別紙（資産一覧表）

パターン1

No.		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
資産名		進捗管理用パソコン	ノートパソコン（無線接続）	ファイアウォール（インターネット）	ファイアウォール（管理棟）	ファイアウォール（工場）	File Server	MES Server	MES Client	エンジ用PC	ルータ	Edgecross搭載PC 1	Edgecross搭載PC 2	HMI	PLC	制御機器 1	制御機器 2	工作機械 1	工作機械 2
資産種別	情報系資産	○	○				○	○	○	○		○	○						
	制御系資産													○	○	○	○	○	○
	ネットワーク資産			○	○	○					○								
資産の持つ機能	入出力	○	○				○	○	○	○		○	○	○					
	データ保存						○												
	コマンド発行							○	○	○		○	○	○	○				
	ゲート			○	○	○					○								
回線種別		LAN(有線)	LAN(有線／無線)	LAN／WAN(有線)	LAN／WAN(有線)	LAN／WAN(有線)	LAN(有線)	LAN(有線)	LAN(有線)	LAN(有線)	LAN(有線)	LAN(有線)	LAN(有線)	LAN(有線)	LAN(有線)	LAN(有線)	LAN(有線)	LAN(有線)	LAN(有線)
設置場所		管理棟	管理棟		管理棟	工場(DMZ)	工場(DMZ)	工場(DMZ)	工場	工場	工場	工場	工場	工場	工場	工場	工場	工場	工場
接続先NW	情報ネットワーク	○	○	○	○														
	DMZ			○		○	○	○											
	制御情報ネットワーク			○		○			○	○	○		○		○				
	制御ネットワーク										○	○						○	○
	コントローラ間ネットワーク													○	○	○	○		
	インターネット		○	○	○	○						○	○						
管理ポートの接続先		×	×	情報ネットワーク	情報ネットワーク	DMZ	×	×	×	×	制御情報ネットワーク	×	×	×	×	×	×	×	×
操作I/Fの有無		○	○	×	×	×	○	○	○	○	×	○	○	○	×	×	×	○	○
USBポート/送信I/Fの利用		○(USB)	○(USB)	○(LAN)	○(LAN)	○(LAN)	○(USB)	○(USB)	○(USB)	○(USB)	○(LAN)	○(USB)	○(USB)	×	×	×	×	×	×
媒体・機器接続の定常運用の有無		×	×	×	×	×	×	×	×	×	×	○	○	×	×	×	×	×	×
無線機能の有無		×	○	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×	×
定常稼働、非定常稼働		定常稼働	定常稼働	定常稼働	定常稼働	定常稼働	定常稼働	定常稼働	定常稼働	定常稼働	定常稼働	定常稼働	定常稼働	定常稼働	定常稼働	定常稼働	定常稼働	定常稼働	定常稼働
データの種別と経路		別途記載													別途記載				
構築ベンダ／機器メーカー		A社／X社	A社／X社	A社／Y社	A社／Y社	A社／Y社	A社／X社	A社／X社	A社／X社	A社／X社	A社／Y社	A社／X社	A社／X社	A社／Z社	A社／Z社	A社／Z社	A社／Z社	A社／Z社	A社／Z社
OSの種類／バージョン		Windows 10	Windows 10	独自OS	独自OS	独自OS	Windows Server 2016	Windows Server 2016	Windows 10	Windows 10	独自OS	Windows 10	Windows 10	独自OS	独自OS	独自OS	独自OS	独自OS	独自OS
使用するプロトコル		TCP,UDP	TCP,UDP	TCP,UDP	TCP,UDP	TCP,UDP	TCP,UDP	TCP,UDP	TCP,UDP	TCP,UDP	TCP,UDP	TCP,UDP	TCP,UDP	CC-LinkIE	TCP,UDP,CC-LinkIE	CC-LinkIE	CC-LinkIE	TCP,UDP	TCP,UDP
セキュリティ対策(※)		デバイス接続・利用制限[19]、権限管理[23]	デバイス接続・利用制限[19]、権限管理[23]	FW(パケットフィルタリング型)[1]	FW(パケットフィルタリング型)[1]	FW(パケットフィルタリング型)[1]	デバイス接続・利用制限[19]、権限管理[23]	デバイス接続・利用制限[19]、権限管理[23]	デバイス接続・利用制限[19]、権限管理[23]	デバイス接続・利用制限[19]、権限管理[23]		デバイス接続・利用制限[19]、権限管理[23]	デバイス接続・利用制限[19]、権限管理[23]						

※IPA「制御システムのセキュリティリスク分析ガイド 第2版」の「表4-29 セキュリティ対策項目一覧」のセキュリティ対策を記載

別紙(資産一覧表)
パターン2

No.		1	2	3	4	6	7	8	9	10
資産名		事務用PC	エンジPC	File Server	生産管理 ｱﾌﾟﾘｹｰｼｮﾝ	L2 Switch	Edgecross 搭載PC	工作機械1	工作機械2	工作機械3
資産種別	情報系資産	○	○	○	○		○			
	制御系資産							○	○	○
	ネットワーク資産					○				
資産の持つ機能	入出力	○	○	○	○		○			
	データ保存			○						
	コマンド発行		○		○		○			
	ゲート					○				
回線種別		LAN(有線)	LAN(有線)	LAN(有線)	LAN(有線)	LAN(有線)	LAN(有線)	LAN(有線)	LAN(有線)	LAN(有線)
設置場所		事務所	事務所	事務所	事務所	工場	工場	工場	工場	工場
接続先NW	情報ネットワーク									
	DMZ									
	制御情報ネットワーク	○	○	○	○	○	○	○	○	○
	制御ネットワーク									
	ｺﾝﾄﾛｰﾗ間ﾈｯﾄﾜｰｸ									
	インターネット									
管理ポートの接続先		×	×	×	×	×	×	×	×	×
操作I/Fの有無		○	○	○	○	×	○	×	×	×
USBポート/送信I/Fの利用		○(USB)	○(USB)	○(USB)	○(USB)	×	○(USB)	×	×	×
媒体・機器接続の定常運用の有無		×	×	×	×	×	○	×	×	×
無線機能の有無		×	×	×	×	×	×	×	×	×
定常稼働、非定常稼働		定常稼働	定常稼働	定常稼働	定常稼働	定常稼働	定常稼働	定常稼働	定常稼働	定常稼働
データの種別と経路		別途記載								
構築ベンダ／機器メーカー		A社／X社	A社／X社	A社／X社	A社／X社	A社／Y社	A社／X社	A社／Z社	A社／Z社	A社／Z社
OSの種類／バージョン		Windows 10	Windows 10	Windows 10	Windows 10	独自OS	Windows 10	独自OS	独自OS	独自OS
使用するプロトコル		TCP,UDP	TCP,UDP	TCP,UDP	TCP,UDP	TCP,UDP	TCP,UDP	TCP,UDP	TCP,UDP	TCP,UDP
セキュリティ対策		デバイス接続・利用制限[19],権限管理	デバイス接続・利用制限[19],権限管理	デバイス接続・利用制限[19],権限管理	デバイス接続・利用制限[19],権限管理		デバイス接続・利用制限[19],権限管理			

※IPA「制御システムのセキュリティリスク分析ガイド 第2版」の「表4-29 セキュリティ対策項目一覧」のセキュリティ対策を記載

別紙（攻撃シナリオ）パターン1

※1：攻撃拠点は、攻撃対象に対して最終攻撃を行う事が出来る機器や場所を想定

No.	事業被害	事業被害レベル	事業被害の概要と攻撃シナリオ							
1	広域での製品供給停止	3	事業被害の概要	製造設備等へのサイバー攻撃により、広域において製品の供給停止が発生し、社会に多大な影響を及ぼし、賠償費用等の高額な損失が生じると共に、当社の信頼が大きく低下する。				影響を受ける A、I、C		
			シナリオ#	攻撃シナリオ	攻撃拠点（※1）	攻撃対象（※2）	最終攻撃	可用性	完全性	機密性
			1-1	MES Serverと各装置間の通信妨害により、生産管理データを消失し、製造工程の管理、作業者への指示ができなくなり、製造が停止する。	情報ネットワーク DMZ 制御情報ネットワーク	MES Server	MES Serverと各装置間の通信妨害による、生産管理データを消失	○	○	－
			1-2	MES Serverがマルウェアに感染する事により、生産管理データを消失し、製造工程の管理、作業者への指示ができなくなり、製造が停止する。	インターネット 情報ネットワーク DMZ 制御情報ネットワーク	MES Server	MES Serverがマルウェアに感染し、生産管理データを消失	○	○	－
			1-3	Edgecross搭載PCがマルウェアに感染し、生産停止が実行され、生産が停止する。	インターネット DMZ 制御情報ネットワーク 制御ネットワーク	Edgecross搭載PC	Edgecross搭載PCがマルウェアに感染し、生産停止操作を実行する	○	－	－
2	限定地域での製品供給停止	2	事業被害の概要	製造設備等へのサイバー攻撃により、限定地域において供給停止が発生し、社会に影響を及ぼし、賠償費用等の損失が生じると共に、当社の信頼が低下する。				影響を受ける A、I、C		
			シナリオ#	攻撃シナリオ	攻撃拠点（※1）	攻撃対象（※2）	最終攻撃	可用性	完全性	機密性
			2-1	Edgecross搭載PCに無許可のアプリケーションがインストールされ、処理性能に支障が発生し、アクセスに遅延が発生する。	制御情報ネットワーク 制御ネットワーク	Edgecross搭載PC	Edgecross搭載PCに無許可のアプリケーションがインストールされる。	○	○	－
			2-2	HMIがマルウェアに感染する事により、監視操作等の作業ができなくなり、製造の一部が停止する。	コントローラ間ネットワーク	HMI	HMIがマルウェアに感染し、監視操作等の作業を不能にする	○	－	－
			2-3	システムの脆弱性についての認識が不十分で、脆弱性が残ったままの状態になっており、システムの脆弱性をついた攻撃を受ける。	インターネット	Edgecross搭載PC	サーバや制御機器の不正操作による、工場停止	○	－	－
			2-4	作業員等の身元確認や行動監視が不十分で、内部作業員等から攻撃を受ける。	制御情報ネットワーク 制御ネットワーク	Edgecross搭載PC	サーバや制御機器の不正操作による、工場停止	○	－	－
			2-5	構内回線の管理が不十分で、勝手に不正な外部回線を引き込まれ、管理外の外部ネットワーク接続経由で不正接続や攻撃を受ける。	インターネット	Edgecross搭載PC	サーバや制御機器の不正操作による、工場停止	○	－	－
			2-6	外部ネットワークに接続された情報系端末のセキュリティ対策が不十分なため、情報系端末経由で、施設内への攻撃を受ける。	インターネット	Edgecross搭載PC	サーバや制御機器の不正操作による、工場停止	○	－	－
			2-7	外部接続用ネットワーク機器のセキュリティ対策が十分でなく、外部ネットワーク接続経由で攻撃を受ける。	インターネット	Edgecross搭載PC	サーバや制御機器の不正操作による、工場停止	○	－	－
			2-8	Edgecross搭載PCが専用の管理区画に設置されておらず、所定の作業員以外による不正操作が行われる。	制御情報ネットワーク 制御ネットワーク	Edgecross搭載PC	不正操作による工場停止や設定値改ざん、情報流出等の発生	○	○	○
			2-9	Edgecross搭載PC設置区画への入退室が適切に管理されておらず、所定の作業員以外による不正操作が行われる。	制御情報ネットワーク 制御ネットワーク	Edgecross搭載PC	不正操作による工場停止や設定値改ざん、情報流出等の発生	○	○	○
			2-10	Edgecross搭載PCが通信相手を認証しておらず、不正な命令を実行してしまい、不正な動作をさせられる。	インターネット DMZ 制御情報ネットワーク 制御ネットワーク	Edgecross搭載PC	不正操作による工場停止や設定値改ざん、情報流出等の発生	○	○	○

別紙（攻撃シナリオ）パターン1

※1：攻撃拠点は、攻撃対象に対して最終攻撃を行う事が出来る機器や場所を想定

No.	事業被害	事業被害レベル	事業被害の概要と攻撃シナリオ							
3	仕様不良 製品の供給	2	事業被害の概要	製造設備等へのサイバー攻撃により、規定の仕様を満たさない製品を顧客に供給してしまい、社会に影響を及ぼし、 賠償費用等の損失が生じると共に、当社の信頼が低下する。				影響を受ける A、I、C		
			シナリオ#	攻撃シナリオ	攻撃拠点（※1）	攻撃対象（※2）	最終攻撃	可用性	完全性	機密性
			3-1	MES Serverがマルウェアに感染する事により、生産管理データの改ざんされ、 製造工程の管理、作業者への指示が意図しない指示になり、仕様不良の製品を供給する。	インターネット 情報ネットワーク DMZ 制御情報ネットワーク	MES Server	MES Serverがマルウェアに感染し、生産管理データの改ざん	○	○	－
			3-2	MES Clientがマルウェアに感染する事により、生産管理データの改ざんされ、 製造工程の管理、作業者への指示が意図しない指示になり、仕様不良の製品を供給する。	DMZ 制御情報ネットワーク 制御ネットワーク	MES Client	MES Clientがマルウェアに感染し、生産管理データの改ざん	○	○	－
4	設備の破壊	3	事業被害の概要	製造設備等へのサイバー攻撃により、設備が破壊されて供給停止が発生すると共に、従業員や近隣住民の死傷者が出て、 社会に多大な影響を及ぼし、賠償費用等の高額な損失が生じると共に、当社の信頼が大きく低下する。				影響を受ける A、I、C		
			シナリオ#	攻撃シナリオ	攻撃拠点（※1）	攻撃対象（※2）	最終攻撃	可用性	完全性	機密性
			4-1	PLCに適切でない目標値を入力されることにより、 設備の制御が異常となり設備が破壊される。	制御情報ネットワーク コントローラ間ネットワーク	PLC	PLCに、不正な目標値を入力する	○	○	－
			4-2	エンジPCがマルウェアに感染する事により、適切でないエンジニアリング設定され、 設備の制御が異常となり、各設備が破壊される。	DMZ 制御情報ネットワーク 制御ネットワーク	エンジPC	エンジPCがマルウェアに感染し、 エンジニアリング設定を改ざんされる。	○	○	－
			4-3	HMIの脆弱性についての認識が不十分で、脆弱性が残ったままの状態になっており、システムの脆弱性をついた攻撃を受ける。	コントローラ間ネットワーク	HMI	HIMの停止による無監視状態の発生	○	－	－
			4-4	端末設置場所に対して、許可された入退者に限定するような管理ができておらず、所定の作業員以外による画面の盗み見、不正操作が行われる。	工場	エンジPC	不正操作による設備停止や設定値改ざん、情報流出等の発生	○	○	○
			4-5	システムの権限管理や作業監視が十分でなく、所定の作業員がその権限を越えて、システムや端末／制御盤に不正操作をする。	工場	エンジPC	不正操作による設備停止や設定値改ざん、情報流出等の発生	○	○	○
			4-6	HMIのログイン管理やログイン情報の管理が不十分であり、正規の作業員以外により不正ログイン、不正操作がされる。	工場	HMI	不正操作による設備停止や設定値改ざんの発生	○	○	－
			4-7	HMIの権限管理や作業監視が十分でなく、所定の作業員が、その権限を越えて、システムや端末に不正操作をする。	工場	HMI	不正操作による設備停止や設定値改ざんの発生	○	○	－
			4-8	セキュリティ確認がされていないUSB等の外部媒体接続時に、外部媒体経由でマルウェアに侵入されてしまう。	外部媒体	Edgecross搭載PC	Edgecross搭載PCの停止や設定改ざん、情報流出等の発生	○	○	○
			4-9	セキュリティ確認がされていない外部持込端末接続時に、外部持込端末経由でマルウェアに侵入されてしまう。	外部持込端末	Edgecross搭載PC	Edgecross搭載PCの停止や設定改ざん、情報流出等の発生	○	○	○
			4-10	ネットワーク機器の空きポートが接続可能な状態で放置されており、不正端末を接続され、マルウェアを送り込まれる。	FWの空きポート	Edgecross搭載PC	Edgecross搭載PCの停止や設定改ざん、情報流出等の発生	○	○	○
			4-11	サーバの脆弱性についての認識が不十分で、脆弱性が残ったままの状態になっており、システムの脆弱性をついた攻撃を受ける。	インターネット 情報ネットワーク DMZ 制御情報ネットワーク	Edgecross搭載PC	Edgecross搭載PCの停止や設定改ざん、情報流出等の発生	○	○	○
			4-12	PLCに通信相手を認証する仕組みがなく、不正な命令を実行してしまい、不正な動作をさせられる。	制御情報ネットワーク コントローラ間ネットワーク	PLC	不正操作による設備停止や設定値改ざんの発生	○	○	－
			4-13	PLCのID・パスワードが適切に設定されておらず、侵入者に容易にアクセスされ、不正操作をされる。	工場	PLC	不正操作による設備停止や設定値改ざんの発生	○	○	－
			4-14	工作機械や制御機器の脆弱性についての認識が不十分で、脆弱性が残ったままの状態になっており、システムの脆弱性をついた攻撃を受ける。	制御ネットワーク コントローラ間ネットワーク	工作機械、 制御機器	攻撃による工作機械、制御機器の停止	○	－	－
			4-15	ゲートウェイ機器に通信先を制限する仕組みがなく、不正な命令を実行してしまい、不正な動作をさせられる。	制御情報ネットワーク 制御ネットワーク	ルータ	不正操作による設備停止や設定値改ざんの発生	○	○	－
			4-16	各種制御盤・分電盤に業界で広く通用する鍵がついており容易に開錠され、所定の作業員以外による不正操作が行われる。	工場	各装置	不正操作による設備停止や設定値改ざんの発生	○	○	－
			4-17	スイッチ等のネットワーク機器の設置場所が安全管理されておらず誰でも触ることができる状態にあり、所定の作業員以外による不正操作が行われる。	工場	FW, ルータ	不正操作による設備停止や設定値改ざんの発生	○	○	－

別紙（攻撃シナリオ）パターン1

※1：攻撃拠点は、攻撃対象に対して最終攻撃を行う事が出来る機器や場所を想定

No.	事業被害	事業被害レベル	事業被害の概要と攻撃シナリオ							
5	大規模対策費用の発生	1	事業被害の概要	サイバー攻撃を受け、製品の供給停止の被害は発生しなかったものの、現行対策の脆弱性が明らかとなり、その解消のために膨大な対策費用が発生する。				影響を受ける A、I、C		
			シナリオ#	攻撃シナリオ	攻撃拠点（※1）	攻撃対象（※2）	最終攻撃	可用性	完全性	機密性
			5-1	保守等の理由で外部接続と知らぬ間に接続されたことにより、管理外の外部ネットワーク接続経由でマルウェア感染や不正侵入を受ける。	インターネット	MES Server	マルウェア感染や不正侵入によるデータ改ざんや情報漏えいの発生	－	○	○
			5-2	ファイアウォールのセキュリティ対策が十分でなく、外部ネットワーク接続経由で侵入を受ける。	インターネット	MES Server	不正侵入によるデータ改ざんや情報漏えいの発生	－	○	○
			5-3	クラウドサーバのクレデンシャル情報の管理が不十分で流出し、不正アクセスされる。	インターネット	クラウド上のサーバ	不正侵入によるデータ改ざんや情報漏えいの発生	－	○	○
6	機密情報の漏洩	1	事業被害の概要	_				影響を受ける A、I、C		
			シナリオ#	攻撃シナリオ	攻撃拠点（※1）	攻撃対象（※2）	最終攻撃	可用性	完全性	機密性
			6-1	工場内への物理的侵入、またはインターネット経由で MES Serverの生産データが抜き取られる事により、機密情報が外部に漏洩する。	インターネット 工場	MES Server	MES Serverの生産データが抜き取られる	－	－	○
			6-2	工場内への物理的侵入、またはインターネット経由で FileServerから機密情報が摂取され、外部に漏洩する。	インターネット 工場	FileServer	FileServerから機密情報が抜き取られる	－	－	○
			6-3	工場内への物理的侵入、またはインターネット経由で Edgecross搭載PCから機密情報が摂取され、外部に漏洩する。	インターネット 工場	Edgecross搭載PC	Edgecross搭載PCから機密情報が抜き取られる	－	－	○

別紙（攻撃シナリオ）パターン2

※1：攻撃拠点は、攻撃対象に対して最終攻撃を行う事が出来る機器や場所を想定

No.	事業被害	事業被害レベル	事業被害の概要と攻撃シナリオ							
1	広域での製品供給停止	3	事業被害の概要	製造設備等へのサイバー攻撃により、広域において製品の供給停止が発生し、社会に多大な影響を及ぼし、賠償費用等の高額な損失が生じると共に、当社の信頼が大きく低下する。				影響を受ける A、I、C		
			シナリオ#	攻撃シナリオ	攻撃拠点（※1）	攻撃対象（※2）	最終攻撃	可用性	完全性	機密性
			1-1	生産管理アプリケーションと各装置間の通信妨害により、生産管理データを消失し、製造工程の管理、作業者への指示ができなくなり、製造が停止する。	制御情報ネットワーク	生産管理アプリケーション	生産管理アプリケーションと各装置間の通信妨害による、生産管理データを消失	○	○	－
			1-2	生産管理アプリケーションがマルウェアに感染する事により、生産管理データを消失し、製造工程の管理、作業者への指示ができなくなり、製造が停止する。	制御情報ネットワーク	生産管理アプリケーション	生産管理アプリケーションがマルウェアに感染し、生産管理データを消失	○	○	－
			1-3	Edgecross搭載PCがマルウェアに感染し、生産停止が実行され、生産が停止する。	制御情報ネットワーク	Edgecross搭載PC	Edgecross搭載PCがマルウェアに感染し、生産停止操作を実行する	○	－	－
2	限定地域での製品供給停止	2	事業被害の概要	製造設備等へのサイバー攻撃により、限定地域において供給停止が発生し、社会に影響を及ぼし、賠償費用等の損失が生じると共に、当社の信頼が低下する。				影響を受ける A、I、C		
			シナリオ#	攻撃シナリオ	攻撃拠点（※1）	攻撃対象（※2）	最終攻撃	可用性	完全性	機密性
			2-1	Edgecross搭載PCに無許可のアプリケーションがインストールされ、処理性能に支障が発生し、アクセスに遅延が発生する。	制御情報ネットワーク	Edgecross搭載PC	Edgecross搭載PCに無許可のアプリケーションがインストールされる。	○	○	－
			2-2	作業員等の身元確認や行動監視が不十分で、内部作業員等から攻撃を受ける。	制御情報ネットワーク	Edgecross搭載PC	サーバやコントローラの不正操作による、工場停止	○	－	－
			2-3	Edgecross搭載PCが専用の管理区画に設置されておらず、所定の作業員以外による不正操作が行われる。	制御情報ネットワーク	Edgecross搭載PC	不正操作による工場停止や設定値改ざん、情報流出等の発生	○	○	○
			2-4	Edgecross搭載PC設置区画への入退室が適切に管理されておらず、所定の作業員以外による不正操作が行われる。	制御情報ネットワーク	Edgecross搭載PC	不正操作による工場停止や設定値改ざん、情報流出等の発生	○	○	○
			2-5	Edgecross搭載PCが通信相手を認証しておらず、不正な命令を実行してしまい、不正な動作をさせられる。	制御情報ネットワーク	Edgecross搭載PC	不正操作による工場停止や設定値改ざん、情報流出等の発生	○	○	○
3	仕様不良製品の供給	2	事業被害の概要	製造設備等へのサイバー攻撃により、規定の仕様を満たさない製品を顧客に供給してしまい、社会に影響を及ぼし、賠償費用等の損失が生じると共に、当社の信頼が低下する。				影響を受ける A、I、C		
			シナリオ#	攻撃シナリオ	攻撃拠点（※1）	攻撃対象（※2）	最終攻撃	可用性	完全性	機密性
			3-1	生産管理アプリケーションがマルウェアに感染する事により、生産管理データの改ざんされ、製造工程の管理、作業者への指示が意図しない指示になり、仕様不良の製品を供給する。	制御情報ネットワーク	生産管理アプリケーション	生産管理アプリケーションがマルウェアに感染し、生産管理データの改ざん	○	○	－

別紙（攻撃シナリオ）パターン2

※1：攻撃拠点は、攻撃対象に対して最終攻撃を行う事が出来る機器や場所を想定

No.	事業被害	事業被害レベル	事業被害の概要と攻撃シナリオ							
4	設備の破壊	3	事業被害の概要	製造設備等へのサイバー攻撃により、設備が破壊されて供給停止が発生すると共に、従業員や近隣住民の死傷者が出て、社会に多大な影響を及ぼし、賠償費用等の高額な損失が生じると共に、当社の信頼が大きく低下する。				影響を受ける A、I、C		
			シナリオ#	攻撃シナリオ	攻撃拠点（※1）	攻撃対象（※2）	最終攻撃	可用性	完全性	機密性
			4-2	エンジPCがマルウェアに感染する事により、適切でないエンジニアリング設定され、設備の制御が異常となり、各設備が破壊される。	制御情報ネットワーク	エンジPC	エンジPCがマルウェアに感染し、エンジニアリング設定を改ざんされる。	○	○	－
			4-4	端末設置場所に対して、許可された入退者に限定するような管理ができておらず、所定の作業員以外による画面の盗み見、不正操作が行われる。	工場	エンジPC	不正操作による設備停止や設定値改ざん、情報流出等の発生	○	○	○
			4-5	システムの権限管理や作業監視が十分でなく、所定の作業員がその権限を越えて、システムや端末／制御盤に不正操作をする。	工場	エンジPC	不正操作による設備停止や設定値改ざん、情報流出等の発生	○	○	○
			4-8	セキュリティ確認がされていないUSB等の外部媒体接続時に、外部媒体経由でマルウェアに侵入されてしまう。	外部媒体	Edgecross搭載PC	Edgecross搭載PCの停止や設定改ざん、情報流出等の発生	○	○	○
			4-9	セキュリティ確認がされていない外部持込端末接続時に、外部持込端末経由でマルウェアに侵入されてしまう。	外部持込端末	Edgecross搭載PC	Edgecross搭載PCの停止や設定改ざん、情報流出等の発生	○	○	○
			4-10	ネットワーク機器の空きポートが接続可能な状態で放置されており、不正端末を接続され、マルウェアを送り込まれる。	L2 Switchの空きポート	Edgecross搭載PC	Edgecross搭載PCの停止や設定改ざん、情報流出等の発生	○	○	○
			4-11	サーバの脆弱性についての認識が不十分で、脆弱性が残ったままの状態になっており、システムの脆弱性をついた攻撃を受ける。	インターネット 情報ネットワーク DMZ 制御情報ネットワーク	Edgecross搭載PC	Edgecross搭載PCの停止や設定改ざん、情報流出等の発生	○	○	○
			4-14	工作機械の脆弱性についての認識が不十分で、脆弱性が残ったままの状態になっており、システムの脆弱性をついた攻撃を受ける。	制御情報ネットワーク	工作機械	攻撃による工作機械の停止	○	－	－
			4-16	各種制御盤・分電盤に業界で広く通用する鍵がついており容易に開錠され、所定の作業員以外による不正操作が行われる。	工場	各装置	不正操作による設備停止や設定値改ざんの発生	○	○	－
			4-17	スイッチ等のネットワーク機器の設置場所が安全管理されておらず誰でも触ることができる状態にあり、所定の作業員以外による不正操作が行われる。	工場	L2 Switch	不正操作による設備停止や設定値改ざんの発生	○	○	－
5	大規模対策費用の発生	1	事業被害の概要	サイバー攻撃を受け、製品の供給停止の被害は発生しなかったものの、現行対策の脆弱性が明らかとなり、その解消のために膨大な対策費用が発生する。				影響を受ける A、I、C		
			シナリオ#	攻撃シナリオ	攻撃拠点（※1）	攻撃対象（※2）	最終攻撃	可用性	完全性	機密性
6	機密情報の漏洩	1	事業被害の概要	_				影響を受ける A、I、C		
			シナリオ#	攻撃シナリオ	攻撃拠点（※1）	攻撃対象（※2）	最終攻撃	可用性	完全性	機密性
			6-1	工場内への物理的侵入によりFile Serverから機密情報が摂取され、外部に漏洩する。	工場	File Server	File Serverから機密情報が抜き取られる	－	－	○
			6-2	工場内への物理的侵入によりEdgecross搭載PCから機密情報が摂取され、外部に漏洩する。	工場	Edgecross搭載PC	Edgecross搭載PCから機密情報が抜き取られる	－	－	○