J-CLICS
設問項目ガイド

STEP
1

—— 制御システムに携わるすべての方へ ——

一般社団法人 JPCERT コーディネーションセンター

2013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）の補足文書であり、各設問で問われている対策項目について分かり易く解説しています。
J-CLICSに記載された設問の意味するところ（背景・目的）や具体的な対策方法が解説されていますので、自社は○をつけてよいのか、×とすべきなのか、といった判断をより的確に下し、×となった項目に対する効果的な対策を立案・実施するためにご活用いただけます。

本ガイドの記載内容

本ガイドは、設問ごとに独立して読めるよう編集されています。通読せずに必要な設問のみを読むという活用も可能です。
本ガイドは、J-CLICSの各設問について、次の形式で深い理解のために参考となる情報を補足しています。

【背景・目的】
J-CLICS設問の背景と目的について説明しています。

【想定されるリスク】
J-CLICS設問が達成されなかった場合のリスクの例について説明しています。これらのリスクは、J-CLICS項目を、次項に解説される内容や施策例を実施することで排除または低減されます。

【内容解説・施策例】
J-CLICS設問の内容の詳細説明と、各設問を達成するための施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のため、これらを参考に、各現場に合った施策例を検討する必要があります。

【参考文献】
J-CLICS設問に関連した書籍・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。

【補足】
J-CLICS設問に関連した補足情報です。施策の検討や実施に役に立ちそうな情報を紹介しています。補足は、各設問の末尾に記載しております。

謝辞

J-CLICSは、SICE/JEITA/JEMIMA セキュリティ合同WGおよびJ-CLICSユーザ合同協議会の協力により、JPCERTコーディネーションセンターが無償配布を行っている日本版SSAT(SCADA Self Assessment Tool)の項目をもとに作成されました。

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 日本電気計測器工業会）
梅田　裕二	株式会社 東芝（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）
北浦　史郎	一般社団法人 日本ガス協会
北川　卓志	電気事業連合会
久保　智	富士電機株式会社（一般社団法人 日本電気計測器工業会）
窪谷　聡	アズビル株式会社（一般社団法人 日本電気計測器工業会）
清水　良昭	富士電機株式会社（一般社団法人 日本電気計測器工業会）
杉谷　洋幸	三菱化学エンジニアリング株式会社
高務　健二	富士電機株式会社（一般社団法人 電子情報技術産業協会）
高宗　直人	三井化学株式会社
瀧田　誠治	一般社団法人 日本電気計測器工業会
山田　勉	株式会社 日立製作所（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	森ビル株式会社

【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 計測制御委員会 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

まえがき

本ガイドについて …… 2

謝辞 …… 3

1. 物理セキュリティ

【設問 No.1-1】 …… 6

【設問 No.1-2】 …… 8

【設問 No.1-3】 …… 10

【補足】 …… 13

2. 機器接続手順

【設問 No.2-1】 …… 16

【設問 No.2-2】 …… 19

【補足】 …… 21

3. パスワードとアカウント

【設問 No.3-1】 …… 23

【設問 No.3-2】 …… 25

【設問 No.3-3】 …… 27

【補足】 …… 29

4. 対応能力の確立

【設問 No.4-1】 …… 32

【補足】 …… 34

5. サード・パーティリスクの管理

【設問 No.5-1】 …… 36

【補足】 …… 38

6. 継続的な評価と改善

【設問 No.6-1】 …… 40

【補足】 …… 42

付録 A

情報セキュリティ関連参考文献 …… 44

1. 物理セキュリティ

【設問 No.1-1】

制御室への入退室は、
許可された関係者だけに限られていますか？

【設問 No.1-2】

制御室への訪問者には、
常に関係者が付き添っていますか？

【設問 No.1-3】

制御室への入退室管理
（記録と管理者による定期的な確認）を行っていますか？

【設問 No.1-1】

制御室への入退室は、許可された関係者だけに限られていますか？

制御室(制御機器または操作端末の設置場所)内の設備へは、許可された関係者のみが入退室が可能であることを確実にするために、適切な入退室管理を行い、許可された関係者のみが入退室できるように制限することが重要です。

背景・目的

制御室内には制御システムを操作・設定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機密情報が取り扱われている場合もあります。制御機器への許可されない操作や機密情報の漏えいを防止するために、制御室への入退室は許可された者のみに制限することが重要です。

想定されるリスク

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、盗難などの被害を受ける恐れがあります。また、関係者以外の人員が制御室内に入室することにより、不用意な操作や変更などが行われ、制御システムの操業に影響を及ぼす可能性があります。その結果、制御システムの異常動作や停止などの事態に陥る恐れがあります。

内容解説・施策例

入退室管理の管理策として、次のような施策があります。

（ア）ルールの策定

①制御室への入室は、許可された関係者のみに制限するルールを策定、運用する。
②入室を許可する関係者のリストを作成し、関係者に周知する。
③制御室の入口に関係者以外立ち入り禁止であることを掲示する。
④訪問者に対しては、必ず関係者が付き添うようにする。訪問者の付き添いに関する施策については、【設問 No.1-2】を参照のこと。

（イ）身分証明書の着用

許可された関係者全員にIDカードなどの身分証明書を配布し、着用を義務付けます。
身分証明書を着用していない場合は、誰であるか問いかけ、入室を許可された人員であるか確認します。

（ウ）入退室管理設備の導入

制御室への入室は、許可された関係者のみに制限できるよう、IDカードや暗証番号などによる認証装置をもつ施錠装置を導入します。

（エ）入退室の記録

制御室への入退室を記録し、一定期間保存します。入退室記録の保存期間は、企業ポリシーに沿って設定、管理します。入退室管理の施策については、【設問 No.1-3】をご参照ください。

（オ）入室許可の見直し

許可された関係者の異動などがあった場合は、直ちに入室許可の見直しを行い、適切な人員に適切な権限を付与するようにします。定期的に関係者リストの妥当性を確認し、必要に応じて更新します。

【参考文献】
・JIS Q 27001「A 9.1.1 物理セキュリティ境界」
・JIS Q 27001「A 9.1.2 物理的入退管理策

【設問 No.1-2】

制御室への訪問者には、常に関係者が付き添っていますか？

業務上、訪問者に制御室(制御機器または操作端末の設置場所)への入室を許可する場合、制御室内でのルールを熟知した入室権限を持った関係者が付き添い、許可されない操作や機器接続、機器の持込みや持出しなどが行われないようにします。

背景・目的

制御室内には制御システムを操作・設定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機密情報が取り扱われている場合もあります。訪問者が制御室へ入室する場合は、常に入室権限を持った関係者が付き添い、不要または不正な操作、機密情報の撮影・複製および持出しなどを防止することが重要です。

想定されるリスク

一旦、制御室への入室が許可されると、訪問者は室内のすべての機器への物理的アクセスが可能となります。その結果、機密情報の漏えい、不正操作や不用意な変更などが行われ、制御システムの操業に影響を及ぼす可能性があります。また、制御システムの異常動作や停止などの事態に陥る恐れもあります。

内容解説・施策例

訪問者の入退室管理の管理策として、次のような施策があります。

（ア）ルールの策定

訪問者が制御室へ入室する際のルールを策定し、運用します。制御室への入室前に、訪問者にルールを説明し、遵守するよう指示します。室内では、関係者が訪問者に付き添い、ルールが遵守されていることを確認します。

＜ルール例＞
①訪問者は、制御室に入室する際、必ず、関係者に目的を知らせ、許可を得る。
②訪問者は、ルールと非常時の対処手順の説明を受け、それに従う。
③訪問者は、室内では、必ず、関係者の付き添いのもとで行動する。
以下の場合、必ず、関係者の許可を得る。
・室内の機器に触れる場合
・室内での写真撮影、ビデオ撮影、録音などを行う場合
・室内への物品持込み、または持ち出す場合（関係者は、入退室時、物品の確認を行う。）
④原則、USBメモリやCD、DVD、磁気テープなどの記録メディア、カメラ、携帯電話などの携帯情報機器は、制御室への持込みはしない。データの持込み、持出しなどで必要な場合は、関係者に申し出、指示に従う。（その場合、関係者によるデータ内容の確認やウイルスチェックを受ける。読み書き可能なデバイスは、備え付けのUSBメモリに移し換えるなど、入退室時に内容の確認を受ける。）
⑤原則、ノートPCなどの情報機器類の制御室への持込みはしない。持ち込む必要がある場合は、関係者に申し出、指示に従う。（関係者は、備え付けのPCを貸与するなどし、入退室時に内容を確認する。）
⑥室内では、携帯電話やスマートフォンなどは使用しない。必要ならば、入室時に受付などで預かる措置をとる。

（イ）訪問者IDカードの着用

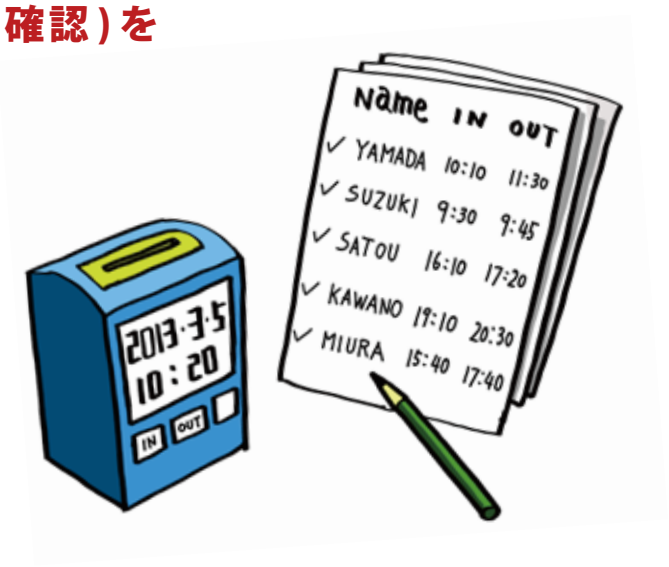
訪問者に訪問者番号や立ち入り許可範囲などを記載したIDカードを配布し、着用を義務付けます。付き添いが伴わない訪問者やIDカードを着用していない人員に対しては、退室を指示し、警備室に連絡します。

【参考文献】
・JIS Q 27001「A 6.2.2 顧客対応におけるセキュリティ」
・JIS Q 27001「A 9.1.5 セキュリティを保つべき領域での作業」
・JIS Q 27001「A 10.7.1 取外し可能な媒体の管理」

【設問 No.1-3】

制御室への入退室管理（記録と管理者による定期的な確認）を行っていますか？

制御室（制御機器または操作端末の設置場所）へ入室している人員が、許可された人員のみであることを確実にするために、日頃から入退室状況を把握し、定期的に入退室記録を確認することが重要です。



背景・目的

制御室内には制御システムを操作・設定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機密情報が取り扱われている場合もあります。入室を許可されていない人員による不要または不正な操作、機密情報の撮影・複製および持出しなどを防止することが重要です。許可されていない人員が制御室へ入室することのないよう、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に調査対象を絞り込むためにも、あるいは監査証跡としても有用です。

想定されるリスク

入退室記録がないと、入退室管理の欠陥を放置することになり、許可されていない人員や物品の入室を見落とし、セキュリティ事故・事件の発生につながる恐れがあります。さらに、セキュリティ事故・事件が発生した際に、その原因や影響範囲を特定することが難しくなり、対応や対策が困難になる恐れもあります。また、入退室管理の適切性を判断できず、管理上の問題を発見し、改善することが困難になります。

内容解説・施策例

入退室記録の管理策として、次のような施策があります。

（ア） ルールの策定

①関係者の入退室を記録するルールを策定し、運用する。

＜関係者の入退室記録例＞

・IDカードや暗証番号などと電気錠を組合せた入退室管理システムにて記録する。
・タイムレコーダにて記録する。
・業務日誌やノートに記録する。この場合、必ず、承認手続きを行う。

②訪問者の入退室を許可・記録するルールを策定し、運用する。

＜訪問者の入退室記録内容例＞

・訪問者の所属、氏名
・訪問先関係者の所属、氏名、連絡先
・訪問目的、作業内容
・入室許可範囲、操作対象機器
・入室時刻、退室予定時刻、退室時刻
・PC、USBメモリなどの持込み情報機器の有無と内容
・PC、USBメモリなどの貸出物品の有無と内容
・入室承認者の氏名、承認印
・入室許可IDカード（名札）の番号
・訪問者のルール承諾署名

③記憶メディア・情報機器の持込み・持出しを許可・記録するルールを策定し、運用する。

＜記憶メディア・情報機器の持込み・持出し記録内容例＞

・持込み、持出し担当者の所属、氏名
・記憶メディア・情報機器の種別、名称、ロット番号
・持込み、持出しの目的、作業内容
・記憶メディア・機器情報に含まれるデータ内容
・接続対象ネットワーク、メディア、機器の範囲
・持込み、持出し時刻
・適用ルール（ウイルスチェックなど）と作業詳細（ウイルス検査ソフトなど）
・持込み、持出しの承認者の氏名、承認印
・持込み時、持出し時のチェック、承認印

（イ） 入退室管理設備の導入

制御室に許可された関係者のみが入室できるように、IDカードや暗証番号などによる認証装置をもつ施錠装置を導入します。但し、企業ポリシーに沿った設置と運用を行います。

1. 物理セキュリティ　【設問 No.1-3】

（ウ） 監視カメラによる入退室管理

制御室の出入口に監視カメラを設置し、入退室を記録します。但し、企業ポリシーに沿った設置と運用を行います。

（エ） 入退室記録の保存

①制御室への入退室を記録し、一定期間、保存する。
②入退室管理に認証装置を用いている場合、そのログを保存する。
③入退室記録の保存期間は、企業ポリシーに沿って設定、管理する。

（オ） 定期的な入退室記録の確認

①入退室記録は、定期的に記録内容を確認し、不審な内容がないことを確認する。
②不審な記録や記録に不備があった場合、関係者に連絡し、セキュリティ上の問題がないかを確認する。

【参考文献】

・JIS Q 27001「A 9.1.1 物理的セキュリティ境界」
・JIS Q 27001「A 9.1.2 物理的入退管理策」

1. 物理セキュリティ

補足　【設問 No.1-1】

制御室への情報の持込み・持出しについて

ウイルス感染や情報漏えいの経路になり得るUSBメモリ、USBハードディスクなどのメモリデバイスや、CD、DVD、磁気テープなどの記録メディア、携帯電話などの携帯情報機器およびノートPCなどの情報機器の持込み・持出しには、ルールを定め、適切に管理することが望まれます。

＜制御室へのデータ持込みルール例＞

①USBメモリやUSBハードディスクなどのメモリデバイスを持ち込む際には、その必要性を十分に確認する。
②最小限のデータのみ、備え付けUSBメモリなどにコピーする。
※コピーする前には、フォーマットなどで初期化を行い、同USBメモリ内に不要なデータが残っていないようにする。
※USBメモリは、AUTORUNをOFFにし、書込み禁止スイッチ付きのものを使用する。
③同USBメモリに対し、ウイルスチェック、AUTORUNをOFFにした上で、持込みを許可する。
④制御室に持ち込む際、書込み禁止に設定する。(スイッチをシールなどで保護し、操作されないようにするとより安全である。)
⑤使用後、フォーマットなどで初期化を行い、同USBメモリからデータを完全に削除する。

制御室内にデータを持ち込む際、読取り専用DVD-RやCD-Rを使用することも、セキュリティ上、有効です。また、制御室へのノートPCなどの情報機器持込みを許可することは危険です。いかなる場合でも、外部からのノートPCなどの情報機器持込みは禁止することが望ましいです。PCによる作業が必要な場合は、備え付けのPCを貸与するなどし、外部からノートPCを持ち込ませないようにします。貸与用PCは、使用前後で訪問者の一時作業向けに環境設定されたバックアップデータのリストアなどにより初期化し、常にクリーンな状態を保つようにします。業務上の理由により、(制御室内のシステムに無線LANが導入されている環境に)外部からノートPCを持ち込む場合、同PCに無線のアクセスポイントをスキャンするソフトウエアやハッキングツール、パスワード解析ツールがインストールされていないことを確認します。

補足　【設問 No.1-2】

制御室内の機密情報について

制御室内には、取扱いに注意すべき情報があります。それらの情報は、訪問者の目に触れないよう、整理・整頓し、適切に管理される必要があります。特にパスワードや鍵の所在など機密情報は、知られる状況にないことを確認しておくことが大切です。

＜制御室内の機密情報の管理例＞

①機密情報が表示されている機器の付近には、訪問者を立ち入らせないようにする。
②ディスプレイの表示内容を簡単に覗き見られないよう、セキュリティフィルタを使用する。
③機密情報が保存されている棚は施錠し、訪問者が容易にアクセスできないようにする。
④プリンタ出力からの情報漏えいを防ぐため、プリンタは訪問者が簡単にアクセスできない場所に設置する。または、印刷物はすぐに回収し、プリンタに放置しないようする。
⑤ゴミ箱に廃棄した資料からの情報漏えいを防ぐため、機密情報の廃棄には十分な注意を払い、訪問者が容易に廃棄物を取得できないようにする。

1.物理セキュリティ

制御室内の機器の施錠管理について

訪問者に許可されていない機器を操作されないよう、制御室内の操作盤・ラックなどは適切に施錠管理される必要があります。

＜施錠管理例＞

①複数の箇所に同一鍵を使用しない。

②訪問者に鍵の貸出はせず、必要な場合は、付き添いの関係者が開錠・施錠を行う。

補足　**【設問 No.1-3】**

入退室記録について

制御室などのセキュリティ区画への入退室記録は、セキュリティ事故・事件が発生した際の重要な手掛かりになります。入室記録だけではなく、併せて退室記録も管理することをお奨めします。また、入退室記録が簡単に偽造・改ざんされないようにするための配慮が必要です。

＜入退室記録の偽造・改ざん防止策例＞

①記録時、書類のカーボンコピーを取る。

②記録時、ボールペンを使用する。

③退室時に内容を確認する。

④承認者や訪問先関係者が書類に捺印する。

監視カメラ(CCTV)の設置について

監視カメラなどの物理的監視システムにより、実際に制御室に入退室した人員を記録することで、セキュリティ事故・事件が発生した場合、分析に有効な情報となります。また、物理的監視システムの設置により、犯罪への抑止力となります。

＜監視カメラの導入例＞

①制御室などのセキュリティ区画の出入口や人が常駐しない重要施設に、設置していることが分かるよう目のつく場所に監視カメラを設置する。(監視カメラの存在を気付かせることで、不正入室や不正操作への抑止力となります。)

②監視カメラの内蔵時計は、常に正確な時刻に調整する。(内蔵時計の時刻がずれている場合、記録確認が正しく行えず、証拠としての価値を失います。)

③制御室への不正入室や重要な機器への不正操作を見落とさないよう、定期的に監視カメラの記録映像を確認する。

2. 機器接続手順

【設問 No.2-1】

**制御システムのネットワークに接続する機器について、
事前にそれらがウイルスに感染していないことを
確認する手順を守っていますか？**

【設問 No.2-2】

**制御システムの機器がITシステムの機器と
同じラックに設置されている場合、
各機器がどちらのシステムのものであるかを
ラベルなどで分かるようにしていますか？**

【設問 No.2-1】

制御システムのネットワークに接続する機器について、事前にそれらがウイルスに感染していないことを確認する手順を守っていますか？

ウイルスの感染を防止するために、制御システムや制御ネットワークに機器（ノートPCなどの情報機器、USBメモリやUSBハードディスクなどのメモリデバイス、CDやDVDなどの記録メディア、携帯電話などの携帯情報機器）を接続する際、事前にウイルスチェックなどを行う手順を定め、遵守することが重要です。

背景・目的

USBメモリ、USBハードディスクなどのメモリデバイスや、CD、DVD、磁気テープなどの記録メディア、ノートPCなどの情報機器および携帯電話などの携帯情報機器は、ウイルス感染の経路になる恐れがあります。近年、これらの機器を介して感染する制御システムを標的にしたウイルスも発見されており、今後はより一層の警戒・対策が必要です。

想定されるリスク

制御システムの機器がウイルスに感染すると、制御システムの動作に悪影響を与え、操業停止などの重大な事態につながる恐れがあります。ウイルスの破壊活動によって、機密情報の漏えい、システムやデータが損傷するなどの被害を受ける恐れがあります。また、ウイルスの駆除には、システムの停止や再インストールが必要となる場合もあり、多大なコスト負担を強いられ、ブランドイメージの低下につながります。

内容解説・施策例

ウイルス感染の防止策として、次のような施策があります。

（ア）ルールの策定

①制御システムや制御ネットワークに接続するPCを設置する際、ウイルス感染防止のための検査手順を策定し、運用する。

・OSやソフトウエアが最新状態になっていることを確認する。必要に応じて、パッチ適用やアップデートを実行する。
・ウイルスチェックの際、ウイルス定義ファイルが最新であることを確認する。
・事前にウイルスチェックを実施し、ウイルスに感染していないことを確認する。
・不要なサービスや通信機能が無効に設定されていることを確認する。（ポートスキャンツールや脆弱性検査ツールを使用するとことができます。）

②制御システムや制御ネットワークに接続されていた機器を撤去する場合、機密情報の漏えいを防止するための手順を策定し、運用する。必要に応じて、ハードディスクの完全消去や物理的破壊を規定する。

③ノートPCなどの情報機器、USBメモリやUSBハードディスクなどのメモリデバイス、CDやDVDなどの記録メディアの持込み・接続は、原則として禁止する。

④充電や給電目的のUSB接続（音楽プレイヤー、携帯電話、スマートフォン、扇風機、LEDライトなど）は禁止する。

⑤業務上の理由により、情報機器類を持ち込む場合は、あらかじめ文書にて申請し、審査後、許可する。また、持込み・持出し時には、第三者による確認を受ける。持込みの記録を文書として残すことで、ウイルス感染事故が発生した際に感染経路を特定できるようにする。

＜申請書類の内容＞
・申請者の所属、氏名
・承認者の所属、氏名
・持込み日時、期間
・持込み機器名称、種別
・持込み目的、作業内容
・接続対象機器またはネットワーク
・想定されるリスク
・適用するルール、手順
・持込み時の確認内容と結果、確認者の所属と氏名
・持出し時の確認内容と結果、確認者の所属と氏名
・使用したウイルス検査ソフトとパターンファイルのバージョン

⑥業務上、使用しないUSBポートなどの接続端子は、機器を接続されないよう、シールなどで封印する。

2. 機器接続手順　【設問 No.2-1】

（イ） ウイルス検査用 PC の設置

＜ウイルス検査用 PC の導入例＞

①USB メモリや USB ハードディスクなどのメモリデバイス、CD や DVD などの記録メディアを検査する専用 PC を準備する。

②検査用 PC のウイルス感染を防止するために、同 PC はネットワークに接続しない。オフライン（ネットワークに接続しない状態）で更新可能なウイルス検査ソフトを使用する。

③検査用 PC の OS とウイルス検査ソフトは、使用前に更新を行い、最新の状態にする。

④検査用 PC には、ハードディスクは搭載せず、DVD などの光学メディアから起動する。

⑤検査用 PC は、使用前後にウイルス検査を実施し、検査用 PC がウイルスに感染していないことを確認する。

（ウ） 備え付け USB メモリの設置

外部からの持込み USB メモリや USB ハードディスクなどのメモリデバイスは、ウイルスに感染している恐れがあるため、これらを制御機器およびネットワークに接続することは危険です。また、外部からの持込みメモリデバイスは、情報漏えいの経路になる恐れもあります。内部でのみ使用する備え付けの USB メモリを準備し、必要なデータのみを同 USB メモリにコピーすることで、リスクを低減することができます。

＜備え付け USB メモリの導入例＞

①備え付け USB メモリは、書込み禁止スイッチ付き USB メモリを使用し、書込み時以外は、書込み禁止に設定する。

②ウイルス感染防止のために、同 USB メモリを接続する PC は、自動起動機能 （AUTORUN）を OFF に設定する。

③外部からの持込み機器をウイルス検査用 PC に接続し、ウイルス感染有無を確認する。

④使用前、同 USB メモリを検査用 PC に接続し、ウイルス感染有無を確認する。

⑤検査用 PC 上にて、持込み機器より必要なデータを同 USB メモリにコピーする。

⑥使用後、同 USB メモリを検査用 PC に接続して、再初期化（フォーマット）し、データを完全消去する。

（エ） 備え付け PC の設置

外部からの持込みノート PC は、ウイルスに感染している恐れがあるため、これらを制御機器およびネットワークに接続することは危険です。また、外部からの持込みノート PC は、情報漏えいの経路になる恐れもあります。PC による操作が必要な場合は、備え付け PC を貸与し、PC を持ち込ませないようにします。

（関連：補足 _ 設問 No.1-1）

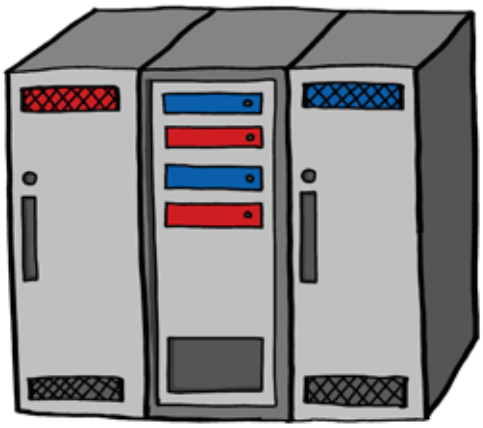
【参考文献】

・JIS Q 27001「A 9.2 装置のセキュリティ」

【設問 No.2-2】

制御システムの機器がITシステムの機器と同じラックに設置されている場合、各機器がどちらのシステムのものであるかをラベルなどで分かるようにしていますか？

制御システムへの許可されない操作や誤操作・誤接続を防止するためには、制御システムの機器を明示し、注意喚起することが重要です。



背景・目的

多くの機器が設置されている環境では、機器やケーブルの取り違えが発生する恐れもあります。このようなシステムメンテナンス時の作業ミスは、システムの安全性、および可用性に影響する大きなリスクとなります。
ITシステムのネットワークには、ユーザが日常的に使用するPCなどのウイルス感染リスクの高い機器が接続されています。同ネットワークに制御システムおよび関連機器（備え付けUSBメモリやPC）が誤接続されると、制御システムがウイルスに感染し、システムの運転に影響を及ぼす恐れがあります。
制御システムの構成機器やネットワークケーブルには、ラベルなどで制御システムの機器であることを明示し、ITシステムと誤認されないよう、注意喚起することが有効です。

想定されるリスク

他システムとの混同により、誤操作や誤接続が行われると、制御システムが停止したり、動作に異常が発生したりする可能性があります。また、制御システムがITシステムのネットワークに誤接続されると、制御システムの機器がウイルスに感染し、制御システムの運転に影響を及ぼす恐れがあります。

内容解説・施策例

誤操作・誤接続を防止する対策として、次のような施策があります。

(ア) ルールの策定

制御システムの機器の取扱いや変更承認手順、異常時の対応方法などについて、ルールを策定し、講習会などを実施して、関係者に周知・徹底します。

(イ) 別ラックへの分載および施錠管理

管理区分(ITシステム、制御システムなど)ごと、別の場所や別ラックに搭載し、別々の鍵で施錠管理します。機器への物理的アクセスを制限することで、取り違え事故を防止します。

(ウ) ラベル表示

制御システムの機器やケーブルであることを、ラベル表示します。ラベルには、「無断操作禁止」などと記載し、注意喚起を行います。また、管理者の連絡先や異常時の対応方法を記載し、無断操作や不正な対応を防止します。ラベルには、赤色系などの目立つ色を使用するとより効果的です。

(エ) 空きポート・端子の封印

誤接続を防止するために、空きポートや空き端子は、物理的に封印します。また、ラベルを使用し、「接続禁止」などと表示することで、注意喚起を行います。

(オ) スイッチなどの封印

電源スイッチなどの誤操作を防止するために、ラベルなどを使用し、注意を促します。また、ラベルなどを用いて、「操作禁止」などと表示すると、より効果的です。

(カ) ネットワークケーブルの色分け

接続するネットワークごとに違う色のケーブルを使用することで、誤接続を防止します。ラベル表示と併せて実施すると、より効果的です。

【参考文献】

・JIS Q 27001「A 9.2.1 装置の設置及び保護」

2. 機器接続手順

補足　【設問 No.2-1】

記録デバイスの廃棄について

USBメモリ、USBハードディスクなどのメモリデバイスや、CD、DVD、磁気テープなどの記録メディア、およびノートPCに搭載されたHDDなどの記録デバイスを破棄する際には、情報漏えいへの対策が必要です。
メモリデバイスについては、データの削除や初期化（フォーマット）してもハードディスク内の管理領域のみが書き換えられ、データ領域が消去されない場合があります。消去したはずの情報を復元される可能性があります。最も確実にデータを消去する手段は、物理的に機器を破壊することです。工具などを使用し、データの復元ができない状態になるよう破壊して、廃棄します。
また、CDやDVDなどの光学メディアについては、ハサミや専用シュレッダーにて裁断し、破棄します。
物理的にハードディスクを破壊できない場合は、ハードディスク内のデータを完全消去するツールを使用します。一般的に、ハードディスク内のデータを完全消去するには長時間（数時間から数十時間）かかります。あらかじめツールの説明書などで所要時間を確認しておくことをお奨めします。
USBメモリやSSDなど、フラッシュメモリを利用したデバイスの場合、書込み回数の制限から、特殊な書込みアルゴリズムを採用しています。そのため、フォーマットや上書きを複数回行ってもデータの消去ができないことがあります。これらのデバイスの完全消去は専用のツールを利用したり、物理的に破壊したりするなどの対応が必要となります。

補足　【設問 No.2-2】

非ラック搭載型PCの施錠管理について

ラック搭載型ではないPCなどは、ラックマウントキットを用いてラックに搭載したり、鍵のかかる棚に設置したりし、施錠管理することで、誤操作や誤接続から保護することが可能です。機器の施錠管理は、不用意なUSBメモリなどの接続によるウイルス感染の防止にも有効です。

3. パスワードとアカウント

【設問 No.3-1】

制御システムのパスワードの強度と有効期限を含むパスワード・ポリシーがありますか？

【設問 No.3-2】

強力なパスワードを使用していますか？

【設問 No.3-3】

制御システムのパスワードを定期的に変更していますか？

【設問 No.3-1】

制御システムのパスワードの強度と有効期限を含むパスワード・ポリシーがありますか？

パスワード文字数の制限、パスワードに使用する文字の種類や有効期限の指定など、パスワードの強度、および管理方法について、パスワード・ポリシーが策定されていることが重要です。

背景・目的

コンピュータや制御装置などを利用した多くの制御システムは、パスワードによって厳重に管理され、システムへの不正アクセスを防止するための対策が施されています。一方、パスワードさえ分かれば、システムへのアクセスが可能となり、重要なデータの読取りや制御装置を思いのままにコントロールできる可能性があるため、悪意をもった者は、さまざな手段によってパスワードを奪取または解析します。（特にシステム全体にアクセスできる管理者用のパスワードを狙います。）
したがって、制御システムのパスワードおよびパスワードの管理は制御システムへの攻撃を防ぐために、強度の高いパスワードの設定方法、運用方法などを定めたパスワード・ポリシーを策定する必要があります。
なお、パスワード・ポリシーがあっても、それを守らなければ意味がありません。パスワード・ポリシーの策定と併せて、一人一人がパスワード・ポリシーを遵守することも重要です。

想定されるリスク

パスワード・ポリシーが策定されていない場合、パスワードの適切な設定や管理が行われず、パスワードが漏えいしてしまう危険性が高くなります。
パスワードが漏えいすると、制御システムに不正にアクセスされ、操業データなどの重要な情報を盗み取られたり、制御装置のプログラムコードや設定値（パラメータ）を書き換えられたりします。その結果、制御システムの挙動が変わり、システムが停止すれば、莫大な損害を被るかもしれません。そのシステムが重要インフラであれば、社会に与える影響は計り知れません。

3. パスワードとアカウント　　【設問 No.3-1】

内容解説・施策例

制御システムで使用するパスワードの設定、変更などの管理方法について、パスワード・ポリシーを策定する必要があります。なお、システムの仕様や運用状況などの理由でパスワード・ポリシーが適用できない場合には、入退室管理や施錠管理などの物理セキュリティ施策を強化して許可されない人員のアクセスからシステムを保護します。

（ア） パスワード・ポリシーの作成

パスワード・ポリシーを策定し、文書化します。なお、パスワード・ポリシーには、例に挙げたような要件を記述します。

①以下の条件を満たすパスワードを使用する。

- 覚えられる文字列を使用する。(メモなどを参照しなければ入力できないような文字列は使用しない。)
- 一般の辞書に記載されている文字列(英単語、辞書に記載されている単語のローマ字表記など)やパスワード設定に多く使用される文字列などは使用しない。
- 当人に関係し、他人も容易に知り得るような情報(名前、誕生日、電話番号、車のナンバーなど) から推測できる文字列を使用しない。
- 小英字、大英字、数字、記号の４種類を組合せた文字列を使用する。
- 可能な限り文字列を長くする（8文字以上とする推奨）。但し、対象機器に設定できるパスワードの最大長が８文字未満の場合は、最大長の文字数とする。

②パスワードは定期的または一定のアクセス回数ごとに変更し、古いパスワードは再使用しない。

③パスワードを他人に教えたり、共有したりしない。

④パスワードの使い回しはしない。

⑤パスワードが他人に知られた可能性がある場合には即座に変更する。

⑥管理用パスワードは秘密情報として厳重に管理する。

- 平常時は管理者以外に知られないようにする。
- 管理者不在時の緊急時対応に備え、管理者パスワードを知る手段を用意しておく。

（イ） パスワード・ポリシーの遵守

パスワード・ポリシーに記載された内容を理解し遵守する。

①パスワードの設定ルールの遵守

②有効期限の遵守

③パスワード情報の管理方法の遵守

④技術的施策の実施

⑤啓発・教育の徹底

【参考文献】

・JIS Q 27001「A 11.3.1 パスワードの利用」

【設問 No.3-2】

強力なパスワードを使用していますか？

不正なアクセスを防ぐために、パスワードは簡単に解析または推測できない文字列にすることが重要です。

背景・目的

パスワードは、文字の組合せ（文字列）です。その組合せは辞書攻撃や総当たり攻撃と呼ばれる手法（【補足＿設問 No.3-2】参照）により、すべての組合せを試すことで、必ずパスワードを解析することができます。住所や電話番号、生年月日などの情報が分かれば、そこからパスワードを推測する攻撃手法も一般的です。また、文字数が少ないパスワードは、解析が容易なため安全とはいえません。パスワードに使用する文字の種類や長さを長くすることで、見つけるまでの時間を指数関数的に伸ばすことができます。
一般的な辞書やパスワードに多く使われる文字列などは避け、第三者から無意味と見られる文字列にすることは、不正アクセスを防ぐことにもつながります。

想定されるリスク

短いパスワードや容易に推測できるパスワードを設定すると、パスワードの解析が容易になります。パスワードが解析されてしまうと、制御システムに不正にアクセスされ、操業データなどの重要な情報を奪取されたり、制御装置のプログラムコードや設定値（パラメータ）を書き換えられたりします。その結果、制御システムの挙動が変わり、システムが停止すれば、莫大な損害を被るかもしれません。そのシステムが重要インフラであれば、社会に与える影響は計り知れません。

3. パスワードとアカウント　　【設問 No.3-2】

内容解説・施策例

使用するパスワードは、可能な限り文字列を長くし（8 文字以上推奨）、簡単に推測できない文字列にすることが重要です。
以下のような文字列は、パスワードとしてふさわしくありません。

- 種々の名前、電話番号、誕生日
- 英単語などの一般辞書に記載された単語
- アカウント名と同一、またはアカウント名から推測可能なもの
- 連続した同一文字や数字のみ
- アカウント作成時に付与されたパスワード

パスワードを設定する場合、以下について考慮すると良いでしょう。

- 大文字と小文字を使用する
- 数字と記号を含める
- 辞書にない文字列にする
- 可能な限り文字列を長くする（8 文字以上推奨）

＜例＞
H!elZl2o

【参考文献】

・IPA: パスワードの管理と注意
http://www.ipa.go.jp/security/fy14/contents/soho/html/chap1/pass.html
・パスワード チェッカー：強力なパスワードの使用
https://www.microsoft.com/ja-jp/safety/pc-security/password-checker.aspx?
・JIS Q 27001「A 11.3.1 パスワードの利用」

【設問 No.3-3】

制御システムのパスワードを定期的に変更していますか？

不正なアクセスを防ぐために、
パスワードは
定期的に変更することが重要です。

背景・目的

悪意をもって、パスワード奪取または、解析に成功した者は、そのことを吹聴などせず、秘かにシステムにアクセスできる状態を維持しようすることでしょう。しかしながら、定期的にパスワードを変更することで、奪取または解析されたパスワードを無効にすることができます。
また、パスワードは、パスワード解析ツールを使って時間をかけて解析が可能です。同じパスワードを使い続けると、時間がかかる総当たり攻撃などでも、いつかはパスワードを解析されてしまいます。したがって、パスワードを定期的に変更することはセキュリティ事故・事件を回避する有効な手段です。

想定されるリスク

パスワードを解析または奪取されると、制御システムに不正にアクセスされ、操業データなどの重要な情報を奪取されたり、制御装置のプログラムコードや設定値（パラメータ）を書き換えられたりします。その結果、制御システムの挙動が変わり、システムが停止すれば、莫大な損害を被るかもしれません。そのシステムが重要インフラであれば、社会に与える影響は計り知れません。

3. パスワードとアカウント　　【設問 No.3-3】

内容解説・施策例

パスワードは定期的に変更することが望ましく、特にさまざまな権限を有する管理者用のパスワードは、一般ユーザのパスワードよりも頻繁に更新することが望まれます。

(ア) ルールの制定

パスワードを定期的に変更するルールを策定し、運用します。パスワードを日常的に変更できないシステムについては、点検時などにパスワードを変更するようにします。また、入退室管理や施錠管理などの物理セキュリティを強化し、許可されない人員が制御室に入退室できないようにします。

(イ) パスワード有効期限機能の利用

OSによっては、パスワードの有効期限を設定できるものもあります。この機能を利用することで、定期的にパスワードを変更することをユーザに促すことができます。

(ウ) 啓蒙活動の実施

ユーザに対してパスワード変更の重要性を説明し、定期的に変更するように呼びかけます。

【参考文献】

・IPA: パスワードの管理と注意
http://www.ipa.go.jp/security/fy14/contents/soho/html/chap1/pass.html
・JIS Q 27001「A 11.3.1 パスワードの利用」

3. パスワードとアカウント

補足　【設問 No.3-1】

ユーザによるパスワード管理の重要性について

技術的な対策（OSの設定など）により、パスワードの長さや有効期限を設定することが可能です。しかし、技術的な対策を用いて強力なパスワードを設定しても、そのパスワードを紙（付箋）に書いて操作端末の近くに貼っていては、パスワードを設定している意味がありません。各自が常にセキュリティ意識を持ち、日々の業務にあたることが重要です。

パスワードの管理施策について

管理者パスワードは、管理者以外の人員に知られないように管理する必要があります。その一方で、管理者不在時の緊急事態に備え、管理者以外の人員が管理者パスワードを知る手段を用意しておく必要があります。緊急時のパスワード管理について、封筒を用いた以下の手法があります。

＜封筒を用いたパスワード管理＞

①管理者が管理者パスワードを紙に書き、封筒に入れ封をする。
②封をした封筒を施錠できる棚にて保管する。鍵は部署にて厳重に管理する。
③非常時、棚から封筒を取り出し、封を切り、パスワードを使用する。
④パスワードの使用後、管理者はパスワードを変更する。
※定期的に封筒の封を確認し、開封されていた場合は、即座にパスワードを変更する。

パスワードを使用しない場合の代替施策について

制御機器の仕様や運用状況により、パスワードを用いたアクセス管理が不可能な場合があります。その場合、制御室（制御機器、または操作端末の設置場所）の入退室管理や施錠管理を強化し、許可のない人員から機器を保護します。入退室管理の施策については、【設問 No.1-1】をご参照ください。

補足　【設問 No.3-2】

パスワードを忘れないように紙に書き、操作端末の近くに貼っているケースが見られます。内部に不正者がいないとも限りません。このような行為は危険ですので、発見したら是正してください。
また、パスワードを解析するのは、人間とは限りません。パスワードを不正に取得する機能をもったソフトウエアやツールが存在します。そのようなソフトウエアは、キーボードからの入力を監視し記録します。またツールを用いて、辞書に登録されているような単語、数字や文字の組合せを解析し、ログインを試みます。これは、「辞書攻撃」、「総当たり攻撃」と呼ばれる攻撃手法で、簡単に推測できる文字や数字の組合せ、パスワードに多用される文字列などの場合、簡単にパスワードを解析されてしまいます。

覚えやすく強固なパスワードの生成方法について

パスワードは、数字や記号が混在し、文字数の多い無作為な文字列を使用することで、強固になります。しかし、そのようなパスワードは覚えにくく、扱いづらいという欠点があります。覚えやすく、強固なパスワードを生成する手法として、独自に決めたパスフレーズやパスワード生成ルールを使用する方法があります。その例を次ページに示します。

3. パスワードとアカウント　【設問 No.3-3】

＜パスフレーズを用いたパスワード生成法＞

自分が覚えやすい文章（フレーズ）から、長いパスワードを生成します。長いパスワードが使用可能なシステムに適用します。辞書に登録されているような文字列を使った場合でも、複数の単語を組合せることで、辞書攻撃への耐性を高くする。数字を組合せることで、より強固になります。

＜例＞ 覚えやすいフレーズから長いパスフレーズを生成
フレーズ　…「あるひ もりのなか くまさんに であった」
→ パスフレーズ　…「1Aruhi2Morinonaka3Kuma3ni4Deatta」

＜独自生成ルールを用いたパスワード生成法＞

あらかじめ独自のパスワード生成ルールを決めておくことで、覚えやすいフレーズや単語から無作為なパスワードを生成します。よく知られているフレーズや単語をもとに、独自のルールによって加工することで、推測しづらいパスワードを生成することが可能です。大文字、記号、数字が混在するようにルールを工夫することで、より強固になります。

＜例1＞ 覚えやすいフレーズから乱雑なパスワードを生成
フレーズ　…「あるひ もりのなか くまさんに であった」
ステップ1：「いち にち さん …」を数字に置換 →「あるひ もりのなか 9ま3に であった」
ステップ2：文節の先頭文字と数字を切り出す →「あ も 93 で」
ステップ3：ローマ字に変換 →「A Mo 93 De」

＜例2＞ 覚えやすい単語から乱雑なパスワードを生成
単語　…「2-propanol」
ステップ1：単語の先頭を大文字にする →「2-Propanol」
ステップ2：英字をアルファベット順に並び換える →「2-alnooPpr」
ステップ3：英字を母音、子音の順に並び換える →「2-lanoPopr」
※パスフレーズやパスワード生成ルールを作成する際、パスワードのもとになるフレーズや単語、生成ルールを他人に知られないように厳重に管理する必要があります。他人に知られた可能性がある場合は、もとになるフレーズや単語、生成ルールの変更が必要です。

補足　【設問 No.3-3】

パスワードの変更周期について

大小英数字（全62文字種）を組合せた8文字のパスワードの解析に要する時間は、以下の条件で考えた場合、250日と計算できます。この場合、1年に1回の変更では、変更する前に見つけ出される可能性があります。

＜計算条件＞

- 1秒間に1000万通りの組合せを試せる一般的なパソコンでパスワード解析ツールを使用。
- 大小英数字、8文字の文字列の組合せは、218兆3401億558万4896通り。
  一定回数、連続してログインに失敗した場合、一定時間ログインできないようロックしたり、ロック解除の手続きをしないとログインできないようしたりすることで、機械的な攻撃を抑止したり、解析時間を大幅に延ばしたりすることが可能です。

4. 対応能力の確立

【設問 No.4-1】

制御システムにおけるセキュリティの監視手順や
警報発生時や異常時の対応方法を理解し、
訓練をしていますか？

【設問 No.4-1】

制御システムにおける セキュリティの監視手順や 警報発生時や異常時の対応方法を 理解し、訓練をしていますか？

制御システムへの攻撃による被害を最小限に抑えるために、不正アクセスや攻撃を監視することが重要です。また、被害を拡大させないためにも、監視手順や警報発生時、異常時の対応方法を理解し、いざという時に慌てないよう訓練をしておくことが大切です。

背景・目的

現実社会の泥棒（空き巣）が侵入しやすい家を探したり、開けやすいドアを下調べたりするのと同様に、制御システムに対して悪意をもった者が対象となる制御システムに弱点がないか、事前に調査します。
弱点調査の手口はさまざまですが、ネットワーク装置やサーバなどの機器に記録されたログ（アクセスログやイベントログなど）を分析することで、攻撃者がどのような調査を行っているのかを把握することができます。さらに、どこまで侵入され、どのような操作が行われたのか推測することが可能です。また、不審なアクセスを検知すると同時に、それに迅速に対処することができれば、重要なデータの窃取や制御系プログラムの不正な書き換え、不正操作によるシステム停止などを回避することができます。
不審なアクセスを検知した場合や攻撃を受けている最中に迅速かつ正確に対処できるよう、対応方法を理解し、定期的にその方法（手順）を用いて訓練しておくことが重要です。

想定されるリスク

不正アクセスなどのセキュリティ事故・事件を監視するための手順や、警告発生時や異常時の対応方法があっても、一度も実施したことがなければ、緊急時に的確に対応できる保証はありません。
攻撃されているかもしれないと気付いても、何もできずに時間だけが過ぎていくのでは被害が拡大するばかりです。誤った対応や措置によって、二次的な被害や事故につながることもあります。
地震や火災などの避難訓練と同様、事前に一連のプロセスを体験しておくことが重要です。

内容解説・施策例

(ア) 監視手順の理解

セキュリティの監視は、ログの監視から不審な配線やネットワーク機器の接続などの物理的な監視までを監視事項とします。一般的な監視事項として、以下に示すものがあります。組織の監視手順に従い、監視を実施します。

＜一般的な監視事項＞

・ファイアウォール、サーバのアクセス記録およびイベントログ
・ログイン/ログアウト時間(監視ポイント:通常ログインしない時間帯のログイン記録)
・パスワードの変更ログ(監視ポイント:身に覚えのない変更の有無)
・アクセス権限のないユーザによる情報へのアクセスログ
・制御システムにおける各種操作ログ
・侵入検知システムのログ
・制御室(制御機器または操作端末の設置場所)など、重要な制御装置の管理区域への入退室記録
・配線やネットワーク機器(ルータやスイッチングHUBなど)の不正接続
・ネットワークの負荷状況の変化(監視ポイント:通常時と比較して、非常に高い負荷の発生)
・不正プロセスが動作していないこと

(イ) 警報発生時や異常時の訓練

実環境で訓練を行うと、稼動しているシステムに影響を及ぼす恐れがあるため、訓練用として、別途、実環境と同等の環境を用意することが理想的です。訓練用の環境を用意することが困難な場合は、システムに影響を及ぼさない範囲で実環境の設定を変更する方法もあります。また、実施したつもりで、実際に行う操作を端末や装置の前で確認しておくだけでも、異常発生時に初めて手順書を見て作業をするよりは、訓練としての効果があります。

【参考文献】

・JIS Q 27001「A 10.6 ネットワークセキュリティ管理」
・JIS Q 27001「A 10.10 監視」

4. 対応能力の確立

補足　【設問 No.4-1】

正確な時刻の設定について

ネットワーク装置やサーバなどの各監視対象機器から収集したログを分析する際には、ログを記録した時刻をもとに因果関係や事象の発生順序などを分析していきます。そのため、各監視対象の機器は、正確な時刻に設定しておくことが大切です。正確な時刻を設定するために電波時計やGPSを利用する方法、タイムサーバと呼ばれるNTPサーバと時刻を同期する方法などがあります。

セキュリティ監視のための製品、サービスについて

下記のようなセキュリティを監視するための製品やサービスがあります。

(ア)ファイアウォール(FW:Firewall)

外部との通信を監視し、必要な通信だけを通すためのソフトウエア、またはハードウエアです。

(イ)不正侵入検知システム(IDS:Intrusion Detection System)

不正な通信を検知する機能をもったソフトウエア、またはハードウエアです。不正な通信を遮断する機能をもった製品もありますが、不正侵入検知システムは、不審だと判断してからファイアウォー ルの設定を変更し、通信の遮断を行います。そのため、遮断した時には盗んだデータは送信先に届いており、攻撃が成功してしまっている場合もあります。

(ウ)不正侵入防御システム
(IPS:Intrusion Prevention System ／ Intrusion Protection System)

不正な通信を遮断する機能をもったソフトウエア、またはハードウエアです。通信するデータが正当なものだと判明するまでは宛先にデータを転送しないため、不審なデータの送信であると検知さえすれば、攻撃が宛先に届くことはなく防御することができます。ただし、誤検知によって正常なアクセスを遮断してしまったり、不正なアクセスを許可してしまったりする可能性があります。そのため、ネットワークの利用に影響を与えないようにしつつも高い検知精度が求められます。

(エ)統合脅威管理(UTM:Unified Threat Management)

ファイアウォールの機能に加え、ウイルスチェック、不正侵入検知・防御などの機能を搭載した統合的なセキュリティ装置です。制御装置や制御用サーバにウイルスチェック用のソフトウエアを導入できない場合にUTM製品が代わりに使われるケースもあります。

(オ)セキュリティ監視のアウトソーシング

セキュリティ関連のログの収集、管理、分析には、ネットワークやシステムの知識だけでなくセキュリティに関する知識も求められます。ログを分析する場合は、ファイアウォールなど、一箇所のログだけを使うのではなく、不正侵入検知システムやサーバ機器のほか、場合によっては制御装置のログなどを使ってイベントの因果関係を意識しながら不正アクセスの痕跡を分析していく必要があります。このように、ログによる監視には、高いスキルと作業時間(量)を要することもあるため、セキュリティ監視をサービスとして提供している事業者にアウトソーシングするという選択肢も有効です。また、セキュリティ監視サービスの多くは、同様の事例のノウハウをもっており効率的な分析が期待できます。アウトソーシングでは、24時間365日、専用回線を使って、セキュリティ監視センターへ必要な監視ログを送信し、監視スタッフが分析結果を報告したり、警報発生時や異常時に通信を遮断したりするなどのサービスを提供しています。

5.サード・パーティーリスクの管理

【設問 No.5-1】

リモート接続のセキュリティを
確保するためのルールを守っていますか？

【設問 No.5-1】

リモート接続のセキュリティを確保するためのルールを守っていますか？

ウイルス感染や情報漏えいを防止するために、制御システムを外部に接続する（リモート接続）際のルールを遵守することが重要です。ここでいうリモート接続とは、制御システムの機器や管理コンソールを、インターネットに接続すること、インターネットに接続されたPCやサーバに接続することを言います。

背景・目的

制御システムにリモート接続することで、ウイルス感染、情報漏えい、外部からの不正な操作などのリスクが発生します。制御システムの機器でメールを読んだり、Webにアクセスできなくても、それが可能なPCやサーバと機器が接続された状態は、インターネット上からPCなどを経由して制御システムの機器にアクセスする手段が確保されたことになります。制御システムが機能を実現するために別拠点の制御システムと通信するような場合に、接続回線にインターネットを利用するときも同様のリスクが発生します。制御システムがインターネット上のデータベースやWebサービスを利用している場合も注意が必要です。

リモート接続は、極力行わないようにし、業務上の理由により、リモート接続を行う場合には、その必要性を十分に確認します。リモート接続は、接続範囲を最小限にとどめ、接続時の承認手順やウイルス感染や情報漏えいの防止策を行い、厳重に管理することが重要です。

想定されるリスク

リモート接続により、外部から制御室（制御機器または操作端末の設置場所）内の機器へのアクセスが可能となります。その結果、ウイルス感染、不正操作や情報漏えいなどの被害を受ける恐れがあります。

内容解説・施策例

リモート接続の管理策として、次のような施策があります。

（ア） ルールの策定

リモート接続に関するルールを策定し、周知・徹底します。

①リモート接続の申請、承認、廃止手順を規定する。
②接続先の要件を規定する。必要に応じて、接続前の審査手順、接続先ネットワークの制限（社内LAN、インターネットへの接続禁止など）、接続機器の制限、接続プロトコルの制限を規定する。
③定期的に各接続の必要性を見直し、不要となった接続は廃止する手順を規定する。
④接続先とのセキュリティに関する契約要件を規定する。必要に応じて、機密保持契約、念書の提出、セキュリティ事故・事件発生時の対応手順と補償範囲を規定する。
⑤リモート接続の技術的な要件を規定する。必要に応じて、通信認証要件、端末認証要件（デジタル証明書の使用）、ファイアウォールの設定要件、アカウント・パスワードの管理要件、通信機器の管理要件を規定する。また、通信記録や操作記録が確認できるようログなどの設定を規定する。

（イ） 接続を最小限にする

リモート接続の目的や作業内容などを十分に検討し、接続相手、接続対象機器、接続時間、接続対象プロトコル、接続帯域（回線速度）、接続先に付与する権限などを最小限に制限します。

＜例＞
①通信機器（ルータなど）のMACアドレスフィルタ、IPアドレスフィルタ機能を使用し、接続対象機器を制限する。
②通信機器のプロトコルフィルタ機能を使用し、通過プロトコルを必要最小限に設定する。
③常時接続の必要がない場合、使用時以外は通信機器の電源を切るなどして、物理的に回線を遮断する。（外部からの攻撃リスクが低減できます。）
④接続の目的や作業範囲を確認し、制御システムの操作権限などを最小限に設定する。通信機器や制御機器の管理権限など、過剰な権限をリモートユーザに付与しないようにする。

（ウ） 通信記録の確認

リモート接続の開始前や終了後、または定期的に通信機器のログや操作対象の制御機器のログを確認し、ルールが遵守されていること、不要な操作や通信が行われていないこと、および機器や通信に異常がないことを確認します。問題を発見した場合は、速やかに原因を調査し、対策に取り組みます。

【参考文献】
・JIS Q 27001「A 10 通信及び運用管理」
・JIS Q 27001「A 11.4.2 外部からの接続する利用者の認証」

補足　【設問 No.5-1】

リモート接続によるリスクの管理について

接続先は、SLAや契約書だけでは「管理不能である」と想定し、あらゆるリスクや対策について検討しておく必要があります。

＜検討すべき事項の例＞

・接続先の機器がウイルスに感染した場合の影響と制御システムの安全性確保対策
（安全性確保のため、ルータやファイアウォールなどの設定内容を規定する。）
・悪意をもった者が接続先の機器を操作した場合の影響
・異常状態の早期発見手順（通信機器や接続対象機器の監視を行う。）
・リモート接続による情報漏えいのリスク
・リモート接続での作業時に通信回線異常が発生した場合の影響と対応手順
・通信回線の応答速度の低下、または遮断した場合の影響と制御システムの安全性確保対策

ノートPCやリモート端末からの接続について

この設問では、主に制御システムが外部の機器やサービスに接続する際の問題点や対策について解説していますが、リモート接続には、外部の端末から制御システムにアクセスして遠隔操作を行ったり、メンテナンスを行ったりする場合もあります。モバイルデバイスの普及により、スマートフォンから制御システムを監視したり操作したりできるシステムも、今後は増えてくる可能性があります。必要に応じて、このようなリモート接続のセキュリティ対策やルールの策定をお奨めします。

6. 継続的な評価と改善

【設問 No.6-1】

定期的に本 J-CLICS
（または、社内、業界団体などにて
作成されたチェックリスト）を用いて
制御システムセキュリティの自己評価を行っていますか？

【設問 No.6-1】

定期的に本J-CLICS（または、社内、業界団体などにて作成されたチェックリスト）を用いて制御システムセキュリティの自己評価を行っていますか？

セキュリティの維持と向上のため、定期的にセキュリティの自己評価を行い、関連する文書（ルール・手順書・管理台帳など）やセキュリティ施策の更新を行うことが重要です。

背景・目的

セキュリティ施策の有効性は、業務や組織の変化、技術の進歩、新たな攻撃手法の発見などにより、日々変化します。セキュリティ施策の有効性を維持するために、PDCA（Plan:計画-Do:実行-Check:点検-Act:処置）サイクルによる定期的なチェックと改善が重要です。また、技術の進歩により、コストの低い対策方法が選択できる場合もあります。セキュリティ管理の効率化やコスト削減のためにも、定期的にセキュリティの自己評価と見直しを行うことが大切です。

想定されるリスク

実情に合わないルールや文書、新たな攻撃手法が発見され、陳腐化したセキュリティ施策を放置すると、それらが弱点となり、攻撃や運用上の混乱を招きます。その結果、制御システムの稼働に悪影響を与えるリスクが高くなります。また、陳腐化したルールや施策を放置することは、最新の攻撃に対して無力というだけでなく、無駄なコストの要因にもなります。

6. 継続的な評価と改善　【設問 No.6-1】

内容解説・施策例

定期的にセキュリティの自己評価を行い、施策の見直しおよび更新を行います。

（ア） ルールの策定

定期的にセキュリティ自己評価を行うためのルールを策定し、実施します。

①セキュリティの評価と見直しを行う責任者を選定する。
②自己評価を行うタイミング（毎年、システム更新時、定期点検時、セキュリティ事故・事件発生時など）を定める。

（イ） セキュリティ自己評価の実施

本チェックリスト（または、社内、業界団体などにて作成された、J-CLICS同等のチェックリスト）を用いて、自己評価を行い、結果を文書化します。また、下記項目を明確にします。

①各チェック項目の評価結果と評価理由
②各チェック項目に対する施策内容と実施状況
③未対応項目の理由と対応予定

（ウ） セキュリティ施策の評価と見直し

セキュリティ施策の内容や効果を評価し、見直しを行い、必要に応じて、更新します。

＜評価ポイントの例＞
・実際にセキュリティ施策は運用されているか
・セキュリティ施策は有効に機能しているか
・セキュリティ施策の費用は妥当か
・セキュリティ施策が業務に与える影響は妥当か
・より効果的またはコストの低い施策はないか
・ルールや文書の内容は現状の業務・システム・組織・人員体制と合致しているか

【参考文献】
・JIS Q 27001「A 5.1.2 情報セキュリティ基本方針のレビュー」

6. 継続的な評価と改善

補足　【設問 No.6-1】

セキュリティ施策の評価方法について

セキュリティ施策の評価指標として、セキュリティ事故・事件の発生件数や事故発生時の対応時間・コストなどを記録する方法があります。実際にセキュリティ事故・事件が発生していない場合は、セキュリティ事故・事件が発生した場合を想定し、被害や対応手順、対応時間・コストなどを検討し、施策がある場合とない場合とで比較することにより、評価する方法があります。

付録 A

情報セキュリティ関連参考文献

情報セキュリティ関連参考文献

情報セキュリティついてさらに知識を得る際に参考になる文献やWebサイトを紹介します。
(文中のWebサイト情報(URL)は2013年1月時点のものです。)

1. 情報セキュリティ関連情報

・JPCERT/CC　ホームページ
https://www.jpcert.or.jp/ics/
https://www.jpcert.or.jp/
制御システムセキュリティに関するガイドライン・規格などの文献、関連ツール、講演資料、情報共有コミュニティなどのコミュニティや、注意喚起情報、脆弱性関連情報などのインシデント対応に役立つ情報が入手できます。また、インシデント発生時の対応依頼受け付けページなどを提供しています。

・JPCERT/CC制御システムセキュリティ関連情報
https://www.jpcert.or.jp/ics/ics-community.html
制御システムセキュリティコミュニティの参加者に、JPCERT/CC が収集・整理した情報、制御システムのセキュリティに関するニュース・動向、脅威に関する事例、標準・規準などの参考情報などを提供しています。

・独立行政法人情報処理推進機構(IPA) ホームページ
http://www.ipa.go.jp/security/index.html
情報セキュリティに関する緊急対策情報や、情報セキュリティ対策に関する資料、セミナー・イベントの情報、届出・相談窓口などの情報、ソフトウェア・エンジニアリング、を提供しています。

・IPA 制御システムのセキュリティ
http://www.ipa.go.jp/security/controlsystem/index.html
重要インフラなどに用いられる制御システムのセキュリティ関連情報を提供しています。

2. 規格・ガイドライン

・日本規格協会、平野芳行、水本政宏、吉田健一郎 共著

・ISO/IEC 17799:2005 (JIS Q 27002:2006) 詳解 情報セキュリティマネジメントの実践のための規範
日本規格協会　中尾康二、平野芳行、吉田健一郎、中野初美 共著
情報セキュリティマネジメントに関するJIS規格「JIS Q 27002:2006」の解説書籍です。情報セキュリティマネジメントで行うべき施策について解説されています。

・グッド・プラクティス・ガイド　プロセス・制御と SCADA セキュリティ
Center for Protection of National Infrastructure(CPNI)著、JPCERT/CC邦訳
https://www.jpcert.or.jp/ics/information02.html
プロセス制御と SCADA システム セキュリティの必要性を概説し、プロセス制御や、SCADA システム セキュリティとITセキュリティの間の違いを明らかにした上で、プロセス制御システム・セキュリティに対応するための7つのステージを示し、各ステージにおけるグッド・プラクティスの原則を示したドキュメントです。

・日本版SSAT(Scada Self Assessment Tool)
Centre for Protection of National Infrastructure(CPNI)開発著、JPCERT/CC日本版開発
https://www.jpcert.or.jp/ics/ssat.html
英国のCPNIが開発したSCADAを用いた監視・制御システム向けのセキュリティ自己評価ツールを日本向けにJPCERT/CCが開発したものです。グッド・プラクティス・ガイド「プロセス・制御と SCADA セキュリティ」と併用することでより深い理解が得られます。

3. 脆弱性に関する情報

・脆弱性対策情報ポータルサイト：JVN (Japan Vulnerability Notes)
https://jvn.jp/
IPAとJPCERT/CCが共同で運営している脆弱性情報提供サイトです。日本で使用されているソフトウエアなどの脆弱性関連情報とその対策情報、製品開発者の対応状況を提供しています。また、JPCERT/CC が製品開発者との調整を行った脆弱性関連情報および協力関係を結んでいる米国 CERT/CC の Technical Cyber Security Alerts や Vulnerability Notes 、英国 CPNI の CPNI Vulnerability Advice を掲載しています。

・Common Vulnerabilities and Exposures (CVE)
http://cve.mitre.org
CVEを運営管理する米国MITRE社が運営している脆弱性情報提供サイトです。ソフトウエアなどの脆弱性に関する情報を提供しています。各脆弱性情報には識別番号CVE-IDが付けられており、このIDが国際的に使用されています。

・Industrial Control Systems Cyber Emergency Response Team(ICS-CERT)
http://www.us-cert.gov/control_systems/ics-cert/
ICS-CERTは、米国国土安全保障省(DHS)が運営する制御システムを対象としたインシデント対応組織です。ICS-CERTのサイトでは、制御システムセキュリティに関するニューズレターやアドバイザリ、レポートなどの情報を提供しています。

4. 情報セキュリティ政策に関する情報

・経済産業省
http://www.meti.go.jp/policy/netsecurity/index.html
経済産業省 商務情報政策室 情報セキュリティ政策室のセキュリティ政策に関する情報を提供するサイトです。セキュリティに関する政府方針の情報や各種報告書、ガイドラインなどなどが掲示されています。

・内閣官房情報セキュリティセンター (NISC)
http://www.nisc.go.jp
内閣官房情報セキュリティセンターのサイトです。各種会議資料や注意喚起文書、セキュリティに関する調査報告書、関連法令に関する情報などが掲示されています。

・総務省
http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/index.html
総務省の情報セキュリティ政策に関するサイトです。セキュリティに関する調査報告書や広報文書などが閲覧できます。

・警察庁
http://www.npa.go.jp/cyber/
警察庁のサイバー犯罪対策に関するサイトです。サイバー犯罪の予防・取締りに関する取り組みの情報や、サイバー犯罪に関する統計情報、サイバー犯罪の相談窓口などの情報が掲示されています。

著作権・引用や二次利用等について