No.	チェック項目	該当章	チェック
	ハードウェア		
1	Edgecrossを搭載する産業用PCを十分に信頼できる調達元から調達している	3.2.1	
2	Edgecrossを搭載する産業用PCを設置する際には以下のような物理的対策を実施している ・セキュリティワイヤのロックや施錠できるPCラックによる盗難対策 ・USB/LANの物理ロックによる接続対策 ・オペレータの入出制限	3.2.1	
3	Edgecrossを搭載する産業用PCの初期設定を適切に実施する ・BIOSパスワード、HDDパスワードなどのパスワード設定 ・ブートドライブの設定 ・USB設定 ・Wake on Lanなどの外部制御を可能にする機能の設定 ・TPMなどのセキュリティチップの設定	3.2.1	
4	Edgecrossを搭載する産業用PCのCPUやチップセットのファームウェア・BIOS、ストレージやネットワークカードのファームウェア・ドライバなどを適切にアップデートする	3.2.1	
5	Edgecrossを搭載する産業用PCのハードウェアのサポート期間内で運用する	3.2.1	
	OS		
6	ユーザの役割に応じてWindowsのアカウントを設定し、他者が推定しにくいパスワードを設定するなど、適切な管理を実施する	3.2.2	

7	Windowsのシステムに重要な変更が行われる場合に、管理者権限ユーザに許可を求めるセキュリティ機能を有効にする	3.2.2	
8	カメラ機能やマイク機能など、Edgecrossの運用に不要な機能は無効化する	3.2.2	
9	USBやBluetoothなど外部からの物理アクセスは可能な限り制限または無効化する	3.2.2	
10	マルウェア対策として、Windows搭載のセキュリティ機能かサードパーティ製のセキュリティソフトウェアを導入する	3.2.2	
11	パーソナルファイアウォールにて不要なネットワークアクセスを遮断する	3.2.2	
12	汎用的に利用するPCについては、Windows Updateにより更新プログラムを適用して、常に最新の状態に保つようにする	3.2.2	
13	特定の用途で利用する産業用PCなどでは、Windows Server Update Servicesを利用する、更新プログラムの動作検証用に試験用機器を用意するなどを行い、Edgecrossの運用に問題ないことを確認してから更新する	3.2.2	
セキュリティソフトウェア			
14	システムの用途や運用に沿ってマルウェア対策ソフトウェア等のセキュリティソフトウェアを選定・導入する	3.3.1	
15	ライセンス契約など、利用期間の制限がある場合、システム稼働中は継続して使用できるように契約を更新する	3.3.1	
16	定期的またはシステム更改のタイミングで、マルウェア対策ソフトウェアのアップデートを行う	3.3.1	
17	マルウェア対策ソフトウェアによるシステム全体のスキャンを定期的に行う	3.3.1	
Edgecross基本ソフトウェア			

データモデル管理			
18	マネジメントシェルエクスプローラが不正なユーザに操作されないように、Edgecross搭載PCには信頼できるユーザのみがログイン（Windowsへのログイン）できるように設定する	3.4.2	
19	エッジアプリケーションは、Edgecrossマーケットプレイスなど、信頼できる提供元から入手する	3.4.2	
20	ITゲートウェイが利用可能な場合、OPC UAはEdgecross搭載PC外からのアクセスを禁止し、エッジアプリケーションをEdgecross搭載PC内に配置する構成とする	3.4.2	
リアルタイムデータ処理			
21	リアルタイムフローデザイナが不正なユーザに操作されないように、Edgecross搭載PCには信頼できるユーザのみがログイン（Windowsへのログイン）できるように設定する（No.18と同じ）	3.4.3	
22	脆弱な状態でMQTTを公開しないように注意する	3.4.3	
23	共有フォルダには適切なユーザアカウント/パスワードを設定する	3.4.3	
24	ユーザアカウントを使用しないリモート共有フォルダは十分信頼できるネットワーク内で限定して使用する	3.4.3	
25	コマンドライン実行を使用する際には、十分な検討を行い、悪意あるデータがプログラムで実行される可能性について考慮する。データ注入による攻撃について懸念が払拭できない場合、診断データをプログラム引数に指定する機能を使用しない	3.4.3	
26	エッジアプリケーションは、Edgecrossマーケットプレイスなど、信頼できる提供元から入手する（No.19と同じ）	3.4.3	

27	プラグインは、Edgecrossマーケットプレイスなど、信頼できる提供元から入手する	3.4.3	
28	外部ITシステムからのEdgecrossへのアクセスをITゲートウェイ経由として堅牢なシステムを構築する（No.20に近い）	3.4.3	
	保守・運用		
29	Edgecross基本ソフトウェアは最新版を利用する	3.4.4	
30	ソフトウェアのアップデートにおいては動作検証の上、実行する	3.4.4	
31	関連するOSSについても脆弱性の対処を実施する	3.4.4	
32	Edgecrossシステムの管理者は、セキュリティインシデント、故障、ソフトウェアの不具合の発生などの情報を得るため、イベント情報の履歴をチェックする	3.4.4	
	ネットワーク		
33	制御情報ネットワークやFAネットワーク上の機器やその機器で使用されるアプリケーション(通信プロトコル)などの情報をリストアップし、資産管理一覧を作成する	3.5	
34	制御情報ネットワークやFAネットワークの物理構成や論理構成、データの流れなどが分かるネットワーク構成図を作成する	3.5	
35	工場の出入口となる制御情報ネットワークと、通常の全社情報システムネットワーク（以下、IT系ネットワーク）を接続する場合、IT系ネットワークからのマルウェア進入を防ぐため、ファイアウォール装置（以下、FW装置）を設置する	3.5	
36	FW装置に侵入防止システム（次世代IPS）の追加、もしくは、これに準ずる機能を搭載した次世代FWを設置する	3.5	

37	制御情報ネットワークには、ネットワーク通信から不正な振る舞いや異常を検知し、リスク脅威と対応優先度を可視化する内部対策装置（サイバー攻撃検知センサー）を設置する	3.5	
38	誤った操作や疑わしい通信を防ぎ、設定を自動生成する機能を備えたホワイトリスト(アクセス許可リスト)スイッチを設置する	3.5	
39	事情によりセキュリティ対策ソフトウェアの追加が困難な制御端末に関しては、代替案として装置のLANポートに産業用次世代IPSの接続を行う	3.5	
40	現場内にUSBデバイスが存在する場合、USBデバイスを使ったデータ収集を行うポイントでは、インストール不要のマルウェア検索・駆除ツールを使用し、端末の健全性を確保する	3.5	
41	未登録の端末やNG登録された端末の接続を防止するネットワーク型の対策を導入する	3.5	
42	大規模ネットワーク環境でメンテナンスサービスを提供する場合には、安全性を確保するため、遠隔GWの接続を行い、以下の対策を検討する ・Dynamic virual private networkの利用 ・接続する設備のホワイトリストアクセス制御 ・産業用次世代FWやGW経由のインターネット接続	3.5	
運用におけるセキュリティ対策			
脆弱性対策			
43	産業用PCに導入されているソフトウェア（Edgecross基本ソフトウェア、OS、その他アプリケーション）のバージョン管理を実施する	4.1	

44	Edgecross基本ソフトウェアは最新版を利用する	4.1	
45	Edgecross基本ソフトウェアに関連するOSS（オープンソースソフトウェア）は動作確認がされた新しいバージョンを利用する	4.1	
46	エッジアプリケーションおよびデータコレクタについては、開発元やマーケットプレイスから情報を入手して脆弱性対策を実施する	4.1	
47	産業用PCやそれに接続された装置のBIOSやドライバについても、開発元から情報を入手し、脆弱性があれば、動作検証の上、脆弱性を解消したバージョンを適用する	4.1	
セキュリティ管理・インシデント対応			
48	Edgecrossシステム内に存在する機器について、セキュリティ上重要なアップデート等を必要なタイミングで適切に実施する方法を検討し、適用する	4.2	
49	Edgecrossシステムの構築者・運用者は、システムの脆弱性情報を収集・分析し、関係者に情報発信する	4.2	
50	システムへの不用意なつなぎ方によるリスクや、守ってもらいたいことを関係者へ周知する	4.2	
51	Edgecrossシステムの各種機器メーカーや提供者、システム管理者や運用者など、関係者の役割を整理する	4.2	
52	脆弱性を持つ機器を把握する仕組みを構築し、定期的な監視を組織的に行う	4.2	
53	脆弱性を持つ機器を特定した場合には、該当する機器の管理者へ注意喚起を行い、できるだけ速やかに脆弱性対応を実施する	4.2	
54	Edgecross基本ソフトウェアの履歴やネットワークのログ等を確認する仕組みを構築して定期的な監視を行い、インシデントを早期に検知できる体制を整備する	4.3	

55	インシデント検知時には、事前に整備した対応手順に基づいて、被害が最小限となるよう対応できる体制を整備する	4.3	
56	関係者との連絡・連携により、インシデントに関する原因究明と復旧作業を迅速に行える体制を整備する	4.3	