J-CLICS 攻撃経路対策編 対策マップ

J-CLICS 攻撃経路対策編では、4つの対策（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、次の表に記した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。

J-CLICS 攻撃経路対策編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	攻撃経路を狭めて、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分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。

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
（N0. 経路の存在）						
	（N0-1. ネットワークが外部と接続）					
		N0-1a. 外部ネットワークに接続されている				
			防御策	緩和策	検知策	回復策
			【QN0】 ▼恒久的な運転に必要ない接続を除去する 狭）システムの動作に必要ない接続経路は持たない	【QN0】 ▼未使用時の外部接続を遮断する 縮）通信ケーブルを抜く 縮）通信機器の電源をOFFにする	–	–
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				
			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	–
	N1-4. ネットワークスキャンによって調査					
		N1-4a. ネットワークスキャンによって制御システムの存在を把握可能				
			防御策	緩和策	検知策	回復策
			【QN2】 N1-3aと同じ	【QN2】 N1-3aと同じ	【QN2】 ▼外部ネットワークからのアクセスを監視する ・IDSを設置して，スキャンを検知する J-CLICS S2-5-1（システム監視）	–
N2. 入口システム(※)にアクセス　※外部から到達可能な最初のホスト機器（サーバ，PC等）						
	N2-1. 入口システムにアクセス					
		N2-1a. 誰でも入口システムにアクセス可能				
			防御策	緩和策	検知策	回復策
			【QN2】 N1-3aと同じ	【QN2】 N1-3aと同じ	【QN2】 ▼外部ネットワークからのアクセスを監視する ・IDSを導入して，組織外からのアクセスを検知する J-CLICS S2-5-1（システム監視）	–

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
N3. システム情報を取得						
	N3-1. 通信をしかけてフィンガープリント情報を収集					
		N3-1a. 認証前の通信（画面など）からシステム（メーカー名・モデル名・バージョン等）の特定が可能				
			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） 狭）不要なサービスを停止する 【QN4】 ▼外部に与える情報を最小化する 狭）サーバのシステムの特定に利用可能な通信内容やレスポンスを抑制する J-CLICS S2-8-1（システムの強化）	–	【QN2】 N2-1aと同じ	–
N4. 攻撃実施						
	N4-1. 【DoS】大量パケットの送信					
		N4-1a. DoSパケット送信可能				
			防御策	**緩和策**	**検知策**	**回復策**
			（DoSの送信自体を防ぐことはできない）	【QN2】 ▼パケットの流量を制限する 縮）アドレス and/or ポート単位でパケットを制限する J-CLICS S2-4-1（ファイアウォール）	【QN2】 ▼大量のパケットが送られていることを認識する ・IDSを設置して，入口システムへのパケットの流量を監視する J-CLICS S2-5-1（システム監視）	–
	N4-2. 【DoS】認証失敗の乱発					
		N4-2a. 大量認証試行可能				
			防御策	**緩和策**	**検知策**	**回復策**
			（認証試行動作自体を防ぐことはできない）	【QN3】 ▼ 認証試行の濫用を制限する 労）ログイン時の再認証時間を設定する 労）ログイン試行回数を制限する	【QN2】 ▼大量の認証試行が行われていることを認識する ・IDSを設置して，認証で使用するパケットの流量を監視する J-CLICS S2-5-1（システム監視）	–
	N4-3. 【不正アクセス】入口境界防衛の突破					
		N4-3a. デフォルトパスワードが使用されている				
			防御策	**緩和策**	**検知策**	**回復策**
			【QN3】 ▼デフォルトパスワード変更を強制する 遮）デフォルトパスワード変更を強制する機能をシステムに導入する 狭）デフォルトパスワード変更を強制する手順を関係者に強制する	【QN3】 ▼認証手段を増やす 労）多要素認証を導入する 労）多段階の認証を併用する	【QN3】 ▼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での認証を試行してみる ・パスワードの更新日時を監視する	【QN3】 ▼セキュアなパスワードに変更する ・パスワードを変更する
		N4-3b. 脆弱なパスワードが使用されている				
			防御策	**緩和策**	**検知策**	**回復策**
			【QN3】 ▼パスワードポリシーをユーザに強制的に守らせる 遮）パスワードポリシーを遵守させる機能をシステムに導入する 狭）パスワードポリシーを遵守させる手順を関係者に強制する 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） 狭）パスワードポリシーに違反している場合に警告する機能をシステムに導入する 【QN3】 ▼セキュアなパスワードを使用する 狭）セキュアなパスワードを使用する J-CLICS S1-3-2（強力なパスワードの使用）	【QN3】 ▼認証手段を増やす 労）多要素認証を導入する 労）多段階の認証を併用する	【QN3】 ▼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 ・定検時などに，スキャナを用いて認証を試行する ・既知パスワードでの認証を試行する 【QN3】 ▼アクセス状況をログに記録して定期的に監査する J-CLICS S2-5-1（システム監視）	【QN3】 N4-3aと同じ
		N4-3c. 総当たり(ブルートフォース)の認証試行が可能				
			防御策	**緩和策**	**検知策**	**回復策**
			【QN3】 ▼パスワードポリシーをユーザに強制的に守らせる 労）セキュアなパスワードを使用する J-CLICS S1-3-2（強力なパスワードの使用）	【QN3】 ▼認証試行の濫用を制限する 労）ログイン時の再認証時間を設定する 労）ログイン試行回数を制限する	–	–

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
		N4-3d. 関係者からパスワードを入手可能				
			防御策	**緩和策**	**検知策**	**回復策**
			【QN1】 N1-2aと同じ	【QN3】 ▼認証手段を増やす 労）多要素認証を導入する 労）多段階の認証を併用する 【QN3】 ▼パスワードの有効期間を制限する J-CLICS S1-3-3（パスワードの定期的な変更） 【QN3】 ▼ID・パスワードの管理を強化する 管）アカウントの使用状況やパスワードの更新状況を常時または定期的に見直し，不要なアカウントを抹消したりパスワードの更新を促すようにする J-CLICS S2-10-1（転入者と転出者用のプロセス） 管）管理者パスワード等の重要なパスワードは必要最小限の人員のみが知るように管理する J-CLICS S1-3-1（パスワードポリシー）	【QN1】 N1-2aと同じ	【QN3】 N4-3aと同じ
		N4-3e. リモート攻撃可能な脆弱性が存在				
			防御策	**緩和策**	**検知策**	**回復策**
			【QN5】 ▼機器の脆弱性を取り除く 遮）機器にパッチを適用する J-CLICS S2-7-1（セキュリティパッチ） 狭）運転に関係ない脆弱性があるプロセスを削除する J-CLICS S2-8-1（システムの強化） 【QN4】 ▼脆弱性のある機器へのアクセスを遮断する 狭）運転に関係ない脆弱性がある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）	－	【QN5】 ▼リモートからの攻撃で注意すべきアクセスを認識する ・MyJVNなどの外部脆弱性DBを利用して，利用しているソフトウェアやシステムコンポーネントの脆弱性を把握する 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） 【QN5】 ▼使用している機器の脆弱性情報を収集する 【QN5】 ▼実際のリモートからの攻撃を検知する ・IDSを設置して，リモートからの攻撃のパケットを検知する	－
N4-4. 【不正アクセス】内部ネットワークへのアクセス						
		N4-4a. IPによる内部ネットワークアクセスが可能				
			防御策	**緩和策**	**検知策**	**回復策**
			【QN4】 ▼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 遮）不要なルーティングパスを削除する J-CLICS S2-4-1（ファイアウォール） 遮）OSのルーティング設定を見直す（IP-forwardingを停止する） 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を介してアクセスさせる 遮）制御機器において，運転に不要なポートを閉鎖する J-CLICS S2-8-1（システムの強化）	－	【QN4】 ▼IPによる内部ネットワークへのアクセスを検知する ・IDSを設置し，規定の経路以外のトラフィックを監視する 【QN4】 ▼内部ネットワークへのアクセス経路を検知する ・pingやnmapなどを用いて到達性のテストを実施する J-CLICS S2-5-1（システム監視）	－
		N4-4b. 入口システム上での任意プロセス起動が可能				
			防御策	**緩和策**	**検知策**	**回復策**
			【QN5】 ▼脆弱性を利用したプロセスの起動を阻止する 遮）機器にパッチを適用する 狭）運転に関係ないプロセス，ライブラリ，ファイルを削除する 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） 【QN5】 ▼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 遮）プロセスを起動可能なI/Fにアクセス制限をかける 遮）起動可能なプロセスをあらかじめ許可したものに制限する（ホワイトリストベース）	【QN5】 ▼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 縮）起動されたプロセスのアクセス権を制限する J-CLICS S2-8-1（システムの強化）	【QN5】 ▼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 ・ウイルス対策ソフトを導入する ・プロセス起動のログを監視する	－

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
（R0. 無線LAN経路の存在）						
	（R0-1. 無線LANの使用）					
		R0-1a. 無線LANが使用されている				
			防御策	緩和策	検知策	回復策
			【QR0】 ▼無線LANを使用しない 遮）有線LANに切り替える	【QR0】 ▼無線機器の利用を最小限にする 縮）傍受されても無害な通信しか行わない 狭）無線機器が接続されるネットワークを限定する 狭）無線機器経由のアクセス権を厳しく設定する	【QR0】 ▼不正アクセスポイントを監視する ・定期的に電波を観測する 【QR0】 ▼システム構成をチェックする ・機器構成の棚卸を行う	【QR0】 ▼不要な無線機器を取り除く ・設置機器を探し出し，停止する
	（R0-1. 敷地外で無線LANを受信）					
		R0-1b. 敷地外で無線LAN電波が受信可能				
			防御策	緩和策	検知策	回復策
			【QR0】 ▼敷地外まで電波が届かないようにする 狭）シールドで電波漏洩を防止する 狭）無線LAN機器の出力を抑える 狭）指向性アンテナへの変更	–	【QR0】 ▼敷地境界を監視する ・定期的に電波を観測する	–
R1. 無線LAN使用箇所の特定						
	R1-1. SSIDマップサービスから情報を入手					
		R1-1a. SSIDマップサービスで検索可能				
			防御策	緩和策	検知策	回復策
			【QR1】 ▼SSIDを非公開にする 遮）公開しないことを要求する機能を利用する 狭）ブロードキャスト設定を無効にする（ステルス化）	–	【QR1】 ▼定期的に外部サービスへの漏えいを調査する ・該当情報を入手できるかチェックする	【QR1】 ▼漏洩した情報と異なる構成に変更する ・SSIDを変更する
	R1-2. 公開情報から入手					
		R1-2a. 公開情報から設置場所とSSIDの情報が入手可能				
			防御策	緩和策	検知策	回復策
			【QR1】 ▼構成情報を秘密管理し関係者の教育を行う	【QR1】 ▼秘密情報拡散の抑制のための手順を実施する	【QR1】 ▼定期的に外部サービスへの漏えいを調査する	【QR1】 ▼漏洩した情報と異なる構成に変更する
	R1-3. 関係者から入手					
		R1-3a. 関係者から設置場所とSSIDの情報が入手可能				
			防御策	緩和策	検知策	回復策
			【QR1】 ▼構成情報を秘密管理し関係者の教育を行う	【QR1】 ▼秘密情報拡散の抑制のための手順を実施する	【QR1】 ▼定期的に外部サービスへの漏えいを調査する	【QR1】 ▼漏洩した情報と異なる構成に変更する
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				
			防御策	緩和策	検知策	回復策
			【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				
			防御策	緩和策	検知策	回復策
			【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）
	R3-2. 【DoS】脆弱性を悪用したDoS					
		R3-2a. 攻撃可能な脆弱性が存在				
			防御策	緩和策	検知策	回復策
			【QR3】 ▼脆弱性を解消する 狭）適宜，セキュリティパッチをあてる J-CLICS S2-7-1（セキュリティパッチ）	【QR3】 ▼脆弱性のある機器へのアクセスを遮断する 狭）運転に関係ない脆弱性があるポートへのアクセスを遮断する	【QR3】 ▼定期的にシステムや電波状態を調査する J-CLICS S2-5-1（システム監視） 【QR3】 ▼使用している機器の脆弱性情報を収集する	【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）
		R3-2b. DoSパケット送信可能				
			防御策	緩和策	検知策	回復策
			【QR3】 ▼通信をセキュアな設定にする 狭）アクセスポイントに通信フィルターを設定する	–	【QR3】 ▼定期的にシステムや電波状態を調査する 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）

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
	R3-3. 【DoS】認証失敗を乱発する					
		R3-3a(1). 誰でも入口システム（アクセスポイント）にアクセス可能				
			防御策	**緩和策**	**検知策**	**回復策**
			【QR4】 ▼アクセスを制限し承認されていない機器の接続を防ぐ 狭）MACアドレスフィルタリングを設定する 【QR4】 ▼認証手段を強化する 縮）認証開始のトリガーに管理者が関与するようにする	–	【QR3】 ▼定期的にシステムや電波状態を調査する 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）
		R3-3a(2). 大量認証試行可能				
			防御策	**緩和策**	**検知策**	**回復策**
			【QR4】 ▼無線LANセキュリティ装置を導入する 狭）無線IDS/IPSを設置する 【QR4】 ▼アクセスを制限し承認されていない機器の接続を防ぐ 狭）MACアドレスフィルタリングを設定する 縮）認証失敗時にインターバルを設ける 縮）認証回数の制限を設ける 縮）多要素認証を導入する	–	【QR3】 ▼定期的にシステムや電波状態を調査する J-CLICS S2-5-1（システム監視） 【QR4】 ▼無線LANセキュリティ装置を導入する ・無線IDS/IPSを設置する	【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）
	R3-4. 【不正アクセス】入口境界防衛を突破する					
		R3-4a. デフォルトパスワードが使用されている				
			防御策	**緩和策**	**検知策**	**回復策**
			【QR4】 ▼認証手段を強化する 【QR4】 ▼セキュアなパスワードを設定する	【QR4】 ▼認証手段を増やす 労）多要素認証を導入する 労）多段階の認証を併用する	【QR4】 ▼アクセス状況のログ分析を行う	【QR4】 ▼セキュアなパスワードを設定する
		R3-4b. 脆弱なパスワードが使用されている				
			防御策	**緩和策**	**検知策**	**回復策**
			【QR4】 ▼認証手段を強化する 【QR4】 ▼セキュアなパスワードを設定する	【QR4】 ▼認証手段を増やす 労）多要素認証を導入する 労）多段階の認証を併用する	【QR4】 ▼アクセス状況のログ分析を行う	【QR4】 ▼セキュアなパスワードを設定する
		R3-4c. 総当たり(ブルートフォース)の認証試行が可能				
			防御策	**緩和策**	**検知策**	**回復策**
			【QR4】 ▼認証手段を強化する 【QR4】 ▼セキュアなパスワードを設定する	【QR4】 ▼認証手段を増やす 労）多要素認証を導入する 労）多段階の認証を併用する	【QR4】 ▼アクセス状況のログ分析を行う	【QR4】 ▼セキュアなパスワードを設定する
		R3-4d. 関係者からパスワードを入手可能				
			防御策	**緩和策**	**検知策**	**回復策**
			【QR4】 ▼認証手段を強化する 【QR4】 ▼セキュアなパスワードを設定する	【QR4】 ▼認証手段を増やす 労）多要素認証を導入する 労）多段階の認証を併用する	【QR4】 ▼定期的にアカウントの棚卸を行う 【QR4】 ▼アクセス状況のログ分析を行う	【QR4】 ▼セキュアなパスワードを設定する
		R3-4e. リモート攻撃可能な脆弱性が存在				
			防御策	**緩和策**	**検知策**	**回復策**
			【QR3】 ▼脆弱性を解消する 狭）適宜，セキュリティパッチをあてる J-CLICS S2-7-1（セキュリティパッチ）	【QR4】 ▼認証手段を増やす 労）多要素認証を導入する 労）多段階の認証を併用する	【QR4】 ▼アクセス状況のログ分析を行う	【QR4】 ▼セキュアなパスワードを設定する
		R3-4f. 既に攻撃方法が知られている通信プロトコル（WEPなど）を使用				
			防御策	**緩和策**	**検知策**	**回復策**
			【QR3】 ▼通信をセキュアな設定にする 狭）新しい通信プロトコルへ切り替える J-CLICS S2-3-1（ネットワークアーキテクチャ）	–	【QR3】 ▼定期的にシステムや電波状態を調査する 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）
	R3-5. 【不正アクセスポイント設置】偽のアクセスポイントを設置して正規端末からの誤接続を狙う					
		R3-5a. 認証が正しく設定されていないため，同名アクセスポイントに誤って接続する（パスワード未設定など）				
			防御策	**緩和策**	**検知策**	**回復策**
			【QR3】 ▼通信をセキュアな設定にする 遮）認証が必要なプロトコルを使用する 狭）多要素認証を行う	–	【QR3】 ▼定期的にシステムや電波状態を調査する ・定期的に疎通確認を取り，正規システムからポーリング監視する 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）

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
		R3-5b. フリーWi-Fiなどへ自動接続する設定となっている				
			防御策	**緩和策**	**検知策**	**回復策**
			【QR3】 ▼通信をセキュアな設定にする 遮）自動的に接続するような設定にはしない J-CLICS S2-8-1（システム強化） 【QR2】 ▼敷地内にフリーWi-Fiがないようにする 狭）個人所有物を持ち込ませない運用を徹底する	–	【QR3】 ▼定期的にシステムや電波状態を調査する ・棚卸（設定のチェック）を行う ・検証用フリーWi-Fiを使って自動接続してくる機器を見つける ・定期的に電波を観測する	【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）
	R3-6. 【盗聴】無線パケットを盗聴する					
		R3-6a. 盗聴耐性の低いプロトコルが使用されている				
			防御策	**緩和策**	**検知策**	**回復策**
			【QR3】 ▼通信をセキュアな設定にする 狭）新しい通信プロトコル、暗号化方式へ切り替える J-CLICS S2-3-1（ネットワークアーキテクチャ）	【QR3】 ▼通信内容をセキュアにする 難）上位レイヤでデータを暗号化する	【QR3】 ▼定期的にシステムや電波状態を調査する 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）

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
（D0. 経路の存在）						
	（D0-1. 持ち込みデバイス使用）					
		D0-1a. 持ち込みデバイスが使用されている				
			防御策	緩和策	検知策	回復策
			【QD0】 ▼持ち込みデバイスを使用させない 遮）制御システム内で管理したデバイスのみを使用する 狭）デバイスの持ち込みを制限する 管）定期的にデバイスの利用状況を確認する J-CLICS S1-2-1（機器接続手順）	–	–	–
D1. 【無差別攻撃】						
	D1-1. 無差別的なウイルス感染					
		D1-1a. 感染リスクのある持ち込みデバイスが存在する				
			防御策	緩和策	検知策	回復策
			【QD1】 ▼接続可能なデバイスを制限する機能を実装する 狭）デバイスのホワイトリスト機能を実装する	【QD1】 ▼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 狭）予めウイルスチェックしたデータを持ち込みデバイスに保存する J-CLICS S2-6-1（ウイルス対策） 【QD1】 ▼持ち込みデバイスの脆弱性を取り除く 狭）持ち込みデバイスにセキュリティパッチを適用し、脆弱性を取り除く J-CLICS S1-2-1（機器接続手順） 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）	【QD1】 ▼持ち込みデバイスのウイルスチェックを行う J-CLICS S2-6-1（ウイルス対策）	–
D2.【標的型攻撃】						
	D2-1. 制御システム関係者の調査					
		D2-1a. 制御システム関係者の情報が入手可能である				
			防御策	緩和策	検知策	回復策
			–	–	–	–
	D2-2. 制御システム関係者機器への感染					
		D2-2a. 感染リスクのある持ち込みデバイスが存在する				
			防御策	緩和策	検知策	回復策
			【QD1】 D1-1aと同じ	【QD1】 D1-1aと同じ	【QD1】 D1-1aと同じ	—
D3.感染したデバイスを持ち込む（持ち込ませる）						
	D3-1.感染した持ち込みデバイスをオフィスエリアに持ち込ませる（持ち込まれる）					
		D3-1a.オフィスエリアへのデバイスの持ち込みが管理されていない				
			防御策	緩和策	検知策	回復策
			【QD2】 ▼持ち込みデバイスを制限・管理する 狭）必要最低限の利用にとどめ、特定目的及びエリアでの使用に制限・管理する 【QD2】 ▼管理外のデバイスの接続を防止する 遮）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する 【QD2】 ▼備え付けのデバイスを使用させる 遮）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	–	【QD3】 ▼持ち込みデバイスのウイルスチェックを行う ・オフィスエリアなどの中間経路にて持ち込みデバイスのウイルスチェックを行う J-CLICS S2-6-1（ウイルス対策）	–
	D3-2.感染した持ち込みデバイスをベンダーに持ち込ませる（持ち込まれる）					
		D3-2a.ベンダによるデバイスの持ち込みが管理されていない				
			防御策	緩和策	検知策	回復策
			【QD2】 D3-1aと同じ	–	【QD3】 D3-1aと同じ	–
D4.攻撃対象への運搬						
	D4-1.中間経路での検知・防御回避					
		D4-1a. 中間経路に検知・防御の仕組みが存在していない				
			防御策	緩和策	検知策	回復策
			【QD3】 ▼検知・防御の仕組みを導入する 狭）中間経路となるオフィスエリアやベンダ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する	▼中間経路にある機器の脆弱性を取り除く 縮）中間経路の機器に最新のパッチを適応する J-CLICS S2-7-1（セキュリティパッチ） 縮）中間経路の機器の不要なプロセスを削除する J-CLICS S2-8-1（システムの強化）	–	–

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
D5.制御システムへの到達						
	D5-1.感染した持ち込みデバイスをオフィスエリアから持ち込ませる（持ち込まれる）					
		D5-1a. オフィスエリアから制御システムの重要エリアへのデバイスの持ち込みが管理されていない				
			防御策	**緩和策**	**検知策**	**回復策**
			【QD2】 D3-1aと同じ 【QD3】 ▼検知・防御の仕組みを導入する 狭）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などの仕組みを導入する	–	【QD3】 ▼持ち込みデバイスのウイルスチェックを行う ・制御システムの機器に接続する前にウイルスチェックを行う J-CLICS S2-6-1（ウイルス対策）	–
	D5-2.感染した持ち込みデバイスをベンダーに持ち込ませる（持ち込まれる）					
		D5-2a. ベンダによる制御システムのエリアへのデバイスの持ち込みが管理されていない				
			防御策	**緩和策**	**検知策**	**回復策**
			【QD2】 D3-1aと同じ 【QD3】 D5-1aと同じ	–	【QD3】 D5-1aと同じ	–
D6.制御システムに接続されてしまう						
	D6-1.感染した持ち込みデバイスを機器やホストに接続し、ウイルス感染させる					
		D6-1a(1). 機器やホストに感染した持ち込みデバイスを接続可能				
			防御策	**緩和策**	**検知策**	**回復策**
			【QD2】 D3-1aと同じ	–	【QD3】 D5-1aと同じ	–
		D6-1a(2). 機器やホストにウイルス感染などの攻撃に利用可能な脆弱性が存在				
			防御策	**緩和策**	**検知策**	**回復策**
			【QD4】 ▼機器の脆弱性を取り除く 遮）機器にパッチを適用する J-CLICS S2-7-1（セキュリティパッチ） 狭）運転に関係ないソフトウェアやプロセスを削除する J-CLICS S2-8-1（システムの強化）	–	【QD4】 ▼使用している機器の脆弱性情報を収集する ・システムや機器ベンダのから情報を収集し、システムの脆弱性を把握する。	–
		D6-1a(3).機器やホスト上でウイルスが起動可能				
			防御策	**緩和策**	**検知策**	**回復策**
			【QD4】 ▼脆弱性を利用したプロセスの起動を阻止する 遮）機器にパッチを適用する 狭）運転に関係ないプロセス，ライブラリ，ファイルを削除する J-CLICS S2-6-1（ウイルス対策） J-CLICS S2-7-1（パッチ） J-CLICS S2-8-1（サービスや通信ポートの無効化や停止） ▼持ち込みデバイスが接続される機器やホストで任意のプロセスを起動できないようにする	【QD4】 ▼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 縮）起動されたプロセスのアクセス権を制限する J-CLICS S2-8-1（システムの強化）	【QD4】 ▼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 ・ウイルス対策ソフトを導入する ・プロセス起動のログを監視する	–

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
P1. 敷地境界防衛の突破						
	P1-1. フェンス乗り越え					
		P1-1a. 誰にも発見されずにフェンス乗り越え可能				
			防御策	**緩和策**	**検知策**	**回復策**
			【QP1】 ▼乗り越え不可能なフェンスを設置する 狭）十分に高さのあるフェンスを設置する 狭）有刺鉄線等を設置する 狭）電気柵を設置する 【QP1】 ▼フェンスの乗り越えを抑止する 抑）侵入禁止や監視中の表示を行う 抑）監視カメラや侵入検知システムを設置する 抑）見回りを強化する 抑）夜間の照明を強化する	–	【QP1】 ▼侵入検知システムを設置し運用する ・監視カメラを設置する ・フェンスセンサを設置する	【QP2】 ▼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
	P1-2. なりすまし					
		P1-2a. 関係者になりすましてセキュリティ境界を突破可能				
			防御策	**緩和策**	**検知策**	**回復策**
			【QP2】 ▼守衛所での入館手続きを厳格化する 狭）写真入り身分証明書の提示を求める 狭）用務先に照会する 狭）用務先の関係者を呼び出し確認・付き添いを求める 狭）身分証明書の発行元に照会する 【QP2】 ▼IDカードによる認証を強化する 狭）多要素認証・生体認証を使用する 狭）出入り状況をチェックして多重入退を防止する（アンチパスバック） 【QP2】 ▼関係者を装ったなりすましによる侵入を抑止する 抑）関係者および外来者にネームカード等の着用を義務付ける 抑）セキュリティ区画には関係者以外立ち入り禁止の表示を行う 抑）監視カメラや侵入検知システムを設置する 抑）セキュリティ区画への順路に人が常駐する場所を設置する	–	【QP2】 ▼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する J-CLICS S1-1-1（身分証明書の着用）	【QP2】 P1-1aと同じ
P2. 建物境界防衛の突破						
	P2-1. 関係者の後について入館					
		P2-1a. 関係者の後についてセキュリティ境界を突破可能				
			防御策	**緩和策**	**検知策**	**回復策**
			【QP2】 ▼共連れ（tail gating）対策を強化する 狭）２重ドア構造のセキュリティゲート（man traps）を設置する 狭）共連れ検知機能付きのセキュリティゲートを設置する 狭）入室時に不審者の確認と排除を徹底する J-CLICS S1-1-2（訪問者への付添い） 抑）「一人ずつお入りください」等の表示を行う 抑）セキュリティゲートの監視を強化する 【QP2】 ▼IDカードによる入退管理を強化する 遮）多重入退（passback）をチェックする 遮）セキュリティゲート内外を壁や多重ドアで分離してIDカードなどの受け渡しができないようにする	–	【QP2】 P1-2aと同じ	【QP2】 P1-1aと同じ
P3. 部屋境界防衛の突破						
	P3-1. 関係者の後について入室					
		P3-1a. 関係者の後について入室可能				
			防御策	**緩和策**	**検知策**	**回復策**
			【QP2】 ▼共連れ（tail gating）対策を強化する 狭）２重ドア構造のセキュリティゲート（man traps）を設置する 狭）共連れ検知機能付きのセキュリティゲートを設置する 狭）入室時に不審者の確認と排除を徹底する J-CLICS S1-1-2（訪問者への付添い） 抑）「一人ずつお入りください」等の表示を行う 抑）セキュリティゲートの監視を強化する 【QP2】 ▼IDカードによる入退管理を強化する 遮）多重入退（passback）をチェックする 遮）セキュリティゲート内外を壁や多重ドアで分離してIDカードなどの受け渡しができないようにする	–	【QP2】 P1-2aと同じ	【QP2】 P1-1aと同じ

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
P4. 機器施錠管理の突破						
	P4-1. 合鍵の利用					
		P4-1a. 合鍵が入手可能				
			防御策	**緩和策**	**検知策**	**回復策**
			【QP3】 ▼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）にする 【QP3】 ▼錠を多重化する 労）別の種類の錠を組み合わせて使用する 【QP3】 ▼鍵や錠の監視を強化する 抑）鍵保管場所をカメラ等で監視する 【QP3】 ▼鍵の管理を強化する 狭）鍵の持ち出しを禁止する 管）鍵の使用を管理台帳に記録する 狭）鍵の貸出・返却を複数の関係者で確認する 狭）鍵の保管場所を複数の関係者が持つ複数の鍵で施錠管理する 【QP3】 ▼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	–	【QP3】 ▼防犯センサを設置する J-CLICS S1-1-3（監視カメラの設置）	【QP3】 ▼鍵が漏えいしている疑いのある錠および鍵を変更する J-CLICS S1-1-2（訪問者への付添い）
	P4-2. 物理的な破壊					
		P4-2a. 錠が物理破壊可能				
			防御策	**緩和策**	**検知策**	**回復策**
			【QP3】 ▼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）にする 【QP3】 ▼破壊されづらいように対策された錠・ドアを使用する 狭）ヒンジ破壊を防止するドアを設置する 狭）ヒンジ破壊時にドアを取り外せないようドアボスを設置する 狭）ドアフレームや防犯プレートなどによりドアの隙間をカバーする J-CLICS S1-1-2（訪問者への付添い）	–	【QP3】 ▼防犯センサを設置する ・振動センサを設置して物理破壊時の振動を検知する ・音響センサを設置して物理破壊時の音響を検知する J-CLICS S1-1-3（監視カメラの設置）	–
P5. 機器への物理アクセス						
	P5-1. デフォルトパスワードの試行					
		P5-1a. デフォルトパスワードが使用されている				
			防御策	**緩和策**	**検知策**	**回復策**
			【ネットワーク経路N4-3aと同じ】 ▼デフォルトパスワード変更を強制する 遮）デフォルトパスワード変更を強制する機能をシステムに導入する 狭）デフォルトパスワード変更を強制する手順を関係者に強制する	【ネットワーク経路N4-3aと同じ】 ▼認証手段を増やす 労）多要素認証を導入する 労）多段階の認証を併用する（前段に認証付きの機器を追加するなど）	【ネットワーク経路N4-3aと同じ】 ▼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での認証を試行してみる ・パスワードの更新日時を監視する	【ネットワーク経路N4-3aと同じ】 ▼セキュアなパスワードに変更する ・パスワードを変更する
	P5-2. 不正入手したID・パスワードの使用					
		P5-2a. ID・パスワードが不正入手可能				
			防御策	**緩和策**	**検知策**	**回復策**
			【ネットワーク経路N4-3dと同じ】 ▼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 ▼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 ▼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 ▼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）	【ネットワーク経路N4-3dと同じ】 ▼認証手段を増やす 労）多要素認証を導入する 労）多段階の認証を併用する（前段に認証付きの機器を追加するなど） ▼パスワードの有効期間を制限する J-CLICS S1-3-3（パスワードの定期的な変更） ▼ID・パスワードの管理を強化する 管）ID・パスワードによる権限付与状況を定期的に見直し，不要な権限は削除する J-CLICS S2-10-1（アカウントの定期見直し） 管）管理者パスワード等の重要なパスワードは必要最小限の人員のみが知るように管理する（覚えられない文字列にして紙ベースなどで施錠管理するのも良い） J-CLICS S1-3-1（パスワードの管理施策）	【ネットワーク経路N4-3dと同じ】 ▼認証手段を増やす 労）多要素認証を導入する 労）多段階の認証を併用する（前段に認証付きの機器を追加するなど） ▼パスワードの有効期間を制限する J-CLICS S1-3-3（パスワードの定期的な変更） ▼ID・パスワードの管理を強化する 管）ID・パスワードによる権限付与状況を定期的に見直し，不要な権限は削除する J-CLICS S2-10-1（転入者と転出者用のプロセス） 管）管理者パスワード等の重要なパスワードは必要最小限の人員のみが知るように管理する（覚えられない文字列にして紙ベースなどで施錠管理するのも良い） J-CLICS S1-3-1（パスワードポリシー）	【ネットワーク経路N4-3dと同じ】 ▼セキュアなパスワードに変更する ・パスワードを変更する

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
	P5-3. ID・パスワードの類推					
		P5-3a. 脆弱なパスワードが使用されている				
			防御策	**緩和策**	**検知策**	**回復策**
			【ネットワーク経路N4-3bと同じ】 ▼パスワードポリシーをユーザに強制的に守らせる 遮）パスワードポリシーを遵守させる機能をシステムに導入する 狭）パスワードポリシーを遵守させる手順を関係者に強制する 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） 狭）パスワードポリシーに違反している場合に警告する機能をシステムに導入する 【QN3】 ▼セキュアなパスワードを使用する 狭）セキュアなパスワードを使用する J-CLICS S1-3-2（強力なパスワードの使用）	【ネットワーク経路N4-3b参と同じ】 ▼認証手段を増やす 労）多要素認証を導入する 労）多段階の認証を併用する（前段に認証付きの機器を追加する）	【ネットワーク経路N4-3bと同じ】 ▼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 ・定検時などに，スキャナを用いて認証を試行する ・既知パスワードでの認証を試行する ▼アクセス状況をログに記録して定期的に監査する J-CLICS S2-5-1（システム監視）	【ネットワーク経路N4-3bと同じ】 ▼セキュアなパスワードに変更する ・パスワードを変更する