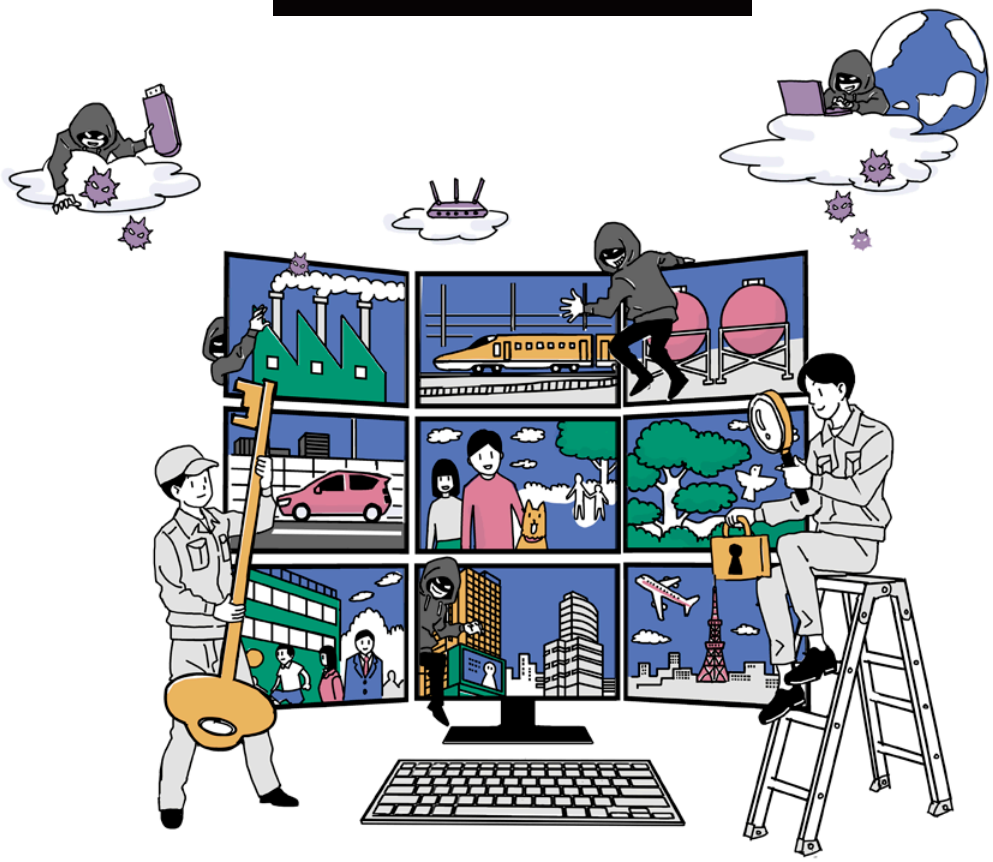
J-CLICS 設問項目ガイド

攻撃経路対策編



多様化する攻撃から制御システムを守るために

一般社団法人JPCERTコーディネーションセンター

2023年3月7日

本ガイドについて

本ガイドは、制御システム向けのセキュリティチェックリストJ-CLICS（Check List for Industrial Control Systems of Japan）攻撃経路対策編の補足文書です。制御システムユーザーの皆さまが、制御システムに存在する代表的な攻撃経路のセキュリティ脅威と対策の状況をセルフチェックして、今後の対策・検討を行う際にご活用いただけます。セキュリティに関する深い専門知識は必要なく、コンピューターやネットワーク技術で広く知られている用語の知識がある方に向けた内容です。

本ガイドでは、チェックリストに記載した設問の意味（背景、目的）や具体的な対策方法を解説していますので、チェックリストの設問に書かれている対策を実施しているのか（○をつける）、まだ実施していないのか（×をつける）、の判断を、より的確に行えます。まだ実施していない項目に対する効果的な対策を立案、実施する際に、各設問の解説ページをご活用いただけます。

本ガイドの記載内容

本ガイドは、イントロダクション部分と、攻撃経路ごとの設問に対する解説部分で構成しています。イントロダクション部分では、攻撃経路対策編の全体像について説明しています。

各経路や設問の解説部分は、それぞれ独立して読めるように構成していますので、通読せずに必要な設問部分だけを読むという活用方法も可能です。各設問を深く理解するために参考となる情報を、以下の表1に示す8つの項目で補足、解説しています。

[表1:J-CLICS 攻撃経路対策編 各設問の解説部分に記載している情報]

攻撃経路の特徴	J-CLICS攻撃経路対策編で扱う攻撃経路に関して、セキュリティ視点での特徴を簡単に解説しています。
攻撃への対策の考え方	攻撃経路ごとに、経路固有の攻撃への対策の考え方について解説しています。この考え方をもとに、各設問の解説をしています。
背景・目的	設問を設定した背景と、設問の目的について説明しています。
想定される攻撃	設問に書かれていることが実施されなかった場合に、発生する恐れがある攻撃の例について説明しています。各項目で解説される内容や対策例を実施することで、これらの攻撃の防御、緩和、検知が行えます。
対策概要	攻撃に対する対策をどのように考えるか、その対策によって得られる効果は何かについて説明しています。
内容解説・対策例	設問の内容の詳細と、各設問を実施済みとするための対策例について説明しています。記載された例は、あくまでも一般化された例ですので、これらの例を参考にして、現場の事情に合った対策を検討する必要があります。
参考文献	設問に関連する書籍・文献・ホームページなどの情報です。より深く知りたい場合などにご活用ください。
コラム	設問に関連した補足情報です。対策の理解や実施に役立ちそうな情報を紹介しています。

謝辞

J-CLICS は、SICE／JEITA／JEMIMA セキュリティ合同WGメンバー、業界の関係者の方々、有識者の皆さまのご協力により作成されました。

J-CLICS作成にご協力いただいた方々（五十音順、敬称略）

新井　貴之	横河電機株式会社（一般社団法人電子情報技術産業協会）
石田　茂	独立行政法人情報処理推進機構
伊東　雄	東芝インフラシステムズ株式会社
梅﨑　一也	富士電機株式会社（一般社団法人電子情報技術産業協会）
梅田　裕二	東芝インフラシステムズ株式会社（一般社団法人日本電気計測器工業会）
遠藤　浩通	株式会社日立製作所（一般社団法人日本電気計測器工業会）
大石　貴之	ＡＢＢ日本ベーレー株式会社（一般社団法人日本電気計測器工業会）
小野　匠史	ＡＢＢ日本ベーレー株式会社（一般社団法人日本電気計測器工業会）
加藤　毅	横河電機株式会社（一般社団法人日本電気計測器工業会）
畔　英之	三菱電機株式会社（一般社団法人電子情報技術産業協会）
澤田　賢治	国立大学法人電気通信大学
澤田　充央	アズビル株式会社（一般社団法人日本電気計測器工業会）
鷲見　直也	一般社団法人日本ガス協会
高務　健二	富士電機株式会社（一般社団法人日本電気計測器工業会）
永作　亮太郎	株式会社日立ハイテクソリューションズ（一般社団法人日本電気計測器工業会）
村上　仁志	株式会社日立ハイテクソリューションズ（一般社団法人日本電気計測器工業会）
山川　秀史	ＡＢＢ日本ベーレー株式会社（一般社団法人日本電気計測器工業会）
横井　昭彦	公益社団法人計測自動制御学会
和田　英彦	横河電機株式会社（一般社団法人電子情報技術産業協会）
渡部　宗一	イーヒルズ株式会社

【一般社団法人 日本電気計測器工業会（JEMIMA）】

日本電気計測器工業会（JEMIMA）PA・FA計装制御委員会セキュリティ調査研究WGは、製造業分野でのセキュリティに対する今後の影響、取り組みなどを調査・研究し、JEMIMA会員各社に有益となる情報のフィードバックを行う。

【一般社団法人 電子情報技術産業協会（JEITA）】

電子情報技術産業協会（JEITA）制御・エネルギー管理専門委員会は、制御システムのセキュリティ対策を普及・浸透させるための課題や解決策の調査・検討を行い、安全安心な工場・プラント操業のあるべき姿を定義し、提言を行う。

【公益社団法人 計測自動制御学会（SICE）】

計測自動制御学会（SICE）産業応用部門計測制御ネットワーク部会は、制御システムにおける情報連携のために、最新のIT技術や標準化活動、制御系セキュリティ技術の産業現場への導入等の調査・研究に取り組む。

目次

イントロダクション

0

攻撃経路対策編の特徴

概要

制御システムがIoT（Internet of Things）技術などを活用した「よりつながる」制御システムとなっていき、新たな技術導入による付加価値の実現が期待される一方で、これまで想定されてこなかったサイバー攻撃が発生することも懸念されています。
SICE／JEITA／JEMIMAセキュリティ合同WGは、これからセキュリティ対策に取り組もうとする制御システムユーザーを主な対象に、システムのセキュリティ対策状況を自己評価できるツール「J-CLICS」を開発し、2013年3月からJPCERT/CCのWebサイトで公開、配布しています。このJ-CLICS公開から時間が経っており、「よりつながる」制御システムが到来しつつあることや、それに伴いセキュリティの状況や環境が変化していることを念頭において、この攻撃経路対策編を開発しました。
このイントロダクションの章では、攻撃経路対策編の開発の背景や目標、想定しているシステム構成、攻撃経路、セキュリティ対策について紹介します。各攻撃経路の設問項目に関する解説は、次章以降に記載しています。

index

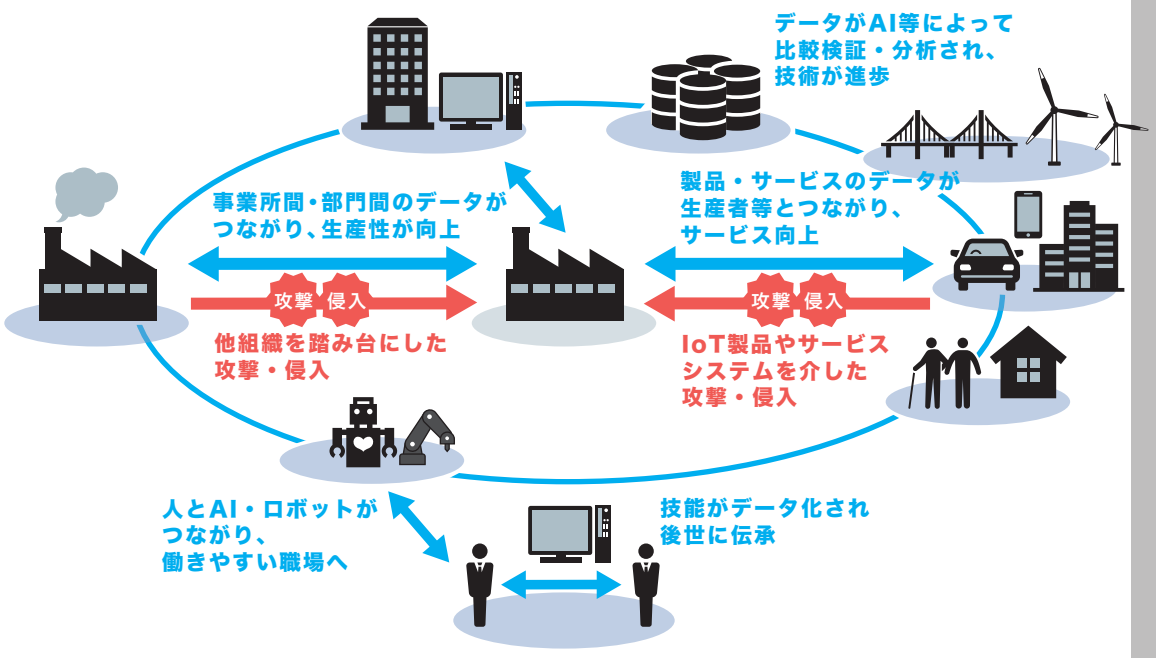
イントロダクション

開発の背景

制御システムの変化

各種産業や社会インフラなどで用いられている制御システムは、IT技術の応用による現場情報と経営情報の相互連携が推進され、生産性や安全、環境の改善などに貢献してきました。近年では、日本政府の「Connected Industries」に代表されるように、IoTを活用したより高度な現場情報の活用や、広域ネットワークを通じた複数・異種のシステム間連携などの「よりつながる」制御システムのアーキテクチャが提唱されています。このようなアーキテクチャを採用することにより、例えばバリューチェーン全体にわたるリソースの最適化が可能になるなど、産業や社会全体において生産性や柔軟性のさらなる向上や新たな付加価値の創出が期待されています。
その一方で、図1に示すように、外部とつながることによる攻撃機会の増加も懸念されています。
このような「よりつながる」制御システムへと変化する状況であっても、自組織で統制ができる制御システムの保護に重点を置き、外部からの攻撃に備える対策を行うことが重要です。

［図1:「よりつながる」制御システムの付加価値とセキュリティ脅威の増加］



J-CLICS STEP1／STEP2との関係

J-CLICS STEP1／STEP2の特徴

「セキュリティ対策を開始したいが何をすればよいかわからない」といった制御システムユーザーへの情報提供を目的として、重要度が高く、現場で実施しやすい21項目の対策をSSAT※より厳選してJ-CLICS　STEP1／STEP2にまとめました。

このJ-CLICSでは、少ない項目数で重要な対策をカバーできることを優先して、対策の網羅性を重視しませんでした。そのため、すべての項目を達成できたとしても、セキュリティ対策上は十分とは言えない点や、リスクが残存していてもそのリスクが明確にわからない点などに改善の余地がありました。

J-CLICS攻撃経路対策編の位置づけ

今回開発したJ-CLICS攻撃経路対策編は、制御システムとの接続点を攻撃経路と定義して、各攻撃経路の攻撃手順に対して実施すべきセキュリティ対策を検討した結果から作成したチェックリストとガイド文章で構成されています。

J-CLICS　STEP1／STEP2とは異なる視点のチェックリストと文章になっていますが、攻撃経路対策編のセキュリティ対策の解説には、STEP1／STEP2の対策と同じ内容も一部含まれています。

※SSAT: 英国の CPNI が開発した 100 以上の設問で構成される SCADA Self Assessment Tool の略称。
どの程度セキュリティ対策が実施されているかを判断するためのツール。

目標

J-CLICS攻撃経路対策編では、表2に記す3つの項目を明確にすることを目標としています。

[表2:J-CLICS攻撃経路対策編で明確にされる項目]

対象とするリスクと効果	セキュリティ対策が対象とするリスク(セキュリティ対策によって低減または除去されるリスク)と効果を明確にする。
対策の実施状況	攻撃経路のどの攻撃に対してセキュリティ対策が導入済みかを俯瞰的に確認でき、対策が不足している経路や攻撃手法を明確にする。
優先度	どのセキュリティ対策を優先するべきか明確にする。

セキュリティ対策導入の考え方

限られたコストで効果的なセキュリティ対策を実現するためには、保護対象となるシステムにおいて、リスクの大きさや対策にかかるコストを考慮して対策に優先度をつけることと、必要な場所で必要な対策を過不足なく実施することが重要です。また、セキュリティ対策は「やればやるほど良い」というものではありません。過剰なセキュリティ対策は、無駄なコストを発生させるだけではなく、新しいリスク要因になる恐れがあります。
例えば、セキュリティ対策のために導入したソフトウェアや機器の設定、構成が堅牢な状態でない場合や、脆弱性情報の管理、運用方法などが不十分であった場合には、その状況を攻撃に悪用されてしまい、その結果、システムへの攻撃機会を増やす要因となってしまいます。

セキュリティ対策の優先度

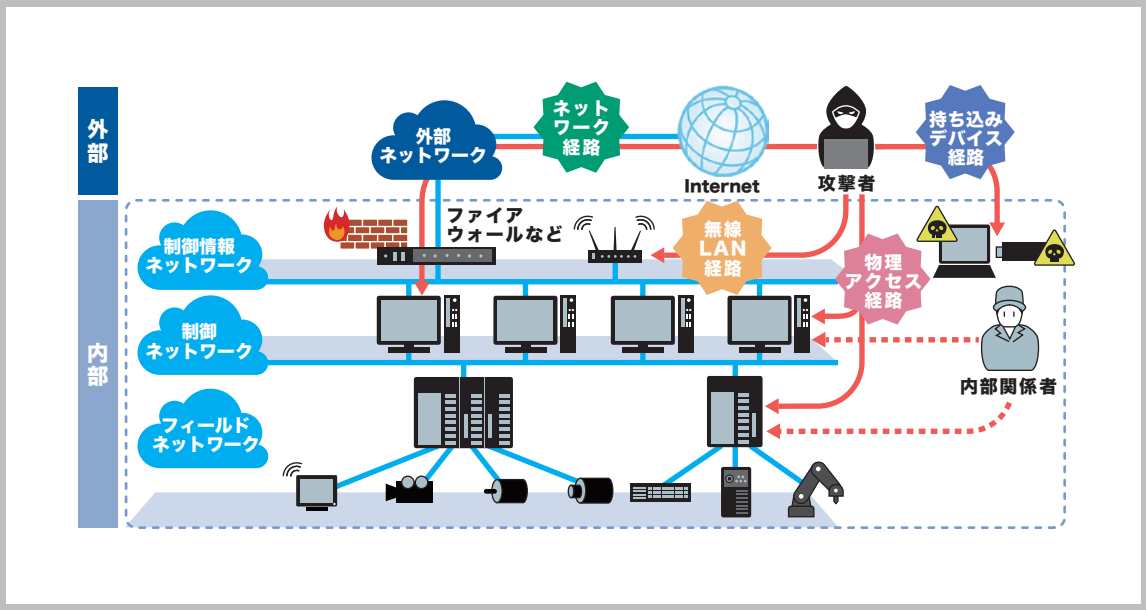
攻撃の可能性がある経路の存在を認識し、制御システム全体として優先度や対策状況を考慮して、有効なセキュリティ対策を実施しなければ、十分な効果が発揮できないことがあります。
例えば、家の施錠管理の場合を考えると、棚や引き出しの施錠よりも玄関や窓の施錠（戸締り）が優先されるべきです。これは「施錠自体は有効な対策であっても、優先度を考慮しなければ十分な効果が得られない」という一例です。また、複数の錠で玄関が厳重に施錠されていても、裏口や窓が施錠されていなければ家全体としての防犯効果は低くなります。この場合は、玄関の施錠を厳重にするのではなく、その他の入り口（経路）にも施錠をすべきという一例です。

この「セキュリティ対策の優先度」を判定するためには、最初に保護対象となるシステムの状況とそこに存在するリスクを把握する必要があります。

想定するシステム構成と脅威

保護対象のシステム構成

J-CLICS攻撃経路対策編では、図2の破線四角で囲われた部分に示すような『フィールドネットワーク・制御ネットワーク・制御情報ネットワークからなるISA95の参照モデルをもとにした3層モデルの制御システム』を保護対象のシステムとして想定しています。



この保護対象のシステムに対して代表的な攻撃経路と攻撃手法の分析を行い、その結果に基づいてセキュリティ対策を選定しているため、モデルシステムに対するセキュリティ対策がもたらす効果と対策対象のリスク、優先度、対策の実施状況が明確になります。
どのような脅威を想定して、どのような分析を実施したかは、次の「想定する脅威」と「脅威分析手法」で解説します。

想定する脅威

本ガイドでは、保護対象のシステム構成図の破線四角で囲った内側を制御システムの内部と定義し、その外側に存在するものはすべて外部と定義しています。本ガイドで想定する脅威は、保護対象システムの外部に存在する、正規のアクセス権限を持たない者による攻撃としています。内部関係者による攻撃も考えられますが、セキュリティ対策においては外部からの攻撃への対策を優先するべきとの考えから、今回の想定する脅威からは除外しています。内部関係者に対しては、JIS Q 27002の人的資源セキュリティで対処する方法が考えられます。

脅威分析手法

セキュリティ対策を計画する際は、保護対象システムにどのような脅威があるのかを明らかにすることが重要です。想定する保護対象システムにおいて、どのような脅威があるのかを分析するために次の3点に着目しました。これらをもとに分析することで、代表的な脅威を洗い出しています。

【攻撃経路】

本ガイドでは、制御システム外部に存在する正規のアクセス権限を持たない攻撃者が制御システム内部に侵入する代表的な経路として、ネットワーク・無線LAN・持ち込みデバイス・物理アクセスの4つを想定しています。

【攻撃手順】

各攻撃経路を通じて保護対象システムを攻撃するためには、特定の手順を踏む必要があります。外部の攻撃者が手順をよく考えずに攻撃対象に到達でき、何の制限もなく攻撃を実行できるケースは稀です。保護対象システム内にある攻撃対象への到達手順を攻撃経路ごとに明らかにすることで、脅威を洗い出しています。

【攻撃手順の成立条件】

攻撃手順が成立するためには、その攻撃を成功させるためのいくつかの条件をすべて満たす必要があります。1つでも条件が満たされなければ、その攻撃手順は利用できません。
セキュリティ対策を検討するときには、攻撃を成立させるために必要となる条件を満たせなくさせる対策を考えれば良いことになります。

攻撃経路

攻撃経路ごとの成立条件

各攻撃経路の攻撃手順と、それを成立させるための条件（例えば、類推可能なパスワードの使用など）を検討し、可能な限り列挙しています。本書の付属資料「J-CLICS 攻撃経路対策編 対策マップ」（以下、対策マップという。）で一覧できます。

経路の優先度

どの攻撃経路から優先して対策すべきかを、攻撃者が攻撃に悪用しやすいかどうかの観点で、各攻撃経路の性質（地理条件・時間条件・手段条件・機会条件）を〇／△／×の3段階で評価しています。

【地理条件】
ネットワークのように接続されていればどこからでも利用可能であるのに対して、持ち込みデバイスは外部から何かの手段で内部に運搬させる必要があります。無線LANや物理アクセスは、その施設に近づかなければ利用できないため、持ち込みデバイスよりもさらに評価値が低くなります。

【時間条件】
ネットワークや無線LANは制御システム内で常時接続しているため、常時利用できる状態になっています。持ち込みデバイスは制御システムに常設されておらず、物理アクセスは、攻撃者の前準備が必要なため、前者2つよりも評価値が低くなります。

【手段条件】
ネットワークや無線LANは常設されており、その経路は誰でも利用可能な状態になっています。持ち込みデバイスや物理アクセスについては、その施設への運搬や接近ができるという条件があるため、ネットワークや無線LANよりも評価値が低くなります。

【機会条件】
その行動の秘匿性の高さで評価しています。ネットワーク経路は物理的に見えないため、4つの中で最も利用されているかどうかを検知することが困難です。無線LANや持ち込みデバイスを利用する場合は、何かしらの機器を伴うため、ネットワークよりは検知が容易です。物理アクセスは不審者として周囲の人が発見しやすいため、評価値は最も低くなります。

この結果、対策すべき経路の優先順位は、表3のとおりネットワーク経路を最優先とし、以下、無線LAN経路、持ち込みデバイス経路、物理アクセス（施設への不正侵入）経路の順とします。

[表3:各攻撃経路の性質から評価する攻撃への悪用のしやすさと対策の優先順位]

経路	地理条件 どこからでも	時間条件 いつでも	手段条件 誰でも	機会条件 こっそりと	優先順位
ネットワーク	○	○	○	○	1
無線LAN	×	○	○	△	2
持ち込みデバイス	△	×	△	△	3
物理アクセス （施設への不正侵入）	×	×	△	×	4

セキュリティ対策

セキュリティ対策の考え方

前述した4つの攻撃経路について、それぞれ想定される攻撃手順を列挙して、セキュリティ対策を検討します。

最も簡単なセキュリティ対策は、攻撃経路となり得る4つの経路を利用しないことですが、すでに設置済みの環境で利用を止めることは容易ではありません。まずは、個々のセキュリティ対策を導入する前に、経路の必要性を見直して、不要な経路を撤去したり、利用機会を縮小したりする（例えば、必要な時だけ使う、使える状態にする）といった経路の必要性を見直す活動を先に行い、その後に残った経路に対してセキュリティ対策を実施することが効果的なアプローチです。
また、本章で挙げるセキュリティ対策を設置済みのすべての経路で実施すると、運用やメンテナンスコストが非常に高くなってしまいます。個々のセキュリティ対策の目的や特徴を認識した上で、システムや組織事情にあった対策を選択してください。また検討にあたっては、対策を導入した後に、効果を維持していくためのメンテナンスコストへの考慮も必要です。

本ガイドでは、セキュリティ対策を選択し導入する場合には、保護対象となる資産（以下、保護対象資産という。）にたどり着く経路で、攻撃が開始される場所に近い方の対策から採用することを推奨します。攻撃には手順があり、手順が進むにつれて被害が大きくなるため、できるだけ早い段階で攻撃を止められる対策の方が導入効果は高くなります。

本ガイドは、攻撃経路に存在する攻撃手順に対するセキュリティ対策に焦点を当てた文章となっています。セキュリティ対策を実施する上では、本ガイドに掲載した対策以外にも、関係者への教育や、資産台帳の維持管理など人的な管理面で補強することも重要です。

4種類の対策

J-CLICS攻撃経路対策編では、1つの攻撃成立条件に対して、目的別に分類した防御・緩和・検知・回復の4種類のセキュリティ対策を提供しています。それぞれの対策について説明します。

【防御】

攻撃が保護対象資産に到達しないようにするための対策です。攻撃による被害の発生を防ぐために、攻撃経路自体の除去や遮断をしたり事前に脆弱な状態を無くしたりするなどの、攻撃が発生する前に行うセキュリティ対策です。例えば、ファイアウォールなどの通信制御機器を使って、外部からの侵入を制御する方法や、システム内の機器やソフトウェアに対する脆弱性対応などの方法があります。

【緩和】

攻撃発生時に、保護対象資産の被害を最小限に抑えるための対策です。防御策を導入できない事情がある場合や、あるいは防御の対策をすり抜けて攻撃者が到達し、攻撃が行われた場合でも、重要な資産への被害を抑えることによって操業への影響をできるだけ小さくすることが期待できます。例えば、データの暗号化による重要データの流出時の解析防止などの方法があります。

【検知】

攻撃や異常な状態が発生していることを知るための対策です。防御策、緩和策をすり抜けた攻撃を検知するだけでなく、異常な状態や脆弱性の検知などを行うことで、攻撃の発生を検知して被害をなるべく早期に防ぐ対策となり、Zero-Day攻撃への対策が期待できます。例えば、OSのログ解析や侵入検知システム（以下「IDS」という。）／侵入防止システム（以下「IPS」という。）の設置などの方法があります。検知策で発見された事象に対しては、組織のインシデントレスポンスのルールに従って対処する必要があります。

【回復】

攻撃が発生した後に、事業継続可能な状態に戻すための対策です。つまり、攻撃による影響を一時的または恒久的に除去する活動全般を指した対策です。回復策は攻撃が起こった後の対策ですが、事前に準備しておくことで、被害から回復するまでの時間を短縮することが期待できます。システム可用性や事業継続性の向上につながるため、重要な対策です。例えば、バックアップからのリカバリーができる状態にしておくことや、セキュリティインシデント発生時の事前訓練、攻撃が発生した時の対応マニュアルの整備などの対策があります。バックアップに関しては、J-CLICS設問項目ガイド STEP2の設問No.9 「バックアップと回復」で具体的に解説しています。

得られる効果

本書では、前述した4種類の対策（防御・緩和・検知・回復）について複数のセキュリティ対策を提供しています。防御と緩和におけるセキュリティ対策は、その方法によって得られる効果が異なるため、表4に記した7つに分類しました。導入するセキュリティ対策を検討する際に、どのような効果が得られるかの参考にご利用ください。

[表4:本書におけるセキュリティ対策によって得られる効果の分類]

略語	効果の種類	得られる効果
遮	攻撃を遮断する	攻撃経路を遮断し、攻撃に使用できないようにする対策です。
狭	攻撃経路を狭める	攻撃を狭めて、攻撃に使用できる条件を厳しくする対策です。
難	保護資産への到達を困難にする	攻撃経路の存在や悪用方法をわかりづらくする対策です。
縮	攻撃の影響を小さくする	攻撃発生時の影響を小さくする対策です。
労	攻撃の手間をかけさせる	攻撃者の手間（コスト）をかけさせる対策です。
抑	攻撃者を躊躇させる	攻撃者を牽制し攻撃を抑止する対策です。
管	保護対象の状態を把握する	異常状態に気付きやすくする対策です。

J-CLICS攻撃経路対策編のチェックリスト構成

J-CLICS攻撃経路対策編のチェックリストは、計19個の設問項目で構成しています。各設問はそれぞれの攻撃経路の攻撃手順に対応しており、本ガイドや対策マップを使って攻撃成立条件の詳細とセキュリティ対策を確認して実施することで、攻撃経路ごとのセキュリティ強化が期待できます。

想定する攻撃経路

外部に存在する攻撃者から保護対象システムへの代表的な攻撃経路として、次の4つの経路を想定しました。

1.ネットワーク経路（接頭文字:N）

2.無線LAN経路（接頭文字:R）

3.持ち込みデバイス経路（接頭文字:D）

4.物理アクセス経路（接頭文字:P）

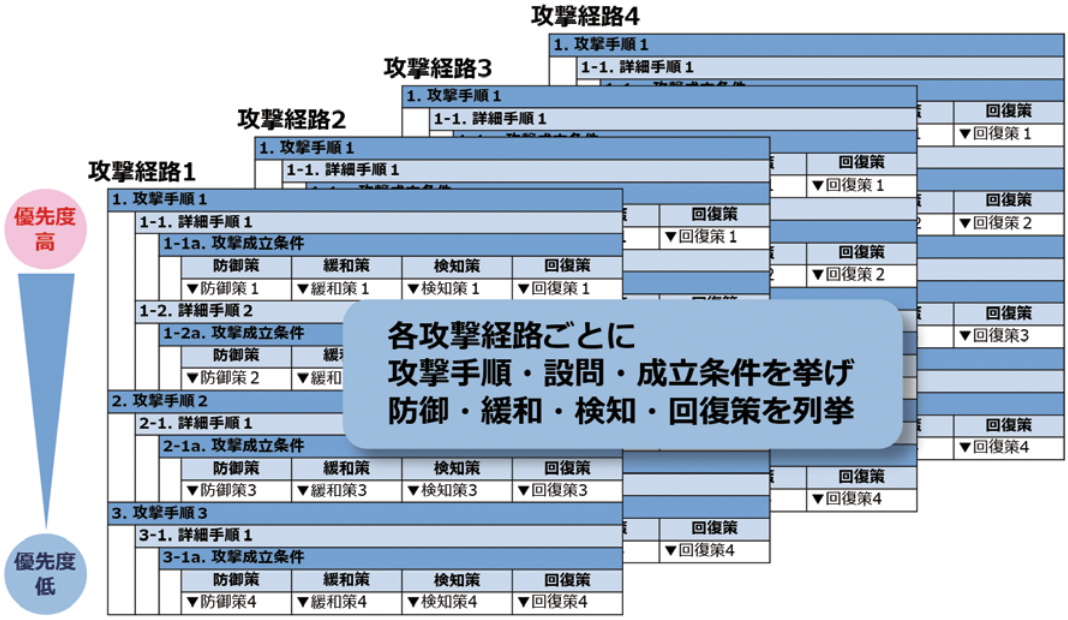
チェックリストの各設問は、想定した4つの経路の接頭文字を用いた設問番号が割り振られています。ネットワーク経路に関する1番目の設問であればQN1、持ち込みデバイス経路に関する2番目の設問であればQD2といった設問番号となります。各経路の設問に関する詳細は、本章以降に経路ごとに説明しています。

セキュリティ対策実施の優先度

チェックリストを使ったチェック結果から、セキュリティ対策を検討すべき攻撃経路とその攻撃手法、成立条件が明らかになった場合に、どこから対策すべきか迷うことがあります。その場合は、本書の攻撃経路の優先度順にしたがって、セキュリティ対策導入の効果と優先度が高い順（対策マップの上側の項目）から検討することを推奨します。対策マップは攻撃経路の攻撃が開始される場所から保護対象資産に向かって攻撃が進むステップを、表の上から下に向かって表現しているため、図3のとおり上側（外からの攻撃）から対策を実施することでセキュリティ対策の導入効果が大きくなることが期待できます。

ネットワーク経路と無線LAN経路、持ち込みデバイス経路には、設問番号0があります。この設問0は、各経路の使用が最小限になっているかを問う設問となっているため、最小化が出来ている場合もしくは外部との接続を持たない場合は、それ以降の設問に対応するセキュリティ対策の実施優先度は下がります。

［図3:対策マップから見るセキュリティ対策の優先度］



さらなる対策強化へ向けて

J-CLICS攻撃経路対策編は、「よりつながる」制御システムへと変化する状況であっても、自組織で統制ができる範囲で外部からの攻撃に備える対策を行うことに重点が置かれています。その上で、各攻撃経路の攻撃手順に対して実施すべきセキュリティ対策を検討した結果から作成されたチェックリストとガイド文章で構成されています。よりセキュアな制御システムを構築し、セキュリティを考慮した制御システムの運用を行うためには、制御システム向けセキュリティに関する知識・理解をより深める事が重要です。

本ガイド文章では各設問に対し、情報システム向けセキュリティガイドラインとして「JIS Q 27001:2014」を、制御システム向けセキュリティガイドラインとして「NIST（アメリカ国立標準情報技術研究所）SP800-82 Rev.2」を「参考文献」に示していますので、今後の対策にお役立てください。また将来これらの標準文章に基づいた制御システムのアセスメントを実施し、よりセキュアな制御システムの構築、維持・管理を実現ください。なおNIST SP800-82の日英対訳版は、JPCERT/CCより入手可能です。

column

コラム-1

千里の道も資産台帳から

【J-CLICS STEP2の設問１】

制御システムの構成を把握し、
変更履歴を含め最新の状態を管理していますか？

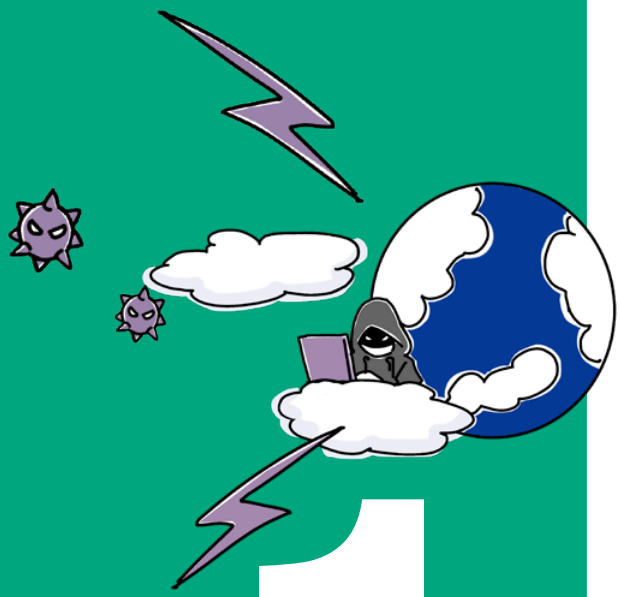
ここで「〇」を付けた方は、このコラムは読み飛ばしてください。「×」とされた方、あなたは他の設問に回答する必要はもはやありません。今すぐ資産台帳の作成に取り掛かってください。

制御システムがサーバーとクライアントの2台のみというならいざ知らず、複数のサーバーとクライアントがスイッチなどのネットワーク機器を介してシステムを構成しているような場合、関係者が「〇〇制御システム」と聞いて思い浮かべる端末が必ずしも一致しているとは限りません。

資産台帳なくして、J-CLICS STEP2の設問3「制御システムに接続されているすべての機器の通信仕様、接続仕様を把握していますか？」に答えられますか？もしこの設問を、制御システムを納入したベンダーに質問したとして、関係者間で対象端末の認識が異なる場合、得られる回答に何の意味があるでしょうか。

セキュリティ対策の初めの第1歩は、情報システム／制御システムの違いはなく、今も昔も資産台帳の作成なのです。

ネットワーク経路



1

攻撃経路の特徴

ネットワーク経路は、他の経路と比較して、攻撃者が制御システムエリアに近づかないで攻撃できる経路です。制御システムのネットワーク化が進んでいるため、本経路での対策として、外部ネットワークとの接点を防御するだけでなく、制御システムの内部ネットワークをセグメント分けし、各境界で防衛することが重要です。また、関係者の教育やネットワーク情報の管理、侵入や攻撃を想定した検知手段を準備しておくなどの対策も有効です。

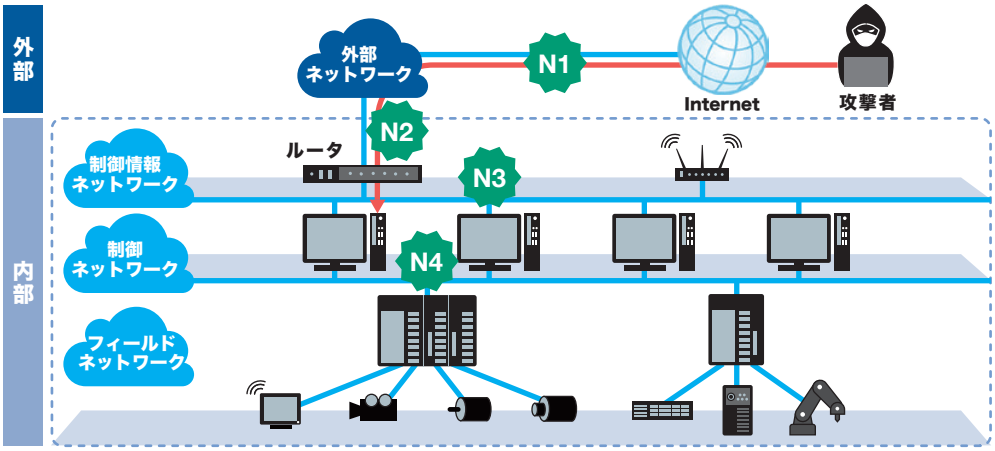
QN index

ネットワーク経路

攻撃への対策の考え方

悪意をもった攻撃者がなるべく低い労力とリスクで制御システムネットワークに侵入しようとする場合、無線LAN、持ち込みデバイス、物理アクセスの他の3つの経路と比較して、常に外部と接続されているネットワーク経路を選ぶ可能性が高いと想定されます。侵入者が活動するリスクを低減するためには、できるだけ外側の層で対策を講じることが重要です。加えて、制御システムネットワークに到達するまでの各階層で多重に防御することも有効な対策となります。
図4のとおり、ネットワーク経路の各層ごとの攻撃として次のものが想定されます。

[図4:ネットワーク経路で想定される各層ごとの攻撃]



N1【入口IPアドレスの特定】→QN1、QN2を参照

攻撃者は、標的とする制御システムにアクセスするため、公開情報の分析や関係者への接触、インターネットに接続されているシステムを公開する外部サービスの利用などによって、制御システムが外部ネットワークと接続されている入口IPアドレスの特定を試みます。対策として、入口IPアドレスなどのネットワーク構成情報が誤って公開されないような管理や、外部サービスに対するアクセス制限などを実施します。

N2【入口システムにアクセス】→QN2を参照

攻撃者は、特定した入口IPアドレスにアクセスし、そこから制御システムと外部ネットワークの境界を越えて制御システムの内部ネットワークへのアクセスを試みます。対策として、制御システムと外部ネットワークが接続するようなネットワークの境界部分で、アクセスの制限や監視を実施します。

N3【システム情報を取得】→QN2を参照

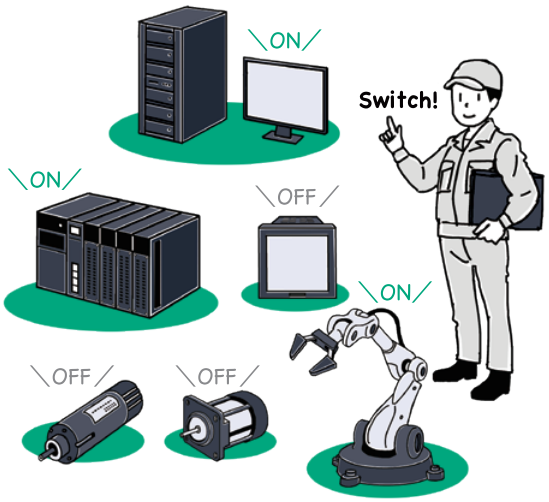
攻撃者は、制御システムにおける攻撃対象や攻撃の踏み台となる機器を探すため、制御システムの内部ネットワークに接続された機器にアクセスしてシステム情報を取得します。その結果、OSが古かったりセキュリティパッチが最新でなかったりする機器が見つかった場合、それらに対する攻撃の危険性が高まります。対策として、制御システムの運転に不要な通信に対する制限や監視を実施します。

N4【攻撃実施】→QN2、QN3、QN4、QN5を参照

攻撃者は、標的とする機器に対して、DoS攻撃や認証試行の乱発など、制御動作を妨害するような攻撃を実行します。また、制御システム機器の不正操作や、マルウェアのインストールなど、制御システムにさらなるダメージを与えるための攻撃を実行します。対策として、強力な認証の導入、制御システムの内部ネットワークに対する通信の制限や監視、機器の脆弱性対策やプログラムの実行制限などを実施します。

設問 QN0 【外部ネットワーク接続の最小化】

外部とのネットワーク接続は必要最小限になっていますか？



背景・目的

「Connected　Industries」に代表されるように、制御システムはインターネット、イントラネットを介してさまざまなシステムとつながることが、当たり前になってくると思われます。つながることによる利便性を追求する一方、不要な接続により無関係な組織からのアクセスが可能な状態となっていないか、確認、把握することが重要となります。

想定される攻撃

制御システムと外部ネットワークとの接続点が複数存在したり、外部ネットワークから制御システムに対して常時接続可能な状態になっていたりすることで、制御システムが攻撃の標的となる危険性が高まることが想定されます。

対策概要

制御システムと外部ネットワークとの接続箇所を見直して、不要な接続を除去したり、運転に影響のない範囲で外部との接続の機会を最小化したりします。これらの対策により、攻撃されるリスクを低減できます。

設問 QN0 【外部ネットワーク接続の最小化】

外部とのネットワーク接続は必要最小限になっていますか？

内容解説・対策例

【防御策】恒久的な運転に必要ない接続を除去する

制御システムと外部ネットワークとの接続は、制御システムを動作させるために必要な最低限のものに留めます。恒久的な運転に必要ない接続はできる限りなくすことで、外部からネットワーク経由で制御システムが攻撃される機会を極力減らします。

【緩和策】未使用時の外部接続を遮断する

制御システムと外部ネットワークとの常時接続が不要である場合には、外部ネットワークとの接続が必要な時のみ機器の電源をONするなどして、ネットワーク経由で攻撃される機会を最小化します。この対策は、接続を遮断した時の影響を十分に確認した上で実施してください。

参考文献

・JIS Q 27001:2014 「A13.1 ネットワーク管理策」
・NIST SP800-82 Rev.2 「5.1 ネットワークの分割と分離」

設問 QN 1 【ネットワーク構成情報の秘匿】

ネットワークの構成情報は秘密情報として管理されていますか？

背景・目的

ネットワークの構成情報が外部に漏えいすると、攻撃に悪用される恐れがあります。制御システムのネットワークの構成情報を厳格に管理し、関係者以外にネットワーク構成を漏えいしないようにすることで、ネットワーク経路からの侵入や攻撃のリスクを低減できます。

想定される攻撃

ネットワークの構成情報は、知られてもすぐに攻撃されるわけではありませんが、攻撃者が侵入経路や攻撃手法を分析、検討する糸口となります。その結果を利用して、制御システムが外部から攻撃されることが想定されます。

対策概要

攻撃者に攻撃の手がかりとなる情報を簡単に与えないことが重要です。この対策を実施することで、攻撃者が制御システムを攻撃する際に必要となる構成情報の入手や調査に労力と時間が必要となり、侵入や攻撃のリスクを低減できます。

設問 QN 1 【ネットワーク構成情報の秘匿】

ネットワークの構成情報は秘密情報として管理されていますか？

内容解説・対策例

【防御策】システム構成に関する情報を秘密情報として管理する

システム構成に関する情報の管理方法を見直します。具体的には、システム構成に関する情報が含まれる資料を秘密情報に指定し、その情報へのアクセスを制限、管理します。

【防御策】秘密情報へのアクセスを管理する

【防御策】秘密情報やそれらの特定・推測につながる情報の漏えいを防止する

秘密として指定したシステム構成などの情報に対するアクセスを制限、管理して、漏えいを防止します。また、情報公開時に秘密情報が含まれていないかチェックしたり、すでに公開された情報の公開可否を見直したりする体制を構築します。

【防御策】関係者の教育を行う

関係者へ秘密情報の管理についての教育を行い、情報漏えいを防止します。

【防御策】契約等で情報漏えいを牽制する

関係者との契約や、従事者の行動に関する規則によって、情報漏えいを抑止します。この対策は、内部犯行に対しても有効です。

【防御策】退職者からの情報漏えいを防止する

アカウントを定期的に見直し、退職者などの不要となったアカウントを削除するなどして、情報漏えいを防止します。

【緩和策】秘密情報の拡散を抑制するための手順を実施する

【検知策】自社機器の情報が公開されていることを認識する

公開資料から秘密情報が拡散してしまう場合を想定し、自組織の内部情報が意図せず外部に知られていないかを監視するとともに、原因となった資料の差し替えや公開停止を速やかに実施できる体制を構築します。

【検知策】関係者へのアプローチがあったことを認識する

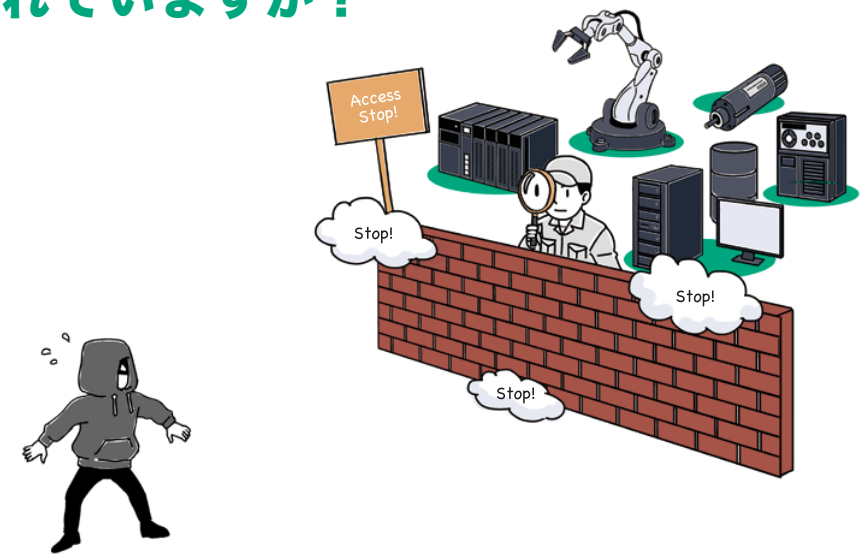
不審者から関係者へ接触があった際に、速やかに通報できる体制を構築します。

参考文献

・J-CLICS S2-10-1（転入者と転出者用のプロセス）
・JIS Q 27001:2014 「A.8.2情報分類」

設問 QN2 【境界防衛の実施】

外部とのネットワーク境界は アクセス制限と監視によって 保護されていますか？



背景・目的

攻撃者は、ネットワークスキャンなどによる情報収集やアクセスの試行によって標的となるシステムへの侵入を試みます。制御システムの運転に無関係な通信を外部ネットワークとの境界で遮断および監視することにより、攻撃者からのアクセス機会を最小化するとともに、攻撃やその予兆を検知して迅速な対応をとることができます。

想定される攻撃

外部ネットワークから制御システムの内部ネットワークへアクセスが可能であると、制御システムを構成する機器が侵入や攻撃の危険にさらされます。また、外部サービスから制御システムへのアクセスが試行され、アクセス可能と判定された場合には、その情報を得た攻撃者に標的として認識される恐れがあります。

対策概要

制御システムと外部ネットワークの境界や、制御システム内のネットワーク間境界における境界防衛として、運転に無関係な相手や内容の通信を遮断し、異常な通信が含まれていないかを監視します。

設問 QN2 【境界防衛の実施】

外部とのネットワーク境界は アクセス制限と監視によって 保護されていますか？

内容解説・対策例

【防御策】自組織・関係組織以外からのアクセスを遮断する

ファイアウォールや侵入防止システム（以下「IPS」という。）などの機器で、制御システムの運転に必要ない送信元アドレス、ポート、プロトコルの通信を遮断します。

【防御策】外部からのアクセス手段・機会を制限する

ファイアウォール、IPSなどの機器によって通信を制限、遮断することや、外部ネットワークと接続する機器の電源をON／OFFすることで、制御システムの運転に必要な場合にだけ外部ネットワークに接続します。

【緩和策】公開範囲を制限する

ファイアウォールやルーターなどの機器を用いてDMZ（非武装地帯）を設定し、外部ネットワークからアクセス可能な機器を、公開用サーバーのように必要な機器だけに制限します。

【緩和策】パケットの流量を制限する

ファイアウォールやIPSなどの機器で、過大な流量のパケットを制限します。

【検知策】外部ネットワークからのアクセスを監視する

侵入検知システム（以下「IDS」という。）などの機器で、外部ネットワークから運転に必要ないアクセスがないか監視します。

【検知策】大量のパケットが送られていることを認識する

IDSなどの機器で、平常時または設計時に想定している流量を上回るパケットが流れていないか監視します。

【検知策】大量の認証試行が行われていることを認識する

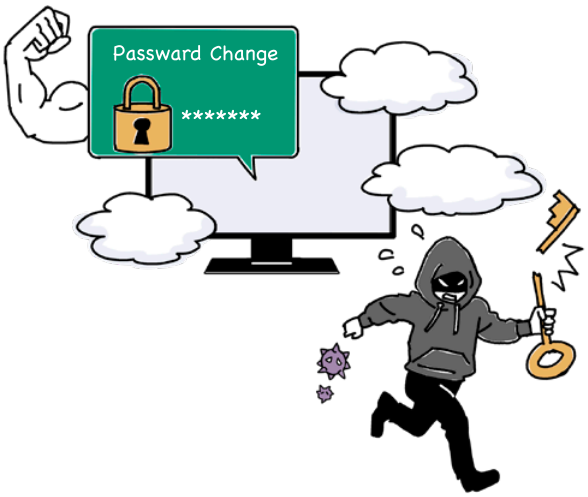
IDSなどの機器で、認証要求や認証応答のパケットが不自然に短い間隔で流れていないか監視します。

参考文献

・J-CLICS S1-5-1（サードパーティリスクの管理）
・J-CLICS S2-4-1（ファイアウォール）
・J-CLICS S2-5-1（システム監視）
・JIS Q 27001:2014 「A.9.1 アクセス制御に関する業務上の要求事項」
・JIS Q 27001:2014 「A.9.2 利用者アクセスの管理」
・JIS Q 27001:2014 「A.12.4 ログ取得および監視」
・JIS Q 27001:2014 「A.13.1 通信のセキュリティ」
・NIST SP800-82 Rev.2 「5.2 境界の保護」
・NIST SP800-82 Rev.2 「5.3 ファイアウォール」

設問 QN3 【強力な認証の実施】

ネットワークに接続された機器は容易に突破されない強力な認証によって保護されていますか？



背景・目的

攻撃者に制御システムへ侵入され、機器が不正に操作されたり、マルウェアなどによって重要なデータが窃取、改ざん、破壊されたりしないようにするために、制御システムの機器は容易に突破されない強力な認証手段で保護する必要があります。

想定される攻撃

PLC、DCSなどの制御装置およびSCADAのような端末機器に、不適切な制御指令やパラメーター類が意図的に投入されたり、開発環境上で制御プログラムが改ざんされたりして、制御システムが想定しない動作を起こすことがあります。
また、これらの機器から知的財産を含む秘匿性が高いデータを盗み出され、ビジネス上の損害を受けることも考えられます。

対策概要

制御システム内の機器は、強力な認証により正規のユーザー以外が操作できないようにします。一般的なIDとパスワードを用いる認証以外に、認証の三要素として知られる「記憶」「所持」「生体」を、複数組み合わせた多要素認証も有効な対策です。導入済システムにおいて強力な認証対応が難しい場合は、QN4記載の内部ネットワークの分離と保護による対策を実施することが重要となります。

設問 QN3 【強力な認証の実施】

ネットワークに接続された機器は容易に突破されない強力な認証によって保護されていますか？

内容解説・対策例

【防御策】デフォルトパスワード変更を強制する

工場出荷時のパスワードは公知となっている場合があるため、ツールやルールなどを利用して必ず変更します。

【防御策】パスワードポリシーをユーザーに強制的に守らせる

組織として求めるパスワードの長さや複雑さをポリシーとして定め、ユーザーに守らせます。

【防御策】セキュアなパスワードを使用する

IDと同一なもの、連続した文字列、他で使用しているパスワードなど安直なものを使用することは避け、容易に推測されないように長く複雑な文字列を使用します。

【緩和策】認証試行の濫用を制限する

認証試行の回数や間隔を制限し、多数回の試行による認証の突破や制御システムの負荷増大を防ぎます。対策にあたっては、認証失敗によって操作不能に陥ったり応答性が悪化したりしないように、制限内容の検討が必要です。

【緩和策】認証手段を増やす

機器に十分な長さや複雑さのパスワードを設定できないなどの場合、当該機器とネットワークの間にゲートウェイなどを追加し、そこで追加の認証を実施します。

【緩和策】パスワードの有効期間を制限する

パスワードに有効期間を設定したり定期的に変更させたりすることにより、パスワードの推測を困難にするほか、パスワードの漏えいにより影響が出る期間を限定します。

【緩和策】ID・パスワードの管理を強化する

退職・異動などで不要となったユーザーのIDを抹消したり、長期間パスワードの更新がないユーザーを常時または定期的にチェックし、更新を促したりします。また、管理者など重要なアカウントのパスワードは、それが必要な人員だけに知らせるようにします。

【検知策】脆弱または既知なパスワードが使用されているかどうかをチェックする
【検知策】デフォルトパスワードのまま使用されているアカウントを見つける

デフォルトパスワードや“111111”“qwerty”などの脆弱なパスワードを使用していないかを、ログの監査や実際の試行などでチェックします。

【検知策】アクセス状況をログに記録して定期的に監査する

IDS／IPSなどの機器や制御システムのログにより、パスワード等の漏えいや予期しない認証突破が疑われるアクセスを監視します。

【回復策】セキュアなパスワードに変更する

万が一認証が突破された場合、更なる侵入や攻撃を許さないように、セキュアなパスワードを再設定します。

設問 QN3 【強力な認証の実施】

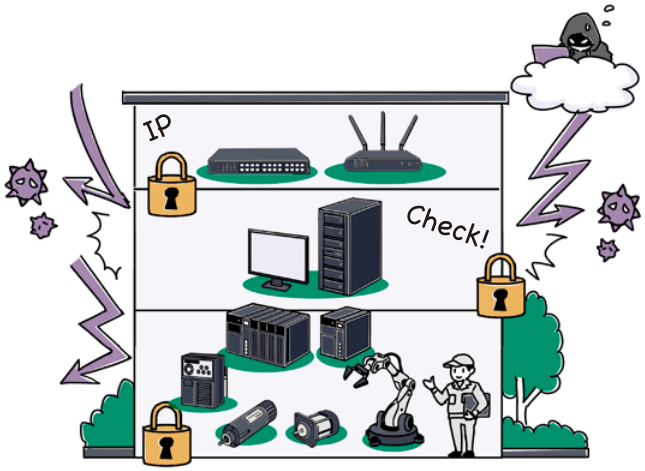
ネットワークに接続された機器は容易に突破されない強力な認証によって保護されていますか？

参考文献

- J-CLICS S1-3-1（パスワードポリシー）
- J-CLICS S1-3-2（強力なパスワードの使用）
- J-CLICS S1-3-3（パスワードの定期的な変更）
- J-CLICS S2-5-1（システム監視）
- J-CLICS S2-10-1（転入者と転出者用のプロセス）
- JIS Q 27001:2014 「A.9.2 利用者アクセスの管理」
- JIS Q 27001:2014 「A.9.3 利用者の責任」
- JIS Q 27001:2014 「A.9.4 システム及びアプリケーションのアクセス制御」
- JIS Q 27001:2014 「A.12.4 ログ取得及び監視」
- NIST SP800-63B: Digital Identity Guidelines
- 総務省 国民のための情報セキュリティサイト: 安全なパスワード管理
- NIST SP800-82 Rev.2 「5.15 認証と権限付与」
- NIST SP800-82 Rev.2 「6.2.7 識別及び認証」

設問 QN4 【内部ネットワークの分離と保護の実施】

制御システムの内部ネットワークは、通信の必要がある機器ごとに分離されていますか？



背景・目的

制御システムの内部ネットワークには重要な機器が接続されており、攻撃者に侵入されると大きな被害が出る恐れがあります。そのため、基本的には制御システムの内部ネットワークに外部の攻撃者が侵入できないようにすることが重要です。その上で、内部ネットワークの分離や機器の保護などの対策を実施し、攻撃者が万が一内部ネットワークに到達できたとしても被害の発生や拡大を防ぐことが重要となります。

想定される攻撃

攻撃者は制御ネットワークに接続された機器の脆弱性を悪用して侵入し、内部ネットワークを介して別の機器に攻撃を拡げることで、より大きな被害を発生させます。想定される攻撃は、制御システムの外部ネットワークに対する場合と同じように考えることができます。

対策概要

想定される攻撃が上述のとおりであるため、その対策も、外部ネットワークの場合と同様に考えることができます。さらに、ネットワークの階層化やセグメント化などによる境界防衛を意識しながら、ネットワーク機器の設定により通信制限をかけたり、通信ログなどを利用してネットワーク上の通信の状態や機器の稼働状態を監視したりします。

設問
QN4【内部ネットワークの分離と保護の実施】

制御システムの内部ネットワークは、通信の必要がある機器ごとに分離されていますか？

内容解説・対策例

【防御策】脆弱性のある機器へのアクセスを遮断する

制御システムの内部ネットワークに接続されている機器に不正なアクセスが到達しないようにします。

【防御策】IPによって内部ネットワークにアクセスできないようにする

制御システムの内部ネットワークに、不正なアクセスがIPレベルで到達できないようにします。

【防御策】外部に与える情報を最小化する

制御システムにある機器のシステムの特定に利用可能な通信内容やレスポンスなどを抑制して、機器に関する情報をなるべく外部に知らせないようにします。

【検知策】IPによる内部ネットワークへのアクセスを検知する

制御システムの内部ネットワークで、不正な通信が発生していないかを検知します。

【検知策】内部ネットワークへのアクセス経路を検知する

制御システムの内部ネットワークに、不正なアクセスが到達しないように、どのような経路で到達できるかを事前にチェックしておきます。

参考文献

・J-CLICS S2-4-1（ファイアウォール）
・J-CLICS S2-5-1（システム監視）
・J-CLICS S2-8-1（システムの強化）
・JIS Q 27001:2014 「A.9.1 アクセス制御に関する業務上の要求事項」
・JIS Q 27001:2014 「A.9.2 利用者アクセスの管理」
・JIS Q 27001:2014 「A.13.1 ネットワークセキュリティ管理」
・NIST SP800-82 Rev.2 「5.1 ネットワークの分割と分離」
・NIST SP800-82 Rev.2 「5.4 論理的に分離された制御ネットワーク」
・NIST SP800-82 Rev.2 「5.5 ネットワークの分離」

設問 QN5 【エンドポイントセキュリティ対策の実施】

ネットワークに接続された機器は、エンドポイント（ネットワークに接続された機器内）セキュリティ対策によって保護されていますか？

背景・目的

攻撃者は制御システムの内部ネットワークに侵入した後、ネットワークに接続されている機器への攻撃や侵入を試みると考えられます。たとえ攻撃者の侵入や攻撃を受けたとしても、それに対応して機器側で防御できることが重要となります。

想定される攻撃

制御システムの内部ネットワークに侵入した攻撃者は、機器やシステムが持つ脆弱性をついたり、攻撃を実行するプロセスを起動しようとしたりします。

対策概要

ネットワークを経由して利用できるサービスや通信ポートは、攻撃者の侵入経路となる恐れがあります。脆弱性を低減するために、制御システムで使用しないOS標準実装のサービスや通信ポートは停止または無効にします。また、機器上では最低限必要なプロセスだけを動作させるとともに、制御システムに必要のないプロセスが起動されないようにします。また、脆弱性の検査やリモートからの攻撃の検知など、システムに異常が発生していないかどうかのチェックを継続して行います。

設問 QN5 【エンドポイントセキュリティ対策の実施】

ネットワークに接続された機器は、エンドポイント（ネットワークに接続された機器内）セキュリティ対策によって保護されていますか？

内容解説・対策例

【防御策】機器の脆弱性を取り除く

ソフトウェア更新などにより機器が保有している脆弱性を取り除きます。更新にあたっては操業への影響を考慮し、計画的に対策に取り組む必要があります。

【防御策】脆弱性を利用したプロセスの起動を阻止する
【防御策】入口システムで任意のプロセスを起動できないようにする

攻撃者は、標的となるシステムの脆弱性を悪用して侵入を試みたり、悪意のあるプロセスを起動したりします。そのような攻撃を阻止するために、プログラムの脆弱性を取り除き、運転に関係ないプロセスが動作しないようにします。

【緩和策】起動されたプロセスがシステムに影響を与えないようにする

想定していない未知のプロセスが起動されたとしても、アクセス権の適切な設定などによりその動作を制限することでシステムに悪影響を与えないようにすることが考えられます。

【検知策】リモートからの攻撃で注意すべきアクセスを認識する

制御システムの脆弱性に対処するために、利用しているソフトウェアがどのような脆弱性をもっているかを正確に把握する必要があります。その一つの方法として世の中に公開されている情報を利用することが考えらます。

【検知策】使用している機器の脆弱性情報を収集する

攻撃者は、侵入の足掛かりとなるような脆弱性を使用しようと試みます。そのことを防ぐためには、システム・機器ベンダーの脆弱性情報などを定期的に確認し、自システムの脆弱性を把握する必要があります。

【検知策】実際のリモートからの攻撃を検知する

ネットワーク内に流れる通信を監視し、リモートからの攻撃を検知します。

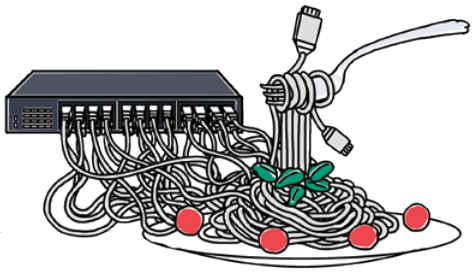
【検知策】意図しないプロセスが起動されていないかをチェックする

制御システム内での攻撃活動を検知する手段の一つとして、例えばウイルス対策ソフトやプロセス起動ログを用いて、構成機器で意図しないプロセスが起動されていないかを常にチェックします。

参考文献

・J-CLICS S2-1-1（システムとビジネスリスクの理解）
・J-CLICS S2-2-1（脅威の理解）
・J-CLICS S2-6-1（ウイルス対策）
・J-CLICS S2-7-1（セキュリティパッチ）
・J-CLICS S2-8-1（システムの強化）
・JIS Q 27001:2014 「A.9.4 システム及びアプリケーションのアクセス制御」
・JIS Q 27001:2014 「A.12.2 マルウェアからの保護」
・JIS Q 27001:2014 「A.12.4 ログ取得及び管理」
・JIS Q 27001:2014 「A.12.5 運用ソフトウェアの管理」
・JIS Q 27001:2014 「A.12.6 技術的ぜい弱性の管理」
・NIST SP800-82 Rev.2 「付録C 脅威源、脆弱性及びインシデント」
・NIST SP800-82 Rev.2 「付録E ICSセキュリティ機能及びツール」

column



コラム-1

ケーブルスパゲッティ

システム導入時はネットワークケーブルや電源の配線をきれいに敷設・結束し、タグもきちんと貼って、どの機器とつながっているケーブルなのかわかるようにしています。しかし時間が経つと、不要となったのに放置されたケーブルや、タグが付いていない見知らぬケーブルが、ハブに挿されている、ということがあると思います。

インターネットで「ネットワークケーブル　スパゲッティ」と検索するとスパゲッティのようにグッチャグチャに絡まるケーブルの写真がたくさん出てきます。こうした写真のようになると、どれが何のケーブルなのかを調べる気にもなりませんね。セキュリティ対策の第一歩が情報資産の把握であるということはご存知と思いますが、制御システムで使われるネットワークケーブルも、他の情報資産と同じように把握、管理しなければなりません。ネットワークケーブルをきちんと管理していないと、新たな侵入経路の把握もできませんし、いざという時、切断すべきネットワークがわからないかもしれません。

不要となったケーブルは撤去し、流用したケーブルのタグは必ずきちんと付け替えるようにしましょう。ケーブルの管理は、ネットワーク経路を把握する重要な第一歩です。

コラム-2

指紋認証とアルコール消毒

COVID-19は、私たちの日常生活にさまざまな影響を与えており、セキュリティの世界も例外ではありません。例えば、ある区画に入る人を制限する場合、入口で何らかの認証を行います。認証にはいろいろなものを利用しますが、指紋を使った認証装置を使っているケースは、比較的よく見ると思います。この指紋による認証、アルコール消毒をした後で装置に指を入れるとうまく認証されない、というケースに出会ったことはありませんか。私は指紋を使った認証をしている場所で、認証されないことを度々経験しました。

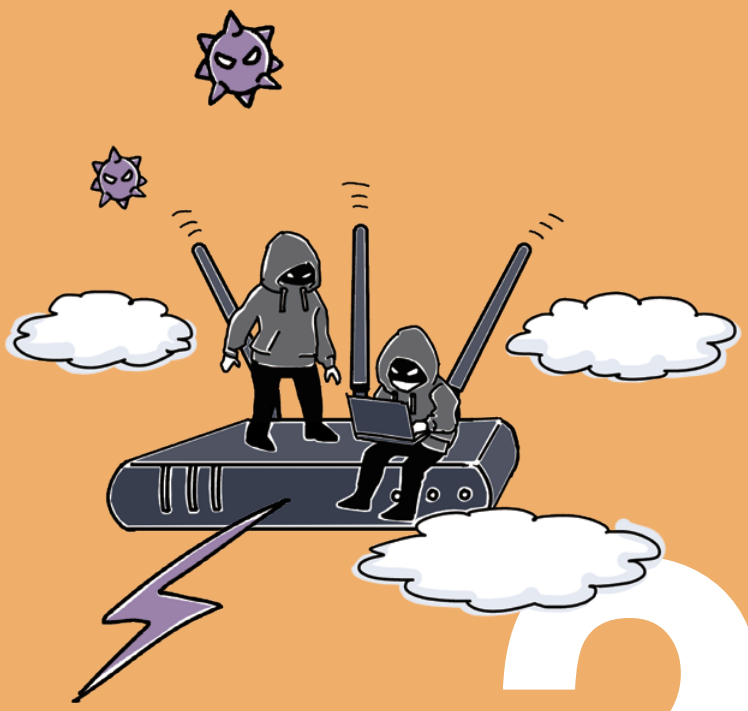
指紋認証装置では、指紋を認識するセンサーの方式として、光学方式、静電容量方式、電解強度測定方式などいくつかの方法があります。どの方式においても、アルコールだけではなく、水などで濡れた指を認証装置に入れると正しく認識しない場合があるそうです。特に、静電容量方式は濡れた指には弱いと言われています。指紋を認識する方式自体、濡れたものには向かないので、認証されないことが起こるのは仕方がないことだと思います。もちろん、間違って認証がOKになるわけではないので、認証装置としては正しく機能しています。

こういう場面ではどう対処するのがよいでしょうか？一番確実な方法は、「指が乾くことを待つ」です。

アルコールですから、時間が経過するとしだいに蒸発していきますので、あわてず騒がず待ちます。そうすると、たいていの場合は認証OKとなって、制限されたエリアに入れます。COVID-19の影響でいろいろと落ち着かない世の中ですが、このように慌てないでじっくりと構えることは、さまざまな場面で有効です。これは、システムのセキュリティ対策を考える場合も同様で、慌てて対処するのではなく、じっくりとシステム全体のことを考えて、有効なセキュリティ対策を考えることが肝要です（もちろん緊急で対応しなくてはいけない場合もありますが）。

なお、アルコール消毒を何回も行うことで、指紋が変化してしまって認証されなくなる場合もあるようです。このような場合には、認証用のデータの登録をやり直す必要があります。

無線LAN経路



2

攻撃経路の特徴

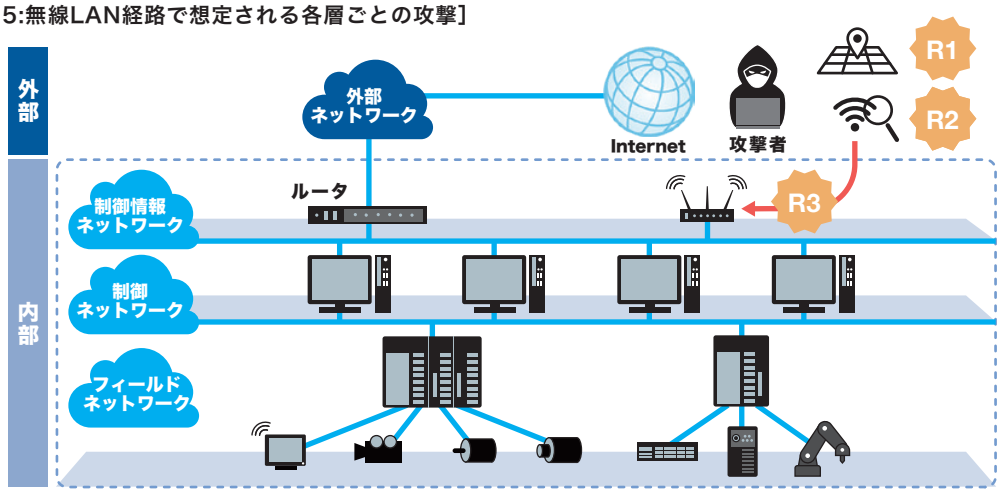
無線LAN経路には、攻撃対象（侵入口）が空間上に多数、または広範囲に存在するため攻撃されやすい性質があります。

QR index 無線LAN経路

攻撃への対策の考え方

無線LAN経路での攻撃活動においては、攻撃の足掛かりとなる無線LAN情報を入手するプロセスを経て、実際の攻撃が仕掛けられます。
図5のとおり、無線LAN経路の各層ごとの攻撃として次のものが想定されます。

［図5:無線LAN経路で想定される各層ごとの攻撃］



R1【無線LAN使用箇所の特定】→QR1を参照

攻撃者は、制御システムの施設に近づくことなしに、攻撃対象となる無線LANがどこに設置されているかを調査します。情報源としては、特定のオンラインサービス、公開情報、関係者からの漏えい、などが想定されます。無線LANが設置されていることが判れば、R2の攻撃ステップである無線LAN使用状況の調査がより効率良く進められます。

R2【無線LAN使用状況の調査】→QR2を参照

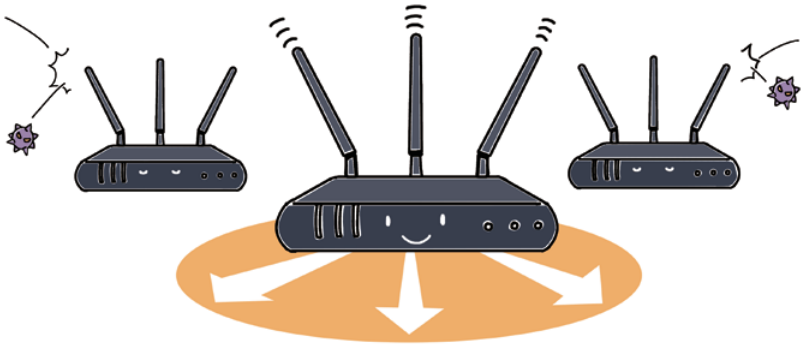
攻撃者は、無線LANの設定など使用状況を調査します。使用している周波数や暗号化などの設定情報を収集し、より具体的な攻撃対象・攻撃内容を特定すると考えられます。

R3【攻撃実施】→QR3、QR4を参照

無線LANの使用状況が把握できたら、攻撃者は、通信の妨害、侵入、なりすまし、など実際の攻撃の選択肢を獲得します。

設問QR0【無線LAN使用の最小化】

無線LANの使用は必要最小限になっていますか？



背景・目的

無線LAN経路には攻撃されやすい性質があるため、原則として、無線LAN自体の使用を必要最小限に留めることが肝要です。その上で、無線LANに関係する情報の流出に備える対策を第一に施すべきと考え、実際の攻撃に備える対策を第二とします。

想定される攻撃

無線LANを使用することで、制御システムの敷地外からであっても無線LANの電波が届けば攻撃を仕掛けることができるため、制御システムが攻撃の標的となる危険性が高まることが想定されます。

対策概要

無線LANの使用を無線LANでしかできない用途、または経済的効果が大きな用途に限定して直接アクセスできる機器を絞り、その上で無線LANの電波が到達する範囲を必要最小限にすることで攻撃を仕掛けるための足場を狭め、親機／子機ともに必要な時以外は無線LANを無効化することで、攻撃可能な機会を減らします。

設問 QR0 【無線LAN使用の最小化】

無線LANの使用は必要最小限になっていますか？

内容解説・対策例

【防御策】無線LANを使用しない
【緩和策】無線機器の利用を最小限にする

攻撃経路をできるだけ減らすため、単に便利という理由で使用している無線LANは、有線LANで代替する、使用するエリアを限定する、盗聴されても問題ない通信だけに限定する、など使用する機器／機会を必要最小限まで減らします。

【防御策】敷地外まで電波が届かないようにする

制御システムが設置されている管理区域の外から通信内容が盗聴されることを防ぐため、通信品質を確保した上で、管理区域外へ電波が届かないように対策します。

【検知策】不正アクセスポイントを監視する
【検知策】敷地境界を監視する

敷地境界には攻撃の足場が仕掛けられやすく、また、管理区域内においても管理の目をかいくぐって不正なアクセスポイントが設置されることがあります。それらを発見するため、定期的に電波を観測するなどして、想定していない機器がないように監視します。

【検知策】システム構成をチェックする
【回復策】不要な無線機器を取り除く

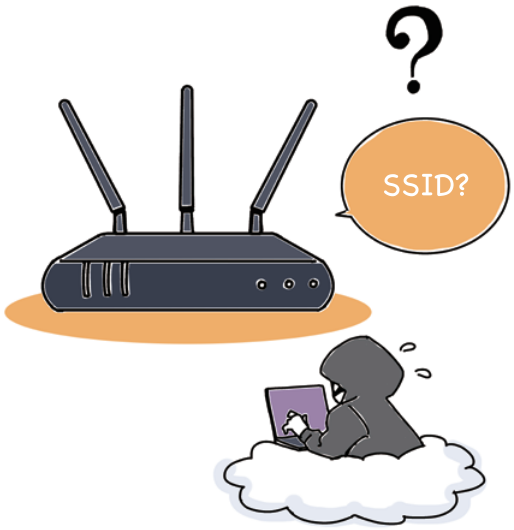
正規に使用している無線機器をきちんと把握し、正規でない通信を発見できるようにするため、無線LANを使用する機器の増設や廃止など、定期的な機器構成の棚卸を行います。また、棚卸で不要となった無線機器は、現物を探し出して停止させます。

参考文献

・JIS Q 27001:2014 「A13.1.1 ネットワーク管理策」
・NIST SP800-82 Rev.2 「6.2.1 アクセス制御」

設問 QR 1 【無線LAN構成情報の秘匿】

無線LANの構成情報は秘密情報として管理されていますか？



背景・目的

外部の悪意ある攻撃者にとって、無線LANは攻撃活動が見つかりにくいため、好都合な攻撃手段です。無線LANの構成情報が知られてしまうと、その後の攻撃への足掛かりを与えてしまうことになるため、秘密情報として取り扱う必要があります。

想定される攻撃

攻撃者が、無線LAN構成情報であるSSIDなどを、公開情報や関係者から入手することが想定されます。
無線LAN構成情報を攻撃者に知られると、攻撃の狙いが定まり、無線LAN使用状況の詳細調査や、実際の攻撃など、次のステップの攻撃に悪用される恐れがあります。

対策概要

システム内での無線LANの使用箇所を特定できないと無線を利用した攻撃ができないため、物理的に侵入しない限り攻撃を成立させることができません。無線LANの構成情報を秘密情報として管理することで、無線を使った攻撃環境を構築する難易度が上がります。

設問 QR 1 【無線LAN構成情報の秘匿】

無線LANの構成情報は秘密情報として管理されていますか？

内容解説・対策例

【防御策】SSIDを非公開にする

SSIDを公開する設定のままだと、SSIDマップサービスでチェックされて不正ログインを許すきっかけになります。SSIDマップサービスの提供者に対して公開しないことを要求する機能（オプトアウト機能）を利用する、ブロードキャスト設定を無効にする（ステルス化）、などの対策が有効です。

【防御策】構成情報を秘密管理し関係者の教育を行う

システム構成に関する情報が含まれる資料を秘密情報に指定し、その情報へのアクセスを制限、管理します。
さらに、関係者へ秘密情報の管理についての教育を行い、情報漏えいを防止します。

【緩和策】秘密情報拡散の抑制のための手順を実施する

関係者との契約や、従事者の行動に関する規則によって、情報漏えいを抑止します。この対策は、内部犯行に対しても有効です。
また、アカウントを定期的に見直し、退職者などの不要となったアカウントを削除するなどして、情報漏えいを防止します。

【検知策】定期的に外部サービスへの漏えいを調査する

公開資料から秘密情報が拡散してしまう場合を想定し、自組織の内部情報が意図せず外部に知られていないかを監視するともに、原因となった資料の差し替えや公開停止を速やかに実施できる体制を構築します。
あわせて、無線LAN特有の対策として、Google Maps Geolocation APIなどのSSIDマップサービスに登録されていないか、定期的に調査する必要があります。

【回復策】漏えいした情報と異なる構成に変更する

制御システムエリア内の機器で使用しているIPアドレスを変更する、SSIDやパスワードを変更する、などの対策が必要です。

参考文献

・JIS Q 27001:2014 「A.8.1 資産に関する責任」
・JIS Q 27001:2014 「A.9.3 利用者の責任」

設問QR2【電波状況の把握と管理】

無線LANの電波状況を把握して電波到達範囲が必要最小限となるように管理されていますか？

背景・目的

無線通信は目に見えないため、外部から電波観測や盗聴をされているかを常に把握することは非常に困難です。定期的な調査方法を確立して実施し、電波観測や盗聴が行われないように管理する必要があります。

想定される攻撃

ウォードライビング（Wardriving:自動車などで移動しながら、無線LANアクセスポイントを探し回る行為）などの電波観測により、無線LANの周波数や暗号化情報が収集されることが想定されます。
もし、これらの情報が攻撃者の手に渡ると、次のステップの攻撃が仕掛けられるようになります。

対策概要

無線LANの使用機会を減らすだけで攻撃できるタイミングが減少します。また、制御システムエリアの外側と内側で電波がつながらない環境では、物理的に侵入しないと攻撃を成立させることはできないため、攻撃環境構築の難易度が上がります。

設問 QR2 【電波状況の把握と管理】

無線LANの電波状況を把握して電波到達範囲が必要最小限となるように管理されていますか？

内容解説・対策例

【防御策】敷地外まで電波が届かないようにする

敷地の外で、制御システムエリア内で使用する無線通信を盗聴されないように、使用している無線LAN機器の電波出力を下げる設定をする、指向性アンテナを利用する、制御システムが屋内にある場合には無線が必要なエリアをシールドで覆って電波漏えいを防止する、などの対策が有効です。

【防御策】通信をセキュアな設定にする

無線通信は、無線が届く範囲を完全には制御できないため、常に盗聴・漏えいのリスクがあります。
そのため、通信を暗号化する、ブロードキャスト設定を無効にする（ステルス化）、などの対策が有効です。

【防御策】敷地内にフリーWi-Fiがないようにする

電池駆動で手のひらサイズのモバイルルーターは、衣類等に忍ばせることができるため、敷地外に電波が届くのと同じリスクがあります。
個人所有物を持ち込ませない運用を徹底するす必要があります。

【緩和策】通信する時だけ無線機能を有効化する

無線LANを使用する機器は使用時のみ電源ONにするなど、使用可能な機会を減らすだけで攻撃できるタイミングが減少します。

【検知策】施設周辺を監視する

無線通信は敷地外からの攻撃に晒されています。攻撃の異変を検知するためには、通信の状況を監視するだけではなく、定期的な施設周辺の見回り、監視カメラの設置、などの対策が有効です。

【回復策】漏えいした情報と異なる構成に変更する

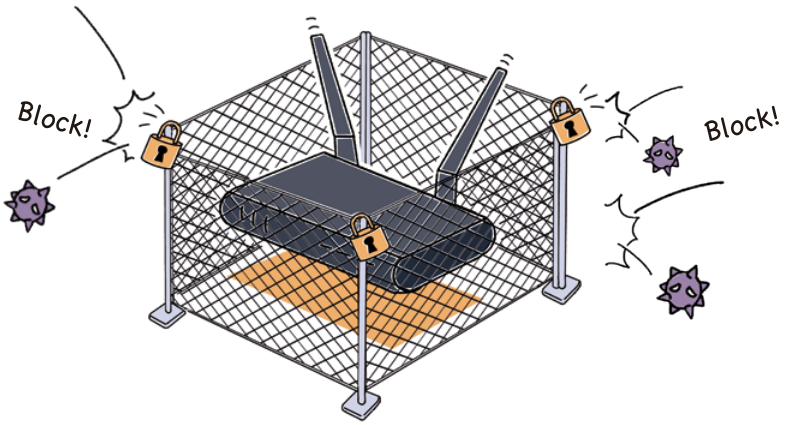
制御システムエリア内で、使用するIPアドレスを変更する、SSIDを変更する、などの対策が必要です。

参考文献

・JIS Q 27001:2014 「A.11.1.1 セキュリティを保つべき境界」
・JIS Q 27001:2014 「A13.1.1 ネットワーク管理策」
・U.S. Army: “FM 3-19.30 Physical Security”, Chapter 4, PROTECTIVE BARRIERS

設問QR3【無線LAN機器のセキュリティ確保】

セキュリティが考慮された無線LAN機器を選定し、不正アクセスを難しくする適切な設定・運用がされていますか？



背景・目的

外部からの攻撃の大部分は、使用する機器の脆弱性を利用したものです。無線LAN機器をセキュアな設定で使用することで、脅威を減らすことができます。

想定される攻撃

Wi-Fiルーター製品の脆弱性を突いたり、アクセスする機器が限定されない設定や破り易い設定などの不適切な設定を突いたりして、無線LANへ侵入されることが想定されます。
もし、侵入されると、Wi-Fiルーターの電波が届く範囲の無線LAN機器や、Wi-Fiルーターに有線接続される機器に次のステップの攻撃が仕掛けられるようになります。

対策概要

ソフトウェア更新などにより無線LAN機器が保有している脆弱性を取り除きます。無線LAN特有の対策として、境界で電波を遮断する（外から届かない）、通信を秘匿する（届いても受け取らない）、などの対策を行うことで、無線LANの安全性を確保します。

設問 QR3【無線LAN機器のセキュリティ確保】

セキュリティが考慮された無線LAN機器を選定し、不正アクセスを難しくする適切な設定・運用がされていますか？

内容解説・対策例

【防御策】敷地外から電波が届かないようにする

敷地外からの妨害電波や不正な無線機器の電波を受信しないように、屋内の制御システムの場合にはシールドで覆って外部からの電波が届かないようにする対策が有効です。

【防御策】脆弱性を解消する

ソフトウェア更新などにより無線LAN機器が保有している脆弱性を取り除きます。更新にあたっては操業への影響を考慮し、計画的に対策に取り組む必要があります。

【防御策】通信をセキュアな設定にする

送り主や形式、内容が不正なパケットの受信を防ぐため、アクセスポイント（Wi-Fiルーター）に通信のフィルタリングを設定して許可されていない機器が接続されないようにする、正規の機器が許可されていないアクセスポイントへ自動的に接続しないようにする、などの対策が有効です。
また、不正な無線機器からの認証の試行に対しては、認証失敗時にインターバルを設ける、認証回数の制限を設ける、などの対策が有効です。

【緩和策】通信路を二重化する

脆弱性の解消までに時間を要する場合、無線LANで使用していた周波数帯とは異なる周波数帯を利用する、無線ではなく有線を利用して通信する、などの対策で脅威を緩和することができます。

【緩和策】脆弱性のある機器へのアクセスを遮断する

脆弱性の解消までに時間を要する場合、常用しているポートと異なるポートを代替利用し、脆弱性のあるポートへのアクセスを遮断することで、脅威を緩和することができます。

【検知策】定期的にシステムや電波状態を調査する

無線LAN機器に不正なアクセスポイントの電波や妨害電波が届いていないか、定期的に調査する必要があります。また、異常を検知できるようにログを有効化する、IDSを導入して不正アクセスを検知する、などの対策も有効です。

【検知策】使用している機器の脆弱性情報を収集する

攻撃者は、侵入の足掛かりとなるような脆弱性を使用しようと試みます。そのことを防ぐためには、自システムの脆弱性を定期的に把握する必要があります。

【緩和策】通信内容をセキュアにする

脆弱性の解消までに時間を要する場合、アプリケーションレイヤーでデータを暗号化するなどの対策により通信内容をセキュアにすることで、脅威を緩和することができます。

【回復策】不審な発信源を特定し、撤去する。必要に応じて警察へ通報する

不審な電波受信を検知した際は、発信源を特定し早急に撤去します。さらに、必要に応じて電波法違反として警察へ通報します。

設問 QR3 【無線LAN機器のセキュリティ確保】

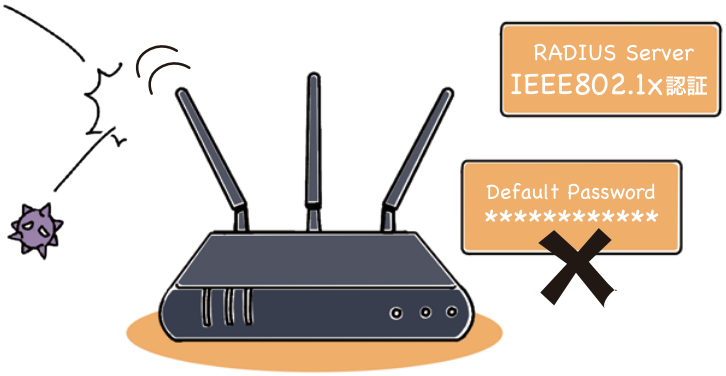
セキュリティが考慮された無線LAN機器を選定し、不正アクセスを難しくする適切な設定・運用がされていますか？

参考文献

・JIS Q 27001:2014 「A.10.1 暗号による管理策」
・JIS Q 27001:2014 「A.11.1 セキュリティを保つべき領域」
・JIS Q 27001:2014 「A.12.6 技術的ぜい弱性管理」
・JIS Q 27001:2014 「A.13.1.1 ネットワークセキュリティ管理」
・NIST SP800-82 Rev.2 「6.2.16 システム及び通信保護」

設問 QR4 【認証管理の実施】

無線LANに接続された機器は容易に突破されない強力な認証機能によって保護されていますか？



背景・目的

無線LAN機器の認証として、工場出荷時のデフォルトパスワードが使われていたために攻撃される事例が多発しています。既知、または、推測容易なパスワードでアクセスされてしまうことを無くすことで脅威を減らすことができます。

想定される攻撃

攻撃者が、無線LAN機器へアクセスし、知り得るデフォルトパスワードを使ってユーザーアカウントや管理者アカウントに認証を試行することが想定されます。
もし、デフォルトパスワードのまま機器を使用していると、攻撃者が認証をクリアし、機器の制御が乗っ取られるようになります。

対策概要

使用する無線LAN機器のアクセス状況や認証情報を定期的に監査し、必要に応じて認証手段を強化することで、攻撃の難易度を高めることができます。

設問 QR4 【認証管理の実施】

無線LANに接続された機器は容易に突破されない強力な認証機能によって保護されていますか？

内容解説・対策例

【防御策】アクセスを制限し承認されていない機器の接続を防ぐ

アクセスポイントなどの入口システムで、MACアドレスでフィルタリングを行うなどの対策が有効です。

【防御策】認証手段を強化する

ブルートフォース攻撃（総当たり攻撃）が困難な強力なパスワードを使用するだけで攻撃への耐性が上がります。また、無線LANに接続する機器の信頼性を確保するためには、RADIUSサーバー（ネットワーク上で利用者の認証や権限の付与、利用状況の記録などを行うためのプロトコルにもとづいて機能を提供するサーバー）を用いたIEEE802.1X認証を取り入れることが有効です。

【防御策】無線LANセキュリティ装置を導入する
【検知策】無線LANセキュリティ装置を導入する

無線LANに侵入検知システム（以下「IDS」という。）／侵入防止システム（以下「IPS」という。）を設置することで、DoS攻撃などの通信を検知し、遮断することが可能です。

【緩和策】認証手段を増やす

機器に十分な長さや複雑さのパスワードを設定できないなどの場合、当該機器とネットワークの間にゲートウェイなどを追加し、そこで追加の認証を実施します。

【検知策】定期的にアカウントの棚卸を行う

退職者や異動者のアカウントが不正ログインに使用される可能性があります。定期的にアカウントの棚卸を行い、常に必要最小限のアカウントとする必要があります。また、ログ分析を実施することにより、削除済みアカウントでのログイン試行がないかを検知できます。

【検知策】アクセス状況のログ分析を行う

ログイン失敗時のイベントログを取得することで、不正ログインの試行を検知することができます。

【防御策】セキュアなパスワードを設定する
【回復策】セキュアなパスワードを設定する

パスワードは、アカウント名と同一なもの、連続した文字列、他で使用しているパスワードなど安直なものを避け、容易に推測されないよう長く複雑な文字列を使わせるようにします。漏えいした恐れのあるパスワードは変更する必要があります。各メーカーで使用されているデフォルトパスワードは広く知れ渡っていると考えられるため、変更する必要があります。

参考文献

・JIS Q 27001:2014 「A.9.1 アクセス制御に関する業務上の要求事項」
・JIS Q 27001:2014 「A.9.2 利用者アクセスの管理」
・JIS Q 27001:2014 「A.12.4 ログ取得及び管理」
・IEEE 802.1X-2020 - IEEE Standard for Local and Metropolitan Area Networks--Port-Based Network Access Control
・NIST SP800-82 Rev.2 「5.16 監視、ロギング及び監査」
・NIST SP800-82 Rev.2 「6.2.7 識別及び認証」

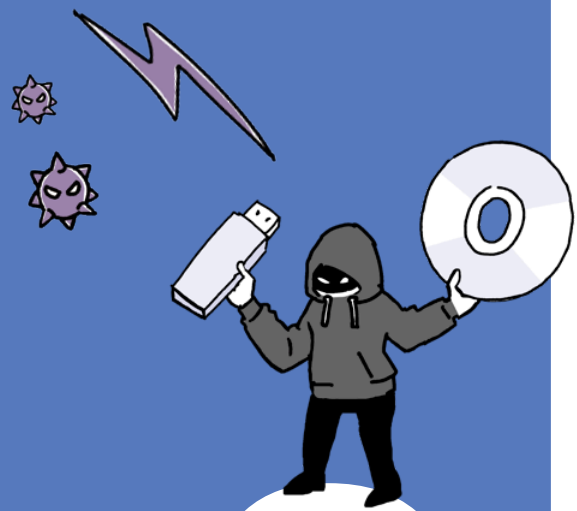
column

コラム-1

壁に耳あり
障子に目あり

無線LAN経路で攻撃を仕掛ける場合、攻撃用の機器やデバイスを見えないように忍ばせます。時代劇風に言うと、自分の屋敷の中であっても、死角から会話が盗み聞きされ、また、命を狙われています。屋敷の中でも糸電話で話しましょう！

持ち込みデバイス経路



3

攻撃経路の特徴

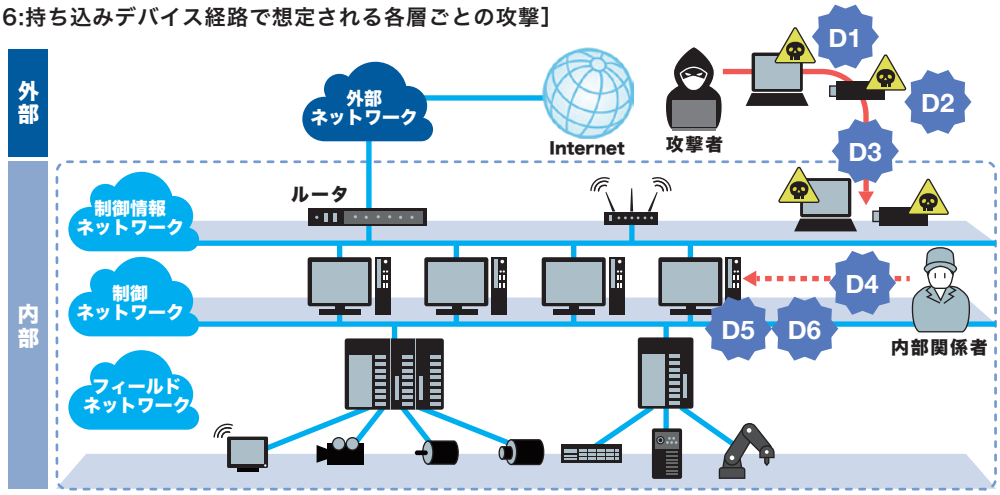
持ち込みデバイスは、USBメモリやCD、DVDなどの記録メディア、ノートPCのような情報機器などがあります。
それらを外部から持ち込む場合には、持ち込みデバイスを介してウイルス感染の経路となる恐れがあります。そのため、持ち込みデバイスを制御システムに接続する場合は、ウイルス検査を行うことが肝要です。同時に使用する持ち込みデバイスを制限するなどの管理を行います。

QD index 持ち込みデバイス経路

攻撃への対策の考え方

制御システムにウイルス感染した持ち込みデバイスを接続することで、制御システム内にウイルスを拡散してしまいます。制御システム外からの持ち込みパソコンや外部記憶媒体等を不用意に制御システムに接続しないように注意しなければなりません。
図6のとおり、持ち込みデバイスの各層ごとの攻撃として次のものが想定されます。

[図6:持ち込みデバイス経路で想定される各層ごとの攻撃]



D1 D2【持ち込みデバイスをウイルス感染させる】→QD1を参照
攻撃者は、制御システムをウイルス感染させるために、まず持ち込みデバイスをウイルス感染させようとすることが想定されます。持ち込みデバイスのウイルス感染対策として、セキュリティパッチの適用や接続機器の限定による感染リスク低減、ウイルスチェックによる感染の早期検知などを実施します。

D3【感染デバイスを持ち込ませる】→QD2、QD3を参照
攻撃者は、ウイルス感染した持ち込みデバイスを、制御システムの外部から内部に持ち込もうとすることが想定されます。対策として、持ち込みデバイスを限定する、事前に制御システム内で管理しているデバイスで作業させる、などを実施します。

D4【感染デバイスを標的まで運搬させる(中間でのセキュリティ対策の突破)】→QD2、QD3を参照
攻撃者は、ウイルス感染した持ち込みデバイスを、制御システムのより内部へと持ち込もうとすることが想定されます。対策として、中間経路上で、デバイスの持ち込みチェックやウイルスチェックなどを実施します。

D5【感染デバイスを制御システムへ到達させる】→QD2、QD3を参照
攻撃者は、ウイルス感染した持ち込みデバイスを、攻撃対象機器がある場所まで持ち込ませることが想定されます。対策として、機器接続前に、持ち込みデバイス内のデータチェックやウイルスチェックを実施します。

D6【感染デバイスを標的に接続させる(デバイスでのセキュリティ対策の突破)】→QD4を参照
攻撃者は、ウイルス感染した持ち込みデバイスを、制御システム内の機器に接続させることで、その機器をウイルス感染させようとすることが想定されます。感染を防ぐ対策として、制御システム内の機器（エンドポイント）の脆弱性除去、ホワイトリストによるマルウェア起動防止、などを実施します。

設問QD0【持ち込みデバイス使用の最小化】

持ち込みデバイスの使用は必要最小限になっていますか？

背景・目的

持ち込みデバイスを制御システムにて使用する場合は、使用する持ち込みデバイスを介してウイルスを持ち込む恐れがあります。また、スマートフォンなどの持ち込みに関しても注意が必要です。使用するデバイスを最小限にすることでセキュリティリスクを抑えることができます。

想定される攻撃

制御システムへのウイルス感染手段として、外部から持ち込むデバイスをウイルス感染させておき、そのデバイスを制御システムに接続させ、ウイルスを制御システムに感染させる攻撃が想定されます。

対策概要

持ち込みデバイスを使用する場合には、使用するデバイスの種類や数、使用する人員や使用目的、使用するタイミングの最小化を行うことでセキュリティリスクを低減できます。

設問 QD0 【持ち込みデバイス使用の最小化】

持ち込みデバイスの使用は必要最小限になっていますか？

内容解説・対策例

【防御策】持ち込みデバイスを使用させない

制御システム内で管理した制御システム内専用デバイスのみを使用する、もしくはデバイスの持ち込みを制限することでセキュリティリスクを低減できます。

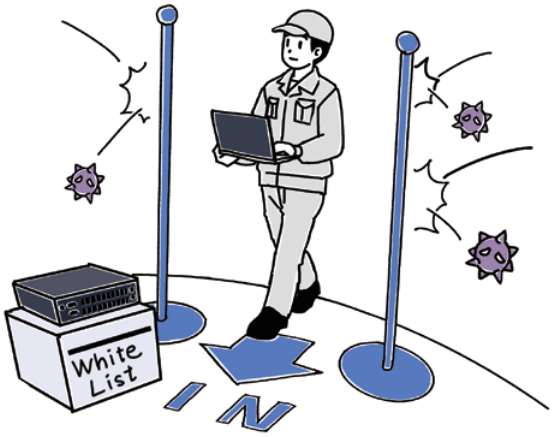
定期的にデバイスの利用状況を確認することも有効です。

参考文献

・J-CLICS S1-2-1（機器接続手順）
・JIS Q 27001:2014 「A.8.1 資産に対する責任」
・JIS Q 27001:2014 「A.8.3 媒体の取扱い」

設問 QD1 【ウイルス対策の実施】

持ち込みデバイスはウイルス感染を防止するための対策がされていますか？



背景・目的

制御システムはネットワークを介してさまざまな機器が設置されています。制御システムのセキュリティリスクを管理するためには、ウイルスを制御システム内に持ち込まないことが重要です。制御システムの外部からデバイスを持ち込む場合には、事前にウイルスチェックすることでセキュリティリスクを抑えることができます。

想定される攻撃

制御システムへのウイルス感染手段として、感染したデバイスを持ち込む（持ち込ませる）ことが想定されます。このリスクを低減するためには、まず持ち込みデバイスがウイルス感染しないように対策を実施することが必要です。

対策概要

持ち込みデバイスにセキュリティパッチを適用して脆弱性を取り除くとともに、使用前やデータ書き込み後等にウイルスチェックを実施します。持ち込みデバイスで取り扱うデータはあらかじめウイルスチェックをします。持ち込みデバイスがノートPC等の場合、接続する機器を制限することにより、ウイルス感染リスクを低減できます。

設問 QD 1 【ウイルス対策の実施】

持ち込みデバイスはウイルス感染を防止するための対策がされていますか？

内容解説・対策例

【防御策】接続可能なデバイスを制限する機能を実装する

持ち込みデバイスがノートPC等の場合、接続するUSB機器などを制限するホワイトリスト機能を適用します。
管理外のUSB機器などの接続によるウイルス感染リスクを低減することができます。

【緩和策】持ち込みデバイスで取り扱うデータのウイルスチェックを行う

持ち込みデバイスで取り扱うデータは、あらかじめウイルスチェックをしてから持ち込みデバイスに保存するようにします。

【緩和策】持ち込みデバイスの脆弱性を取り除く

持ち込みデバイスにセキュリティパッチを適用し、脆弱性を取り除きます。

【検知策】持ち込みデバイスのウイルスチェックを行う

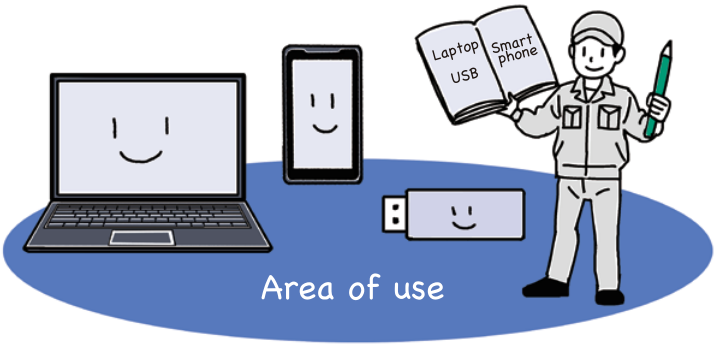
持ち込みデバイスは、その使用前やデータ書き込み後にウイルスチェックを行います。

参考文献

・J-CLICS S1-2-1（機器接続手順）
・J-CLICS S2-6-1（ウイルス対策）
・JIS Q 27001:2014 「A.8.3 媒体の取扱い」
・JIS Q 27001:2014 「A.12.2 マルウェアからの保護」
・NIST SP800-82 Rev.2 「付録C 脅威源、脆弱性及びインシデント」
・NIST SP800-82 Rev.2 「付録E ICSセキュリティ機能及びツール」

設問 QD2 【持ち込みデバイスの限定】

持ち込みデバイスは用途や使用エリアが制限され、管理された状態になっていますか？



背景・目的

システム内のデータの利用や更新等で持ち込みデバイスを制御システムに接続する場合、持ち込みデバイスを介し、ウイルスが制御システム内に持ち込まれる可能性があります。制御システムの外から持ち込むデバイスを限定し台帳管理を行うこと、接続先機器を最小限に制限することでセキュリティリスクを抑えることができます。

想定される攻撃

制御システム内で使用する持ち込みデバイスを管理していないと、意図的または偶発的にウイルス感染したデバイスが制御システム内に持ち込まれてしまう恐れが高まります。

対策概要

持ち込みデバイスを使用する場合には、持ち込みデバイスを利用する用途や使用するエリアを制限して、台帳管理を行うことが推奨されます。またメンテナンス等でベンダーが持ち込むデバイスについても、システム管理者が作業内容を把握し、作業者へ管理手順を徹底させることで感染リスクを低減することができます。

設問 QD2 【持ち込みデバイスの限定】

持ち込みデバイスは用途や使用エリアが制限され、管理された状態になっていますか？

内容解説・対策例

【防御策】持ち込みデバイスを制限・管理する

持ち込みデバイスは必要最低限の利用にとどめ、特定目的およびエリアでの使用に制限・管理します。

【防御策】管理外のデバイスの接続を防止する

管理された持ち込みデバイスしか接続できない仕組みを導入します。あらかじめUSBメモリのデバイスIDをローカルグループポリシーに登録することで登録外のデバイスのインストールを拒否することができます。また物理的にUSBポート、イーサネットポートをふさぐことも有効な対策になります。

【防御策】備え付けのデバイスを使用させる

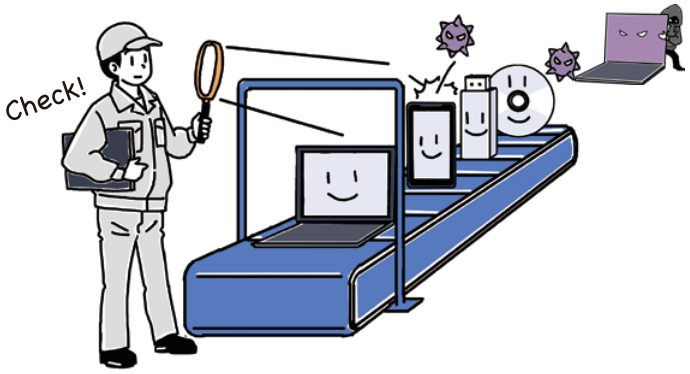
外部ベンダーによる作業は、制御システム内で管理しているデバイスを使用し作業させるようにします。

参考文献

・JIS Q 27001:2014 「A.8.1 資産に対する責任」
・JIS Q 27001:2014 「A.8.3 媒体の取扱い」
・JIS Q 27001:2014 「A.11.1 物理的及び環境的セキュリティ」
・NIST SP800-82 Rev.2 「6.2.10 メデイア保護」

設問QD3【持ち込みデバイス内のデータの制限・検査】

持ち込みデバイス内のデータは使用用途が制限され、検査・管理された状態になっていますか？



背景・目的

制御システムはネットワークを介してさまざまな機器が設置されています。制御システム施設のセキュリティリスクを管理するには、ウイルスを制御システム内に持ち込まないことが重要です。制御システムに持ち込みデバイスを使用する場合は、利用目的に応じたファイルだけを格納し、接続前のチェックを確実に実施することでセキュリティリスクを抑えることができます。

想定される攻撃

制御システムへのウイルス感染手段として、感染したデバイスを持ち込む（持ち込ませる）ことが想定されます。外部から持ち込むデバイスを介して、制御システムをウイルス感染させる攻撃が想定されます。

対策概要

持ち込みデバイスを制御システムへ接続する前にウイルスチェックにより正常性の確認を行うことが推奨されます。また使用するデータ、用途を限定することで、デバイスへのウイルス混入リスクを低減することができます。

設問 QD3 【持ち込みデバイス内のデータの制限・検査】

持ち込みデバイス内のデータは使用用途が制限され、検査・管理された状態になっていますか？

内容解説・対策例

【防御策】検知・防御の仕組みを導入する

中間経路となるオフィスエリアやベンダーの作業環境、制御システムの重要な機器があるエリアに、持ち込みデバイスのウイルスチェックや保存データチェックの仕組みや手順を導入します。

【緩和策】中間経路にある機器の脆弱性を取り除く

中間経路にあり、持ち込みデバイスおよびデータ等を取り扱う機器は、常にセキュリティパッチやファームウェアの更新を行い、その状況を管理します。また、デバイスメーカーのセキュリティ情報を定期的に確認し、脆弱性情報を把握します。また、中間経路にある機器の不要なソフトウェアやプロセスを削除することも有効です。

【検知策】持ち込みデバイスのウイルスチェックを行う

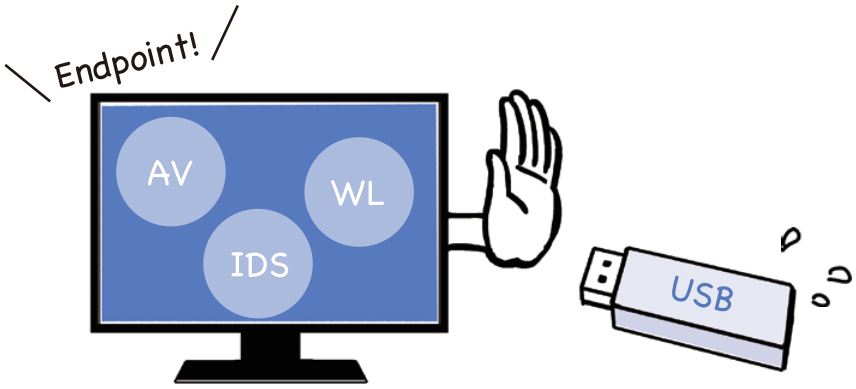
中間経路となるオフィスエリアやベンダーの作業環境や、制御システムの重要な機器があるエリアにおいて、持ち込みデバイスのウイルスチェックを行います。

参考文献

・JIS Q 27001:2014 「A.12.2 マルウェアからの保護」
・NIST SP800-82 Rev.2 「付録C 脅威源、脆弱性及びインシデント」

設問 QD4【エンドポイントセキュリティ対策の実施】

持ち込みデバイスを接続する機器（エンドポイント）はセキュリティ対策によって保護されていますか？



背景・目的

制御システム施設のセキュリティリスクを管理するには、ウイルスを制御システム内に持ち込まないことが重要です。しかし持ち込み防止の対策をすりぬけて、ウイルス感染した持ち込みデバイスが制御システムに接続されてしまう可能性も想定する必要があります。
エンドポイントセキュリティ対策を実施することにより、万が一接続された場合の被害発生の可能性を低減することができます。

想定される攻撃

ウイルス感染した持ち込みデバイスにより、制御システムが感染することが想定されます。

対策概要

エンドポイントセキュリティ対策として、システムの更新、要塞化（OSやアプリケーションの弱点を修正して堅牢にする）、物理的対策（使用しない物理ポートをふさぐ等）、AV（アンチウイルス）、WL（ホワイトリスト）、IDS（侵入検知システム）等が考えられます。これらのセキュリティソフト・機能の導入は、持ち込みデバイスからのウイルス感染予防に有効です。また、不使用時電源OFF、デバイス管理ソフトによる接続デバイス限定などを実施することも有効です。

設問 QD4【エンドポイントセキュリティ対策の実施】

持ち込みデバイスを接続する機器（エンドポイント）は セキュリティ対策によって保護されていますか？

内容解説・対策例

【防御策】機器の脆弱性を取り除く

ソフトウェア更新などにより機器が保有している脆弱性を取り除きます。運転に関係ないソフトウェアやプロセスを削除するのも有効です。更新にあたっては操業への影響を考慮し、計画的に対策に取り組む必要があります。

【防御策】持ち込みデバイスが接続される機器やPC、サーバーで任意のプロセスを起動できないようにする

持ち込みデバイスが接続される制御システム内の機器において、ホワイトリスト機能によって、起動可能なソフトウェアやプロセスを限定することにより、持ち込みデバイスから機器内に侵入したマルウェアの起動を阻止します。

【緩和策】起動されたプロセスがシステムに影響を与えないようにする

想定していない未知のプロセスが起動されたとしても、アクセス権の適切な設定などによりその動作を制限することでシステムに悪影響を与えないようにすることが考えられます。

【検知策】使用している機器の脆弱性情報を収集する

攻撃者は、侵入の足掛かりとなるような脆弱性を使用しようと試みます。そのことを防ぐためには、システム・機器ベンダーの脆弱性情報などを定期的に確認し、自システムの脆弱性を把握する必要があります。

【検知策】意図しないプロセスが起動されていないかをチェックする

制御システム内での攻撃活動を検知する手段の一つとして、例えばウイルス対策ソフトやプロセス起動ログを用いて、構成機器で意図しないプロセスが起動されていないかを常にチェックします。

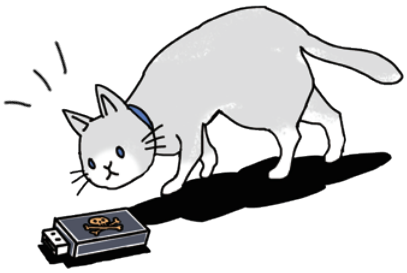
参考文献

・J-CLICS S2-6-1（ウイルス対策）
・J-CLICS S2-7-1（セキュリティパッチ）
・J-CLICS S2-8-1（システムの強化）
・JIS Q 27001:2014 「A.12.2 マルウェアからの保護」
・NIST SP800-82 Rev.2 「付録C 脅威源、脆弱性及びインシデント」
・NIST SP800-82 Rev.2 「付録E ICSセキュリティ機能及びツール」

column

コラム-1

USBメモリが落ちていたら？



USBメモリが道に落ちているのを見つけたらどうしますか？
誰が落としたのだろう？　何が入っているのだろう？　落とした人は困っているのでは？
いろいろと興味が湧いてくるのではないでしょうか？　USBメモリに「重要」、「秘」などと書かれていたらなおさらです。

しかし、USBメモリを拾ってそのまま自分のパソコンに接続するのは大変危険です。
USBメモリの中にマルウェアが仕込まれているかもしれません。その結果、大切な情報を盗み取られたり、ランサムウェアを仕掛けられて身代金を要求されたりするかもしれません。

拾ったUSBメモリは絶対にパソコンへの接続は行わないようにしましょう。

コラム-2

そのUSBデバイス、接続しても大丈夫？

USBデバイスは便利ですよね。USBメモリやUSBキーボード、マウスやスマートフォンの充電もできますね。
でも、お使いのUSBデバイスは本当に大丈夫でしょうか？
BadUSBと呼ばれるUSBデバイスは、USBメモリやUSBマウスの様なありとあらゆるUSBデバイスに偽装されているため、見た目では判別できません。

また、O.MG Cableと呼ばれる通常のUSBケーブルと見分けがつかないハッキングツールなどもあります。
このような不正なUSBデバイスへの対策として、ホワイトリスト機能があります。あらかじめ正規のUSBデバイスのIDを登録しておくことで、それ以外のUSBデバイスの不正接続を防止できます。

USBデバイスを接続する際には十分に注意しましょう。

物理アクセス経路

4

攻撃経路の特徴

悪意をもった攻撃者が、制御システムの施設に物理的に侵入して不正アクセスや破壊行為を行う攻撃経路です。物理アクセス経路では、攻撃者が標的となる施設まで移動し、守衛や施錠などの境界における防衛を突破して、標的となるシステムに物理的にアクセスします。移動のためのコストがかかる点、侵入や攻撃が発見されやすい点などから、攻撃者にとっては不利な経路と言えます。しかし、攻撃者が侵入に成功し、標的としている機器に物理的にアクセスできた場合には、物理的な破壊を含むさまざまな攻撃が可能となり、大きな被害が出る恐れがあります。したがって、攻撃者による侵入を許さないようにしっかりと防御することが肝要です。

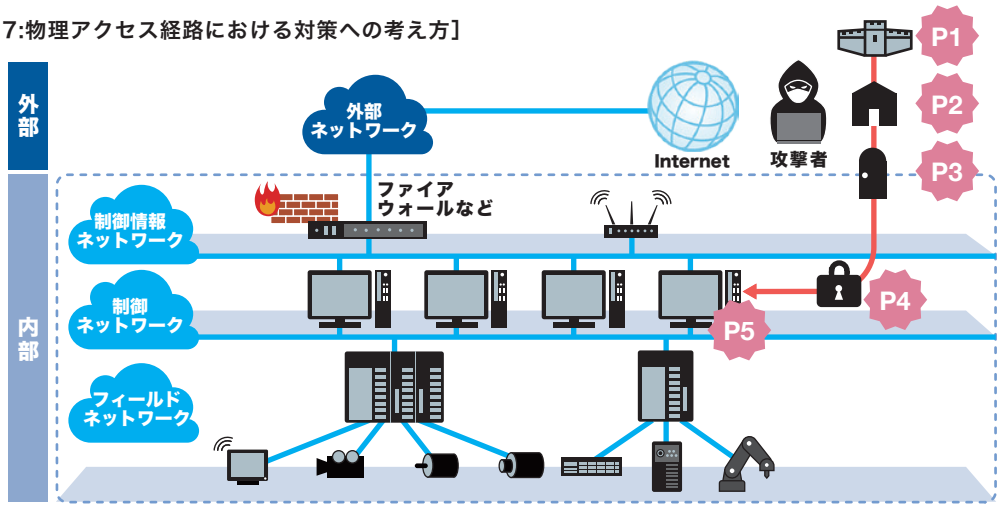
QP index

物理アクセス経路

攻撃への対策の考え方

悪意をもった攻撃者が、制御システムの施設に侵入するには、何重にも設置された防衛を突破する必要があります。侵入者が活動をするリスクを低減するためには、なるべく入口側の層で侵入を食い止めなければなりません。
図7のとおり、物理アクセス経路における各層ごとの攻撃と、その対策として次のものが想定されます。

［図7:物理アクセス経路における対策への考え方］



P1【敷地境界防衛突破】→QP1、QP2を参照
敷地境界は侵入者にとって、最初に突破しなければならない境界であり、フェンスを乗り越えて敷地の内部に侵入することや関係者になりすましてセキュリティ境界内へ侵入することが想定されます。フェンス乗り越えの対策として、有刺鉄線の設置や夜間照明の強化などを実施します。なりすましへの対策として、生体認証の導入やネームカード着用の義務付けなどを実施します。

P2【建物境界防衛の突破】→QP1、QP2を参照
建物の入り口にセキュリティゲートが設置されていたとしても、関係者の後について内部へ侵入すること（共連れ）が想定されます。共連れの対策として、2重ドア構造のセキュリティゲートの設置やゲートの監視強化などを実施します。

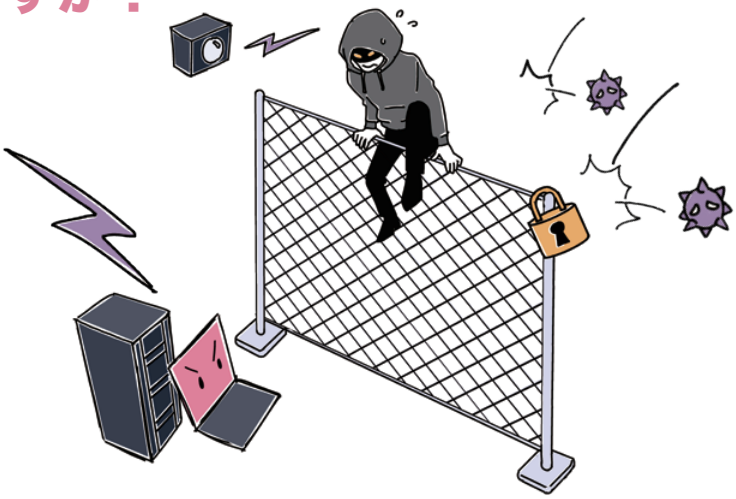
P3【部屋境界防衛の突破】→QP1、QP2を参照
部屋へ侵入する手段としては、建物への侵入と同様に共連れが想定されます。対策として、建物への侵入の場と同様に、2重ドア構造のセキュリティゲートの設置やゲートの監視強化などを実施します。

P4【機器施錠管理の突破】→QP1、QP2を参照
侵入者は、重要な設備の施錠に対して、合鍵を入手して利用することや、錠を物理的に破壊することが想定されます。合鍵の流出への対策として、合鍵を作成しづらい鍵の使用や、鍵の保管場所への監視カメラの設置が挙げられます。錠の物理的破壊への対策として、ヒンジ破壊を防止するドアの設置や、振動センサー設置による破壊活動の検知などを実施します。

P5【機器への物理アクセス攻撃】→QP3を参照
機器へアクセスする際にパスワードがかかっている場合、悪意をもった侵入者はID・パスワードを類推したり、不正に入手したパスワードを使用したりすることが想定されます。対策として、強力な認証の導入、内部ネットワークに対する通信の制限や監視、機器の脆弱性対策やプログラムの実行制限などを実施します。

設問 QP 1 【セキュリティ区画の設定】

重要な設備や機器が設置された場所は、セキュリティ区画として管理されていますか？



背景・目的

制御室や計器室には、制御システムを操作や設定をするための重要な機器が設置されています。また、制御室内では保護されるべき秘密情報が取り扱われている場合もあります。これらが攻撃者によって物理的にアクセスされると大きな被害が出る恐れがあります。対策として、重要な資産が設置されている場所をセキュリティ区画に指定してセキュリティレベルを設定し、セキュリティレベルに応じて段階的に施錠管理や入退出管理を行うことで、許可されていない人員の入室を制限します。

想定される攻撃

攻撃者がセキュリティ区画に侵入する手段として、フェンスの乗り越え、関係者を装ったなりすまし、錠の物理的な破壊などが想定されます。セキュリティ区画の境界にセキュリティ対策が十分でない部分があると、そこから侵入されてしまう恐れがあります。

対策概要

事業継続に影響する重要な設備・機器・情報を不正な物理アクセスから保護するために、重要な資産を扱う場所をセキュリティ区画に指定し、重要度や業務内容に応じたセキュリティレベルを設定します。各セキュリティ区画は、管理者・入室者を明確にし、フェンスや施錠管理などによって管理者の許可を持たない人員がアクセスできないようにします。また、監視カメラなどによって侵入者をいち早く検知します。
これらの対策により、許可をもたない人員による攻撃や操作のリスクが低減できます。セキュリティ区画を明確にし、セキュリティ管理対象を限定することで、管理コストが低減できます。

設問 QP 1 【セキュリティ区画の設定】

重要な設備や機器が設置された場所は、セキュリティ区画として管理されていますか？

内容解説・対策例

【防御策】乗り越え不可能なフェンスを設置する

外部との境界に設置されたフェンスの乗り越えによる侵入を防止するために、フェンスのセキュリティを強化します。例として次の対策があります。

【防御策】フェンスの乗り越えを抑止する

外部との境界に設置されたフェンスの乗り越えを抑止するために、警告表示や監視の強化を行います。例として次の対策があります。

【検知策】 侵入検知システムを設置し運用する

外部からの侵入者を検知するために、監視カメラの設置などの侵入検知システムを導入して運用します。

参考文献

・JIS Q 27001:2014 「A.8.1.1 資産目録」
・JIS Q 27001:2014 「A.8.1.2 資産の管理責任」
・JIS Q 27001:2014 「A.11.1.1 物理的セキュリティ境界」
・JIS Q 27001:2014 「A.11.1.3 オフィス，部屋及び施設のセキュリティ」
・JIS Q 27001:2014 「A.11.1.4 外部及び環境の脅威からの保護」
・U.S. Army: “FM 3-19.30 Physical Security”, Chapter 4, PROTECTIVE BARRIERS
・NIST SP800-82 Rev.2 「6.2.11 物理環境上の保護（PE）」

設問 QP2【入退管理の実施】

セキュリティ区画は、入退出管理によって保護されていますか？

背景・目的

制御室内には制御システムを操作や設定をするための重要な機器が設置されています。また、制御室内では保護されるべき秘密情報が取り扱われている場合もあります。これらの重要な機器と秘密情報を保護するために、セキュリティ区画内に出入りする人物の管理をセキュリティレベルに応じて実施し、許可されていない人員の出入りを制限します。

訪問者が制御室へ入る場合は、常に入室権限をもった関係者が付き添うことで、不要または不正な操作、秘密情報の撮影・複製および持出しなどを防止します。また、日頃から制御室に、いつ、誰が、何の目的で入室し、いつ退室したのかを記録し、定期的に入退室記録を確認することで、許可されていない人員の制御室への入室や、許可されている人員でも目的外の入室をすることを抑止します。

入退室記録は、セキュリティ事故・事件が発生した場合の調査や監査のための証跡としても有用です。

想定される攻撃

セキュリティ区画内へ出入りする人物の管理が不十分だと、侵入者は関係者になりすましたり、関係者の後ろについていくことで、セキュリティ区画内へ侵入したりすることが想定されます。

もし、悪意をもった者が制御室内に入室すると、制御室内の機器への物理的アクセスが可能となり、不正操作や情報漏えい、機器の物理的破壊、盗難などが発生する恐れがあります。

設問 QP2【入退管理の実施】

セキュリティ区画は、入退出管理によって保護されていますか？

対策概要

設定したセキュリティ区画とセキュリティレベルに準じて、人の出入りを必要最小限にするように運用します。また、来訪者の不審な行動を抑止するために、必要に応じて、関係者が付き添い、来訪者の行動をチェックします。これらの対策により、許可をもたない人員による攻撃や操作のリスクを低減できます。また、セキュリティ区画内に出入りする人員を限定することで、管理コストが低減できます。

内容解説・対策例

【防御策】守衛所での入退出手続きを厳格化する

許可のない人員の侵入を防止するために、守衛所での身分確認や用務先照会などを厳格化します。

【防御策】IDカードによる認証を強化する

許可のない人員の侵入を防止するため、セキュリティ境界に設置されたドアやゲートにおいてIDカードやパスワード等を用いて認証を強化します。

【防御策】関係者を装ったなりすましによる侵入を抑止する

関係者を装ったなりすましによる侵入を抑止するため、ネームカードの着用や確認を徹底します。

【防御策】共連れ（tail gating）対策を強化する

関係者の後ろに付いて侵入する手法である共連れを防止する対策を強化します。

【検知策】不審者を見かけたら照会する

不審者（付き添いのない来訪者・IDを着用していない人員など）を見かけた場合には、所属・用務先を確認し、用務先や守衛に照会します。

【回復策】侵入者を即座にセキュリティ区画から退去させ，警備担当や警察に引き渡す

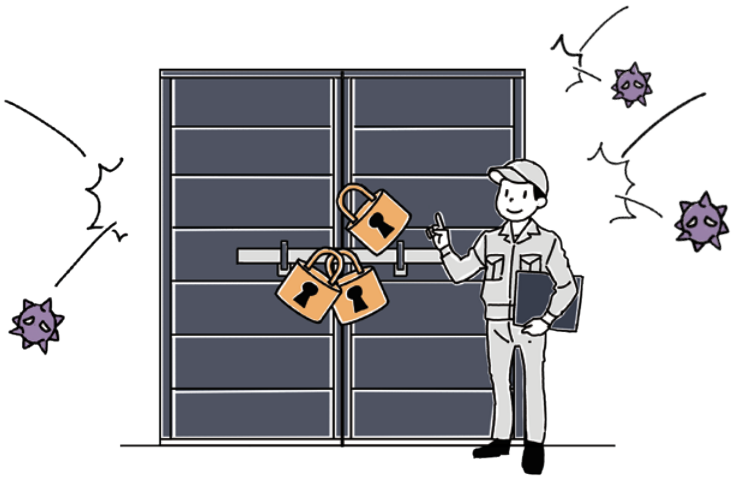
許可のないまたは関係者ではない人員を見つけた場合は、セキュリティ区画を警備する担当者または警察へ連絡し、その人員を引き渡します。

参考文献

・J-CLICS S1-1-1（身分証明書の着用）
・J-CLICS S1-1-2（訪問者への付添い）
・JIS Q 27001:2014 「A.11.1.2 物理的入退管理策」
・JIS Q 27001:2014 「A.11.1.6 受渡場所」
・U.S. Army: “FM 3-19.30 Physical Security”, Chapter 7 ACCESS CONTROL
・NIST SP800-82 Rev.2 「6.2.11 物理環境上の保護（PE）」

設問 QP3 【施錠管理の実施】

重要な設備や機器は、施錠管理によって保護されていますか？



背景・目的

制御室内には制御システムを操作や設定をするために重要となる機器が設置されています。また、制御室内では秘密情報が取り扱われている場合もあります。重要な機器や秘密情報は、鍵のかかるラックや棚の中に置き、厳密な施錠管理によって保護します。正規の権限を持つ人だけが施錠や開錠を行えるように運用することで、許可を持たない人による不正操作や情報漏えいのリスクが低減できます。

想定される攻撃

セキュリティ区画内に設置してある機器の施錠管理が不十分だと、侵入者は合鍵を入手したり、錠を物理的に破壊したりすることでセキュリティ区画に侵入し、重要な機器を不正に操作することが想定されます。
悪意をもった者がセキュリティレベルの高く設定された重要な機器に物理的アクセスが可能となれば、事業継続に深刻な影響を与えるような不正操作や情報漏えい、機器の物理的破壊、盗難などが発生する恐れがあります。

対策概要

セキュリティレベルに応じて、施錠管理を厳重に行うことで、許可を持たない人によるアクセスによる攻撃や操作のリスクを低減できます。

設問 QP3【施錠管理の実施】

重要な設備や機器は、施錠管理によって保護されていますか？

内容解説・対策例

【防御策】容易にアクセスされない配置にする

重要な機器や配線類は、許可を持たない者が容易にアクセスできない配置（高所、地下、施錠された部屋、施錠されたラックなど）にします。

【防御策】錠を多重化する

施錠管理を突破するための労力を増加させるために、複数の錠を設置して多重化します。

【検知策】鍵や錠の監視を強化する

錠に対する攻撃や鍵の不正使用を早期に発見するために、鍵の保管場所や錠の場所に監視カメラを設置するなどして、鍵や錠の監視を強化します。

【防御策】鍵の管理を強化する

鍵の不正使用を防止するため、鍵の管理を強化します。

【防御策】合鍵を作製しづらいよう対策された鍵（メーカー受注生産品など）を使用する

合鍵の不正作成を防止するために、合鍵を作製しづらいように対策された錠を使用します。

【防御策】破壊されづらいように対策された錠・ドアを使用する

破壊による施錠管理の突破を防止するため、対策された錠やドアを使用します。

【検知策】防犯センサーを設置する

防犯センサーを設置し、許可されない開錠や、破壊活動を検知します。

【回復策】鍵が漏えいしている疑いのある錠および鍵を変更する

侵入に利用された経路の錠は、新しい錠に交換して再利用されないようにします。

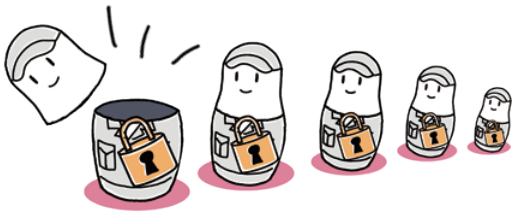
参考文献

・J-CLICS S1-1-2（訪問者への付添い）
・J-CLICS S1-1-3（監視カメラの設置）
・JIS Q 27001:2014 「A.11.2.1 装置の設置および保護」
・JIS Q 27001:2014 「A.11.2.3 ケーブル配線のセキュリティ」
・公益社団法人 全国防犯協議会連合会:　防犯性の高い建物部品目録
・U.S. Army: “FM 3-19.30 Physical Security”, Chapter 8, LOCK AND KEY SYSTEMS
・NIST SP800-82 Rev.2 「6.2.11 物理環境上の保護（PE）」

column

コラム-1

セキュリティ区画は「入れ子構造」で



セキュリティ区画にはセキュリティレベルを設定して、段階的に制限を厳しくすることでアクセス可能な人員を限定します。各セキュリティレベルでの制限は、業務内容や組織構造などにあわせて設定します。例えば、次のような設定が考えられます。例では、レベル1（最低レベル）、 2、 3、 4（最高レベル）の順で段階的に制限を厳しくしています。

レベル1:**社員や訪問者以外の立ち入りを禁止（敷地内、構内、応接スペースなど）**
レベル2:**レベル1の制限に加えて、社員以外の立ち入りを禁止（社員会議室、一般オフィスなど）**
レベル3:**レベル2の制限に加えて、関係者以外の立ち入りを禁止（開発室、実験室、コントロールルームなど）**
レベル4:**レベル3の制限に加えて、担当者以外の立ち入りを禁止（計算機室、計器室など）**

セキュリティレベルは、制限を入れ子構造に設定することがポイントです。すなわち、上記例の下線部で示したように、レベルごとに制限を追加していきます。例えば、セキュリティレベル2はセキュリティレベル1を前提とし、セキュリティレベル3はセキュリティレベル2を前提として、新たに制限を追加していきます。

また、セキュリティ区画も入れ子構造に設定することが理想です。上位のセキュリティレベルの区画に到達するには、下位のセキュリティレベルの区画を通過しなければならないように設定します。例えば、セキュリティレベル4の区画に入るためには、必ずセキュリティレベル1、2、3、4の順で通過しなければならないように動線を設定します。例えば、セキュリティレベル3の開発室からセキュリティレベル1の構内に出るには、必ずセキュリティレベル2のオフィスを通らなければならず、開発室から構内に直接出られるような常用の経路が存在しないことが理想です。非常口や荷物搬入口などの経路については、日常的に使用されないよう厳重に管理します。

このように、セキュリティレベルやセキュリティ区画を「入れ子構造」とし、段階的に制限を加えることで、より強固な入退出管理ができます。

コラム-2

その錠は大丈夫？

インターネット上には、錠のこじ開け方や破壊方法などの情報が多数公開されており、誰でも簡単に入手できる状況です。また、特定の機器（信号設備、鉄道設備、自動販売機、計器盤、計算機ラックなど）の合鍵が販売され、オークションサイトで販売された鉄道設備の合鍵が悪用された事例もあります。使用する錠の選定にあたっては、インターネット上の情報を収集し、簡単に突破されるものでないことを確認することをお薦めします。また、ピッキングなどへの耐性が強く、できるだけ鍵パターンの数が多い錠を選ぶようにしましょう。

column

コラム-3

フェンスの点検は侵入者視点で

フェンスは敷地内への侵入対策の基本です。フェンスにはさまざまな素材、高さ、素材、形状があり、それらによって侵入対策としての強度が異なります。フェンスからの侵入を防止するため、容易に破壊されない素材であること、容易によじ登れない高さや形状であることを点検しましょう。金網フェンスでは網目の小さなものを選択するとよじ登りが困難になります。また、フェンス上部に剣先や忍び返しを設置するとさらに侵入が困難になります。忍び返しは、フェンスを乗り越えようとする人に覆いかぶさるように斜めに張り出した構造で、外側からの侵入者を防ぐよう外側に張り出した外忍び、内側からの脱走者を防ぐよう内側に張り出した内忍び、空港などで使用される両側に張り出した両忍びがあります。目的にあわせて正しく使い分けましょう。また、フェンスの周囲に侵入に悪用できそうな電柱などの構造物、樹木やツタなどの植物などがないことを確認しましょう。普段からフェンスを眺めていると忍び返しが逆のものやフェンス前の電柱から簡単に侵入できそうなものを見かけることがあります。侵入者視点でフェンスをチェックすると良いでしょう。

コラム-4

来訪者の動線に注意

来訪者を受け入れる会議室や打ち合わせスペースまでの通路など、来訪者が通る動線をチェックすることが重要です。来訪者から見える範囲に、情報漏えいや盗難の危険があるもの（書類、コピー機、FAX機、ゴミ箱、掲示物など）を置かないようにします。リスクがある場所に来訪者を通す場合には、必ず関係者が同伴するようにします。来訪者が通る動線を日常的にチェックし、問題があれば改善するようにしましょう。

コラム-5

パスワード入力は見せない・見ない

ショルダーハッキングという攻撃手法があります。パスワードを入力している人の肩越しにキー操作を覗き込んで、パスワードを不正に入手する手法です。パスワードを覗き見る意思がない場合でも、パスワードの入力操作が見えてしまう場合があります。パスワードを入力する際には、周囲に人がいないことを確認して手早く入力します。周囲に人がいる場合には、離れてもらったり、後ろを向いてもらったりするなどして、入力操作を見られないように工夫しましょう。万一、パスワードが漏えいした恐れがある場合には、早急にパスワードを変更しましょう。パスワードは、お互いに、見せない・見ないように配慮することが重要です。

Appendix 対策マップの使い方

5

J-CLICS 攻撃経路対策編 対策マップの使い方

記載内容

付属資料の対策マップは攻撃経路ごとにシートが分けられており、各経路の攻撃手順と攻撃の成立条件、関連する設問、「防御・緩和・検知・回復」の4つの対策例を一覧で確認できます。このシートを使い、保護対象システムに存在する脅威を理解して、どういった対策を取るのが良いかを検討することができます。
各攻撃経路のシート全体像は図8のようになっています。

[図8:対策マップにおける各攻撃経路のシート全体像]

攻撃手順2	成立条件	防御策	緩和策	検知策	回復策
		防御策	緩和策	検知策	回復策
		【QN1】 ▼システム構成に関する情報を秘密情報として管理する 管）システム構成情報が含まれる設計資料や文書を社外秘などの秘密に指定する 【QN1】 ▼秘密情報やそれらの特定・推測につながる情報の漏洩を防止する 狭）公開資料のチェック体制を強化する	【QN1】 ▼秘密情報の拡散を抑制するための手順を実施する 縮）公開資料の差し替えや公開停止できる体制を確立する	【QN1】 ▼自社機器の情報が公開されていることを認識する ・コミュニティ（掲示板・SNS，ダークウェブ）で流通している情報を監視する	－
N1-2. 関係者から入手					
	N1-2a. 関係者からIPアドレスが入手可能				
		防御策	緩和策	検知策	回復策
		【QN1】 ▼関係者の教育を行う 狭）関係者内で秘密情報の保護意識を醸成する 狭）ソーシャルエンジニアリングへの注意を喚起する 狭）資料の持ち出しを制限し，資料格納メディアや紙の保管・廃棄方法を徹底する 【QN1】 ▼秘密情報へのアクセスを管理する 縮）秘密情報ごとにアクセスできる関係者を設定し，それぞれ最適化（必要最小限）する 【QN1】 ▼契約等で情報漏洩を牽制する 抑）関係者とNDAを締結する 抑）罰則付きの就業規則を規定する 【QN1】 ▼退職者からの情報漏洩を防止する 狭）退職者が秘密情報にアクセスできないようにする J-CLICS S2-10-1（転入者と転出者用のプロセス）	－	【QN1】 ▼関係者へのアプローチがあったことを認識する ・不審な接触者からのアクセスがあった場合にはすぐに通報する運用にする	－
N1-3. 外部サービスで調査					
	N1-3a. 外部サービスで検索可能				
		防御策	緩和策	検知策	回復策
		【QN2】 ▼自組織・関係組織以外からのアクセスを遮断する 遮）他組織からアクセスされる可能性がある経路を遮断する 遮）不要なプロトコルとポートへのアクセスを遮断する J-CLICS S2-4-1（ファイアウォール） 【QN2】 ▼外部からのアクセス手段・機会を制限する 狭）サードパーティと接続している部分のアクセス手段を最小限に制約する J-CLICS S1-5-1（サードパーティリスクの管理） 遮）内部ネットワークをプライベートアドレス化し，外部へはNA(P)Tを介してアクセスする	【QN2】 ▼公開範囲を制限する 縮）DMZを設置する	【QN2】 ▼外部ネットワークからのアクセスを監視する ・IDSなどを設置して，クローラからのアクセスを検知する ・調査サイトなどの外部サービスに自社機器が登録されているかどうかをチェックする	－

攻撃手順の見方

シートの一番左側（A列）に攻撃手順1があります。その攻撃手順1を詳細な手順に分解したものを隣列（B列）に記載しています。
この攻撃手順1、2は、制御システム外部の攻撃者が保護対象システム内の攻撃対象に到達する手順を想定して、シートの上側から下側に向かって、制御システム外部から内部に侵入していく攻撃手順を表すように記載しています。シートの上側に位置する攻撃手順の攻撃成立条件に対するセキュリティ対策を導入することにより、高い効果を得ることが期待できます。

攻撃手順の識別子として、各攻撃経路を示すアルファベット1文字を添えています。

ネットワーク経路　　:N（Network）
無線LAN経路　　:R（Radio frequency network）
持ち込みデバイス経路:D（Device）
物理アクセス経路　　:P（Physical）

攻撃手順1は、上側から順に算用数字を添えています。攻撃手順2は、攻撃手順1を分解した詳細な手順のため、X-x（ハイフンと数字）という表現をしています。

例）持ち込みデバイス経路の攻撃手順1つ目:D1.

持ち込みデバイス経路の攻撃手順1つ目を分解した手順1つ目:D1-1
持ち込みデバイス経路の攻撃手順2つ目を分解した手順1つ目:D2-1
持ち込みデバイス経路の攻撃手順2つ目を分解した手順2つ目:D2-2

成立条件の見方

攻撃手順に対する成立条件をシートの左から3列目（C列）に記載しています。成立条件には以下の3つの種類があります。シートでは、表5に記す3種類を、アルファベットと数字を使って表現しています。

[表5:攻撃手順に対する成立条件の種類と表記]

成立条件	記載方法
単独で成立するもの	攻撃手順の識別子にアルファベットを添えています。 例）攻撃経路D1-1の成立条件:D1-1a
複数種類の独立した条件で成立するもの	攻撃手順の識別子にアルファベットをaから順に添えています。 例）攻撃経路R3-4の成立条件1つ目:R3-4a 攻撃経路R3-4の成立条件2つ目:R3-4b
複数種類が組み合わさった条件で成立するもの	攻撃手順の識別子にアルファベットを添えて、組み合わせの数だけ(x)の数字を添えています。 例）攻撃経路R3-3の成立条件1つ目:R3-3a(1) 攻撃経路R3-3の成立条件2つ目:R3-3a(2)

「単独で成立するもの」「独立した条件で成立するもの」は、1つ1つにセキュリティ対策を検討する必要があります。
「複数種類が組み合わさった条件で成立するもの」は、どれか1つの攻撃手順に対策できれば、保護効果が得られます。

セキュリティ対策の見方

成立条件ごとに、セキュリティ対策として「防御・緩和・検知・回復」の4種類の対策を記載しています。成立条件によっては、対策が空欄の物もあります。空欄部分は、推奨のセキュリティ対策を提示していませんが、実際のシステムや組織の運用にあわせて、独自に対策を立案し、導入する事をご検討ください。

各セキュリティ対策のセル内には、J-CLICK攻撃経路対策編の設問番号（例:物理経路の設問1つ目【QP1】）を記載しているので、各設問がどの攻撃手順の成立条件に関係しているのかを確認することができます。また、各セキュリティ対策で実施すべきこと（▼印）と、対策例も記載しています。セキュリティ対策の方法によって得られる効果が異なるため、得られる効果を表す1文字漢字（「得られる効果」を参照）を添えてあります。
各セキュリティ対策のセルに、他の攻撃経路を参照するように記載されている場合もあります。攻撃手順の見方や成立条件の見方で紹介した識別子の見方を参考に、関連する他経路のシートを確認してください。

著作権・引用や二次利用等について