J-CLICS
設問項目ガイド

STEP
2

── 制御システムの技術担当者／管理者の方へ ──

一般社団法人 JPCERT コーディネーションセンター

2013年3月27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

1. システムとビジネスリスクの理解

【設問 No.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？

制御システムに関係するビジネスリスクを理解し、軽減するためには、制御システムのシステム構成を把握しておくことが重要です。また、障害発生時の原因の速やかな特定および対応策の実施のため、システムの変更履歴を含め最新の状態を管理することが必要です。

1

1. システムとビジネスリスクの理解　【設問 No.1】

背景・目的

制御システムに関係するビジネスリスクとしては、停電、故障、地震、火事などの災害による制御システムの操業やサービス提供の中断、設備の暴走などによる人命を含む物理的な事故の引き金、業務上の秘密情報の漏えいなどが考えられます。

制御システムに関係するビジネスリスクの発生回避、また発生時の迅速な対応のために、ビジネスリスクをもたらす要因を正確に分析・評価し、適切な対応策を検討・実施することが重要です。そのためには、制御システムのシステム構成を把握し、定期的に制御システム（オペレーティングシステム（以下「OS」と記す）やソフトウエアを含む）の棚卸と評価を実施します。そして、どんなシステムが存在しているか、機能、重要な業務 / 安全性、設置場所、所有者、サポート担当者などを記載した管理台帳を作成し、最新の状態を管理しておくことが重要です。
システムの最新の状態が管理されていると、想定される影響やサポート担当者への迅速な対応、早期復旧方法を把握することにより、ビジネスリスクを最小限に抑えることができます。

想定されるリスク

制御システムの管理台帳がない、または最新の状態で管理されていない（システム構成への変更を管理台帳に反映してない）場合、前述のような各種の障害、災害（自然災害のみならず、不正アクセスなどの人的災害を含みます）への対策が不十分になり、システム構成変更時の思わぬ副作用や、不具合発生時の原因追求までの遅延、対策漏れなどにより、ビジネスそのものへ大きな影響を及ぼす恐れがあります。

1. システムとビジネスリスクの理解　【設問 No.1】

内容解説・施策例

システム構成の管理策として、次のような施策があります。

（ア） 管理台帳の作成、管理

制御システムを構成する資産の管理台帳を作成し、各資産の管理責任者を特定します。また、各機器・ソフトウエアに対する脅威、脅威につながる脆弱性を把握し、それらに起因する障害が発生した場合の業務への影響を理解します。

ここでは、システムを構成する資産の管理台帳に記載する内容の例を紹介します。管理台帳を作成する際、制御システムに関係するすべての機器やソフトウエアを洗い出し、その重要度を把握します。管理台帳に書き込む情報としては、以下の項目があげられます。

- 機器、ソフトウエアの管理責任者（資産の所有者、管理者名など）
- 機器、ソフトウエアの形態（形式、バックアップメディア、ライセンスなど）
- 機器、ソフトウエアの接続状況（使用インターフェース、接続機器名、接続図、VLAN※1 設定情報など）
- 機器、ソフトウエアにおける変更記録（設定変更、バージョンアップなど）
- 設置（保管）状況
- 設置（保管）場所
- 設置（保管）期間
- 用途
- 利用者範囲
- システムアカウント所有者リスト
- 破棄方法
- 災害から復旧に必要な情報
- 他のシステムなどとの依存性
- ネットワーク構成図

※1　Virtual LAN: スイッチングハブの内部で複数のネットワークに分割する機能。どの様に分割したかの設定情報を明確にしておきます。

システム構成を変更する際の管理台帳への反映や定期的な見直しを行い、最新の状態で管理していくことが、制御システムを理解するとともに、脅威や脆弱性の識別（【設問№2】参照）の手助けにもなります。

【参考文献】

・独立行政法人 情報処理推進機構（IPA）「情報セキュリティ」
http://www.ipa.go.jp/security/index.html
・ISMS ユーザーズガイド（リスクマネジメント編）
http://www.isms.jipdec.or.jp/isms.html
・JIS Q 27001「A 7.1.1 資産目録」
・JIS Q 27001「A 7.1.2 資産の管理責任者」

2.脅威の理解

【設問 No.2】

制御システムの各構成要素について、想定される脅威を把握していますか？

制御システムに関係するビジネスリスクの発生を回避するには、制御システムを構成する各要素において、どのような攻撃や障害が生じうるのか把握し、脅威に対しての対策を検討することが重要です。

2. 脅威の理解　【設問 No.2】

背景・目的

制御システムの管理者は、そのシステムへの脅威と脆弱性を把握し、考えられるリスクを評価します。そして、そのリスク発生への対応を検討することが必要です。
例えば、制御システムへの脅威には何があるのか（停電、不正アクセスなど）、脆弱性は何があるのか（電源設備のメンテナンス不足、不適切なパスワード管理など）、影響度はどの程度なのか（高い、低い）を把握し、最終的なリスク対応を検討します。その検討を通じて、各構成要素の対策優先順位を決めることにもつながります。

想定されるリスク

このような制御システムの構成要素に対する脅威・脆弱性の把握やリスク対策を行わない場合、ビジネスそのものに対して大きな影響を及ぼす恐れがあります。

2. 脅威の理解　　【設問 No.2】

内容解説・施策例

システム構成の管理策として、次のような施策があります。

（ア） 脅威の把握

制御システムの各構成要素につき、脅威を識別します。
ここでの「脅威」は、制御システムや組織・ビジネスに損失や損害をもたらす事故の原因を指します。どのような脅威があるのか（地震、洪水、火事、停電、盗難、ほこり、記録媒体の劣化、ソフトウエア故障、不正アクセス、情報漏えい）を抽出し、その脅威の中からセキュリティに関連する項目を特定し、分類します。脅威は、故意による脅威・偶発的な脅威・環境による脅威に分類されます。

＜脅威と対策の例＞
・故意による脅威
　脅威として、内部関係者の情報漏えいなどがあります。この場合は、教育の実施などによる対策が考えられます。
・偶発的な脅威
　脅威としては、入力ミスや操作ミスがあります。この場合は、二重入力する、確認フローの追加などの対策が考えられます。
・環境による脅威
　脅威としては、地震や火事が一例としてあげられます。この場合は、免震床やバックアップメディアの分散管理、制御システムの二重化などによる対策が考えられます。

（イ） 脅威の評価と対策

前記の「脅威の把握」で識別された脅威の分類にもとづき、リスク評価とリスク対応（適切な電源対策、不正アクセス対策など）を検討し、実施します。また、個々の脅威と分類されたものにもとづき、リスクの優先順位を考え、優先順位を考慮した対策を行います。
例えば、「不正アクセス」という脅威に対しては、リスクとして「不正操作」「データの改ざん」などがあげられます。このリスクへの対策として、「ファイアウォールの設置、アクセス制限の強化」などがあります。
これらの脅威すべてにつき、対策を実施することは理想的ですが、予算や実施時期の関係を考慮し優先順位付けを行った効果的な対策を検討することが重要です。

なお、「不正アクセス」「ウイルス」については、制御システムの「ネットワーク・アーキテクチャ」の設問内容を把握した上で、ファイアウォールの設定やウイルス対策を行います。

【参考文献】
・独立行政法人 情報処理推進機構（IPA）「情報セキュリティ」（ウイルス対策、ボット対策、不正アクセス対策など）
　http://www.ipa.go.jp/security/index.html

3. ネットワーク・アーキテクチャ

【設問 No.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？

システムの状況を把握するために、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、接続仕様を記載した管理台帳を作成します。管理台帳を作成する際、【設問 No.1】で作成した管理台帳へ通信や接続の仕様に関する項目を追加すると、より効率的です。また、管理台帳を一つに纏めることで、資産管理を簡素化できます。

3

3. ネットワーク・アーキテクチャ　【設問No.3】

背景・目的

制御システムのネットワークセキュリティを確保するためには、まず、制御システムの通信仕様、接続仕様を把握することが重要です。制御システムに接続されている機器の名称、目的、管理者、通信仕様、接続仕様などを把握し、管理台帳を作成します。管理台帳は、セキュリティリスクの評価や対策の検討に使用できます。また、許可されていないシステム変更の監査にも有用です。システム接続や通信の正常状態を把握することは、システム異常の解析やセキュリティインシデント発生時の検討資料としても使用できます。

想定されるリスク

制御システムに接続されている機器の通信仕様、接続仕様を把握していないと、システムの正常状態が正しく把握できず、システムの異常の検出が十分に行えない恐れがあります。
例えば、許可されない機器の接続や通信の変更が放置される恐れがあります。その結果、ウイルス感染や侵入経路、予期せぬ不具合の原因となり、操業停止などの重大な事態につながる恐れがあります。

内容解説・施策例

制御システムに接続されているすべての機器について、通信仕様、接続仕様の管理台帳を作成します。作成にあたっては、システム構築に携わったベンダに問い合わせ、最新情報を含んだ管理台帳を提出してもらうことが推奨されます。

＜管理台帳の項目例＞
・通信名称
・通信目的
・使用プロトコル名
・使用ポート番号
・使用タイミング（運転時、メンテナンス時など）

この管理台帳を用いて、接続状況の監査やセキュリティ対策の検討を行います。監査では、接続の必要性を再検討し、必要のなくなった接続や通信は放置せずに廃止し、接続の取り外しや通信ポートの閉鎖設定を行います。

【参考文献】
・独立行政法人 情報処理推進機構（IPA）「情報セキュリティ」
http://www.ipa.go.jp/security/index.html

4.ファイアウォール

【設問 No.4】

制御システムと他のネットワークの境界にファイアウォールを設置し、不要な通信を遮断していますか？

ネットワークに接続された制御機器への許可されないアクセスやウイルス感染を防止するため、制御システムと他のネットワークの境界にはファイアウォールを設置して不要な通信を遮断します。

4

4. ファイアウォール　【設問No.4】

背景・目的

ネットワーク接続は、必要な通信手段であると同時に攻撃やウイルスの侵入経路にもなります。そのため、制御システムのネットワークは、イントラネットやインターネットなどの外部ネットワークに接続しないほうが安全です。業務上の理由により、制御システムのネットワークを他のネットワークに接続する場合には、ネットワークの境界にファイアウォールを設置して、必要な通信のみを通過させるようにします。

想定されるリスク

ファイアウォールを設置せずに外部ネットワークとの接続を行うと、外部からの攻撃を受けたり、ウイルス感染したりします。

4. ファイアウォール　　【設問No.4】

内容解説・施策例

ファイアウォールはセキュリティ向上に有用ですが、適切に設定・運用しないと、かえってシステムの異常動作の原因になったり、期待した効果が得られなかったりすることがあります。
設置や設定にあたっては、事前に十分な調査・検討を行うことが重要です。制御システムベンダに相談・問い合わせしてアドバイスを受けることも有効です。以上を踏まえた実施内容の例を次に示します。

（ア） 他のネットワークとの接続の必要性の精査

制御システムのネットワークをイントラネットやインターネットなどの他のネットワークと接続すると、そこからの攻撃や侵入を受ける恐れがあります。他のネットワークとの通信を行う場合には、接続の必要性を再検討し、必要のなくなった接続や通信は放置せずに廃止し、接続の取り外しを行います。

（イ） ファイアウォールの設置

他のネットワークと接続する際には、その境界にファイアウォールを設置して必要な通信のみを通過させるようにします。設置にあたっては次の点に留意します。

①制御機器ベンダに推奨の構成や設定を問い合わせる。

ファイアウォールで制御機器関連の通信を通過させる場合は、制御機器ベンダに当該機器の通信仕様を問い合わせ、推奨するファイアウォール機器や設定がある場合にはそれを使用します。

②ファイアウォールを不正アクセスから保護する。

ファイアウォールの設定変更や接続変更は、管理者のみが行うようにします。そのため、ファイアウォールは鍵付きのラックなどに格納して物理的に保護し、ネットワーク経由での設定機能も極力使用しないようにします。また、管理者パスワードは、デフォルト値から変更せずに使用していると、容易に攻撃されてしまう恐れがあるので、変更することをお奨めします。これにより、不正アクセスによる設定変更を防止します。

【参考文献】

・独立行政法人 情報処理推進機構（IPA）「情報セキュリティ」
http://www.ipa.go.jp/security/index.html

5. システム監視

【設問 No.5】

平常時にも
制御システムの稼働状況やログを
定期的に確認・分析していますか？

平常時から制御システムの稼動状況やログを確認・分析し、通常の状態を把握し、異常事態にいち早く気づけるようにすることが重要です。

5

5. システム監視　　【設問No.5】

背景・目的

ウイルス感染や機器故障により制御システムに生じる異常に早期に気づくために、制御システムの稼働状況やログを確認・分析することが重要です。制御システムの運用に影響が出る前に異常に気付き、異常が現れた場合でもサポート担当者との迅速な対応に向けた情報収集ができれば、操業への影響を最小限に抑えられる可能性があります。そのためにも、普段から制御システムのCPU 負荷、メモリの使用量、ハードディスクの空き容量、ネットワークの通信状況、制御システムのOS が出力するログなどを確認し、異常の兆候にいち早く気付くための体制や意識が必要です。

想定されるリスク

平常時に制御システムの定期的な確認を行っていないと、正常なのか異常なのかを的確に判断することができず、異常の兆候を見逃しかねません。その結果、制御システムの動作に影響が出るまで異常に気付かず、最終的に、操業停止などの重大な事態につながる恐れがあります。

5. システム監視　　【設問No.5】

内容解説・施策例

システムの異常を早期に発見するために、ログやシステムの稼働状態を日常的に確認します。具体的には、次のような項目の使用率や空き容量を確認・分析します。

・CPU負荷
・メモリ使用量
・HDD空き容量
・ネットワーク通信状況
・システムログ
・プロセス/サービス稼働状況
・ログイン/ログアウト記録

これらを記録し、状態を確認することで平常時の傾向が把握しやすくなります。
ツールを使用する場合には、稼動状況の表示だけでなく履歴記録ができるツールを選定すると便利です。稼動状況の記録は異常時の解析資料としても有効です。
制御システムの状態を確認するには次の手段があります。

（ア） 制御システムベンダが推奨する方法

システムの稼動状況の確認や分析、記録について、制御システムベンダが推奨する方法がある場合にはそれを使用します。

（イ） OSに付随するツール

OSに付随するツール（Windowsのタスクマネージャなど）を使用するとシステムの稼動状況に関する情報が得られます。

（ウ） 専用のツール

システムを監視するための市販ツールなどを使用する方法もあります。また、監視ツールを利用する際には、制御システムへの影響をテストしたうえで導入します。システムの稼動状況を表示するだけでなく、履歴を記録できるツールを選定すると有効です。

【参考文献】
・独立行政法人 情報処理推進機構（IPA）「情報セキュリティ」
http://www.ipa.go.jp/security/index.html
・JIS Q 27001「A 10.10 監視」

6.ウイルス対策

【設問 No.6】

制御システムに
ウイルス対策を行っていますか？

制御システムへのウイルス感染被害を可能な限り抑止するために、
何らかのウイルス対策を行うことが推奨されます。

6

6. ウイルス対策　【設問 No.6】

背景・目的

近年、制御システムにおいても汎用 OS が導入され、また業務上の理由（制御システムと他のシステムとのデータ連携など）で、他のネットワークと接続されるようになるのに伴い、ウイルス感染の危険性が高まっています。制御システムがウイルスに感染すると、システムの異常動作や停止につながる恐れがあります。そのため何らかのウイルス対策を行う必要があります。
ウイルス対策の方法によっては、システムの動作に影響が出る場合があるため、ウイルス対策の計画・実施にあたっては、あらかじめ制御システムベンダに問い合わせてベンダが推奨する方法で実施します。

想定されるリスク

制御システムがウイルスに感染すると、制御システムが機能不全を起こし、操業やビジネスに大きな影響を及ぼす恐れがあります。

6. ウイルス対策　【設問 No.6】

内容解説・施策例

ウイルスの感染を防止するためには、外部からウイルスを持ち込まないように管理することが重要です。制御システムについては、他のネットワークから、極力分離し、ウイルスなどへの感染の機会を減らすことが有効です。業務上の理由により、制御システムと他のネットワークを接続する場合には、ファイアウォールなどを導入して不要な通信を制限することでウイルス感染を抑止します。また、USB メモリなどの外部記憶媒体を用いて、制御システムとデータ連携を行う場合には、ウイルス検査などの対策を行うことが推奨されます。なお、制御システム製品によっては、ウイルス対策のためのシステムの設定強化や追加ソフトウエアが用意されている場合もあります。
その一方で、制御システムによっては、ウイルス対策ソフトなどの対策が導入できない場合があります。また、制御システムでは、システムの停止や再起動が容易に行えない場合もあるため、パッチの適用やソフトウエアの更新などの変更が困難な場合があります。このような場合には、ウイルス対策ソフトは導入せず、制御システムそのものを分離して管理する方法もあります。

ウイルス対策としては、ネットワーク経由での感染対策・持込み媒体経由での感染対策・制御システム PC 上での対策などの施策があります。
ウイルス対策の方法によってはシステムの動作に悪影響を及ぼす場合がありますので、対策の計画・実施にあたっては、制御システムベンダに問い合わせて、ベンダの推奨する方法で行うことをお奨めします。

（ア） ネットワーク経由での感染対策

ネットワーク経由でのウイルス感染を防止する対策として、不要なネットワーク接続の除去、常時使用しないネットワーク接続の切断（ネットワーク機器の電源 OFF など）、ファイアウォールの設置や設定強化などがあります。

（イ） 持ち込み媒体経由での感染対策

USB メモリや持ち込み PC 経由でのウイルス感染を防止する対策として、媒体持ち込みの制限、媒体内の不要なファイルの削除、持ち込み時のウイルスチェックなどがあります。

（ウ） 制御システム PC 上での対策

制御システム PC 上でのウイルス対策として、機器の施錠管理、不要接続ポート（USB ポートやネットワークポート）の封鎖、常時使用しない機器の切断（電源 OFF など）、ウイルス対策ソフトの導入、OS やソフトウエアの設定強化（ハードニング※2）、プログラム起動制限などのセキュリティ対策ソフトの導入などがあります。

※2　詳しくは、【設問 No.8】を参照。

【参考文献】

・独立行政法人 情報処理推進機構（IPA）「ウイルス対策のしおり」
http://www.ipa.go.jp/security/antivirus/shiori.html

7.セキュリティパッチ

【設問 No.7】

制御システムおよびシステム上で稼働しているアプリケーションのパッチの適用について、適用に伴う不具合による業務への影響も勘案して、ベンダの提供する情報をもとに対応手順を確立していますか？

制御システムをサイバー攻撃から安全な状態に保つために、セキュリティパッチの迅速な適用が欠かせません。セキュリティパッチに関する情報の入手方法や適用するタイミング、作業手順を明確にします。作業手順には、万一セキュリティパッチ適用による悪影響が発生する場合も想定し、バックアップにより最新の状態への復旧も可能な計画を立てることを推奨します。

7

7. セキュリティパッチ　【設問 No.7】

背景・目的

制御システムに脆弱性（攻撃に悪用される恐れがある弱点）や問題が発見された場合、システムベンダからセキュリティパッチなどの対策が発行されます。システムを安全な状態に保つためには、対策情報を迅速に入手して対応することが重要です。情報の入手方法やセキュリティパッチが発行された際の対応手順については、平常時から確認しておきます。また、対応作業に際して起きうるウイルス感染や動作不全などの恐れを考慮して、作業前にシステムのバックアップを取り、一度にすべての機器に適用するのではなく、数台ずつに分割し、動作確認を行いながら適用するなどの対策手順を作成します。

想定されるリスク

セキュリティパッチが適用されていない場合、システムが攻撃に屈しやすい状況になったり、システムの動作が保証されない状態になったりする恐れがあります。また、セキュリティパッチ適用作業が正しい手順で行われないと、作業時にウイルス感染したり、セキュリティパッチ自体の不具合によってシステムが異常な状態になったりする恐れがあります。なお、セキュリティパッチが適用されたとしても、場合によっては問題が発生する恐れがあります。

7. セキュリティパッチ　　【設問 No.7】

内容解説・施策例

セキュリティパッチ適用の検討と実施にあたっては、次の点を考慮します。

（ア） セキュリティパッチ情報の入手方法について制御システムベンダに確認する。

制御システムに対するセキュリティパッチ情報の入手方法について制御システムベンダに確認し、セキュリティパッチが発行された場合に迅速に情報が得られるようにしておきます。セキュリティパッチ情報が発行された場合には、セキュリティパッチ適用の必要性や影響について確認します。

（イ） セキュリティパッチ適用手順について制御システムベンダに確認する。

制御システムに対するセキュリティパッチ適用の手順について制御システムベンダに確認し、ベンダが推奨する手順がある場合にはその手順を把握しておきます。

（ウ） セキュリティパッチ適用時のリスク対策を検討する。

適用によって制御システムが異常になる恐れがあるため、対処として次の点を考慮します。

①セキュリティパッチ適用時に使用する記録媒体や PC のウイルスチェックを実施する。

適用時のウイルス感染を防止するため、使用するCD、DVDなどの記録メディアやUSBメモリ、USBハードディスクなどのメモリデバイスのウイルスチェックを実施します。作業用のPCについては、制御システムに接続する前にウイルスチェックを実施します。

②セキュリティパッチ適用前にバックアップを実施する。

適用作業の失敗やセキュリティパッチ自体の不具合によってシステムが異常な状態になる恐れがあります。適用前には、システムのバックアップを取り、万一の場合にはシステムを適用前の状態に復元できるようにしておきます。

③操業への影響が少ない機器から段階的にセキュリティパッチを適用する。

適用によってシステムが異常になるリスクを考慮し、適用は一度にすべての機器へ行わず、操業への影響が少ない機器から動作確認をしながら段階的に行います。

【参考文献】

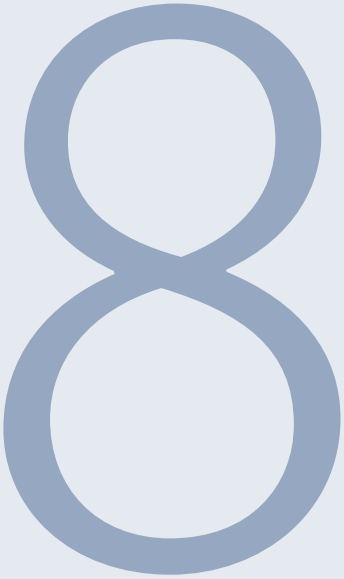
・独立行政法人 情報処理推進機構（IPA）「情報セキュリティ」
http://www.ipa.go.jp/security/index.html

8. システムの強化

【設問 No.8】

制御システムで使われるOSや アプリケーションの初期導入や バージョンアップ時に、 使っていないOSのサービスや通信ポートを 停止または無効にしていますか？

制御システムの脆弱性低減のために、使用していないOSなどのサービスや通信ポートを停止または無効にします。



8. システムの強化　　【設問 No.8】

背景・目的

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（脆弱性）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ていない OS などのサービスや通信ポートは停止または無効にします。

想定されるリスク

OS のサービス機能（ftp、telnet など）や通信ポートの脆弱性を使った攻撃により、システムの動作が不安定になる、またはシステムが異常となり操業停止となる恐れがあります。

8. システムの強化　　【設問No.8】

内容解説・施策例

セキュリティ向上のためにシステム上の不要な機能を停止することを「要塞化」または「ハードニング（hardening）」と言います。ハードニングはセキュリティ向上に有効ですが、設定を誤るとシステムの異常動作の原因にもなります。ハードニングの実施にあたっては、事前に制御システムベンダに確認し、ベンダが推奨する方法や設定がある場合はそれを使用します。独自に設定する場合でも、設定内容について制御システムベンダからアドバイスを受けることをお奨めします。

ハードニングの実施においては次の事項を考慮します。

（ア） 不要なアプリケーションをアンインストールする。

使用していないアプリケーションを、システムからアンインストールします。また不要なアプリケーションをインストールしないようにします。

（イ） 不要なアカウントを削除する。

不要なアカウントを放置することはシステムの脆弱性になる恐れがあります。使用していないアカウントを削除します。

（ウ） ファイルやフォルダのアクセス権は必要最小限のユーザにのみ許可する。

ファイルやフォルダのアクセス権が適切であることを確認し、書込み・読込み・実行などの権限は、必要なユーザに必要な権限だけを与えるようにします。

（エ） 使用していない機能を無効にする。

使用していない OS の機能（共有フォルダ、プリンタ共有、自動再生など）を無効に設定します。

（オ） 使用しない端子（USB 端子、IEEE1394 端子、ネットワーク端子など）は物理的に使用できないようにします。

制御システムで使用しない端子は、封印のための治具や封印シール（剥されたことが検知できるシール）などで封鎖して、許可なく使用されないようにします。

【参考文献】

・独立行政法人 情報処理推進機構（IPA）「情報セキュリティ」
http://www.ipa.go.jp/security/index.html

9. バックアップと回復

【設問 No.9】

制御システムの復旧に
必要なデータのバックアップを
ベンダが推奨する方法で行っていますか？

制御システムにおいて復旧に必要なデータのバックアップを行うことが必要です。

9

9. バックアップと回復　【設問No.9】

背景・目的

万が一に備え、システム復旧に必要なデータ（パラメータや操業データなど）は、定期的にバックアップを行い、バックアップデータのベリファイ（破損していないことの確認）を行っておくことが必要です。
そのためにもまずはベンダの推奨する方式でデータが保存されているか確認します。

想定されるリスク

制御システムがシステム機能不全になり、復旧のためにシステムの復元を行う場合があります。
このような場合には、機能不全前の直近のデータが必要ですが、短い間隔で定期的なバックアップを行っていれば、直近に近いバックアップデータからの復元が可能となります。
バックアップデータがない場合には、本来の運用状態への復旧までに手間取るなどの大きな影響が発生する恐れがあります。

9. バックアップと回復　　【設問No.9】

内容解説・施策例

バックアップを行う際には以下の点を考慮することをお奨めします。

（ア）バックアップの頻度

システムの復旧が必要なときに、どれくらいの最新性が必要かをもとに、バックアップを取るタイミングを検討します。システムのデータ更新がオンラインで毎日行われている場合は、毎日バックアップを取ります。一方で情報更新の頻度が少ないシステムの場合は、システム変更時や月次で定期的にバックアップを取ります。このように、システムの運用の特性を考えて、バックアップの頻度を決める必要があります。

（イ）バックアップデータの世代管理

バックアップデータの保存期間も、上記項目（ア）で検討したバックアップの頻度にあわせて決定します。バックアップデータを世代管理することにより、例えば、システム変更後にしばらくしてから障害が発見された場合、複数世代前のデータから復元することもできます。システム復元の有効性を担保するためには、世代管理・保存期間も適切に決める必要があります。

（ウ）バックアップデータの遠隔地管理

火災、洪水などの災害が発生した場合でも復旧ができるようにするためには、バックアップデータを現地だけでなく遠隔地にも保管する必要があります。

（エ）バックアップの方法

バックアップの方法には、データ全体のバックアップを取る方式と、毎回のバックアップの時間短縮のため差分でバックアップを取っていく方式があります。バックアップ方法も併せて検討すると、効率的な運用ができます。

また、バックアップデータが、記憶媒体の不良などにより読み出せない恐れがあるため、バックアップ時にはベリファイを併せて行い、不完全だった場合には、バックアップを取り直す必要があります。

【参考文献】

・独立行政法人 情報処理推進機構（IPA）「情報セキュリティ」
http://www.ipa.go.jp/security/index.html
・JIS Q 27001「A 10.5.1 情報のバックアップ」

10. 転入者と転出者用のプロセス

【設問 No.10】

システムに登録されている関係者に、役割や責任の変更を含む異動があった場合に備えて、アカウントの追加・削除やパスワード変更の手順を文書化し、実施していますか？

システムを操作する権限を与えたメンバに変更があった時やその役割・責任に変更があった場合には、システム管理者は関係するメンバのアカウントの追加・削除や管理用アカウントのパスワードの変更を行う必要があります。

10

10. 転入者と転出者用のプロセス　【設問 No.10】

背景・目的

システム管理者は、制御システムの操作権限が必要な者だけに限定して許可します。また、操作権限が付与されたアカウントの権限が適切であることを、定期的に確認する必要があります。
制御システムの操作権限を付与されたスタッフが増員されたり、退職したりして、操作権限のあるメンバに変更があった場合、またメンバの役割や責任が変わった場合は、権限の確認が必要です。

想定されるリスク

アカウントとパスワードが適切に管理されていない場合、退職者や現在は操作権限を与えられるべきでないメンバなどによる不正アクセスによる業務妨害や情報流出が発生し、ビジネスそのものへの大きな影響を及ぼす恐れがあります。

内容解説・施策例

海外で報告されている制御システムのインシデントの中には、過去に組織に所属していたメンバが、退職後に外部から不正を行うといった事例もあることから、技術的・物理的対策に加え、運用面の対策が必要です。
運用面の対策例として、制御システムの操作権限は、必要最小限の人員に必要最小限の権限を付与する、不要になったアカウントは速やかに削除して、システムの悪用・破壊・情報の持出しなどができない環境にする、などの施策があります。
これらの手順は、セキュリティ実施手順書などで文書化し、パスワードの定期的な変更、システムログイン履歴による不正なアクセスの確認、異動退職時に早期に報告があがる仕組みなどを決めて運用することが大切です。また、運用している手順が適切かどうかを、定期的に見直すことも必要です。

【参考文献】
・独立行政法人 情報処理推進機構（IPA）「情報セキュリティ」
http://www.ipa.go.jp/security/index.html

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