つながる時代の
制御システムセキュリティ対策自己評価ツール
「J-CLICS 攻撃経路対策編」

日本電気計測機器工場会
産業計測機器・システム委員会
セキュリティ調査研究合同WG（SICE/JEITA/JEMIMA）
阪田 恒晟　株式会社日立製作所
加藤 毅　横河電機株式会社
畔 英之　三菱電機株式会社

Contents

1. はじめに
2. 制御システムセキュリティの概要
3. J-CLICS STEP1／STEP2との比較
4. J-CLICS 攻撃経路対策編について
5. まとめ

1. SICE/JEITA/JEMIMAセキュリティ合同WG

活動目的

製造業分野におけるセキュリティ標準化動向や技術等の調査・研究活動と
会員企業・ユーザへの成果提供，展示会・各種会議での広報

設立

2005年4月

メンバー（50音順）

アズビル(株)，東芝インフラシステムズ(株)，(株)日立製作所，
(株)日立ハイテクソリューションズ，富士電機(株)，(株)堀場製作所，
三菱電機(株)，横河電機(株)

活動実績

ISA SP99　TR2を利用したセキュリティ対策の実践
NIST SPP-ICS ver1.0を利用したセキュリティ要件の分析
セキュリティ標準規格の調査
CPNI グッドプラクティスの検討
セキュリティ評価ツールの調査・改良
セキュリティ評価ツール J-CLICS の作成・拡充

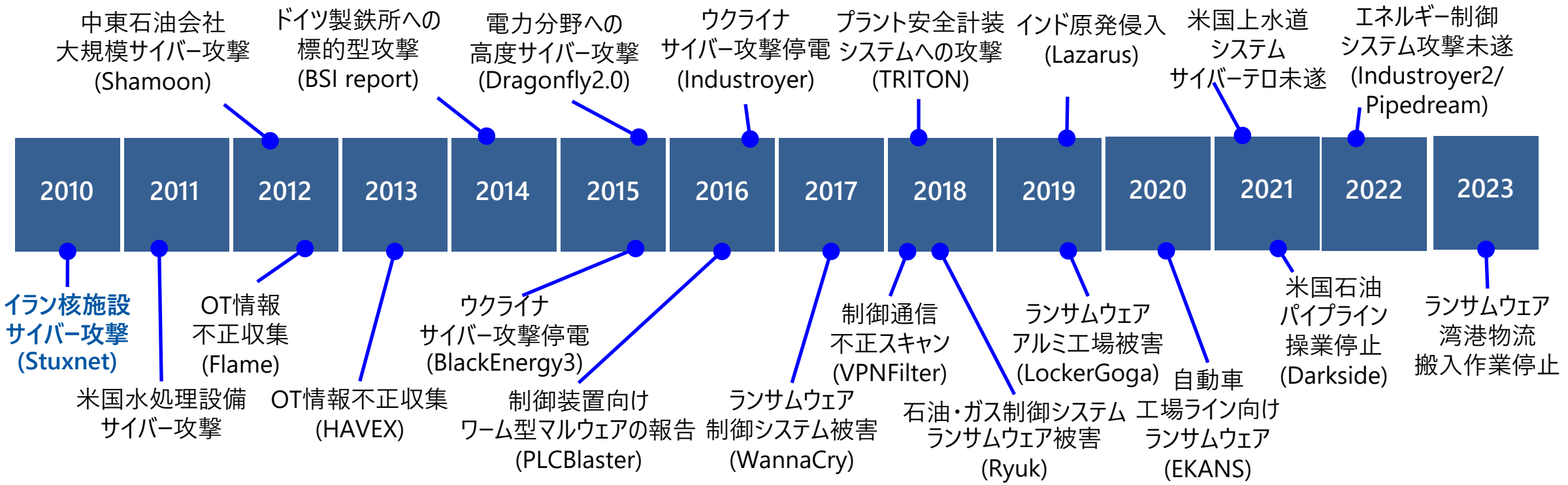
JEMIMA本部　計測会館

1. はじめに
2. **制御システムセキュリティの概要**
3. J-CLICS STEP1／STEP2との比較
4. J-CLICS 攻撃経路対策編
5. まとめ

2.1　制御システムに対するサイバー攻撃の変遷

- 2010年以降，制御システムに対するサイバー攻撃の脅威が拡大

制御システムを狙うサイバー攻撃の主な事例 (ごく一部)　*公開情報を元に作成[1]



制御システムの変化に合わせて，攻撃手法も巧妙化/高度化

[1] 阪田: 産業制御システムにおけるサイバーセキュリティ, 日本機械学会年次大会, 2024

2.2　制御システムの特徴

	情報システム	制御システム
セキュリティの優先順位	情報漏洩を防ぐ！ 機密性＞完全性＞**可用性**	**安全第一！** **可用性**＞完全性＞機密性
求められる可用性	サービスの停止を許容	サービスの停止は許容されないケースが多い (24時間365日稼働)
守るべき対象	情報	設備，製品，サービス
技術のサポート期間	3~5年	10~20年
運用管理	情報システム部門	現場技術部門

優先事項が異なるため，制御システムの環境に合わせたセキュリティ対策が必要！

2.3　制御システムセキュリティの現状と課題

- 既設システムのセキュリティ対策で不十分なものも散見
  →予算・リソースとの兼ね合いで対策が実施できない…
- 既存のガイドラインでは対応困難
  →リスク評価や管理体制の構築等，プロセス面の負担が大きい

2013年　セキュリティ合同WG　セキュリティ対策チェックツール　J-CLICS開発
（協力：ユーザ企業，JPCERT/CC）

J-CLICS：Check List for Industrial Control System of Japan

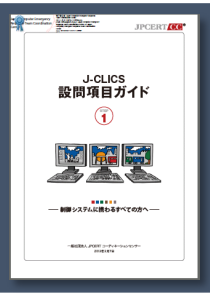
J-CLICSの目的

① 現状把握，セキュリティ対策の足掛かりとなるツール
② セキュリティの専門家ではない制御システム関係者にとって，わかりやすく実施しやすい！
③ 少ない設問数で，高い効果の期待できる対策

現場担当者～経営者のセキュリティスキル・意識の底上げが期待される

1. はじめに
2. 制御システムセキュリティの概要
3. J-CLICS STEP1／STEP2との比較
4. J-CLICS 攻撃経路対策編について
5. まとめ

3.1　J-CLICS STEP1/STEP2，攻撃経路対策編

	基本対策	バランスを考慮した対策(本報告)
項目	J-CLICS STEP1/STEP2 	J-CLICS 攻撃経路対策編 
位置づけ	セキュリティ対策の**最初のステップ**	セキュリティ対策の**次のステップ**
提供情報	まず何をすべきか	何を何のためにやるべきか
掲載内容	実施しやすく，高い効果が期待できる 推奨対策を掲載	**優先度と過不足が分かる形**で 推奨対策を記載
着眼点	対策の実施難易度・重要度	攻撃経路・手順・成立条件

3.2 J-CLICS 攻撃経路対策編　見直しのポイント

J-CLICS STEP1/STEP2作成時から，対策状況，リスク，技術のニーズが変化
攻撃経路対策編では対策の過不足，優先順位を検討

対策の過不足

・不足　全体を知ってわかる
・過剰　重複を知ってわかる

攻撃＝攻撃経路＋攻撃手順
成立条件 ← 条件を崩せば攻撃は成立しない

「全体」：攻撃経路
「重複」：攻撃経路に対する対策の重複　→ 過不足

対策の優先順位

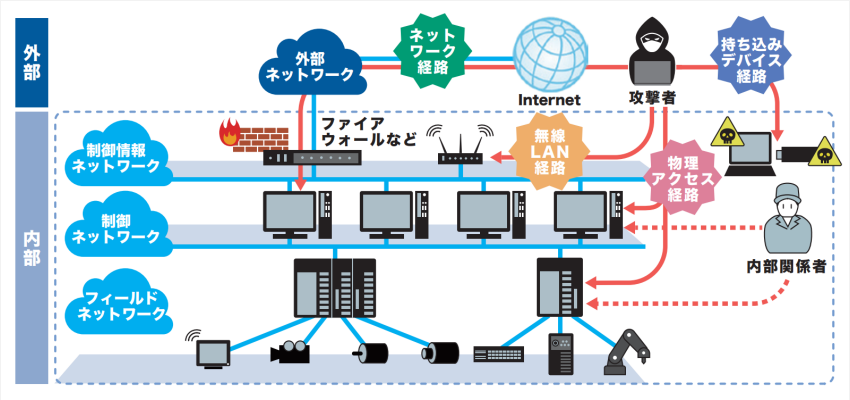
・優先度の考え方

リスク ＝ 想定被害額 × 発生頻度 ←予測困難

・危険な経路への対策を優先
　物理：どこからでも　時間：いつでも
　手段：誰でも　機会：こっそり
・経路ごとに初期の手順への対策を優先
　攻撃＝外部→内部への侵攻　※外部で防ぐ

3.3 J-CLICS 攻撃経路対策編の検討手順

1.保護対象と想定脅威の定義



ISA-95　Purdue Model

攻撃者の想定
・セキュリティ境界外
・正規アクセス権無

攻撃経路の想定
・ネットワーク
・無線LAN
・持ち込みデバイス
・物理アクセス

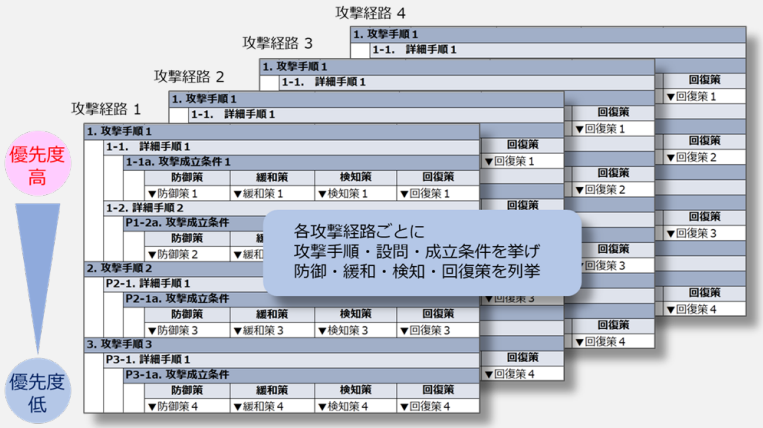
2.脅威分析の実施

攻撃経路	脅威	
	攻撃手順	成立条件
経路 1	手順 1	条件 1
	手順 2	条件 2-a
		条件 2-b
	手順 3	条件 3
経路 2	手順 1	条件 1
	手順 2	条件 2
	手順 3	条件 3

脅威分析手法の検討
・攻撃経路　必ず経路を通る
・攻撃手順　特定手順が存在
・成立条件　条件を満たす必要

脅威分析の実施
・手順と成立条件を列挙
　存在する脅威を把握

3.対策マップの作成

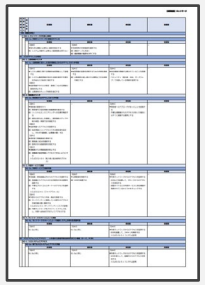


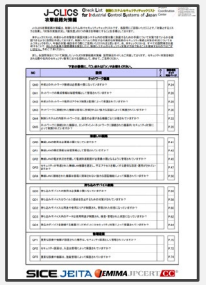
対策目的の分類
防御、緩和、検知、回復

優先度の検討
①悪用されやすい経路
　地理/時間/手段/機会
②攻撃初期を優先

経路別対策マップの作成
・攻撃手順と成立条件
・成立条件を崩す対策

4.設問項目の検討と設問項目ガイドの作成


対策マップ


チェックリスト

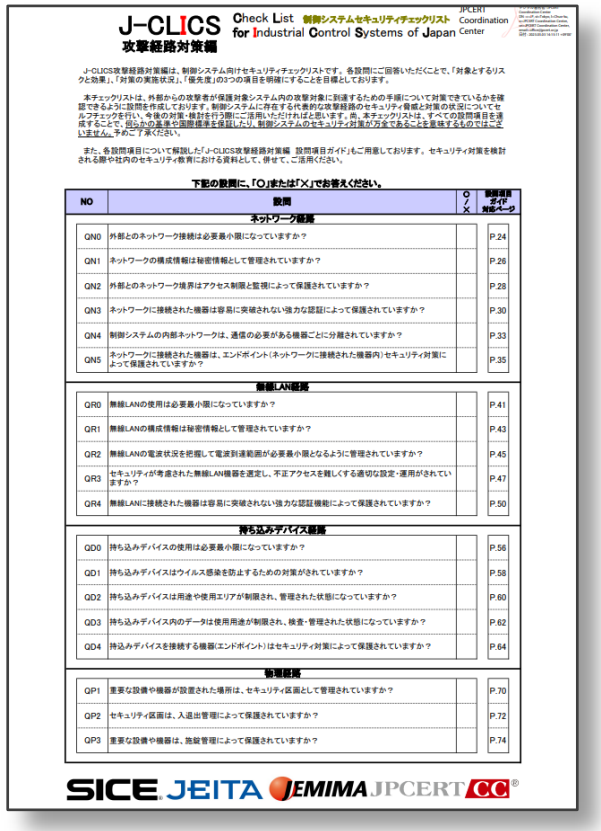
設問項目ガイド

設問項目の検討
・できるだけ少ない設問で
　対策マップの広い範囲を
　カバーする内容

設問項目ガイドの作成
・チェックリストを解説
・ユーザー、有識者がレビュー

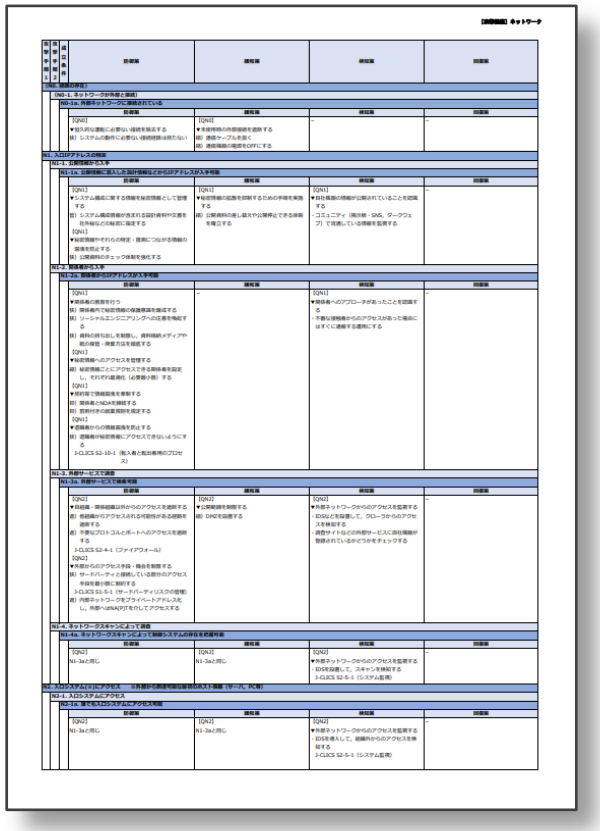
1. はじめに
2. 制御システムセキュリティの概要
3. J-CLICS STEP1／STEP2との比較
4. **J-CLICS 攻撃経路対策編について**
5. まとめ

4.1　J-CLICS 攻撃経路対策編の構成



チェックリスト

設問項目ガイド

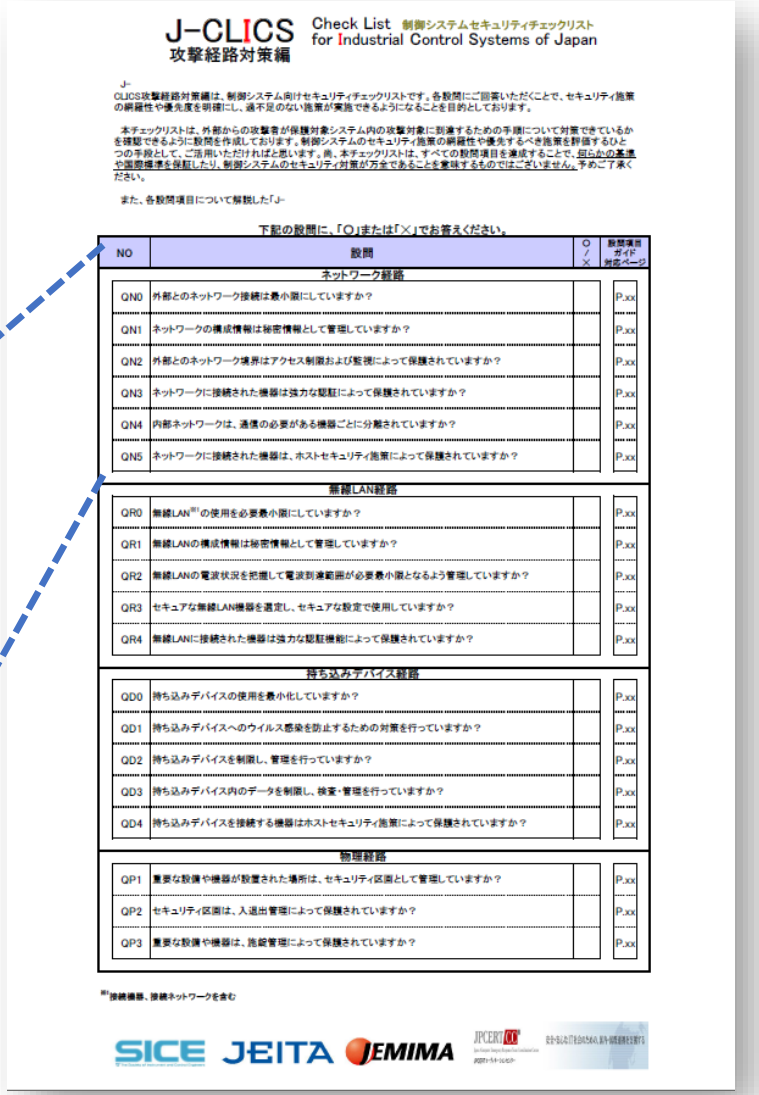


対策マップ

4.2　J-CLICS 攻撃経路対策編　チェックリスト

- 設問数は19項目
- 設問Noと設問で構成
- 設問を読むだけで内容が把握できるように
  具体的かつ簡潔に記載

NO	設問	○／×
	ネットワーク経路	
QN0	外部とのネットワーク接続は最小限にしていますか？	
QN1	ネットワークの構成情報は秘密情報として管理していますか？	
QN2	外部とのネットワーク境界はアクセス制限および監視によって保護されていますか？	
QN3	ネットワークに接続された機器は強力な認証によって保護されていますか？	
QN4	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？	
QN5	ネットワークに接続された機器は、ホストセキュリティ施策によって保護されていますか？	



J-CLICS 攻撃経路対策編 Check List 制御システムセキュリティチェックリスト for Industrial Control Systems of Japan

J-CLICS攻撃経路対策編は、制御システム向けセキュリティチェックリストです。各設問にご回答いただくことで、セキュリティ施策の網羅性や優先度を明確にし、過不足のない施策が実施できるようになることを目的としております。

本チェックリストは、外部からの攻撃者が保護対象システム内の攻撃対象に到達するための手順について対策できているかを確認できるように設問を作成しております。制御システムのセキュリティ施策の網羅性や優先すべき施策を評価するひとつの手段として、ご活用いただければと思います。尚、本チェックリストは、すべての設問項目を達成することで、何らかの基準や国際標準を保証したり、制御システムのセキュリティ対策が万全であることを意味するものではございません。予めご了承ください。

また、各設問項目について解説した「J-

下記の設問に、「○」または「×」でお答えください。

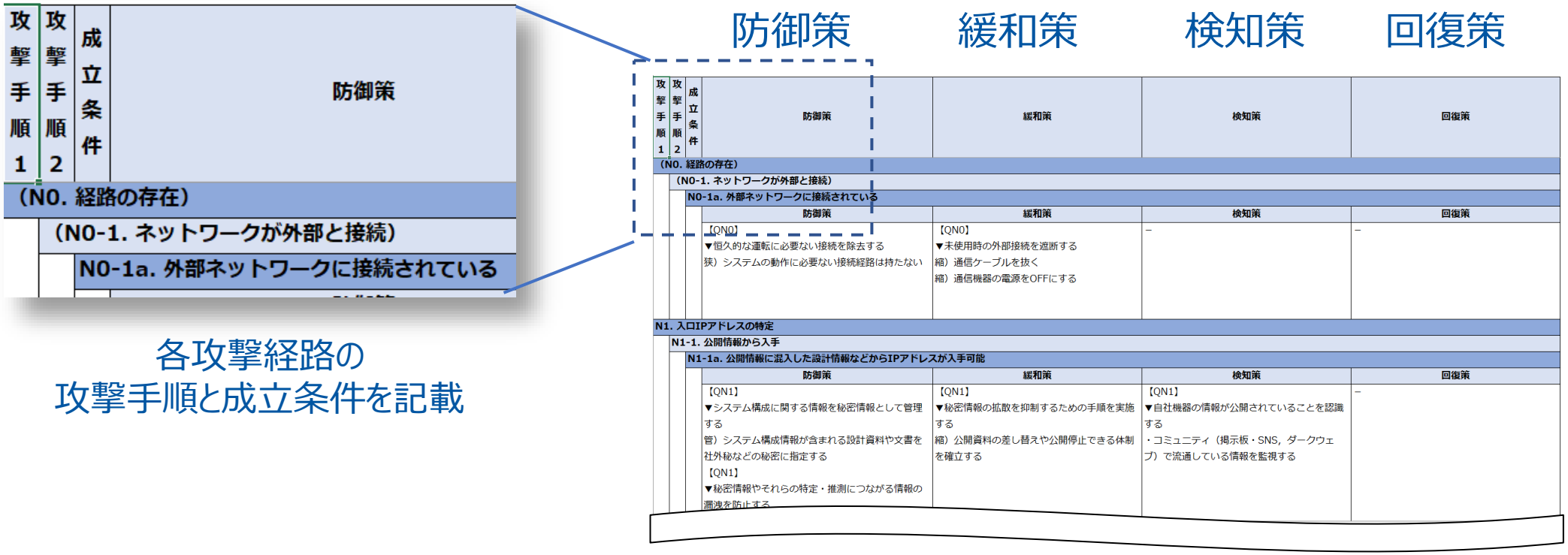
NO	設問	○／×	設問項目ガイド対応ページ
	ネットワーク経路		
QN0	外部とのネットワーク接続は最小限にしていますか？		P.xx
QN1	ネットワークの構成情報は秘密情報として管理していますか？		P.xx
QN2	外部とのネットワーク境界はアクセス制限および監視によって保護されていますか？		P.xx
QN3	ネットワークに接続された機器は強力な認証によって保護されていますか？		P.xx
QN4	内部ネットワークは、通信の必要がある機器ごとに分離されていますか？		P.xx
QN5	ネットワークに接続された機器は、ホストセキュリティ施策によって保護されていますか？		P.xx
	無線LAN経路		
QR0	無線LAN[※1]の使用を必要最小限にしていますか？		P.xx
QR1	無線LANの構成情報は秘密情報として管理していますか？		P.xx
QR2	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管理していますか？		P.xx
QR3	セキュアな無線LAN機器を選定し、セキュアな設定で使用していますか？		P.xx
QR4	無線LANに接続された機器は強力な認証機能によって保護されていますか？		P.xx
	持ち込みデバイス経路		
QD0	持ち込みデバイスの使用を最小化していますか？		P.xx
QD1	持ち込みデバイスへのウイルス感染を防止するための対策を行っていますか？		P.xx
QD2	持ち込みデバイスを制限し、管理を行っていますか？		P.xx
QD3	持ち込みデバイス内のデータを制限し、検査・管理を行っていますか？		P.xx
QD4	持ち込みデバイスを接続する機器はホストセキュリティ施策によって保護されていますか？		P.xx
	物理経路		
QP1	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していますか？		P.xx
QP2	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？		P.xx
QP3	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？		P.xx

※1 接続機器、接続ネットワークを含む

SICE JEITA JEMIMA JPCERT/CC

4.3　J-CLICS 攻撃経路対策編　対策マップ

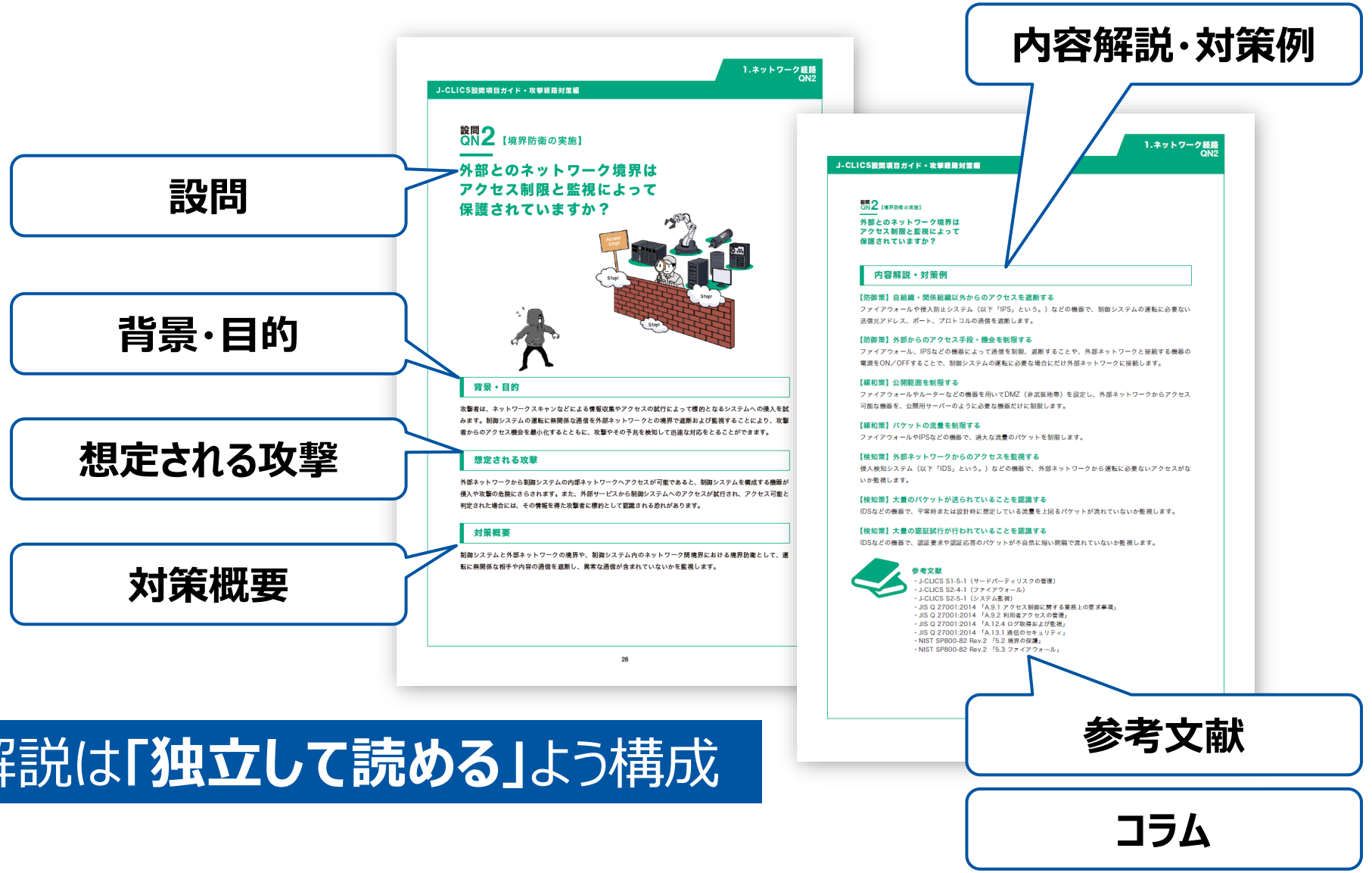
- 攻撃経路（ネットワーク、無線LAN、持ち込みデバイス、物理アクセス）ごとに作成
- 攻撃手順と攻撃の成立条件を記載
- 成立条件ごとに対策（防御策、緩和策、検知策、回復策）を検討



各攻撃経路の
攻撃手順と成立条件を記載

4.4　J-CLICS 攻撃経路対策編　設問項目ガイド

- 設問の解説書
- 攻撃経路対策の考え方
- 設問ごとの解説
- 背景・目的
- 想定される攻撃
- 対策概要
- 内容解説
- 参考文献
- コラム（読み物）



各経路や設問の解説は「独立して読める」よう構成

4.5　J-CLICS 攻撃経路対策編　対策マップからチェック項目を作成

ネットワーク経路		
QN0	外部とのネットワーク接続は最小限にしていますか？	
QN1	ネットワークの構成情報は秘密情報として管理していますか？	
QN2	外部とのネットワーク境界はアクセス制限および監視によって保護されていますか？	
QN3	ネットワークに接続された機器は強力な認証によって保護されていますか？	
QN4	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？	
QN5	ネットワークに接続された機器は、ホストセキュリティ施策によって保護されていますか？	

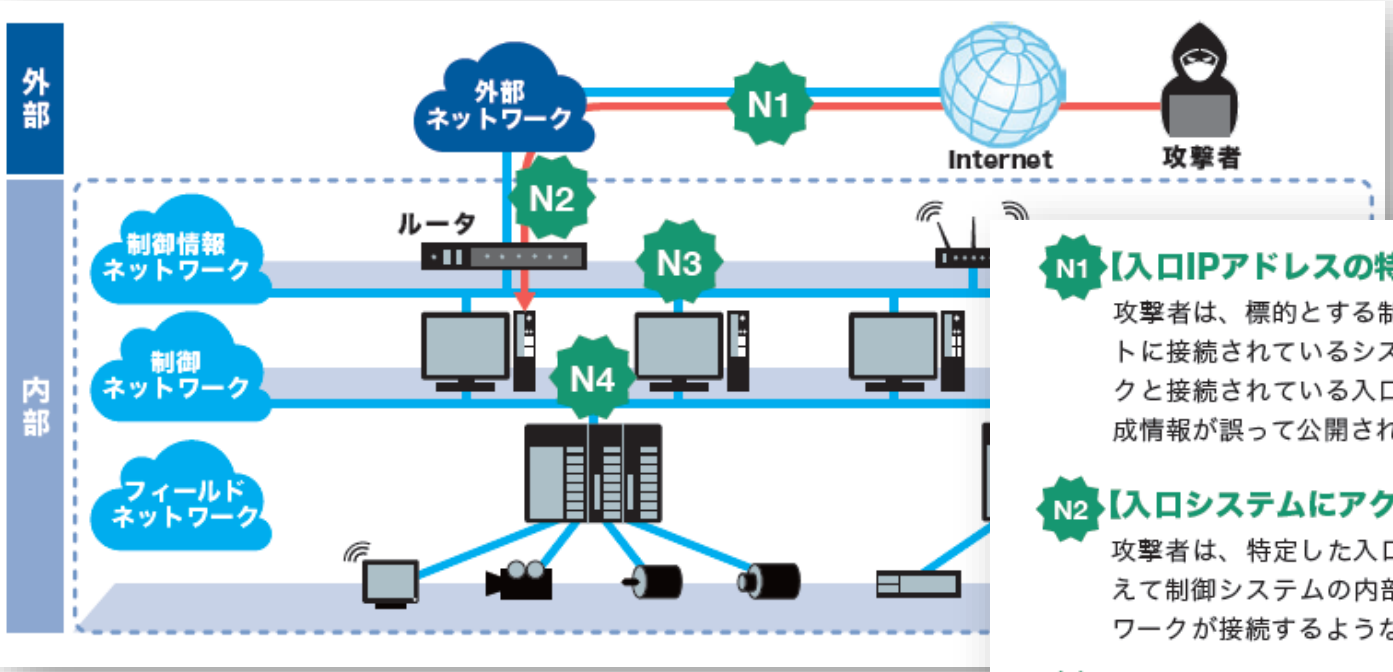
チェックリスト

対策を広範囲にカバーするよう
設問を設定

攻撃手順1	攻撃手順2	成立条件	防御策	緩和策	検知策	回復策
N1. 入口IPアドレスの特定						
	N1-1. 公開情報から入手					
		N1-1a. 公開情報に混入した設計情報などからIPアドレスが入手可能				
			【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 禁）システム構成情報が含まれる設計資料や文書を社秘など秘密に指定する …やそれらの特定・推測につながる情報の漏…する …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. …から入手					
		N1-2a. 関係者からIPアドレスが入手可能				
			【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				
			【QN2】 ▼自組織・関係組織以外からのアクセスを遮断する	【QN2】 ▼公開範囲を制限する	【QN2】 ▼外部ネットワークからのアクセスを監視する	－

対策マップ

4.6　設問項目ガイド記載例①　攻撃経路



ネットワーク経路の場合

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

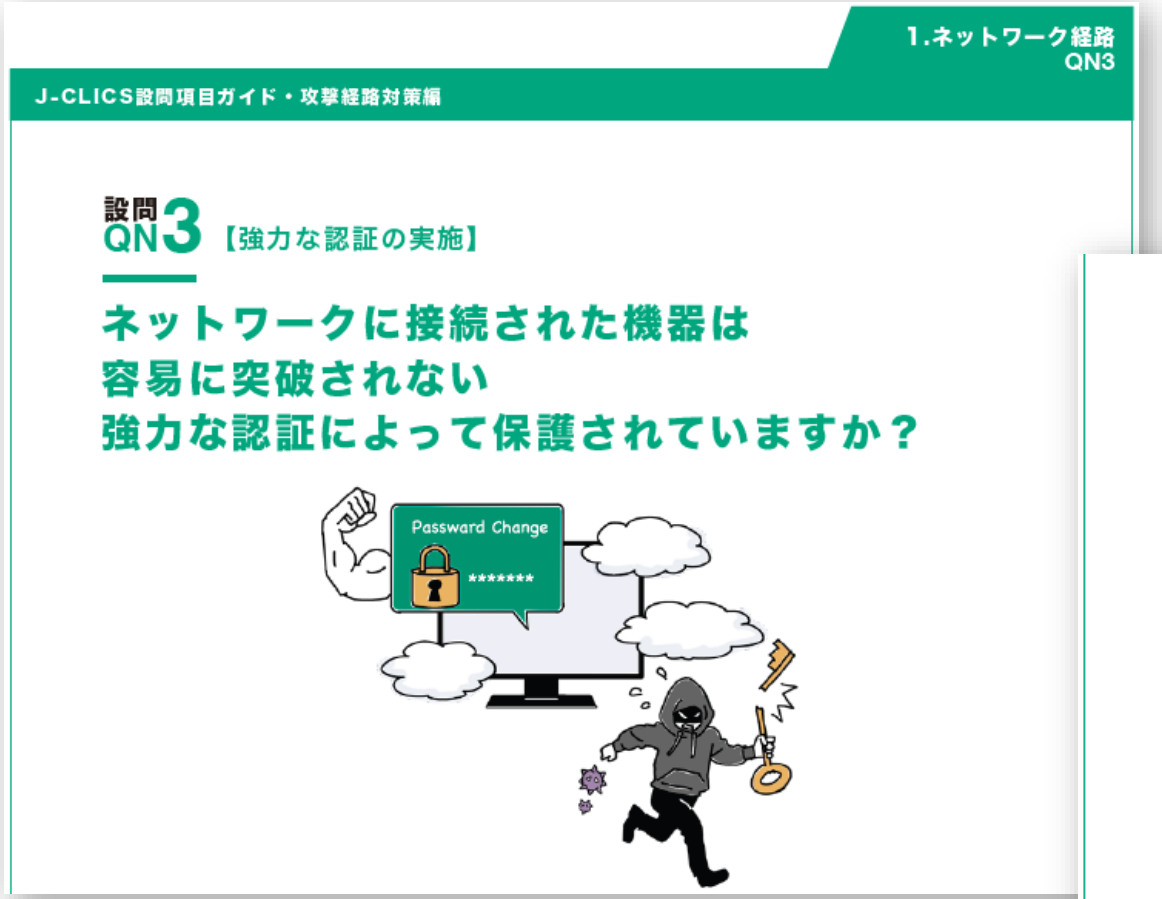
攻撃者は、制御システムにおける攻撃対象や攻撃の踏み台となる機器を探すため、制御システムの内部ネットワークに接続された機器にアクセスしてシステム情報を取得します。その結果、OSが古かったりセキュリティパッチが最新でなかったりする機器が見つかった場合、それらに対する攻撃の危険性が高まります。対策として、制御システムの運転に不要な通信に対する制限や監視を実施します。

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。

4.7　設問項目ガイド記載例②　各設問への解説

4.8　設問項目ガイド記載例③　想定される攻撃，対策概要



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

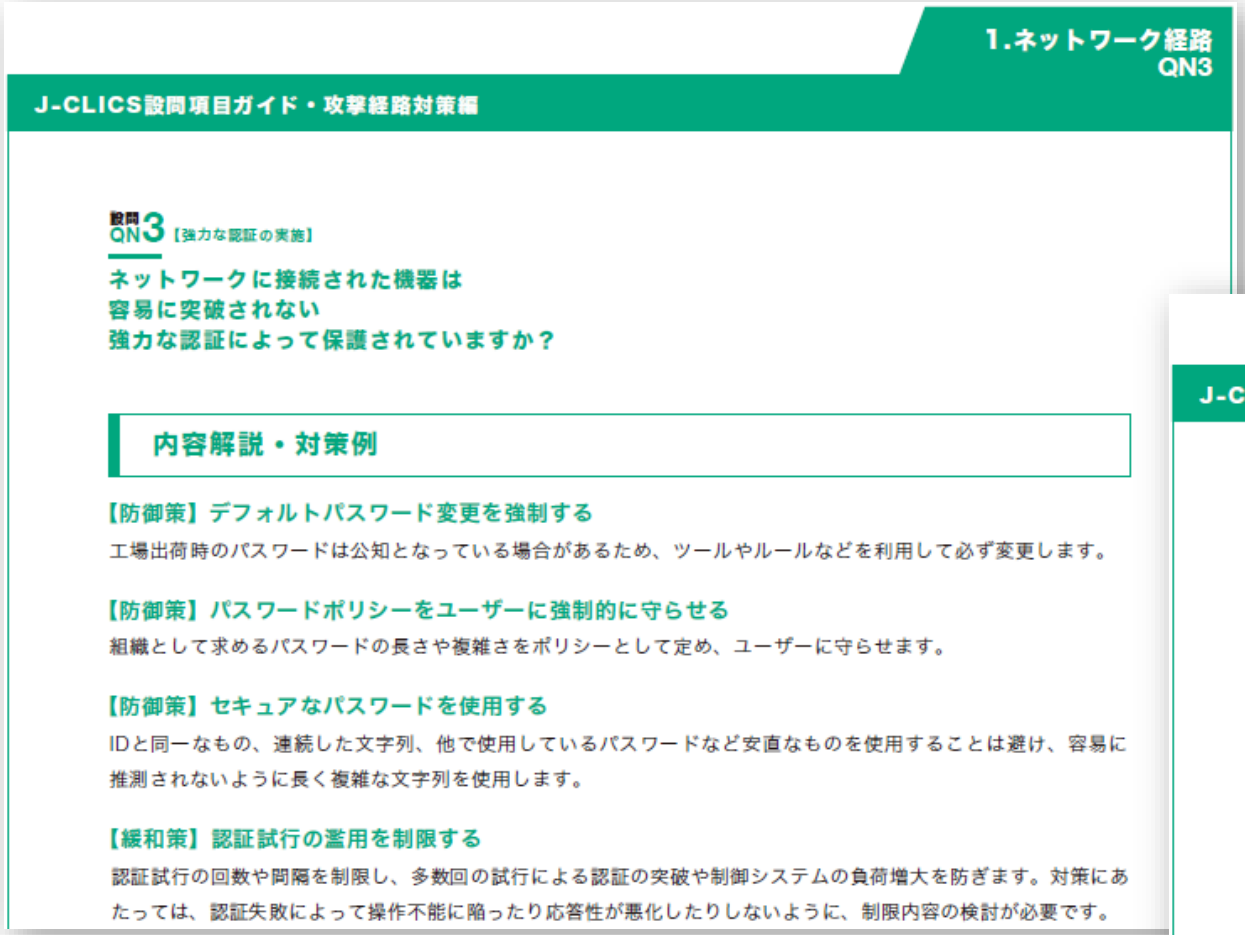
PLC、DCSなどの制御装置およびSCADAのような端末機器に、不適切な制御指令やパラメーター類が意図的に投入されたり、開発環境上で制御プログラムが改ざんされたりして、制御システムが想定しない動作を起こすことがあります。
また、これらの機器から知的財産を含む秘匿性が高いデータを盗み出され、ビジネス上の損害を受けることも考えられます。

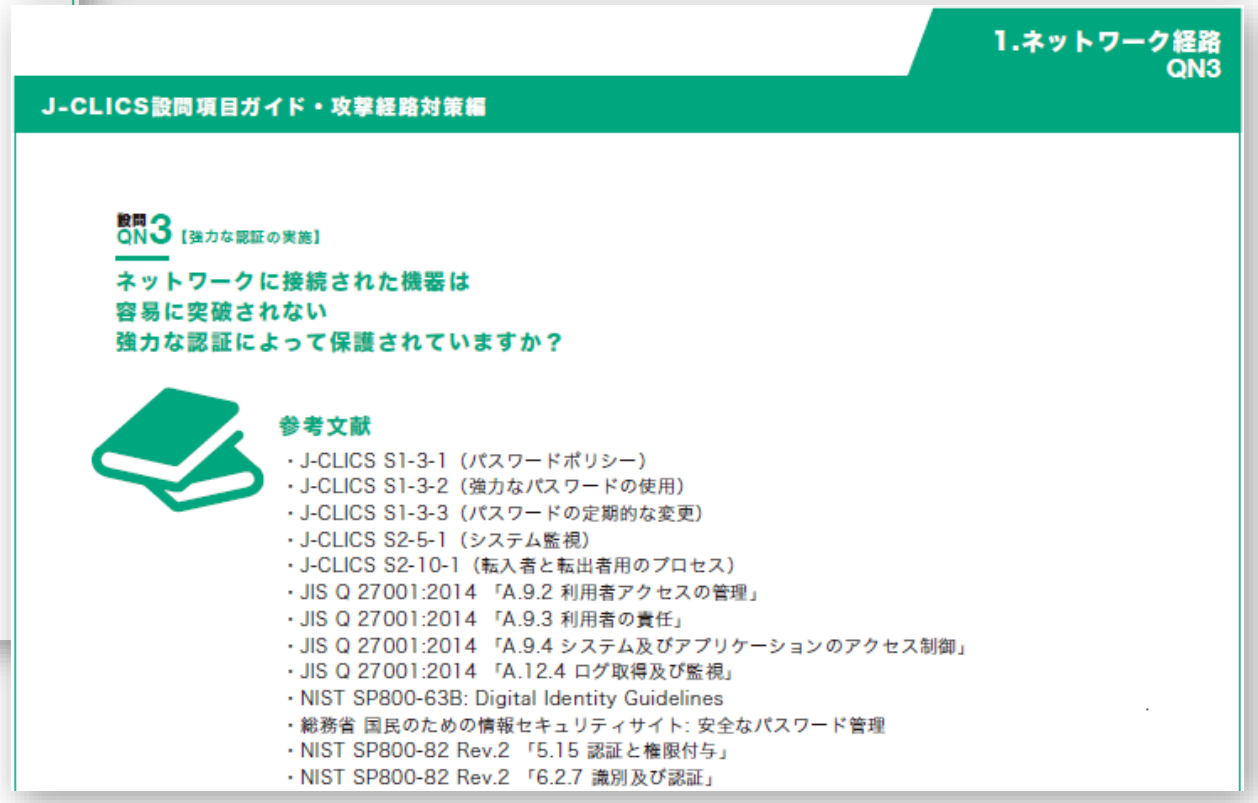
対策概要

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。

ネットワーク経路
設問：QN3[強力な認証の実施]の場合

4.9　設問項目ガイド記載例④　内容解説・対策例，参考文献



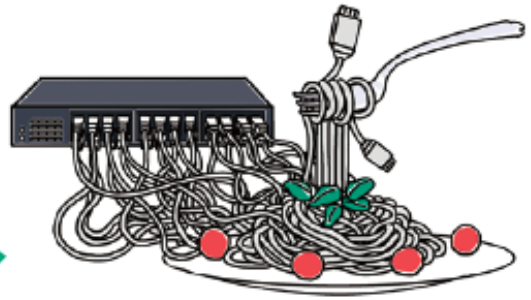


4.10　設問項目ガイド記載例⑤　コラム

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。

ではロールプレイをご覧ください

ロールプレイ概要

Player1

現場監督　**監督さん**

・制御システム全般は論理物理共に熟知している

・日々の業務でIT部門のシステムを活用しているが、セキュリティには詳しくない

①制御システムへのサイバーセキュリティ対策の導入が決まり、業務経験のあるITさんが担当となったので、現場監督に依頼をした。

②ITさんに貰った各種標準やガイドラインを読んでサイバーセキュリティ対策を検討しているが制御システムへの導入に苦戦している。
何か良い手段はないか相談させてほしい。

Player2

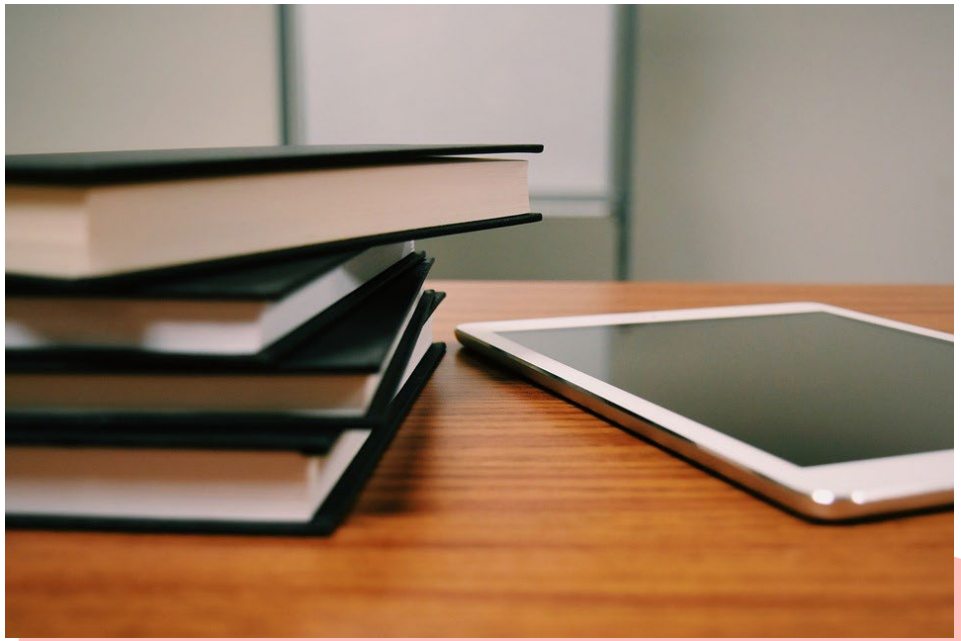
IT部門担当　**情シスさん**

・制御システムの全体像は把握しているが、普段関わりがない

・日々の業務はITシステムのリスク管理やセキュリティ対策を取り扱っている

数日後…

制御システムへのサイバーセキュリティ対策導入に苦戦



制御システム

「システム構成はわかる」
「リスクアセスメントは実施している」

サイバーセキュリティ対策

「脅威分析??」
「ネットワークセキュリティ??」

Player1

現場監督　**監督さん**

J-CLICS 攻撃経路対策編 ダウンロード

公開日	タイトル	PDF	Excel
2023-03-07	J-CLICS 攻撃経路対策編 設問項目ガイド	9.00MB デジタル署名付き	-
	J-CLICS 攻撃経路対策編 チェックリスト	0.34MB デジタル署名付き	68KB
	J-CLICS 攻撃経路対策編 対策マップ	0.99MB デジタル署名付き	46KB

ガイド文書

JPCERT CC®

JPCERT Coordination Center

J-CLICS
設問項目ガイド

攻撃経路対策編

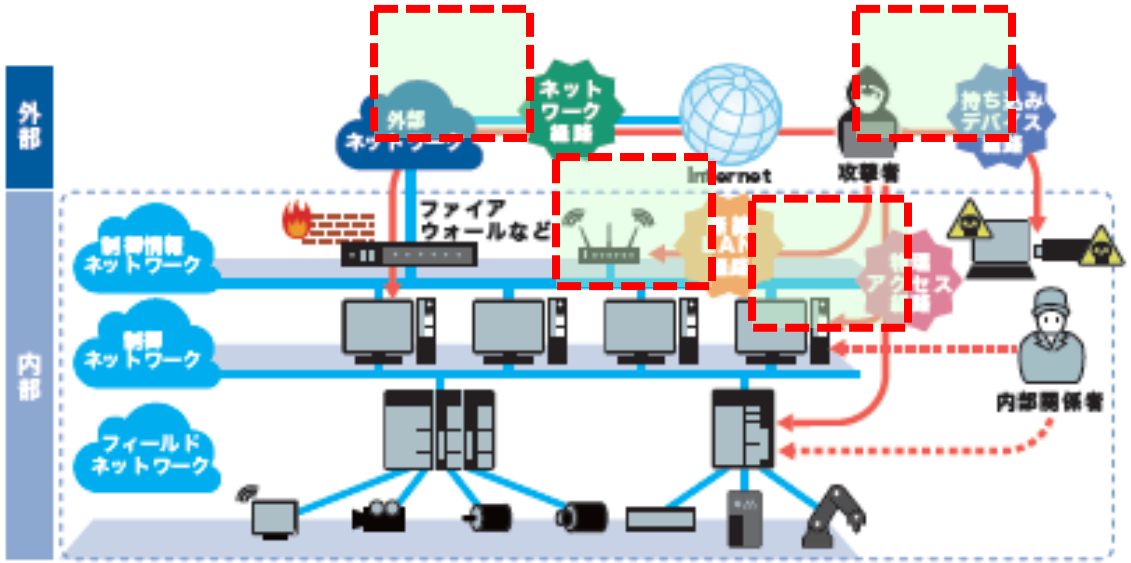
―― 多様化する攻撃から制御システムを守るために ――

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

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。

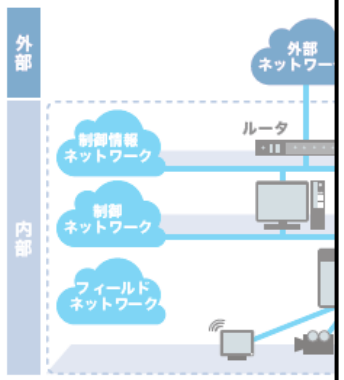


ガイド文書

攻撃への対策の考え

無線LAN経路での攻撃活動においては、
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

[図5:無線LAN経路で想定される各層ごとの

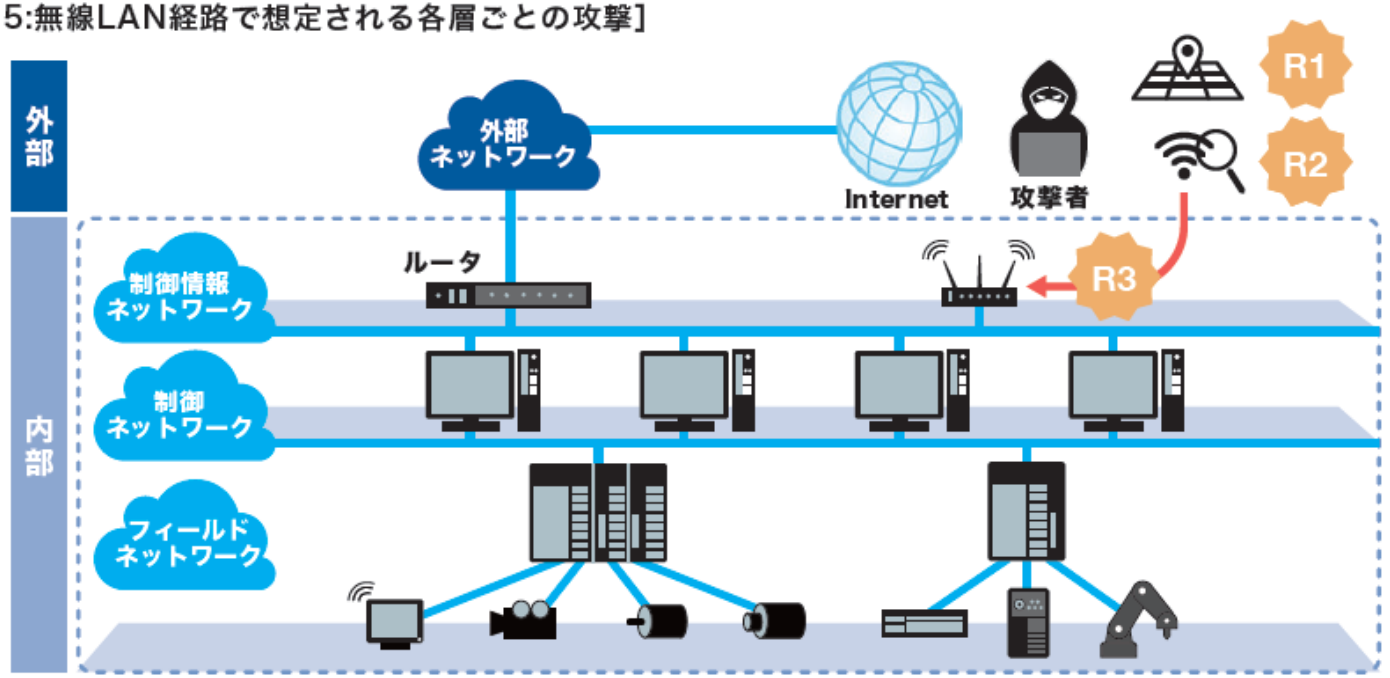


R1【無線LAN使用箇所の特定】→Q
攻撃者は、制御システムの施設に近づ
を調査します。情報源としては、特定
定されます。無線LANが設置されてい
査がより効率良く進められます。

R2【無線LAN使用状況の調査】→Q
攻撃者は、無線LANの設定など使用状
集し、より具体的な攻撃対象・攻撃内

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、
肢を獲得します。

[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。

ガイド文書

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。

2.無線LAN経路
QR2
J-CLICS設問項目ガイド・攻撃経路対策編

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

対策マップ

攻撃手順1	攻撃手順2	成立条件	防御策	緩和策	検知策	回復策
R2. 無線LAN使用状況の調査						
	R2-1. 電波観測により無線LANの周波数・暗号化などの情報を収集（ウォードライビング:Wardrivingなど）					
		R2-1a. 無線LAN使用状況の調査が可能				
			【QR2】 ▼敷地外まで電波が届かないようにする 狭）シールドで屋外への電波漏洩を防止する 狭）無線LAN機器の出力を抑える 狭）指向性アンテナへ変更する 【QR2】 ▼通信をセキュアな設定にする 難）暗号化する 狭）ブロードキャスト設定を無効にする（ステルス化）	【QR2】 ▼通信する時だけ無線機能を有効化する 狭）無線を使用するときのみ、アクセスポイントの電源や接続機器の無線LAN設定をONにする	【QR2】 ▼施設周辺を監視する ・敷地周辺の見回り ・監視カメラを設置する	【QR2】 ▼漏洩した情報と異なる構成に変更する ・SSIDを変更する
R3. 攻撃実施						
	R3-1.【ジャミング】強力な送信器（マグネトロンなど）を用いて通信を妨害					
		R3-1a. 電波発射により無線LAN通信の妨害が可能				
			【QR3】 ▼敷地外から電波が届かないようにする 狭）シールドで屋外からの電波侵入を防止する	【QR3】 ▼通信路を二重化する 縮）異なる周波数帯を利用する 縮）有線を利用する	【QR3】 ▼定期的にシステムや電波状態を調査する ・ログ分析を行う ・定期的に電波を観測する J-CLICS S2-5-1（システム監視）	【QR3】 ▼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 J-CLICS S1-4-1（対応能力確立）

1. はじめに
2. 制御システムセキュリティの概要
3. J-CLICS STEP1／STEP2との比較
4. J-CLICS 攻撃経路対策編について
5. **まとめ**

まとめ

J-CLICS 攻撃経路対策編を2023年3月に公開しました

- 攻撃経路ごとの対策に着目したセキュリティ自己評価ツール
- 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経路について攻撃手順と対策を検討し、マップ化
- 検討結果に基づいて、19項目の設問を作成
- チェックリスト、設問項目ガイド、対策マップで構成
- 対策の過不足、優先順位がわかる内容
- JPCERT/CCで無償公開中

JEMIMA委員会活動ページ
↓
産業計測機器・システム委員会

JPCERT/CC J-CLICS公開ページへのリンク

JPCERT/CC J-CLICS 公開ページ

表中の図はSICE/JEITA/JEMIMAセキュリティ合同WG内で作成したJ-CLICSから引用したものです.
J-CLICSは下記リンク先よりダウンロードできます. ご活用ください.

J-CLICS STEP1／STEP2（ICSセキュリティ自己評価ツール） (jpcert.or.jp)
J-CLICS 攻撃経路対策編（ICSセキュリティ自己評価ツール） (jpcert.or.jp)