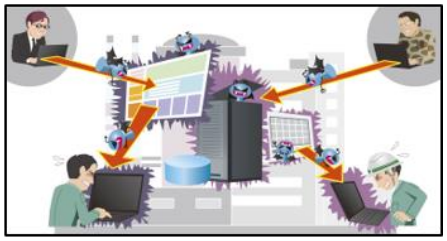
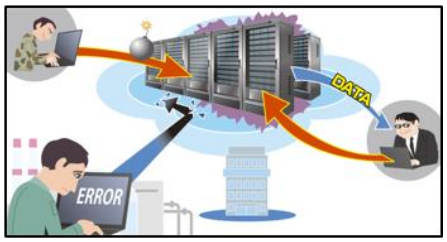
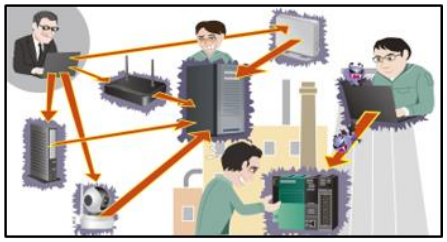
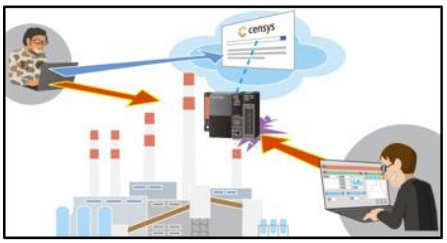
ドイツ連邦政府　情報セキュリティ庁（BSI）

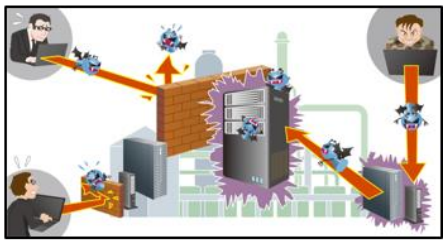
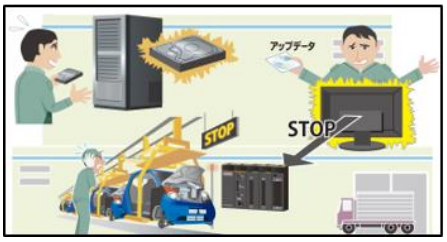
産業用制御システム（ICS）のセキュリティ

10大脅威と対策　2019



2020 年 1 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

2020 年 1 月 14 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 2019」

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 2019”（英語版：2019 年 6 月 6 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 v1.3 [German/English]
https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/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 2019

総称して産業用制御システム（ICS）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生産・供給、ガス・水の供給から産業オートメーション、交通管制システム、最先端の施設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。資産の所有者は、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 ICS インフラへの高度な技術を駆使した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インフラおよび間接的にサイバー攻撃の標的となるインフラにあてはまる。

BSI は、サイバーセキュリティに関する分析と産業界のパートナーとの協力によって、ICS に対す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：原因の提示と、脆弱性または脅威の状況が存在する決定的な要因。
2. 潜在的な脅威のシナリオ：上記 1.で確定した要因を使用した攻撃実行の、具体的な可能性の説明。
3. 対策：脅威に対抗し、未解決のリスクを最小限に抑えるのに適していると考えられる選択肢の説明。

この文書は、脅威のシナリオと対策の完全なリストではない。むしろ本文書で説明されているシナリオは、関連する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。また引用されている対策は、それぞれの脅威への対応の出発点を表しており、防御に必要なあらゆる努力の最初の評価を可能としている。最終的には、個々のユースケースをテストし、どの対策が適切で、どの代替策が必要かをリスク分析の観点で評価する必要がある。また、効率と費用対効果も考慮する必要がある。すべてのケースにおいて、稼働中のオペレーションとの互換性および設定されているリアルタイム要件、安全要件を確保する必要がある。さらに、対策の実装が、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、このトップ 10 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。

1. 脅威とその被害

脅威による ICS に対するリスクは、脆弱性が存在することによって、ICS や関連する企業に被害をもたらす可能性がある。次の表は ICS に対して最も危険で最も一般的な脅威の概要を示している。

この文書では、最初の攻撃と後続の攻撃を区別している。最初の攻撃は、攻撃者が産業施設に侵入するために使用することに焦点が当てられている。また、後続の攻撃は、攻撃者が内部システムをさらに脅かす、またはアクセスすることを可能とする。

10 大脅威	2016 年からの傾向
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	↗
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	↗
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機器	→
リモートアクセスからの侵入	→
技術的な不具合と不可抗力	↘
スマートデバイスへの攻撃	→

最初の攻撃から始まり、攻撃者は後続の攻撃ごとに組織にさらに侵入することができる。 次の図は、そのつながりを表している。

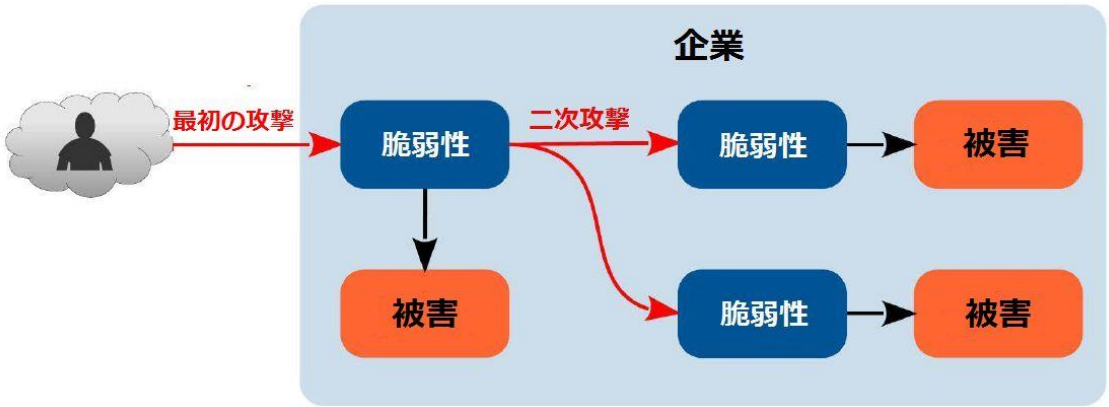


図 1 ：最初の攻撃と、関連する被害を含む後続の攻撃のシーケンス

後続の攻撃には、特に下記が含まれる。

・権限昇格のための認証情報の収集：OS、アプリケーションサーバ、データベースなどの産業環境で使用される標準の IT コンポーネントには、通常、バグと脆弱性が含まれている。攻撃者はこれらを巧みに利用する。

・さらなる内部システムへの不正アクセス：企業ネットワークまたは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適切な方法を使用していない場合、特に内部関係者による攻撃や後続の攻撃が容易となる。たとえば、認証メカニズムに対するブルートフォース攻撃や辞書攻撃によって、この種の後続の攻撃が可能となる。

・フィールドバス通信の操作：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、または発行が容易となる。

・ネットワークコンポーネントの操作：攻撃者が、セキュリティメカニズムを無効化するためにルータまたはファイアウォールを改ざんしたり、データトラフィックを再ルーティングしたりする。

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]

不十分な組織のポリシー、知識不足またはヒューマンエラーは攻撃を助長し、後続の攻撃を促進する。さらに、攻撃の検出と、攻撃が成功した後のシステムの健全化と復旧を妨げる。 潜在的な被害は多くの形態をとることがあり、かなり重大であると評価する必要がある。

・ICS の可用性の喪失／生産の損失
・データ漏洩／ノウハウの損失（知的財産）
・施設への物理的被害
・セーフティ手順の発動またはセーフティシステムへの干渉
・製品の品質の低下

[1] ICS-CERT, Recommended Practices, https://ics-cert.us-cert.gov/ Recommended-Practices, Zugriff im Januar 2019

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。

2. アセスメントの基準

脅威を評価する基礎としているのは、セキュリティインシデントから得た知見、および脅威インテリジェンスレポート、および産業界からの報告である。その結果である今年の脅威の順序は、まさに最近の脅威の変化を示している。例え傾向に変化がない、または減少傾向である場合でも、それらの脅威についても深刻に受け止める必要がある。

リスクの評価には脅威の普及の基準は不可欠であるため、今年のアセスメント基準は、脅威の普及度が脅威のリスク評価に最も重要であることから、過去のものとは異なっている。[2] [3]これは、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）がほとんど変わっていない一方で、脅威の普及度は犯罪グループの活動に非常に大きく依存するためである。自組織の脅威とリスクを見積もるには、技術的または組織的な実現可能性について自組織の個々の対策を評価する必要がある。この評価は、それぞれの対策のコストの見積もりと合わせて行う必要がある。一方、ビジネスへの影響、例えば企業への経済的な影響を各ケース個別に評価することが特に重要である。通常、これは資産所有者が一般的な条件と潜在的な後続の攻撃を考慮することによってのみ実行できる。

[2] BSI, Industrial Control System Security: Top 10 Threats and Countermeasures, 2014

[3] BSI, Industrial Control System Security: Top 10 Threats and Countermeasures, 2016 https://www.gi-de.com/fileadmin/user_upload/MS/Industries/Manufacturing_and_IIOT/SIV_Solutions/BSI-CS_005E.pdf

3. 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

3.1 問題と原因の説明

USB フラッシュドライブのようなリムーバブルメディアは広く利用されおり、企業の従業員はオフィスや ICS ネットワークでそれらを利用している。また、仕事の続きをするためや最新の音楽をコピーしたりするために頻繁に家に持ち帰る。さらに、社外の人間が外部のデータやメンテナンスソフトの入った、別の会社で使われているノート PC を持ち込むこともある。

ICS の歴史から見ると、セキュリティ意識は主に可用性や、セーフティ、アクセス制限、外部の影響からの保護といった物理的セキュリティの側面に限られている。その結果、従業員はマルウェアによる影響に気付かないことがよくある。

3.2 潜在的な脅威のシナリオ

1. USB フラッシュドライブは、社内ネットワークまたはプライベート環境で感染したかもしれない。この方法によって、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 は、インターネット、複数の社内ネットワーク、または各サービスプロバイダのインフラにアクセスする際に感染したかもしれない。ICS ネットワークでそうしたノート PC が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。

3.3 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導入：
   a. インベントリとホワイトリストへの承認されたリムーバブルメディアの登録。
   b. リムーバブルメディアのセキュリティ境界（メンテナンスコンピュータとは異なる OS を使用するコンピュータで提供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. 社内専用のリムーバブルメディアの使用（可能であれば、従業員毎に専用のリムーバブルメディア）。
   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. USB デバイスの（不正な）接続を防止する物理的障壁（樹脂封止、USB ロック、または回路基板からのハンダ除去）。
   f. データメディア全体の暗号化。
2. メンテナンスに使用される外部ノート PC に関する厳格な組織ポリシーと技術的管理策の導入：
   a. 上記の管理対象のリムーバブルメディアのみを介したデータ交換。
   b. 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導入。
   c. 実際のシステムにアクセスする前に外部ノート PC のウイルススキャンを実施。
   d. 資産所有者によるメンテナンス用ノート PC の全体の暗号化。

4. 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

4.1 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の新たな脆弱性は、ほぼ毎日発見されている。サイバー犯罪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使用する。あるいは、感染したリムーバルメディアからマルウェアを展開する場合もある。いずれの場合も、重要な情報または機密情報が攻撃者に盗まれる。さらに、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、エンタープライズコンピューティング（ファイルサーバ、ERP および MES システム）への接続が、適切な IT セキュリティの維持を妨げている。攻撃者が社内ネットワークに侵入しようとした場合、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を介して ICS ネットワークに侵入する可能性がある。これらの関係は、すぐには明らかにならないことがよくある。

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、標的型攻撃および非標的型攻撃が発生する可能性がある

4.2 潜在的な脅威のシナリオ

1. 既知の脆弱性、またはいわゆるゼロデイ・エクスプロイトの悪用。後者はウィルス対策製品などでまだ検知できない未知の攻撃である。
2. 外部ウェブページの改ざんによって、被害者がウェブサイトにアクセスするだけで感染する

可能性がある（たとえばドライブバイダウンロードの実行）。1 つの例として、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. 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）。
4. コンポーネントが、非標的型のマルウェア（ワームなど）に感染し、機能や可用性が制限される。
5. スマートフォン、ゲーム用 PC やゲーム機を使用するための無線 LAN ルータなどの私物ハードウェアの設置。このハードウェアがすでに感染している可能性があるか、攻撃ベクトルに使用される可能性がある（「5. ヒューマンエラーと妨害行為」を参照）

4.3 対策

1. 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）することによって、ICS ネットワークに繋がる攻撃パスを大幅に排除する。保護されていない／パッチが適用できないシステムを分離する（"secure islands"）。
2. 境界（ファイアウォール、ウィルス対策ソフトなど）または ICS（アプリケーションのホワイトリスト、該当する場合はファイアウォールなど）での従来の予防策の使用。
3. 重要な情報の漏洩を防ぐために、企業内で利用可能な情報を制限する（ファイルサーバ上またはデータベース内など）（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、および該当する場合は ICS ネットワークの OS およびアプリケーションの定期的かつタイムリーなパッチ適用。
5. 異常な接続または接続試行のログファイルの監視。
6. オフィスおよび ICS 環境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）の最適な強化。

5. ヒューマンエラーと妨害行為

5.1 問題と原因の説明

ICS 環境で働くスタッフは、セキュリティに関して特別な立場にある。これは、社内スタッフのみならずメンテナンスや建築などに携わる外部のスタッフも同様である。施設で作業をするか、遠隔地からリモートで作業するかといったことは問題ではない。技術的な管理策だけではセキュリティは保証できないため、組織的な規則が必要となる。

5.2 潜在的な脅威のシナリオ

1. ネットワークコンポーネント、ファイアウォールなどのセキュリティに関するコンポーネント、または一般的な ICS コンポーネントの不適切な設定。
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. 機器や設備の損傷や、盗聴機器の設置などの意図的な行動の副作用を考慮する。
4. 無許可な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。これには、ゲーム、デジタルカメラ、スマートフォン、オペレータが所有する USB デバイスが含まれる。
5. インフラおよびセキュリティコンポーネントの公開されない設定の作成。例えば、モバイルエンドポイントを介した外部からの不正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。

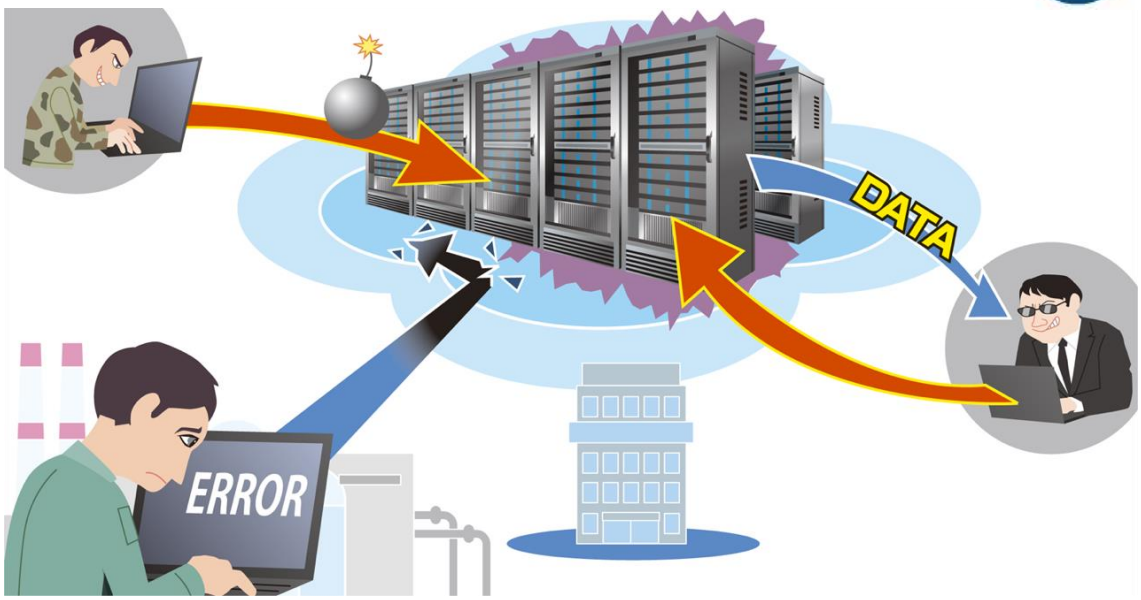
上記のシナリオは通常、スパイ行為と妨害行為によって引き起こされるが、不注意とヒューマン

エラーによっても発生する。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大幅に制限される可能性がある。多くの侵害は、そのような欠陥によってのみ起こる。

5.3 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）の導入：システムの詳細についての知識、パスワードや機密データへのアクセスは必要な場合にのみ提供する。
2. 機能上およびセキュリティコンポーネントに対するオペレータおよび管理者の能力を確保するために、意欲的で、資格があり、関連するスタッフのための汎用的なフレームワークを作成する。資格と訓練プログラム、および意識向上策は、持続可能かつ強制的なものとして設計されるべきである。
3. 制御システムおよび生産環境に近接しているシステムのインターネットアクセスを無効にする。さらに、電子メールやその他のオフィスアプリケーションなど、ICS とは別の運用タスクのコンポーネントは、十分に保護され、異なるネットワークに統合されなければならない。
4. 雇用されたばかりのスタッフと退職したスタッフ、および製品サプライヤ、ベンダ、サービスプロバイダなどの外部請負業者向けの標準化されたプロセスの導入。
5. 技術システムの取り扱いに関するポリシーや手順などの適切な基準。例えば、リムーバルメディアの取り扱い、電子メールおよびソーシャルネットワークでのコミュニケーションにおける振る舞い、パスワードポリシー、個々のソフトウェアのインストールなど。
6. ICS ネットワークの重要なプロセスに適したポリシーの導入：例えば、セキュリティ専門家やその他の関連する役割の関与を統制するセキュリティおよび構成管理に関する基準。これによって、変更またはアップデートは、彼らに相談した後にのみ実装されるようになる。これに関連して、4 つの目の原則（訳注：少なくとも二人による承認を行う）の使用などの、追加の取り決めによって裏付けられたすべての合意を文書化す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。

6. 外部ネットワークやクラウドコンポーネントの攻撃



6.1 問題と原因の説明

IT コンポーネントをアウトソース（訳注：外部委託）するという従来の IT における一般的な傾向は、ICS 分野においても勢いを増している。これは通常、レイテンシー（訳注：遅延）がリアルタイム要件を妨げるため、実際のプロセスを直接制御するコンポーネントには関係ない。ただし、ヒストリアン上のデータキャプチャの領域では、機器の設定や製造プロセス（ビッグデータ）を最適化する複雑な計算のために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の数は増え続けている。またセキュリティコンポーネントが、クラウドベースのソリューションとして提供される場合がある。例えば、リモートメンテナンスソリューションのサービスプロバイダは、メンテナンス技術者が様々なコンポーネントへのアクセスに使用するクラウドに、リモートアクセス用のクライアントシステムを配置する。

この種のソリューションは、中小企業（SMB）にとって特に興味深いものである。一企業が独自で運用することは多くの場合不経済であるが、クラウドベースのシステムは手頃な価格で、スケーラビリティ、冗長性、従量制などの利点があるからである。しかし、これらのクラウドソリューションにおいて、資産所有者は、コンポーネントのセキュリティ管理策を非常に限定的に制御できる。しかし、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。

6.2 潜在的な脅威のシナリオ

1. DoS 攻撃などによって引き起こされる、生産設備とアウトソース（クラウド）コンポーネン

ト間の通信の妨害または中断。また、カスケード効果によって生産設備が被害を受ける可能性がある。

2. 外部に保存されたデータにアクセスするための、実装エラーや不十分なセキュリティメカニズムの悪用（データの盗難、削除）。
3. クラウドサービスの提供者の環境において、各顧客の環境が十分に分離されていない場合、クラウド上の他のサービスへの攻撃が、連鎖反応を引き起こす可能性がある（二次的被害）。

6.3 対策

1. 外部コンポーネントのオペレータが、十分なサービスレベルを提供するための契約上の義務。たとえばサービスレベル契約（SLA）。
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。
4. クラウドに保存されているデータを保護するための暗号化や完全性保護などにおける、十分に強力な暗号メカニズムの使用。
5. ローカルの運用コンポーネント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。

7. ソーシャルエンジニアリングとフィッシング

7.1 問題と原因の説明

ソーシャルエンジニアリングは、通常は非技術的な手段によって情報または IT システムへの不正アクセスを取得する方法で、好奇心、有用性、信念、恐れ、権威の尊重などの人間の特性を利用する。これらの特徴は、従業員が軽率にまたは不注意に行動するよう誘導するための陽動戦略として、攻撃者によってしばしば使用される。典型的な例は、詐欺メール（フィッシングメール）である。これは従業員に、マルウェアを含む添付ファイルを開くよう仕向ける。あるいは、悪意のあるウェブサイトに誘導しようとする。

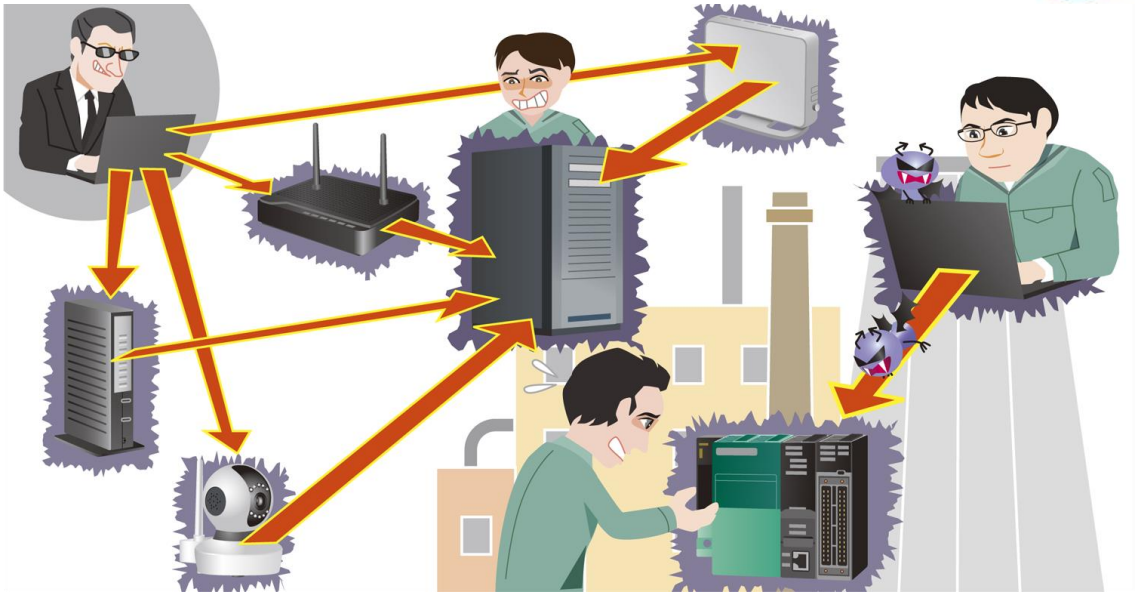
7.2 潜在的な脅威のシナリオ

1. 攻撃者が被害者のログイン認証情報を取得したり、不正なメッセージを介してマルウェアを配布したりするために使用するフィッシング攻撃。
2. 実行時に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、一見無害なリンクまたは添付ファイルを含む電子メール。
3. スピアフィッシングは、通常、少数の攻撃対象者を攻撃するために使用され、攻撃対象となる人物に合わせた電子メールを送信する。また、この目的のために会社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、友好的な態度で接したり、サービス技術者のふりをするなどの虚偽の情報を提供することで、建物または敷地へ不正アクセスする可能性もある。

7.3 対策

1. 攻撃対象者に対するセキュリティ意識向上トレーニングの実施。
2. 組織の予防措置：セキュリティポリシーの作成と施行。
   a. 企業にとって価値のある情報の識別と分類。
   b. データバックアップポリシーの確立。
   c. 社内スタッフだけでなく、パートナーやサービスプロバイダ向けにも機密性やプライバシーに関する合意を導入。
   d. 細断など、紙に印刷された情報の破壊に関して制定したポリシー。
   e. デジタルストレージメディアのセキュアな廃棄。
   f. プライバシーフィルムやセキュアなストレージなどのモバイルデバイスの取り扱いに関する規制。
3. インシデントおよびすでに疑わしい動作に対して危険を知らせる手段の導入。これらの報告は定義されており、明確に伝達する必要がある。また、報告するスタッフ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、デバイス制御やアクセス制御などの技術的なセキュリティメカニズムの使用。
5. インシデント発生時に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。

8. DoS/DDoS 攻撃



8.1 問題と原因の説明

ICS コンポーネント間の通信には、有線接続と無線接続が使用されている。これらの接続が中断されると、たとえば測定データや制御データを送信できなくなる。（分散）サービス拒否（(D) DoS）攻撃は、非常に多数のクエリでコンポーネントをオーバーロードし、タイムリーな回答を提供できないようにする。つまり、意図的に不具合を引き起こす。場合によっては、この攻撃は複数の攻撃者から分散して実行される。

8.2 現在の脅威の状況

「感染機器が数十万台にも及ぶ IoT ボットネットがさらに発生すると、DDoS 攻撃の発生確率と潜在的な影響はさらに増加する。」[4]

したがって、IT／OT 間の相互接続性の継続的な増加の観点から、ICS 環境をこれらの攻撃から保護する必要がある。

8.3 潜在的な脅威のシナリオ

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。たとえば、これはレンタル可能なボットネットによって実行できる。さら

[4] BSI, The State of IT Security in Germany 2018, 2018
https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Securitysituation/IT-Security-Situation-in-Germany-2018.pdf?__blob=publicationFile&v=3

に、Anonymous などの「ハクティビズム」グループが、このタイプの攻撃において台頭してきている。

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：このタイプの攻撃は、特定のメッセージを使用してコンポーネントの処理ロジックを中断し、クラッシュさせる。 これは、特に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）に影響を与える可能性がある。
3. WLAN やモバイル通信ネットワーク（GSM、UMTS、LTE）などのワイヤレス接続への攻撃。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中断または妨害するトランスミッターの使用。
   b. 攻撃されたシステムを不正な無線ネットワークに接続させる偽の基地局の使用。
   c. 既存の接続を中断させる、特別に細工されたデータパッケージの送信。
4. Trickbot などのランサムウェアの助けを借りた DoS 攻撃。[5]

8.4 対策

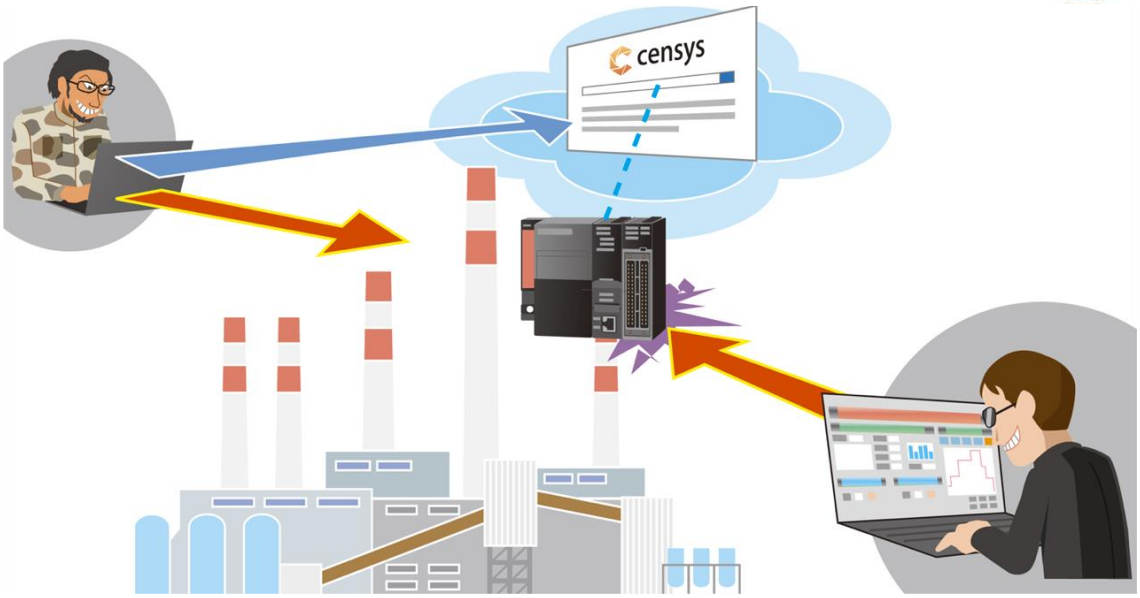
1. ネットワークアクセスポイントと通信チャネルの厳密な設定と強化。
2. 重要なアプリケーションに専用の有線接続を使用。
3. 該当する場合：侵入検知システム（IDS）をインストールして、代替チャネル経由で攻撃とトリガーアラームを検出。
4. 異なるプロトコルおよび/または通信チャネルを使用したコンポーネントの冗長接続。

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）」[6]のウェブページで DDoS 緩和に関する文書を提供している。各自の対策との比較を実施することが望ましい。

[5] https://www.tz.de/muenchen/region/fuerstenfeldbruck-computervirus-legt-kreisklinik-lahm-betrieb-mit-starken-einschraenkungen-10563771.html

[6] BSI, Abwehr von DDoS - Angriffen v2.0
https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_002.pdf, 2018

9. インターネットに接続された制御機器



9.1 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簡単に検出される。さらに、これらのコンポーネントは多くの場合、標準的な IT に見られる十分なセキュリティレベルを提供していない。さらに、脆弱性が発見された場合、これらのコンポーネントに（タイムリーに）パッチを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。

9.2 潜在的な脅威のシナリオ

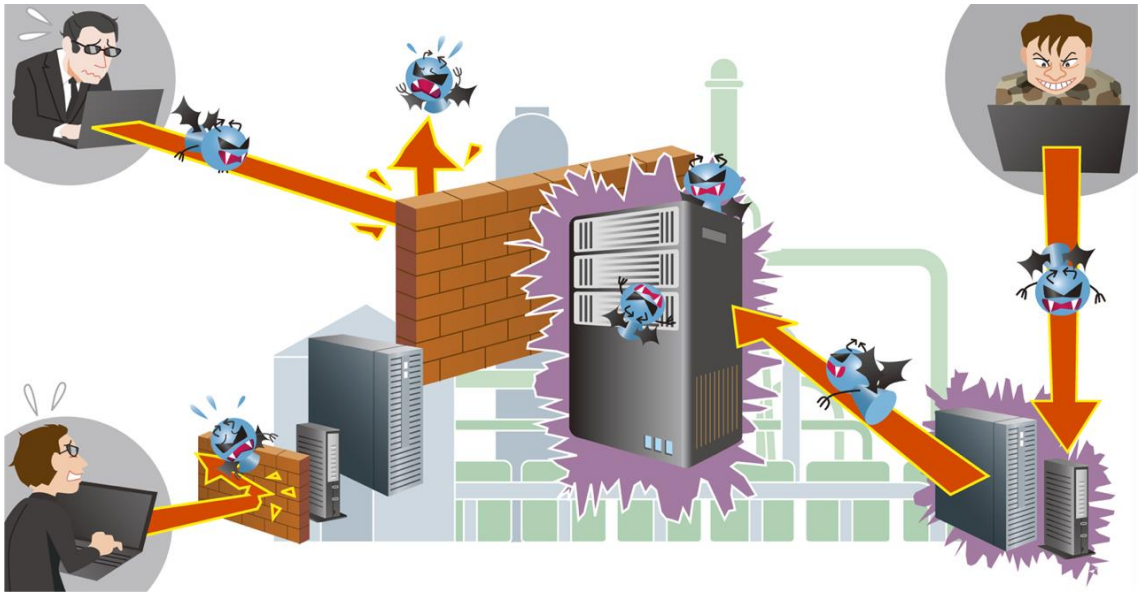
1. 一般的な検索エンジンを用いた制御コンポーネントの検索（Google ハッキング）または Shodan[7]、Censys、カスタムインターネットスキャンなどの特殊な検索エンジンによる制御コンポーネントの検索。
2. 保護されていないコンポーネントへの直接アクセス、または公的に利用可能なデフォルトのパスワードを使用した、不正操作。
3. ウェブインタフェース（WWW）、FTP、SNMP、または TELNET などの利用可能なサービスの脆弱性を悪用した、コンポーネントへのアクセス、またはコンポーネントの可用性の制限。

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

9.3 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。
2. 不要なサービスの無効化、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構成の強化。
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、更新またはパッチによる脆弱な製品のタイムリーな更新。

10. リモートアクセスからの侵入



10.1 問題と原因の説明

メンテナンス目的の外部からのアクセスは、ICS において非常に一般的である。デフォルトのパスワードやハードコードされたパスワードなどによる安全性の低いアクセスは、広く知られた問題となっている。さらに、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、特定のシステムにおいて制限されていない場合があり、結果として、他のシステムにもアクセス可能となる。要するに主な原因は、認証と認可の欠如、およびフラットなネットワーク構造である。

多くの場合、各製品サプライヤと外部サービスプロバイダは、コンポーネントのメンテナンスとプログラミングについて契約している。これには、複数の関係者間のセキュリティ概念の一致が必要となるため、セキュリティ管理にさらなる課題をもたらしている。

10.2 潜在的な脅威のシナリオ

1. メンテナンス用アクセスポイントへの直接攻撃。

   例：下記の手段による。

   a. パスワードで保護されたアクセスポイント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。

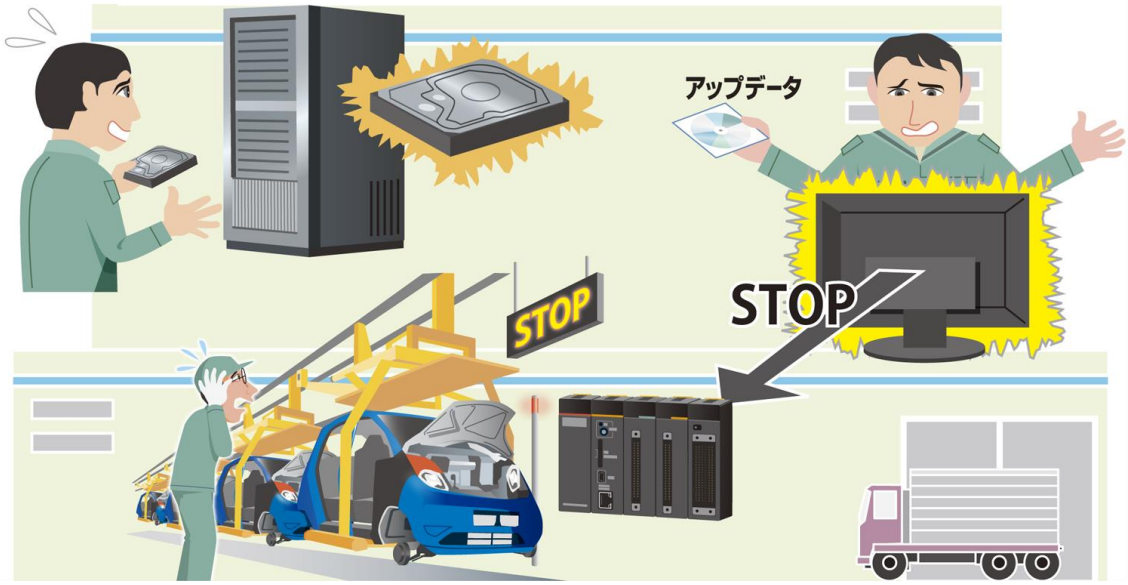
   c. ウェブ固有の攻撃、例：メンテナンスに使用されるアクセスポイントでのインジェクションまたは CSRF（訳注：クロスサイトリクエストフォージェリ）。

2. 外部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、またはログインの詳細を取得するその他の方法（例：権限を持つスタッフに賄賂を贈る／脅迫する）。
   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、盗品ノートパソコンの使用。

10.3 対策

1. 製品サプライヤによるデフォルトのユーザー／パスワード（製品出荷時の設定）は、（製品受け入れ手順や規定にしたがって）無効化、ブロック、または削除しなければならない。
2. 十分に安全な認証手順を使用する。例えば、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。
3. SSL/TLS 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する。サービスプロバイダは最初に ICS ネットワークではなく DMZ に接続する。そして、ターゲットシステムだけにアクセスできる。
6. リモートアクセスは、常にターゲット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するのが望ましい。これは、メンテナンスに必要な IP アドレス、ポート、およびシステムのみを公開することに制限する。
7. 内部保守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る。
8. 追跡可能性を確保するためのリモートアクセスのロギング。ログに記録されたデータを評価およびアーカイブできるように、追加のプロセスを使用しなければならない。
9. すべてのアクセス手段はパーソナライズされている必要がある。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。ユーザーごとに 1 つのログインのみが許可される。
10. これらのシステム／アクセス手段の監査。

11. 技術的な不具合と不可抗力



11.1 問題と原因の説明

セキュリティコンポーネントや ICS コンポーネントの、予期しない不具合、および潜在的なハードウェア障害やネットワーク障害につながる可能性があるソフトウェアエラーを除外することはできない。特にハードウェアの障害は、必要な予防措置が講じられていない場合、汚れや温度などの環境条件によって、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。

11.2 潜在的な脅威のシナリオ

1. 即故障につながる実行中のハードディスクまたはスイッチの障害、またはケーブル破損などのコンポーネントの欠陥。
2. ハードウェアの欠陥とソフトウェアコンポーネントのエラーは、長い間発見されないままである可能性があり、システムが再起動されるか特定の制約が適用されるまで問題にならない場合がある。
3. ソフトウェアエラーにより、システムに障害が発生する可能性がある。たとえば、中核のセキュリティコンポーネントの OS を更新すると、再起動後にシステムに不具合が発生する可能性がある。

特にこの種のインシデントは、組織的な対策がなされていない場合、可用性を著しく低下させる可能性がある。

11.3 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ビジネス継続性管理の確立。
2. 交換または交換用デバイスの提供。
3. 本番システムにインストールする前に、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徹底的にテストするためのテスト、診断システムを提供および適用する。
4. 製品サプライヤが独自に開発したものではない、標準化されたインタフェースを使用する。これにより、未発見の脆弱性のリスクが最小限に抑えられる。
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の選択については、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。これに関連するいくつかの重要な側面は次のとおり。
   a. 製品ベンダの信用性と信頼性。
   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。

これらの側面およびその他の側面のための健全な基盤は、BDEW のホワイトペーパー[8]に記載されている。

[8] BDEW, Requirements for Secure Control and Telecommunication Systems, 2018 https://www.bdew.de/media/documents/Awh_20180507_OE-BDEW-Whitepaper-Secure-Systems-engl.pdf

12. スマートデバイスへの攻撃

12.1 問題と原因の説明

スマートフォンまたはタブレットでの運用や生産の表示および変更は、ICS コンポーネントの追加の製品機能として、広く使用されている。これによって、リモートメンテナンス用アクセスの特殊なケースが生じ、更なる攻撃ベクトルとなっている。

12.2 潜在的な脅威のシナリオ

1. スマートフォンの盗難または紛失。
2. デバイス上の十分に保護されていない情報を収集しようとするプログラムをスマートフォンへインストールさせる攻撃。
3. ICS コンポーネントで使用されるスマートフォンの通信チャネルへの攻撃。
   a. ICS との通信のロギング。
   b. 以前に記録された通信の送信によるリプレイ攻撃。
   c. 使用済みアプリケーションまたは使用済みプロトコルのリバースエンジニアリング。
   d. 中間者攻撃（MITM）。

12.3 対策

1. スマートフォンから ICS システムへのアクセス制限を読み取りアクセス（制限）とする。操作または生産パラメータを変更することは不可能とするのが望ましい。

2. アクセス保護、マルウェアに対する保護、およびリモート削除機能（モバイルデバイス管理）のために製品または OS に含まれる機能を使用する。
3. ジェイルブレイクやルート化など、セキュリティ上禁止されている、またはセキュリティ上重要な変更は、スマートフォンで実行できないようにする。
4. スマートフォンアプリケーション（アプリ）は、正規のソース（App Store）から取得する必要がある。アプリは IT 部門によって一元的に監査および配布するのが理想的である。
5. 暗号化された接続（VPN）の使用。
6. スマートフォンを使用するメリットがリスクを上回るかどうかを評価する。
7. ICS に直接アクセスするアプリを使用しない。ただし、必要なプログラムのみを提供する、セキュリティで保護されたターミナルサーバによる間接的な暗号化アクセスは許可して良い。

13. 追加の予防策

13.1 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 または企業全体で構造化されたセキュリティプロセスを使用可能とすることだけを意図しているに過ぎないということを、強調しておきたい。代わりに、特に一般的なサイバーセキュリティと ICS セキュリティの両方について確立された標準類に基づいて、適切な情報セキュリティ管理を導入することを目標とすることが望ましい。

下記は役立つ標準類の例である。

•ISO 27001 に基づく IT-Grundschutz（「IT ベースライン保護」）[9]
•ISO/IEC 27000 シリーズ[10]
•VDI/VDE 2182[11]
•IEC 62443[12]

これらの標準類に基づいて、企業の全体的な管理システムの一部として、ICS 運用のための情報セキュリティ管理システム（ISMS）を理解する必要がある。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、確認、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、下記の基本的な管理策として、ISMS の導入を検討することが望ましい。これらは、責任を定義し、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、可能な限り包括的で費用効率の高い計画を立てるために、できるだけ早く管理策を実装することが役立つ。

•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と、ICS コンポーネントのセキュリティに関連する責任を定義するのに役立つ。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

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

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･維持し､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必要がある。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、インフラおよび含まれる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、適切な技術的および組織的な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未解決リスクを実質的に評価する唯一の方法である。

•緊急時対応計画の管理および再始動手順：インシデント後、組織化された再委任を可能とする継続的な運用プロセスが定義されなければならない。セキュアで中断のない運用を行うには、サービス／保守担当者と管理者がすべての ICS 機能を知っており、それらを操作できる必要がある。これには、管理者／ユーザーガイドの形式での運用および試運転に関するすべてのドキュメントが、責任者および認定スタッフが利用可能でアクセス可能であることが必要である。

•脆弱性の削減：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、コンポーネントベンダや「Allianz für Cybersicherheit」などによるスタッフトレーニング、セキュリティ通知のサブスクリプションに加えて、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。[13]

[13] https://www.allianz-fuer-cybersicherheit.de/ACS/DE/Meldestelle/meldestelle.html

13.2 企業経営の役割

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、適切な管理メカニズム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には、技術担当者が適切なサポートを提供する必要がある。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、初期段階ですべての重要な決定に関与する必要がある。この様な状況においては、残りの未解決リスクや、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。

13.3 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。しかし、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」という考え方が、悲惨な結果を招く可能性がある。したがって、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。

14. 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」かどうかを評価する。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足し、対応する行に合計を入力する。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、最後の行に入力する。

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 で公開している「The State of IT Security in Germany 2018」と「ICS の脅威と対策のトップ 10」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
ウィルス対策は、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（最新のウィルス対策など）。	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 ホワイトペーパーなど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ーは、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アラート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
スマートデバイスへの攻撃	0-3	4-6	7-10
ICS システムの読取アクセスのみが許可され、操作または製造パラメータの変更を許可しない。	0	2	4
スマートフォンは、ジェイルブレイク（脱獄）やルート化などを行っていない正規の基本設定で使用している。	0	1	3
スマートフォンアプリは、App Store などの正規のソースから取得しなければならない。	0	1	3
合計スコア			(0-100 ポイント)

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、特定の未解決リスクが常に残る、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および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、セキュリティ管理、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

参考文献

1: ICS-CERT, Recommended Practices, https://ics-cert.us-cert.gov/ Recommended-Practices, Zugriff im Januar 2019

2: BSI, Industrial Control System Security: Top 10 Threats and Countermeasures, 2014

3: BSI, Industrial Control System Security: Top 10 Threats and Countermeasures, 2016

4: BSI, The State of IT Security in Germany 2018, 2018

5: BSI, Abwehr von DDoS - Angriffen v2.0, https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_002.pdf, 2018

6: BDEW, Requirements for Secure Control and Telecommunication Systems, 2018