準手順も含めることが望ましい。この文書により、特定のバージョンおよび構成におけるソフトウェアの非互換性およ

[8] https://www.bsi.bund.de/grundschutz
[9] https://www.iso.org
[10] http://www.vdi.de/uploads/tx_vdirili/pdf/9875774.pdf
[11] https://webstore.iec.ch/preview/info_iec62443-1-1{ed1.0}en.pdf

び不整合を回避できる。さらに、脆弱性の影響を受ける設備のパーツを特定できる。さらに、特に物理的および論理的なネットワーク計画により、インフラおよびそのコンポーネントの厳格な管理が可能となる。

•リスク管理：最も重要なタスクの 1 つはリスク管理である。これに関連して、ICS のすべての機能、およびセキュリティのリソースを考慮する必要がある。これらは体系的に分析および評価されることが望ましい。目標は、脅威を特定して優先順位を付け、適切な技術的対策および組織的対策を導き出すことである。実際、これは企業がセキュリティレベルと残留リスクを実質的に評価する唯一の方法である。

•事業継続管理（BCM: Business Continuity Management）：BCM の目的は、大規模な被事象が発生しても事業活動が中断しないこと（予防）、または障害発生後も適切な時間内に事業を継続できること（対応）である。BCM は、組織的、技術的、構造的、人的な対策から構成される。この目的を達成するために、企業は ISMS などの他のマネジメントシステムの既存のセキュリティ対策を部分的に利用したり、必要に応じてそれらを拡張したりすることができる。

•脆弱性の低減：脅威は絶えず変化し、進化するため、潜在的な攻撃を防ぐために定期的な対策が必要である。対策には、スタッフトレーニング、コンポーネントベンダや「Allianz für Cybersicherheit」などのセキュリティ通知（訳注：脆弱性情報等の情報源）への加入に加えて、脆弱性の積極的な探索が含まれる。これらの対策は定期的に実行する必要がある。

•攻撃の検出と適切な応答：攻撃を検出して理解するには、IT および ICS 固有の手順と、内部および外部の通知チャネルを定義する必要がある。[12]

企業経営者の役割

サイバーセキュリティを管理するルールを定義し、それらを適正な方法で関係者全員に伝えることは、企業の経営者の義務である。これらの期待の実現を維持するには、適切な管理体制を導入する必要がある。したがって、サイバーセキュリティを、機能要件の実装によってもたらされる二次的な目標としないことが重要である。実際、サイバーセキュリティは、企業の目標を達成するための重要な側面の 1 つである。経済的な考慮事項は別として、経営陣は十分なセキュリティレベルを付与する個人的な責任がある。結局のところ、サイバーセキュリティは経営陣自身の利益となるのである。

企業経営者がサイバーセキュリティの一般的な条件を十分なレベルで達成できるようにするためには、技術担当者が適切なサポートを提供すしなければならない。これには、潜在的なセキュリティインシデントの影響の認識と、サイバーセキュリティの実装の現状に関するターゲットグループ固有の情報の提供が含まれる。企業経営者は、戦略的計画の一環として、初期段階です

[12] https://www.allianz-fuer-cybersicherheit.de/Webs/ACS/DE/Service/Meldungen/meldungen_node.html

べての重要な決定に関与しなければならない。この様な状況においては、残りの残留リスクや、緊急対応の必要性を示す事例を重視すべきである。また、技術担当者は、セキュリティが企業経営の利益になることを認識しておく必要がある。さらに、企業経営者がそれに応じて行動できるように、意思決定に関連する基盤を透明化する必要がある。

後続の攻撃に対する対策

潜在的な後続の攻撃から保護するために、さまざまな適切な対策が存在する。これらには、不正なローカルアクセスに対するインフラの物理的保護、ログデータの記録と評価、および IT／ICS コンポーネントの強化が含まれる。これらの管理策と追加の対策は、BSI の「ICS Security Compendium」で詳しく説明されている。こうした種類の管理策を実装することを強く推奨する。その反対に、広く行き渡っている「十分なセキュリティレベルを達成するためには、単一のセキュリティ対策またはセキュリティ製品で十分である」という考え方は、悲惨な結果を招く可能性がある。その代わりに、いわゆる多層防御アプローチ、すなわち選択したセキュリティメカニズムが適切な冗長性を形成し、相互サポートを提供する多層セキュリティコンセプトを実装することによって、望ましい結果が得られる。

セルフチェック

次の質問リストは、企業のセキュリティレベルの自己評価に役立つ。中小企業（SME）は、会社全体を念頭に置いて質問に答えることができる。大企業は、これをひとつの生産ラインなどの個々の部門に限定することが望ましい。また、質問には自分だけで答えるのではなく、IT および製造現場の担当者と話し合うことをお勧めする。

個々の対策について、企業または分析対象のセグメントに対して、「完全に実装」、「部分的に実装」、または「未実装」の何れであるかを評価する。各フィールドにはスコアが与えられている。各セクションで得られたスコアを加算して、対応する行に合計を記入する。次の図に例を示す。

	未実装	部分的に実装	完全に実装
ソーシャルエンジニアリングとフィッシング	0-3	**6** 4-6	7-10
すべての従業員に対して、サイバーセキュリティに関する定期的なトレーニングと意識向上対策が実施されている。	0	2	4 ✖
標準とポリシーによって、スタッフによる技術システムの使用が規制されており、ポリシーへの準拠が管理されている。	0	2 ✖	4
技術的なセキュリティメカニズムは、ポリシーへの準拠が必須となっている。	0 ✖	1	2
リムーバブルメディアや外部機器経由のマルウェア感染	**3** 0-3	4-6	7-10
個人利用および職務で、同じハードウェアを使用することが禁止されている。	0	1 ✖	2
リムーバルメディアは、使用前にマルウェアのチェックが実施されている。	0 ✖	2	4
サードパーティの担当者によるハードウェアの使用に関するルールが存在している。	0	2 ✖	4

4 + 2 + 0 = 6

1 + 0 + 2 = 3

図 2：記入済みのセルフチェックシートの例

予防策が不要な場合は、満点のスコアを記入する。たとえば、「リモートアクセスによる侵入」において、企業全体でリモートメンテナンス用のアクセスポイントが必要でないため適用されていない場合がこれに該当する。最後に、取得したすべてのスコアを合計し、最後の行に記入する。

このチェックシートの結果によって、ICS および/または産業用 IT の分野における最も重大な脅威に対する保護の予備的な自己評価が提供される。このセルフチェックは、導入、または企業のセキュリティ評価の最初のオリエンテーション、と見なすことができる。これは包括的な

サイバーセキュリティ分析の代わりとなるものではない。したがって、得られた合計スコアは慎重に扱う必要がある。取得したスコアに応じて、次の推奨事項が適用される。

- 0-25：www.allianz-fuer-cybersicherheit.de での現在の状況と「ICS の 10 大脅威と対策」には、 あなたが今すぐ実施すべき行動が示されている。
- 26-50：いくつかのセキュリティメカニズムが既に実装されている。ただし、現在のトップ 10 に挙げられている基本的な対策に関するアクションが必要である。
- 51-75：特定の脅威から保護するために最も緊急に改善する必要があるセキュリティメカニズムを分析するために、リスク分析を実行する。
- 76-100：あなたの会社はすでに責任を持ってサイバーセキュリティに対処している。ただし、サイバー攻撃から確実に保護されるわけではない。IT-Grundschutz や IEC 62443 などの体系的で包括的なアプローチへの道を追求する必要がある。BSI の ICS Security Compendium は、この点においてあなたをサポートする。

これらの質問に取り組む過程で、あなたはセキュリティを改善するためにどの手段が必要で有用であるかについて同僚と既に話し始めているかもしれない。これは、さらなるステップへの出発点を設定する絶好の機会だ。また、セルフチェックから得られた結果を使用して、エンタープライズセキュリティの一般的な問題、特に製造現場の問題を経営陣と話し合うことができる。

	未実装	部分的に実装	完全に実装
ソーシャルエンジニアリングとフィッシング	0-3	4-6	7-10
すべての従業員に対して、サイバーセキュリティに関する定期的なトレーニングと意識向上対策が実施されている。	0	2	4
標準とポリシーによって、スタッフによる技術システムの使用が規制されており、ポリシーへの準拠が管理されている。	0	2	4
技術的なセキュリティメカニズムは、ポリシーへの準拠が必須となっている。	0	1	2
リムーバブルメディアや外部機器経由のマルウェア感染	0-3	4-6	7-10
個人利用および職務で、同じハードウェアを使用することが禁止されている。	0	1	2
リムーバルメディアは、使用前にマルウェアのチェックが実施されている。	0	2	4
サードパーティの担当者によるハードウェアの使用に関するルールが存在している。	0	2	4
インターネットおよびイントラネット経由のマルウェア感染	0-3	4-6	7-10
企業ネットワークは、特にオフィスネットワークと ICS ネットワークが分離され、セグメント化されている。	0	2	4
ウイルス対策は、電子メール、ファイルサーバ、PC だけでなく、ICS と他のネットワーク間のネットワーク境界にも導入されている。	0	2	4
ICS ネットワークからインターネットにアクセスできない。	0	1	2
リモートアクセスからの侵入	0-3	4-6	7-10
リモートアクセスは常に認証を必要とし、暗号化されている。	0	2	4
リモートアクセスはきめ細かく制御されている。例えば、サブネット全体ではなく、必要なコンポーネントのみにアクセスしている。	0	1	3
リモートメンテナンスを実施するコンピュータに関するセキュリティポリシーがある（最新のウイルス対策など）。	0	1	3
ヒューマンエラーと妨害行為	0-3	4-6	7-10
機密情報が必要以上に広く配布されるのを防ぐために、“need to know”の原則が導入されている。	0	2	4
セキュリティおよび構成管理に関して、十分な基準がある。	0	1	3
技術的管理策によって、現在のシステム構成と状態を監視している。	0	1	3

	未実装	部分的に実装	完全に実装
インターネットに接続された制御機器	0-3	4-6	7-10
制御コンポーネントはインターネットに直接接続されていない。	0	2	4
不要なサービスの無効化やデフォルトのパスワードの変更など、制御コンポーネントの設定が強化されている。	0	1	3
ファイアウォールや VPN ソリューションなどの追加の管理策が使用されている。	0	1	3
技術的な不具合と不可抗力	0-3	4-6	7-10
コンポーネントの選択において、ISA 99 または BDEW ホワイトペーパーやその他の適切な標準類に基づいたセキュリティの側面を考慮している。	0	2	4
重要な IT システムは冗長設計され、分散構造を持っている。	0	1	3
システム障害に対応する手順が定義されている。	0	1	3
外部ネットワークやクラウドコンポーネントへの攻撃	0-3	4-6	7-10
外部コンポーネントのユーザは、サービスレベル合意書（SLA）などを通じて、十分なセキュリティレベルを順守する義務がある。	0	2	4
信用のある、可能であれば認定されたサービスプロバイダのみを利用している。	0	1	3
プライベートクラウド形式で運用されている、またはクライアントの厳密な分離が保証されている。	0	1	3
DoS/DDoS 攻撃	0-3	4-6	7-10
ネットワークトラフィックが大幅に変化した場合の検出および警告のメカニズムが導入されている。	0	2	4
重要なシステムの外部接続は、様々な通信技術による冗長性を持った設計がなされている。	0	1	3
緊急時対応計画（※）のドキュメントには、DDoS 攻撃が発生した場合の対処方法と、関係のある外部連絡先が記載されている。	0	1	3
サプライチェーンにおけるソフトウェアおよびハードウェアの脆弱性	0-3	4-6	7-10
資産/機器の一元管理はできているか？	0	2	4
メーカやインテグレータから脆弱性情報を入手し、定期的に評価を行っている。	0	1	3
提供された更新をスケジュール化し、メンテナンスプロセスに取り込んでいる。	0	1	3
合計スコア			(0-100 ポイント)

（※）訳注：2019 年版には、「追加のセキュリティ対策」の一つとして「緊急時対応計画の管理および再始動手順」が存在し、緊急時対応計画を策定して文書化することが推奨されていたたが、2022 年版においては削除され、「事業継続管理（BCM）」に置き換わっている。
詳細は、『産業用制御システム（ICS）のセキュリティ - 10 大脅威と対策 2019』を参照。

多くのリスクと脅威は、技術的な管理策の実装だけでは最小化することはできず、組織の規制と技術的な管理策の組み合わせによって最小化することができる。

本文書で提案されている対策は、一般に、発生の確率および影響に関して、特定された脅威を限定するのに適している。ただし、関係するすべての人々にとってのセキュリティを理解するために重要なことは、特定の残留リスクが常に残る、ということである。

ファクトリオートメーションとプロセス制御のセキュリティの詳細については、BSI の「ICS Security Compendium」を参照（無料で入手可能）。ここでは特に、多層防御アプローチの観点で、ここで説明している最初の攻撃に加えて、後続の攻撃から保護するために使用されることを目的とした管理策について説明している。「ICS Security Compendium」、および追加の出版物とツールは、BSI のウェブサイトで入手できる。

https://www.bsi.bund.de/ICS

上記ウェブサイトでは、従業員の意識向上、セキュリティマネジメント、技術的要件などの問題、および ICS に関連するトピックに関する追加情報も入手できる。

ICS のセキュリティに関してさらに質問がある場合は、下記 BSI のメールアドレス宛に連絡可能である。

ics-sec@bsi.bund.de

情報セキュリティ庁（BSI）は、サイバーセキュリティの分野における現在のトピックに関するドキュメントを BSI の出版物として発行している。ほとんどの参照ドキュメントはドイツ語でのみ利用可能であることに注意願いたい。読者からのコメントやアドバイスを歓迎しているので、下記メールアドレス宛に送信していただきたい。
info@cyber-allianz.de