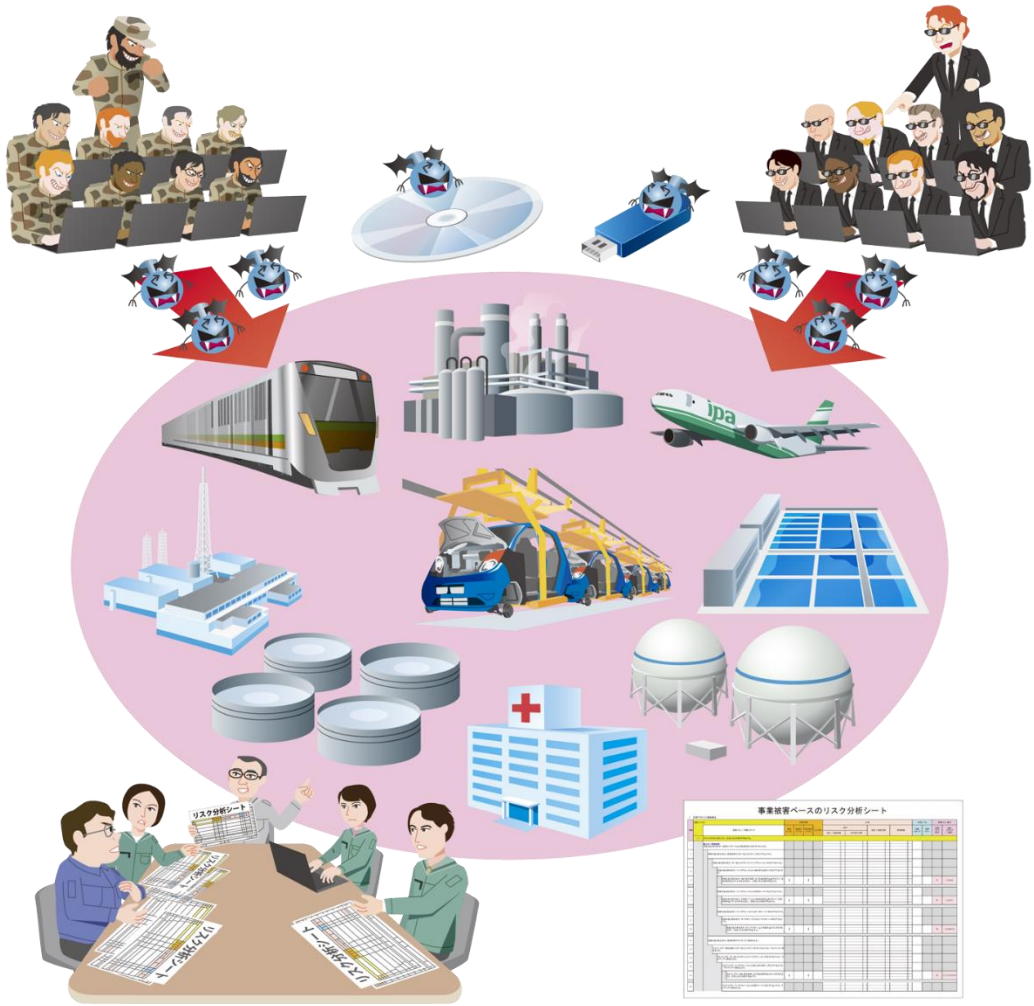
制御システムに対する
リスク分析の実施例
第2版

～制御システムのセキュリティリスク分析ガイド　別冊～



2020 年 3 月

IPA
独立行政法人情報処理推進機構
セキュリティセンター

目　次

図 目 次

表 目 次

はじめに

「制御システムのセキュリティリスク分析ガイド　～セキュリティ対策におけるリスク分析実施のススメ～」（以下、「ガイド本体」と呼ぶ）は、セキュリティリスク分析の正しい理解と具体的なリスク分析シートの作成手順などの方法論の解説に主眼を置いている。従って、紙面の制約の下で、一部のシステム資産に対する資産ベースのリスク分析シートや、一部の事業被害に対する攻撃シナリオと攻撃ツリーの事業被害ベースのリスク分析シートを例示した解説に留めている。

この別冊では、典型的なモデルシステムに対して、資産ベースのリスク分析と事業被害ベースのリスク分析の実施事例を解説、提示している。その目的は、以下の 3 点である。

（１） リスク分析の全体イメージと評価結果の提示

詳細リスク分析は、その工数や生成物の膨大化への懸念が、敬遠される要因の一つである。あるモデルシステムに対して、実際のリスク分析を実施し、どの程度の工数を要し、どの程度の分析成果物を作成するのかの全体イメージを示す。具体的な手順の理解、評価素材（脅威、対策、その対応表、分析シートのフォーマット等）の活用、分析対象の絞り込みの手法の利用等によって、実際にはどうであるのか、「案ずるより産むが易し」のたとえとしたい。

（２） リスク分析シートの結果の提示による全体素材の提供

制御システムの典型的なモデルシステムに対するリスク分析シートの結果の提示により、自組織のシステムの分析を実施する際の、可能な範囲での流用やカスタマイズの素材とすることで、工数の削減につながることを期待している。

（３） リスク分析シートのまとめ方のバリエーションの紹介

事業被害ベースのリスク分析においては、分析対象モデルの複雑さやリスク分析結果の活用の目的によって、リスク分析シートの様々なまとめ方が考えられる。そのバリエーションを具体的に示すことで、自組織の対象システムをリスク分析する際に、最適なまとめ方の選択の参考として欲しい。

この別冊が、全体の工数や成果物のイメージの把握を可能とし、制御システムを有する事業者の多くが、詳細リスク分析の実施に踏み出す一助となることを期待している。

2017 年 10 月 2 日

独立行政法人　情報処理推進機構	木下　　仁
独立行政法人　情報処理推進機構	小助川　重仁
独立行政法人　情報処理推進機構	辻　　宏郷
独立行政法人　情報処理推進機構	岡下　博子
独立行政法人　情報処理推進機構	工藤　誠也
独立行政法人　情報処理推進機構	塩田　英二
独立行政法人　情報処理推進機構	福原　　聡
独立行政法人　情報処理推進機構	吉田　和之
独立行政法人　情報処理推進機構	桑名　利幸
独立行政法人　情報処理推進機構	金野　千里

第 2 版改定にあたって

ガイド本体の第 2 版改定で追加・変更された内容にあわせて、別冊で提示しているアウトプット例の追加・変更を行った。また、リスク分析作業の過程で作成した方がいい中間アウトプット例を、新たに追加している。

この別冊が、全体の工数や成果物のイメージの把握を可能とし、制御システムを有する事業者の多くが、詳細リスク分析の実施に踏み出す一助となることを期待している。

独立行政法人　情報処理推進機構	小助川　重仁
独立行政法人　情報処理推進機構	木下　　弦
独立行政法人　情報処理推進機構	木下　　仁
独立行政法人　情報処理推進機構	辻　　宏郷
独立行政法人　情報処理推進機構	岡下　博子
独立行政法人　情報処理推進機構	塩田　英二
独立行政法人　情報処理推進機構	福原　　聡
独立行政法人　情報処理推進機構	吉田　和之
独立行政法人　情報処理推進機構	桑名　利幸

このページは空白です。

1. 本書の構成

本書ではガイド本体で説明したリスク分析手法に基づき、リスク分析の実施例を紹介する。

- **本書の前提**

  本書は、ガイド本体で説明されているリスク分析手法の内容とリスク分析結果の活用方法を理解していることを前提とする。また、本書ではリスク分析の手順の詳細はガイド本体を参照する記載としており、文中の青字斜体の章節項番号(*x.y.z*)と図表番号(*図 x-y*、*表 x-y*)はガイド本体を参照していることを意味している。

- **本書のリスク分析対象システム**

  ガイド本体の *3.2.3.項 図 3-8* では“典型的な制御システムの構成図”の制御システムが紹介されているが、これをリスク分析の対象システム(以下、「モデルシステム」と呼ぶ)としている。また、ガイド本体と同様に非定常稼働機器をリスク分析の対象から外し、定常時稼働機器を対象としたリスク分析を行う。

- **本書の構成と特徴**

  ガイド本体ではモデルシステムを対象とした資産ベースと事業被害ベースのリスク分析の実施例(分析シート)の一部を紹介しているが、本書ではリスク分析の実施例全体を提示する。また、ガイド本体と本書の実施例では、脅威レベル・脆弱性レベル・リスク値といった評価値が異なる場合がある。

  - 資産ベースのリスク分析の実施例

    モデルシステムの定常時稼働資産全てについて資産ベースのリスク分析を実施した例を提示する。

  - 事業被害ベースのリスク分析の実施例

    モデルシステムにおける 5 種類の事業被害を設定し、これらについて攻撃シナリオを検討した事業被害ベースのリスク分析の実施例を提示する。

    また、事業被害ベースのリスク分析結果である分析シートの形式は、典型的な分析シートの形式と、それ以外にまとめ方が異なる 2 種類の形式の、合計 3 種類の形式の分析シートを提示している。リスク分析の対象モデルや目的に応じて、どの形式のまとめ方の分析シートが適しているか検討する上での参考として欲しい。

  - リスク分析結果の活用例

    事業被害ベースのリスク分析の実施例をもとに、モデルシステムの事業被害リスクを低減するための改善策を提示する。

- リスク分析の流れとアウトプット

  リスク分析の流れと2～5章で説明する実施例のアウトプットを、図 1-1 に示す。(図 1-1 は、ガイド本体の*図 2-2* に別冊で示すアウトップットを数字(1～17)で示したものである)図中の  はリスク分析者が作成するアウトプットを意味し、  はガイド本体に示された例をカスタマイズして得られるアウトプットを意味している。

表 1-1 アウトプット一覧表

2. リスク分析のための事前準備				
本書見出し	アウトプット		アウトプットの利用	ガイド本体
2.1.	①	資産一覧	資産/事業被害ベース	*3.1.5. 表 3-9*
2.2.	②	システム構成図	資産/事業被害ベース	*3.2.3. 図 3-8*
2.3.①	③	データフローマトリクス	資産/事業被害ベース	*3.3.1. 表 3-10*
2.3.②	④	データフロー図	資産/事業被害ベース	*3.3.2. 図 3-14*
2.4.	⑤	資産の重要度の判断基準	資産ベース	*4.2.2. 表 4-5*
2.5.	⑥	各資産に対する重要度一覧	資産ベース	*4.2.3. 表 4-9*
2.6.	⑦	事業被害レベルの判断基準	事業被害ベース	*4.3.2. 表 4-11*
2.7.	⑧	事業被害及び各事業被害に対する事業被害レベル一覧	事業被害ベース	*4.3.3. 表 4-12*
2.8.	⑨	脅威レベルの判断基準	資産/事業被害ベース	*4.4.5. 表 4-20～表 4-24*
3. 資産ベースのリスク分析				
本書見出し	アウトプット			ガイド本体
3.1.	⑩	脅威レベルまとめ表		―
3.2.	⑪	資産ベースのリスク分析シート		*5 章*
3.3.①	⑫	脆弱性レベルまとめ表		―
3.3.②	⑬	リスク値まとめ表		―
4. 資産ベースのリスク分析				
本書見出し	アウトプット			ガイド本体
4.1.	⑭	攻撃シナリオ一覧		*6.2.2. 表 6-6*
4.2.	⑮-1	攻撃ルート一覧		*6.5.1. 表 6-11～表 6-12*
4.2.	⑮-2	攻撃ルート図		*6.5.1. 図 6-9*
4.3.	⑯	事業被害ベースのリスク分析シート		*6.6.4.~ 6.11.*
4.4.	⑰	リスク値まとめ表		*6.11.3.*
5. リスク分析の活用				
本書見出し	アウトプット			ガイド本体
5.	⑱	制御システムのリスク分析結果		*7 章*

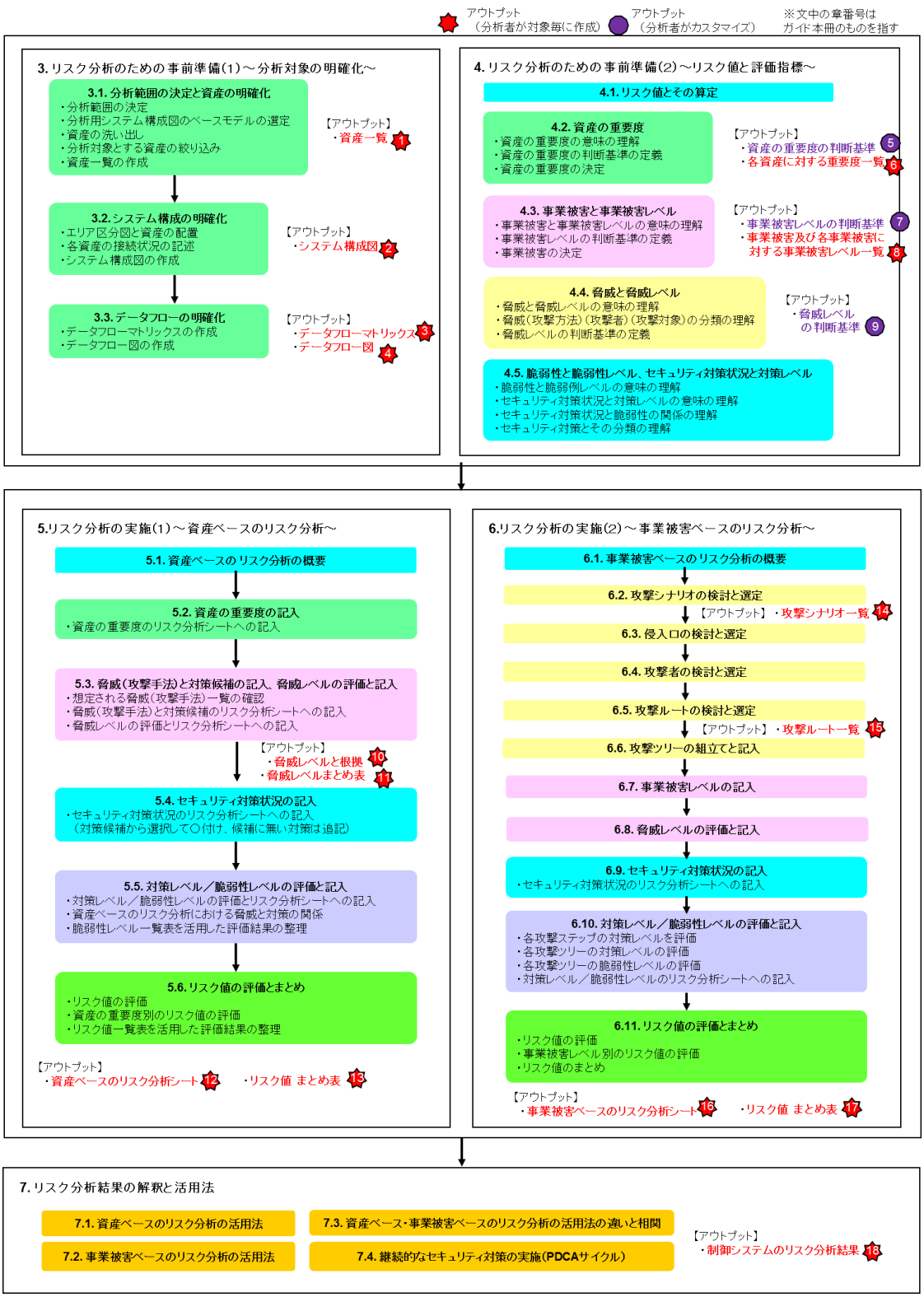


図 1-1 リスク分析の流れと成果物

- アウトプットの例示と解説

  本書でのリスク分析は「リスク分析の流れ」に沿って実施し、各ステップではリスク分析を完了させるための中間的な資料（アウトプット）を作成する。それらアウトプットをリスク分析の流れに沿って例示するとともに、アウトプットを作成するための要点を以下のように示す。

（例）

【作業 2.1.①】分析対象システムにおける資産一覧表を作成すること。

- ガイド本体 *表 3-9* を参考に、資産の分類(機器または通信経路)、機能、設置場所、接続先 NW、管理ポートの有無、扱っているデータの種類、ベンダー、OS、プロトコルを明記すること。

【アウトプット 2.1.①】

No		1	2
資産名		監視端末	ファイアウォール
資産種別	情報系機器	○	
	制御系機器		
	ネットワーク資産（通信制御機能有）		○
	ネットワーク資産（通信制御機能無）		
資産の持つ機能	入出力	○	
	データ保存		
	コマンド発行		
	ゲート		○
回線種類			
設置場所		執務室	サーバ室
接続先NW	情報NW	○	○
	DMZ		○
	制御NW(情)		○
	制御NW(フ)		
	フィールドNW		
	その他		
管理ポートの接続先		×	情報NW
操作I/Fの有無		○	×

【解説 2.1.(1)】

- 詳細リスク分析を行う上で必要となる情報の分析に利用しやすい形への整理

  これらをどこまで精度良く実施するかで、後の工程での工数、分析精度に大きく影響する。資産一覧表に全て記載する必要はなく、既存のドキュメントを参照する記載でも構わない。また、分析を進めながら必要となった事項を順次詳細化することでも構わない。

2. リスク分析のための事前準備

リスク分析のための事前準備作業で作成するアウトプットを以下に示す。

表 2-1 事前準備作業のアウトプット一覧

別冊見出し	アウトプット	アウトプットの利用	ガイド本体
2.1.	資産一覧	資産/事業被害ベース	*3.1.5. 表 3-9*
2.2.	システム構成図	資産/事業被害ベース	*3.2.3. 図 3-8*
2.3.①	データフローマトリクス	資産/事業被害ベース	*3.3.1. 表 3-10*
2.3.②	データフロー図	資産/事業被害ベース	*3.3.2. 図 3-14*
2.4.	資産の重要度の判断基準	資産ベース	*4.2.2. 表 4-5*
2.5.	各資産に対する重要度一覧	資産ベース	*4.2.3. 表 4-9*
2.6.	事業被害レベルの判断基準	事業被害ベース	*4.3.2. 表 4-11*
2.7.	事業被害及び各事業被害に対する事業被害レベル一覧	事業被害ベース	*4.3.3. 表 4-12*
2.8.	脅威レベルの判断基準	資産/事業被害ベース	*4.4.5. 表 4-20～表 4-24*

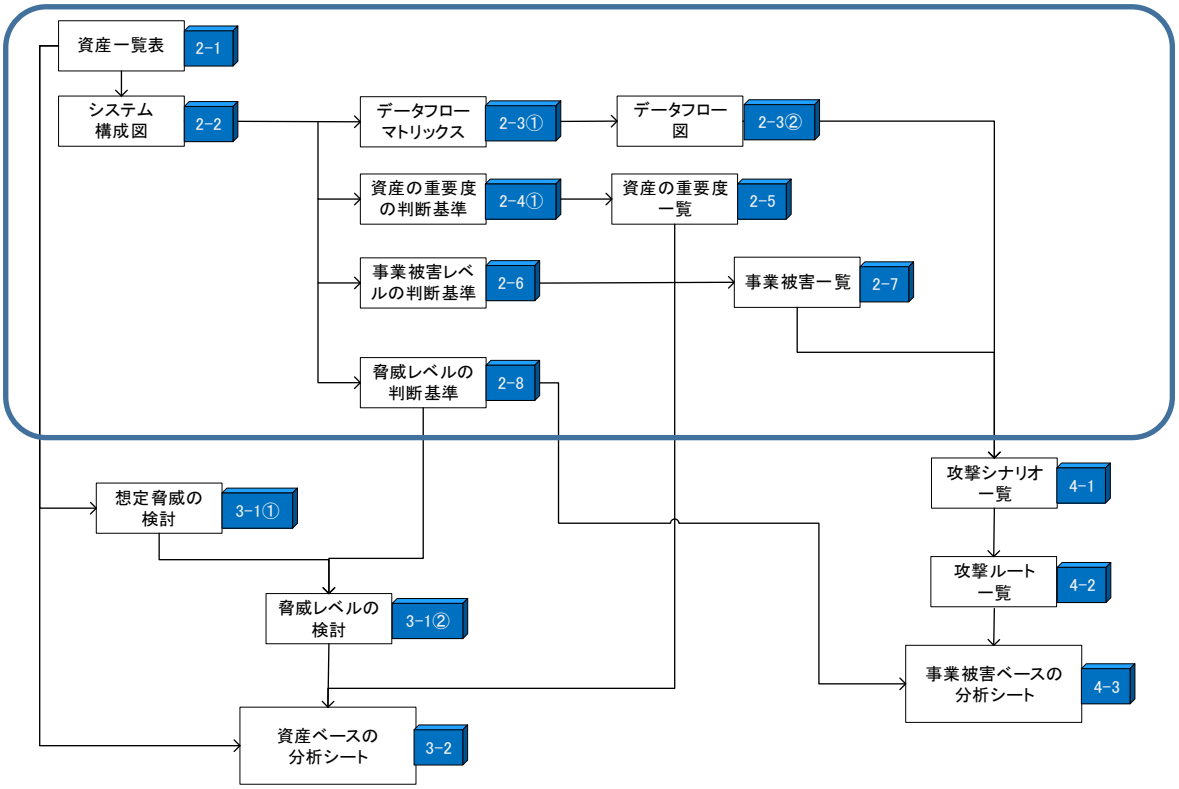


図 2-1 事前準備作業の流れ

2.1. 資産一覧

【作業 2.1①】分析対象システムにおける資産一覧表を作成すること。

- ガイド本体 *表 3-9* を参考に、資産の分類、機能、設置場所、接続先 NW、管理ポートの有無、ベンダー、OS、プロトコルを明記すること。

【アウトプット 2.1①】

資産一覧表を次項に示す（表 2-2）。

【解説 2.1①】

- 詳細リスク分析を行う上で必要となる情報の分析に利用しやすい形への整理

  詳細リスク分析を行う上で必要となる情報を資産一覧表にまとめることを推奨する。これらをどこまで精度良く実施するかで、後の工程での工数、分析精度に大きく影響する。

  ただし、資産一覧表に全て記載する必要はなく、項目によっては既存のドキュメントを参照する方式でも構わない。また、分析を進めながら必要となった事項を都度資産一覧表に追加・詳細化しても構わない。

- 接続先ネットワーク（NW）の明確化

  資産が通常のネットワーク経路とは別の管理ネットワークや監視ネットワークに接続されている場合がある。これらのネットワークは自社のネットワーク図に記載されていない場合もあるため、明確化が必要である。

- 資産一覧表作成に必要な調査工数の配慮

  細心の資産一覧表を整備されていない事業者においては、制御システムの運用者や構築業者、ベンダーへのヒアリングが必要になる場合がある。この作業はそれなりの工数を伴うため、事前準備の期間を長めに用意する必要があることを留意すること。

表 2-2 資産一覧表 *1

No		1	2	3	4	5	6	7	8	9	10	11	12	13
資産名		監視端末	ファイア ウォール	スイッチ、 DMZ	データ ヒストリアン （中継）	データ ヒストリアン	スイッチ、 制御ネットワーク （情報側）	EWS	制御サーバ	HMI （操作端末）	スイッチ、 制御ネットワーク （フィールド側）	フィールド ネットワーク	コントローラ、 コントローラ （マスター）	コントローラ （スレーブ）
資産 種別	情報系機器	○												
	制御系機器				○	○		○	○	○			○	○
	ネットワーク資産 （通信制御機能有）		○	○			○							
	ネットワーク資産 （通信制御機能無）										○	○		
資産の 持つ 機能	入出力	○			○	○		○	○	○			○	○
	データ保存				○	○		○	○	○				
	コマンド発行								○	○			○	○
	ゲート		○	○			○				○	○		
回線種類				LAN			LAN				LAN	フィールドNW		
設置場所		執務室	サーバ室	サーバ室	サーバ室	サーバ室	サーバ室	サーバ室	サーバ室	計器室	サーバ室、 計器室、フィールド （敷地内）	フィールド(敷地内)、フィールド （敷地外）	フィールド （敷地内）	フィールド （敷地外）
接続先 NW	情報NW	○	○											
	DMZ		○	○	○									
	制御NW(情)		○			○	○	○	○	○				
	制御NW(フ)							○	○	○	○		○	
	フィールドNW											○	○	○
	その他													
管理ポートの接続先		×	情報NW	×	×	×	×	×	×	×	×	×	×	×
操作I/Fの有無		○	×	×	○	○	×	○	○	○	×	×	×	×
USBポート／通信I/Fの利用		○	○	○	○	○	○	○	○	○	○	×	×	×
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
データの種類と経路		データフローマトリックスに記載												
構築ベンダー／機器メーカー		AB/XX	AB/YY	AB/ZZ	AB/XX	AB/XX	AB/ZZ	AB/XX	AB/XX	AB/XX	AB/ZZ	AB/XX	AB/XX	AB/XX
OSの種類／バージョン		Windows 7	独自OS	独自OS	Windows Server 2008	Windows Server 2008	独自OS	Windows XP	Windows Server 2008	Windows XP	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, 独自	TCP, UDP, 独自	TCP, UDP, 独自	TCP, UDP, 独自	TCP, UDP, 独自	独自	独自	独自

*1 本表・以降の文中での資産の略語

FW：ファイアウォール、SW：スイッチ、NW：ネットワーク、制御 NW(情)：制御ネットワーク（情報側）、制御 NW(フ)：制御ネットワーク（フィールド側）

*2 EWS の設置場所をサーバ室としている（EWS が計器室に設置されている制御システムも多い）。

【作業 2.1②】資産一覧表に、物理的対策・運用的対策といった資産の外部環境の対策と、資産自身の技術的対策を追記すること。

【アウトプット 2.1②】

資産一覧表に、役割・機能、影響範囲、セキュリティ対策を追加したものを 17 頁以降に示す。（表 2-3）。

【解説 2.1②】

- 役割や影響範囲の明確化

  資産の重要度、事業被害レベルの判定を容易にするために、資産の機能停止時の影響や資産上のシステムの不正操作による影響を明確にしておくことを推奨する。

- 外部公開サービス（特にリモート接続機能）の明確化

  資産が明示的にリモートで接続できる機能を提供しているかは、事業被害ベースのリスク分析において攻撃ツリーを検討する上で重要な情報となる。

- セキュリティ対策の記載

  物理的セキュリティ対策と運用的セキュリティ対策、資産に導入された技術的セキュリティ対策を分けて記載することを推奨する。

  物理的セキュリティ対策は、資産が設置してある建屋や室内への物理的侵入や盗難の対策レベルを検討する際に利用する。

- 運用的対策と技術的対策の詳細を記載化

  対策レベルを検討する際に対策をより詳細に記載することを推奨する。例えば、スマートフォンや USB デバイス接続が技術的に禁止されているか、持込が禁止されているか、接続することが運用ルールで禁止されているのか等。

- 資産一覧表の活用

  制御システムのセキュリティ状況の早期把握を助けることになるため、一度作成した資産一覧表は定期的にメンテナンス（更新）することを推奨する。

表 2-3 資産一覧表（役割・機能、影響範囲・事業継続への影響、セキュリティ対策を含む）

No	1	2	3	4	5
資産名	監視端末	ファイアウォール	スイッチ、DMZ	データヒストリアン(中継)	データヒストリアン
役割・機能	・プロセスや現場の状況を確認するための端末。 ・監視端末から制御ネットワーク内の機器にアクセスする業務フローはない。	・外部のネットワークからの攻撃や侵入を防ぐための機能を有する機器。	・複数のネットワークを集線、中継する機器。	・情報系から制御ネットワーク（情報系）にあるデータヒストリアンを参照するためのサーバ。	・長期間のプロセス値や管理パラメータが保存され分析されるサーバ。
影響範囲・事業継続への影響	・保有データの改ざんや機能停止による事業継続への直接的な影響はない。	・設定情報を改ざんされると、攻撃や侵入を許す可能性がある。 ・機能停止してもフィールド機器の直接操作により事業継続可能。	・機能停止してもフィールド機器の直接操作により事業継続可能。	・機能停止による事業継続への直接的な影響はないが、制御プロセスのデータ解析が不能になり、制御システムの運転効率が落ちる。	・保有データの改ざんや機能停止による事業継続への直接的な影響はないが、制御プロセスのデータ解析が不能になり、制御システムの運転効率が落ちる。
セキュリティ対策状況（物理的・運用的）	・事業者敷地、建屋には、物理セキュリティ対策（警備員の配置、施錠管理、入退管理等）が実施されている。 ・執務室の機器に物理的にアクセスできる人間は、事業者の内部関係者となっている。	・制御システム機器が設置されている事業者敷地、建屋、部屋（サーバ室、計器室）、ラック等には、物理セキュリティ対策（警備員の配備、施錠管理、入退管理、監視カメラ、侵入センサ等）が実施されている。 ・制御システム機器の操作者は、物理的・論理的に、必要最低限の内部関係者に制限されている。	・制御システム機器が設置されている事業者敷地、建屋、部屋（サーバ室、計器室）、ラック等には、物理セキュリティ対策（警備員の配備、施錠管理、入退管理、監視カメラ、侵入センサ等）が実施されている。 ・制御システム機器の操作者は、物理的・論理的に、必要最低限の内部関係者に制限されている。	・制御システム機器が設置されている事業者敷地、建屋、部屋（サーバ室、計器室）、ラック等には、物理セキュリティ対策（警備員の配備、施錠管理、入退管理、監視カメラ、侵入センサ等）が実施されている。 ・制御システム機器の操作者は、物理的・論理的に、必要最低限の内部関係者に制限されている。 ・運用ルールで外部記憶媒体とスマートフォンの機器への接続を禁止しているが、技術的対策はしていない。	・制御システム機器が設置されている事業者敷地、建屋、部屋（サーバ室、計器室）、ラック等には、物理セキュリティ対策（警備員の配備、施錠管理、入退管理、監視カメラ、侵入センサ等）が実施されている。 ・制御システム機器の操作者は、物理的・論理的に、必要最低限の内部関係者に制限されている。 ・運用ルールで外部記憶媒体とスマートフォンの機器への接続を禁止しているが、技術的対策はしていない。
セキュリティ対策状況（技術的）	・OSはWindows 7で、アップデートを随時適用している。 ・情報系システムのセキュリティ対策と同等の対策がされており、アンチウィルス、メールフィルタ、Webフィルタ等の対策製品がある。 ・リモート接続や直接操作によるログイン時はユーザ認証あり。	・リモート接続や直接操作によるログイン時はユーザ認証あり。 ・アカウントは管理者のみで、操作者用アカウントはない。リモート管理機能は、管理者アカウントのみ利用可能。 ・ファイアウォールはパケットフィルタ型で、ファイアウォールルールの許可通信（IPプロトコル）は下記の2つのみ。 監視端末 ⇔ データヒストリアン（中継） データヒストリアン（中継） ⇔ データヒストリアン ・ファイアウォールのファームウェアアップデートを随時実施。アップデートタイミングは保守ベンダー主導で実施する。	・リモート接続や直接操作によるログイン時はユーザ認証あり。 ・アカウントは管理者のみで、操作者用アカウントはない。リモート管理機能は、管理者アカウントのみ利用可能。 ・スイッチのファームウェアアップデートを随時実施。アップデートタイミングは保守ベンダー主導で実施する。	・OSはWindows Server 2008でアップデートの適用はしていない。 ・リモート接続や直接操作によるログイン時はユーザ認証あり。 ・アカウントは操作者用と管理者用があり、リモート管理機能は管理者アカウントのみ利用可能。 ・バックアップ間隔は週次、3世代分を保管。 ・緊急パッチがリリースされたときのみリリースから1週間以内に適用している。 ・アンチウィルス対策製品を入れているが、シグネチャパターンの日次更新はなく、半年に1回頻度でシグネチャパターンを更新している。	・OSはWindows Server 2008でアップデートの適用はしていない。 ・リモート接続や直接操作によるログイン時はユーザ認証あり。 ・アカウントは操作者用と管理者用があり、リモート管理機能は管理者アカウントのみ利用可能。 ・バックアップ間隔は週次、3世代分を保管。

表 2-3 資産一覧表（役割・機能、影響範囲・事業継続への影響、セキュリティ対策を含む）

No	6	7	8	9	10
資産名	スイッチ、制御NW（情報側）	EWS	制御サーバ	HMI（操作端末）	スイッチ、制御NW(フィールド側)
役割・機能	・情報ネットワークまたはDMZ上の機器（サーバ等）との間で、制御目的に使用するためのステータス（接点の状態）情報やデータを転送するためのネットワーク。	・コントローラのプログラムの改造や制御サーバのプログラムの変更等を行うための機器。 ・外部記憶媒体（主にUSBメモリ）をEWSに接続して外部からデータを持ち込む運用がある。	・制御機器や現場機器に対し設定値やコマンドを送出するサーバ。	・制御機器や現場機器に対する指示を入力する端末。 ・広域供給停止コマンド（予め決められた対象エリアへの供給を一括して停止するコマンド）を発行可能。	・自ネットワーク及びフィールドネットワーク上の機器（コントローラ）との間で、制御目的に使用するためのステータス情報やデータを即時転送するためのネットワーク。制御に特化した高い応答性を持つ。 ・IP系独自プロトコルを利用している。
影響範囲・事業継続への影響	・機能停止してもフィールド機器の直接操作により事業継続可能。	・コントローラや制御サーバのプログラムや設定値を改ざんされると、正常な監視制御が不能になる可能性がある。 ・営業秘密となるプログラムやデータを保存しており、漏えいすると競合他社に類似製品を生成され、企業の競争力が落ちる可能性がある。	・改ざんされると、システム障害が発生し、広域供給停止を引き起こす可能性のある重要なデータを保有。 ・機能停止すると事業継続に影響を及ぼす。	・機能停止しても、設備・機器の直接操作により事業継続が可能。	・機能停止してもフィールド機器の直接操作により事業継続可能。
セキュリティ対策状況（物理的・運用的）	・制御システム機器が設置されている事業者敷地、建屋、部屋（サーバ室、計器室）、ラック等には、物理セキュリティ対策（警備員の配備、施錠管理、入退管理、監視カメラ、侵入センサ等）が実施されている。 ・制御システム機器の操作者は、物理的・論理的に、必要最低限の内部関係者に制限されている。 ・配線は管路で物理的に保護されている。	・制御システム機器が設置されている事業者敷地、建屋、部屋（サーバ室、計器室）、ラック等には、物理セキュリティ対策（警備員の配備、施錠管理、入退管理、監視カメラ、侵入センサ等）が実施されている。 ・制御システム機器の操作者は、物理的・論理的に、必要最低限の内部関係者に制限されている。 ・運用ルールで外部記憶媒体とスマートフォンの機器への接続を禁止しているが、技術的対策はしていない。	・制御システム機器が設置されている事業者敷地、建屋、部屋（サーバ室、計器室）、ラック等には、物理セキュリティ対策（警備員の配備、施錠管理、入退管理、監視カメラ、侵入センサ等）が実施されている。 ・制御システム機器の操作者は、物理的・論理的に、必要最低限の内部関係者に制限されている。 ・運用ルールでスマートフォンの機器への接続を禁止しているが、技術的対策はしていない。	・制御システム機器が設置されている事業者敷地、建屋、部屋（サーバ室、計器室）、ラック等には、物理セキュリティ対策（警備員の配備、施錠管理、入退管理、監視カメラ、侵入センサ等）が実施されている。 ・制御システム機器にアクセスできる人間は、物理的・論理的に、必要最低限の内部関係者に制限されている。	・制御システム機器が設置されている事業者敷地、建屋、部屋（サーバ室、計器室）、ラック等には、物理セキュリティ対策（警備員の配備、施錠管理、入退管理、監視カメラ、侵入センサ等）が実施されている。 ・制御システム機器の操作者は、物理的・論理的に、必要最低限の内部関係者に制限されている。
セキュリティ対策状況（技術的）	・リモート接続や直接操作によるログイン時はユーザ認証あり（スイッチ）。 ・アカウントは管理者のみで操作者用アカウントはない（スイッチ）。 ・リモート管理機能への接続は接続元IPアドレスが制限されている（スイッチ）。	・OSはWindows XPでアップデートの適用はしていない。 ・アンチウィルス対策製品は導入していない。 ・アカウントは操作者用と管理者用があり、リモート管理機能は管理者アカウントのみ利用可能。 ・リモート接続や直接操作によるログイン時はユーザ認証あり。	・OSはWindows Server 2008でアップデートの適用はしていない。 ・リモート接続や直接操作によるログイン時はユーザ認証あり。 ・アカウントは操作者用と管理者用があり、リモート管理機能は管理者アカウントのみ利用可能。 ・アンチウィルス対策製品は導入していないが、ホワイトリストによるプロセス起動制御のセキュリティ対策を実施。	・OSはWindows XPでアップデートの適用はしていない。 ・アンチウィルス対策製品は導入していない。 ・アカウントは操作者用と管理者用があり、リモート管理機能は管理者アカウントのみ利用可能。 ・リモート接続によるログイン時はユーザ認証あり。 ・常時ログイン状態でスクリーンロックを設定していない。	・配線は管路で物理的に保護されている。 ・制御ネットワーク（フィールド側）はIP系プロトコルを利用している。

表 2-3 資産一覧表（役割・機能、影響範囲・事業継続への影響、セキュリティ対策を含む）

No	11	12	13
資産名	フィールドネットワーク	コントローラ、コントローラ（マスター）	コントローラ（スレーブ）
役割・機能	・コントローラ（マスター）とコントローラ（スレーブ）間のネットワーク。	・センサからの信号により接点や操作器を制御するなど入出力信号を扱う機器。 ・制御サーバやデータサーバとコントローラとの間の通信を中継するコントローラも存在し、中継する側を「コントローラ（マスター）」、中継される側を「コントローラ（スレーブ）」と示す。 ・コントローラ（マスター）は、上位システムからの供給停止コマンドを、下位のコントローラ（マスター）に中継して発行。 ・制御対象機器とはシリアルポート等で接続している。	・センサからの信号により接点や操作器を制御するなど入出力信号を扱う機器。 ・コントローラ（マスター）の下位システムで、コントローラ（マスター）より供給停止コマンドを受けつける。 ・制御対象機器とはシリアルポート等で接続している。
影響範囲・事業継続への影響	・機能停止してもフィールド機器の直接操作により事業継続可能。	・改ざんされると、システム障害が発生し、供給停止を引き起こす可能性のあるプログラムを保有。 ・機能停止すると、安全機構の発動により供給が停止する。 ・コントローラ（マスター）の下位には、広域供給停止を引き起こしうる数のコントローラ（スレーブ）が存在。	・改ざんされると、システム障害が発生し、供給停止を引き起こす可能性のあるプログラムを保有。 ・機能停止すると、安全機構の発動により供給が停止する。
セキュリティ対策状況（物理的・運用的）	・事業者敷地外のフィールドネットワークは、鍵付きのコンテナや設置箱等の中に設置されている。	・制御システム機器が設置されている事業者敷地、建屋、部屋（サーバ室、計器室）、ラック等には、物理セキュリティ対策（警備員の配備、施錠管理、入退管理、監視カメラ、侵入センサ等）が実施されている。 ・制御システム機器の操作者は、物理的・論理的に、必要最低限の内部関係者に制限されている。	・事業者敷地外のフィールド機器は、鍵付きのコンテナや設置箱等の中に設置されている。
セキュリティ対策状況（技術的）		・OSは独自で、コントローラ用のアンチウィルス対策製品は存在しない。 ・コントローラのファームウェアアップデートは適用していない。 ・リモート接続や直接操作によるログイン時はユーザ認証あり。 ・アカウントは管理者のみで、リモート管理機能がある。	・OSは独自OSとし、コントローラ用のアンチウィルス対策製品は存在しない。 ・コントローラのファームウェアアップデートは適用していない。 ・リモート接続や直接操作によるログイン時はユーザ認証あり。 ・アカウントは管理者のみで、リモート管理機能がある。

このページは空白です。

2.2. システム構成図

【作業 2.2】分析対象システムのシステム構成図を作成すること。

- ガイド本体 *図 3-8* を参考にすること。
- システム構成図で、ネットワーク接続状況と資産の物理的な設置場所が把握できるようにすること。

【アウトプット 2.2】

本書ではガイド本体 *図 3-8* と同じ図をシステム構成図として使用する(図 2-2)。

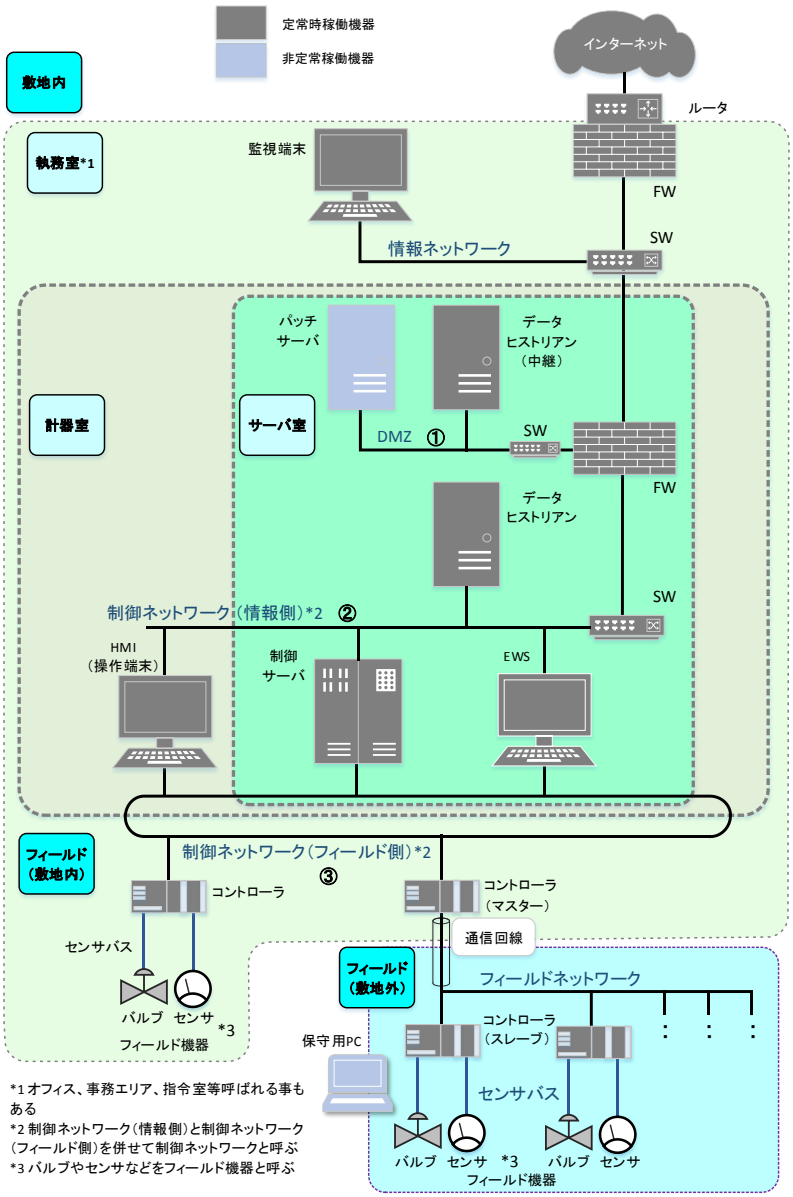


図 2-2 システム構成図

【解説 2.2】

- リスク分析を目的としたシステム構成図を作成

  既存のネットワーク構成図(情報システム構成図、制御システムの構成図など)を参照しながら、リスク分析を行う上で必要な資産を記載する。

  ネットワーク図に存在しない資産やネットワーク経路が存在する場合がある。これらはセキュリティテストなどリスク分析の過程で見つかることもあるので、注意が必要である。

- 資産のネットワーク接続と物理的配置を表現

  資産の論理的なネットワーク接続状況と、資産の物理的な配置が同時に把握できるよう工夫するとよい。事業被害ベースのリスク分析で物理的な侵入を伴う脅威に対して、第三者や制御システムに無関係な内部関係者が侵入できるかを検討する際に役に立つ。

- システム構成図では冗長構成の資産などを省略可能

  ネットワーク構成図に記載されている全ての機器のシステム構成図への記載は不要である。

  例:同一ネットワークに複数あるネットワークスイッチは、1 つとする。

  例:複数ある HMI やコントローラも 1 つとして表現してもよい。

  ただし、システム構成図から省略した資産は別途資産一覧表などに記録して欲しい。

2.3. データフローマトリクス

【作業 2.3①】分析対象システムの資産間で送受信されるネットワークデータを、データフローマトリクス表にまとめること。

- 表のフォーマットはガイド本体 *表 3-10* を参考すること。

【アウトプット 2.3①】

データフローマトリクスを以下に示す（表 2-4）。

表 2-4 データフローマトリクス

受信側 / 送信側	経路	監視端末	データヒストリアン（中継）	データヒストリアン	制御サーバ	EWS	HMI（操作端末）	コントローラ	コントローラ（マスター）	コントローラ（スレーブ）
監視端末	情報NW									
データヒストリアン（中継）	DMZ	プロセス値（ヒストリアンデータ）								
データヒストリアン	制御NW(情)		プロセス値（ヒストリアンデータ）							
制御サーバ	制御NW(情)			プロセス値						
	制御NW(フ)							制御コマンド	制御コマンド	
EWS	制御NW(情)									
	制御NW(フ)							エンジニアリング設定	エンジニアリング設定	
HMI（操作端末）	制御NW(情)									
	制御NW(フ)							制御コマンド	制御コマンド	
コントローラ	制御NW(フ)				プロセス値		プロセス値			
コントローラ（マスター）	制御NW(フ)				プロセス値		プロセス値			
	フィールドNW									制御コマンド
コントローラ（スレーブ）	フィールドNW								プロセス値	

【解説 2.3①】

- データフローの把握

  リスク分析の攻撃ツリーを検討するために、資産同士の通信と通信の目的を明確化する。
  また、プログラム変更、設定値変更といった制御システムへの最終攻撃に繋がるデータフローは、他のデータフローと区別すること。

- 簡単なデータフローの記載方法

  データフローマトリクスを簡素化するために本表では、資産 A→参照要求→資産 B→応答→資産 A となるデータフローなどで、資産 A→資産 B のデータ参照要求を省略し、資産 B から資産 A へデータが送付されるものとして記載している。

- データフローが流れるネットワークを明確化

  資産が複数のネットワークに接続している場合は、データフローがどちらのネットワークを使って送受信されるかを明らかにして欲しい。本書では、HMI、EWS、制御サーバ、コントローラ(マスター)が送受信するデータフローが該当する。
  また、異なるネットワークをまたぐデータフローは、可能な限りすべてのデータフローを記載すること。

- ネットワーク経路以外のデータフロー

  USB デバイスなどの外部記憶媒体や保守用 PC の持込など、ネットワーク経路以外で入出力されるデータも存在する。本書では、資産一覧表で外部記憶媒体の利用を明記し、データフローには入れていない。

【作業 2.3②】分析対象システムの資産間で送受信されるデータを、データフロー図にまとめること。

- ガイド本体 *図 3-14* を参考すること。
- システム構成図の上にデータフローを追記すること。

【アウトプット 2.3②】

分析対象システムのデータフロー図を以下に示す。

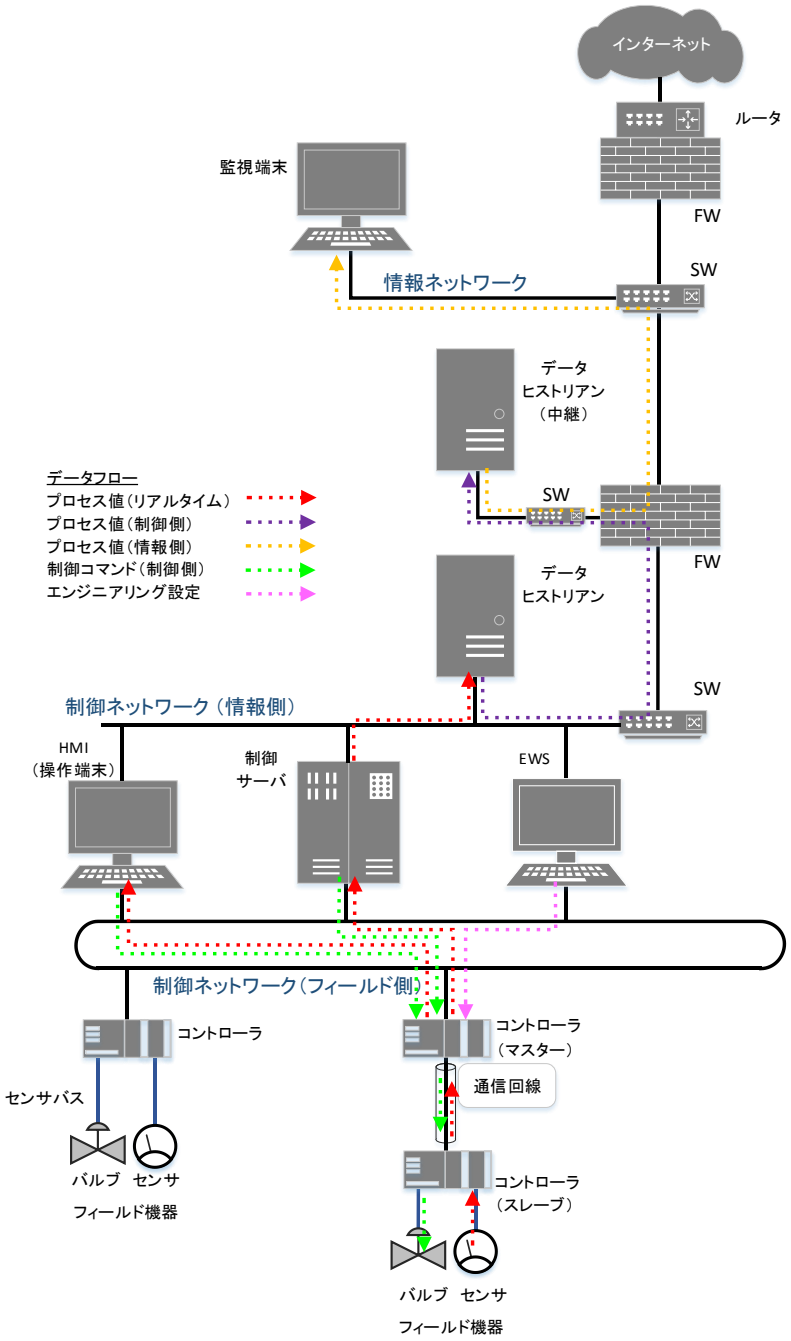


図 2-3 データフロー図

2.4. 資産の重要度の判断基準

【作業 2.4】資産の重要度を 3 段階で評価する場合の判断基準(被害大:3＞被害中:2＞被害小:1)を作成すること。

- ガイド本体 *表 4-5* を参考にして、事業者の事業特性に応じた明確な数値を評価値の境界値として定義すること。また、境界値の根拠をあわせて記載すること。

【アウトプット 2.4】

資産の重要度の判断基準例を以下に示す(表 2-5)。

表 2-5 資産の重要度の判断基準の定義例

評価値	判断基準
3	・資産が失われた、もしくは不正に操作された場合、事業上の被害大となる。 ーシステムが長期間停止(2 週間以上停止)する恐れがある。 ーシステムが制御不能になり周辺環境の破壊・汚染が発生する恐れがある。
2	・資産が失われた、もしくは不正に操作された場合、事業上の被害中となる。 ーシステムが一定期間停止(3 日～2 週間未満停止)する恐れがある。 ーシステムが制御不能になり事業会社敷地内での被害が発生する恐れがある。
1	・資産が失われた、もしくは不正に操作された場合、事業上の被害小となる。 ーシステムが一定期間停止(3 日未満)する恐れはない。 ーシステムが制御不能になることで制御システムの損傷が発生する恐れはない。

制御システム運転停止期間の基準: 備蓄在庫が 2 週間あるため、2 週間未満の制御システム運転停止につながる場合は重要度(事業被害)2、 それ以上は重要度(事業被害)3 とする。

- 重要度異なる評価値となる判断基準に該当する場合は、重要度が高い評価値とする。

【解説 2.4】

- 重要度の判断基準

  制御システムの資産の重要度の判断基準は、まずは可用性の観点から設定すると分かりやすい。この場合、可用性観点のみの重要度の判断基準だと、情報ネットワークと制御ネットワークの境界ファイアウォールや、機密情報を含む資産（ここでは EWS）に対する重要度が低くなることに注意して欲しい。

- 制御システム（プラント）停止期間の基準

  事業継続計画（BCP）等の社内規定を参照し、制御システムの機能停止期間の基準を決めるのが望ましい。例えば、制御システムの復旧目標期間（製品の製造再開や供給再開の目標期間）が 2 週間で製造製品の備蓄在庫が 2 週間ある場合、2 週間を超える制御システム運転停止が被害大と考えることができる。

2.5. 各資産に対する重要度一覧

【作業 2.5】資産の重要度を決定すること。

- 「2.4 資産の重要度の判断基準」に従い、各資産の重要度を決定する。
- 重要度を決定した根拠を記載すること。

【アウトプット 2.5】

資産の重要度とその判断根拠を以下に示す(表 2-6)。

表 2-6 資産の重要度

#	資産	重要度	判断根拠
1	監視端末	1	当該機器が操作不能になっても制御システムの安定稼働に影響はない。
2	ファイアウォール	3	ファイアウォールのフィルタ設定が改ざんされた場合、情報ネットワークからセキュリティ対策水準が低い制御ネットワークへ直接不正アクセスが可能になる。
3	スイッチ(DMZ 内)、DMZ	2	DMZ のネットワークが停止しても、制御システムに直ちに影響はない。
4	データヒストリアン(中継)	2	ヒストリアンが停止しても制御システムの安定稼働に影響はないが、データ解析が不能となるため制御システムの運転効率が落ちる可能性がある。
5	データヒストリアン	2	ヒストリアンが停止しても制御システムの安定稼働に影響はないが、データ解析が不能となるため制御システムの運転効率が落ちる可能性がある。
6	スイッチ(制御ネットワーク(情報側))、制御ネットワーク(情報側)	2	制御ネットワーク(情報側)のネットワークが停止しても、制御システムに直ちに影響はない。
7	EWS	3	EWS 自身が乗っ取られると、コントローラのプログラムロジックが改竄される可能性がある。
8	制御サーバ	3	当該機器が動作不能になる、もしくは、不正操作により、制御システムの安定稼働に影響を与える可能性は非常に高い。
9	HMI(操作端末)	3	全ての HMI が監視操作不能になると監視操作不能になる。制御システムを一時的に停止する可能性がある。
10	制御ネットワーク(フィールド側)	3	当該ネットワークが止まってもシステムは停止しないが、監視・操作ができなくなる。
11	フィールドネットワーク	3	当該ネットワークが輻輳したり停止したりすると、正常な監視制御ができなくなり、制御システムの安定稼働ができなくなる可能性が高い。
12	コントローラ、コントローラ(マスター)	3	当該機器が動作不能になる、もしくは、不正操作により、制御システムの安定稼働に影響を与える可能性は非常に高い。
13	コントローラ(スレーブ)	3	当該機器が動作不能になる、もしくは、不正操作により、制御システムの安定稼働に影響を与える可能性は非常に高い。

【解説 2.5】

- 冗長化されている資産の重要度（可用性観点）評価

  資産の重要度を可用性の観点で評価する場合、複数台あるため 1 つ資産が喪失しても可用性に影響はないため評価値を下げるのではなく、資産が全て喪失した場合の影響から可用性の評価値を付ける。冗長化は、実施済みの対策として整理しておく。

  資産が「機能停止（喪失）」する脅威を防ぐ対策「冗長性」が取られているかどうかは、詳細リスク分析（資産ベースのリスク分析や事業被害ベースのリスク分析）で確認する。

- 完全性・機密性観点での重要度評価

  資産によっては、完全性や機密性の観点で評価をすべきものがある。今回の例では、ファイアウォールと EWS が該当する。

  ファイアウォールは機能停止しても制御システムの安定稼働には影響が少ないが、ファイアウォールが不正アクセスされて設定が改ざんされた場合は、情報ネットワークから制御ネットワークへの直接のサイバー攻撃を許し、制御システムの安定稼働に大きな影響を与える。このため、完全性・機密性観点でファイアウォールの重要度評価を高く設定している。

  EWS が機能停止した場合、コントローラの設定変更等が出来なくなり、制御システムに悪影響を与えるが、直ちに制御システムの安定稼働に影響は出ない。これらが競合他社に流出すると長期的には営業利益に損失が発生する可能性がある。このため、EWS の機密性観点で EWS 重要度評価を高く設定している。

2.6. 事業被害レベルの判断基準

【作業 2.6】事業被害を 3 段階で評価する際の判断基準(3:被害大＞2:被害中＞1:被害小)を決めること。

- ガイド本体 *表 4-11* で提示している判断基準を具体化することが望ましい。

【アウトプット 2.6】

事業被害レベルの判断基準例を以下に示す(表 2-7)。

表 2-7 事業被害レベルの判断基準例

評価値		判断基準
3	事業上の被害が大きい	・障害が発生した場合、以下の事象となる。 - システムが長期間停止(2 週間以上停止)する恐れがある。 - 損失コストが 5 億円以上発生する恐れがある。 - 周辺環境の破壊・汚染が発生する恐れがある。
2	事業上の被害が中程度	・障害が発生した場合、以下の事象となる。 - システムが一定期間停止(3 日～2 週間停止)する恐れがある。 - 損失コストが 1 億円以上 5 億円未満発生する恐れがある。 - 事業会社敷地内での被害が発生する恐れがある。
1	事業上の被害が小さい	・障害が発生した場合、以下の事象となる。 - システムが短期間停止(3 日未満停止)する恐れがあるが、大きな影響はない。 - 損失コストが 1 億円未満発生する恐れがあるが、大きな影響はない。 - 事業会社敷地内での被害が発生する恐れはない。

制御システム運転停止期間の基準: 備蓄在庫が 2 週間あるため、2 週間未満の制御システム運転停止につながる場合は重要度(事業被害)2、 それ以上は重要度(事業被害)3 とする。

- 事業被害が異なる評価値となる判断基準に該当する場合は、事業被害レベルが高い評価値とする。

【解説 2.6】

- 判断基準の例

  省令・ガイドラインの規定（例えばガイド本体 *表 4-8* 参照）や事業者の社内規定（例えば事業継続計画）を参照し、事業被害レベルの判断基準を具体化することを推奨する。

  事業被害レベルの判断基準の具体的な例として、ガイド本体 *表 4-6* で紹介している“IEC 62443-2-1 における典型的な尺度例”が参考になる。事業被害レベルの判断基準（表 2-7）では、3 つの判断基準を選択している。

  - 一定期間の製造停止
  - 損失コスト（品質基準の製品出荷、または情報漏えいによる損失を想定）
  - 事業所敷地内外の環境への影響

2.7. 事業被害と事業被害レベルの検討

【作業 2.7①】分析対象システムで想定される事業被害とその概要を決定すること。

- 事業被害の概要には、事業被害を引き起こす「原因」とその「影響」を簡単に記載すること。
- ガイド本体「*4.3.1* 項 事業被害と事業被害レベルの意味」や、*表 4-12* 事業被害の定義例（1）が参考になる。

【アウトプット 2.7①】

分析対象システムの事業被害を以下に示す（表 2-8）。

表 2-8 事業被害の一覧表

#	事業被害	事業被害の概要
1	広域での製品供給停止	供給設備へのサイバー攻撃により、正規の供給停止機能を悪用され、広域で製品の供給が停止し、社会に多大な影響を及ぼし、当社への信頼が大きく低下する。
2	火災・爆発事故の発生	製造設備へのサイバー攻撃により、危険物取扱い設備の制御異常や操作監視不能が発生し、火災・爆発等が発生する。近隣住民や環境に影響を及ぼし、賠償費用等の損失が発生するとともに、当社への信頼が大きく低下する。
3	仕様不良製品の供給	製造設備へのサイバー攻撃により、品質基準を満たさない製品が製造・供給され、顧客に多大な迷惑を掛け、賠償費用等の損失が発生するとともに、当社への信頼が大きく低下する。
4	製造停止の発生	製造設備へのサイバー攻撃により、プロセスの制御異常や操作監視不能が発生し、プロセス停止を余儀なくされて製造が停止する。
5	機密情報の漏洩	制御システムへのサイバー攻撃により、製造に関わる企業機密が外部に漏洩し、競合他社との差別化に影響を及ぼし、競争力が低下する。

【作業 2.7②】事業被害レベルを重要度判断基準に従って決定すること。

- 「2.6 事業被害レベルの判断基準」に従った事業被害レベルの判断根拠をあわせて記載すること。

【アウトプット 2.7②】

事業被害の事業被害レベルとその判断根拠を以下に示す（表 2-9）。

表 2-9 事業被害一覧と事業被害レベル

事業被害	事業被害の概要	事業被害レベル	根拠
広域での製品供給停止	供給設備へのサイバー攻撃により、正規の供給停止機能を悪用され、広域で製品供給が停止し、社会に多大な影響を及ぼし、当社への信頼が大きく低下する。	3	損失コストが 5 億円以上発生する恐れがあるため、レベル「3」の評価とする。
火災・爆発事故の発生	製造設備へのサイバー攻撃により、危険物取扱い設備の制御異常や操作監視不能が発生し、火災・爆発等が発生する。近隣住民や環境に影響を及ぼし、賠償費用等の損失が発生するとともに、当社への信頼が大きく低下する。	3	周辺環境に大きな被害が出るため、レベル「3」の評価とする。
仕様不良製品の供給	製造設備へのサイバー攻撃により、品質基準を満たさない製品が製造・供給され、顧客に多大な迷惑を掛け、賠償費用等の損失が発生するとともに、当社への信頼が大きく低下する。	2	損失コストが 1 億円以上 5 億円未満になる想定で、レベル「2」の評価とする。
製造停止の発生	製造設備へのサイバー攻撃により、プロセスの制御異常や操作監視不能が発生し、プロセス停止を余儀なくされて製造が停止する。	1	停止期間が 3 日未満と想定し、レベル「1」の評価とする。
機密情報の漏洩	制御システムへのサイバー攻撃により、製造に関わる企業機密が外部に漏洩し、競合他社との差別化に影響を及ぼし、競争力が低下する。	3	他社との差別化に影響を及ぼす機密情報が外部に漏洩すると、5 億円以上の大きな損失が発生する可能性があると判断し、レベル「3」の評価とする。

【解説 2.7①②】

- 事業被害の定義

  ガイド本体「*4.3.1 項* 事業被害と事業被害レベルの意味」では、CIA 観点(C:機密性、I:完全性、A:可用性)と HSE 観点(H:健康、S:安全性、E:環境への影響)から、広い視点での事業被害例を紹介している。これらを参考に、事業者の制御システムの特性に合わせた事業被害を定義するとよい。

- 事業被害の概要の記載レベル

  事業被害の原因では、どの資産にサイバー攻撃が発生してどのような異常が発生するか、という記載レベルが望ましい。事業被害の影響度の記載は、「事業被害レベルの判断基準」と合わせた内容が望ましい。(事業被害の影響度の記載ではあいまいな記載とし、事業被害レベルを決める根拠として影響度の大中小を明確にしてもよい。)

<table>
<tr><th>事業被害</th><th>事業被害の概要</th><th>項目</th><th>備考</th></tr>
<tr><td rowspan="3">火災・爆発
事故の発生</td><td>製造設備へのサイバー攻撃により、危険物取扱い設備の制御異常や操作監視不能が発生し、</td><td>事業被害の原因</td><td rowspan="2">攻撃シナリオの
策定で利用</td></tr>
<tr><td>火災・爆発等が発生する。</td><td>事業被害(事故)</td></tr>
<tr><td>近隣住民や環境に影響を及ぼし、賠償費用等の損失が発生するとともに、当社への信頼が大きく低下する。</td><td>事業被害の影響</td><td>事業被害レベルの
策定で利用</td></tr>
</table>

2.8. 脅威レベルの判断基準

【作業 2.8】脅威レベルの判断基準(発生可能性 3:高＞2:中＞1:低)を決定すること。

- ガイド本体 *表 4-20～4-24* に判断基準の例を参考にしてもよい。

【アウトプット 2.8】

脅威レベルの判断基準を以下に示す(表 2-10)。

表 2-10 脅威レベルの判断基準

脅威レベル	悪意のある第三者による攻撃による判断基準	資産の論理的な配置による判断基準	資産の物理的な配置による判断基準
3	・個人の攻撃者(スキルは問わない)によって攻撃された場合、攻撃が成功する可能性が高い。	・インターネットと接続可能なネットワーク(情報ネットワーク)上にある資産。	・敷地と部屋への入室制限がなく、誰でもアクセスできる場所にある資産。
2	・一定のスキルを持った攻撃者によって攻撃された場合、攻撃が成功する可能性がある。	・情報ネットワークと間接的に接続しているネットワーク(制御ネットワーク)上にある資産。	・敷地と部屋への入室制限がある場所にある資産。
1	・国家レベルのサイバー攻撃者(軍隊及びそれに準ずる団体)によって攻撃された場合、攻撃が成功する可能性がある。	・隔離されたネットワーク上にある資産。	・厳重な有人監視体制と、敷地と部屋への入室制限に厳重な認証を有する部屋にある資産。

※脅威が異なる脅威レベルに当てはまる場合は、総合的に脅威レベルを判断するものとする。

【解説 2.8】

- 脅威の判断基準における攻撃者のスキル

  攻撃者のスキルには様々な分類があるが、脅威の判断基準では下記の 3 つについて総合的に判断するとよい。

  - ネットワーク経由での侵入に必要な情報セキュリティの知識・技術
  - 物理的侵入に必要なソーシャルエンジニアリングの知識・技術
  - 制御システムに不具合を発生させるための制御システムの知識・技術

- リスク分析フェーズでの脅威の判断基準の見直し

  資産ベースのリスク分析と事業被害ベースのリスク分析で、脅威レベルの判断基準について変化することがある。

  資産ベースのリスク分析においては、分析対象資産以外のセキュリティ対策を“対策レベル（脆弱性レベル）”として評価せず、“脅威レベルを低下する要素”としてリスク分析をしてもよい。

  一方、事業被害ベースのリスク分析では、分析対象システムに含まれるセキュリティ対策は、対策レベルとして評価し、脅威レベルを低下させる要素として評価してはならないことに注意が必要である。

3. 資産ベースのリスク分析

資産ベースのリスク分析では、事前準備で作成した下記のアウトプットを利用して、リスク分析作業を実施する。

表 3-1 利用する事前準備のアウトプット

別冊見出し	事前準備のアウトプット	ガイド本体
2.1.	資産一覧	*3.1.5. 表 3-9*
2.2.	システム構成図	*3.2.3. 図 3-8*
2.3.①	データフローマトリクス	*3.3.1. 表 3-10*
2.3.②	データフロー図	*3.3.2. 図 3-14*
2.4.	資産の重要度の判断基準	*4.2.2. 表 4-5*
2.5.	各資産に対する重要度一覧	*4.2.3. 表 4-9*
2.8.	脅威レベルの判断基準	*4.4.5. 表 4-20～表 4-24*

資産ベースのリスク分析作業で新たに作成するアウトプット一覧を下記に示す。

表 3-2 資産ベースのリスク分析作業で作成するアウトプット

別冊見出し	資産ベース アウトプット	ガイド本体
3.1.	脅威レベルまとめ表	―
3.2.	資産ベースのリスク分析シート	*5 章*
3.3.①	脆弱性レベルまとめ表	―
3.3.②	リスク値まとめ表	―

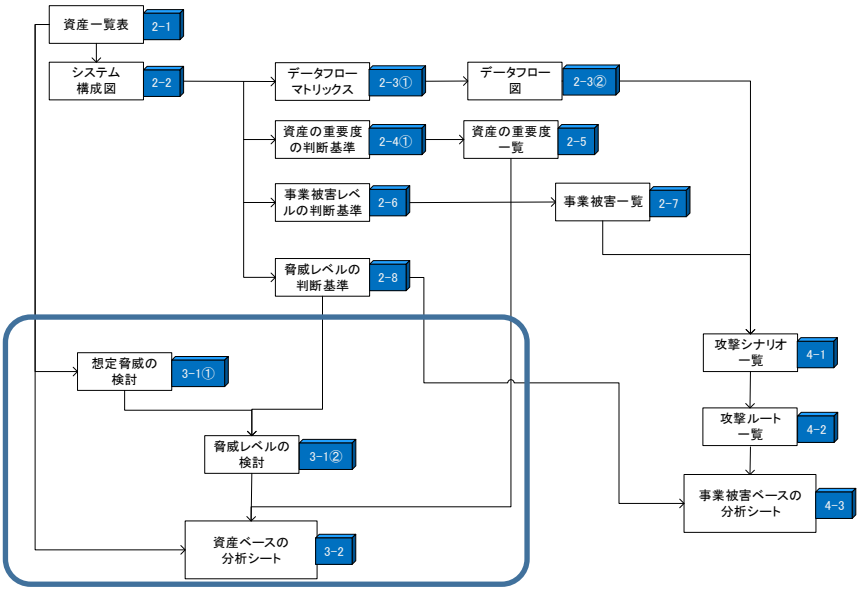


図 3-1 資産ベースのリスク分析作業の流れ

3.1. 脅威レベルの検討

【作業 3.1①】分析対象の資産に対して発生する脅威(攻撃手法)を検討し決定すること。

- ガイド本体「*表 5-4* 想定される脅威(攻撃手法)一覧と資産種別の対応」を参照すること。
- 分析対象資産の資産種別は「2.1 節 表 2-2 資産一覧」を参照すること。

【アウトプット 3.1②】

分析対象の資産に対して発生する脅威(攻撃手法)のまとめ表を以下に示す(表 3-3)。

表 3-3 分析対象の資産に想定される脅威一覧表

脅威 ＼ 資産	監視端末	ファイアウォール	DMZ	データヒストリアン(中継)	データヒストリアン	制御NW(情)	EWS	制御サーバ	HMI(操作端末)	制御NW(フ)	フィールドネットワーク	コントローラ(マスター)	コントローラ(スレーブ)
情報系機器	○	○											
制御系機器			○	○	○		○	○	○			○	○
NW系資産(通信制御機能有)			○			○							
NW系資産(通信制御機能無)										○	○		
不正アクセス	✔	✔	✔	✔	✔	✔	✔	✔	✔			✔	✔
物理的侵入	✔	✔	✔	✔	✔	✔	✔	✔	✔			✔	✔
不正操作	✔	✔	✔	✔	✔	✔	✔	✔	✔			✔	✔
過失操作	✔	✔	✔	✔	✔	✔	✔	✔	✔			✔	✔
不正媒体・機器接続	✔	✔	✔	✔	✔	✔	✔	✔	✔			✔	✔
プロセス不正実行	✔	✔	✔	✔	✔	✔	✔	✔	✔			✔	✔
マルウェア感染	✔	✔	✔	✔	✔	✔	✔	✔	✔			✔	✔
情報窃取	✔	✔	✔	✔	✔	✔	✔	✔	✔			✔	✔
情報改ざん	✔	✔	✔	✔	✔	✔	✔	✔	✔			✔	✔
情報破壊	✔	✔	✔	✔	✔	✔	✔	✔	✔			✔	✔
不正送信	✔	✔	✔	✔	✔	✔	✔	✔	✔			✔	✔
機能停止	✔	✔	✔	✔	✔	✔	✔	✔	✔			✔	✔
高負荷攻撃 DDOS	✔	✔	✔	✔	✔	✔	✔	✔	✔			✔	✔
窃盗	✔	✔	✔	✔	✔	✔	✔	✔	✔			✔	✔
盗難・廃棄時	✔	✔	✔	✔	✔	✔	✔	✔	✔			✔	✔
経路遮断			✔			✔				✔	✔		
通信輻輳			✔			✔				✔	✔		
無線妨害													
盗聴			✔			✔				✔	✔		
通信データ改ざん			✔			✔				✔	✔		
不正機器接続			✔			✔				✔	✔		

✔:資産に対して発生する脅威(攻撃手法)

グレーアウト:資産に対して発生しない脅威(攻撃手法)

機器(情報系機器・制御系機器)の場合に、#1～#15 の脅威が発生しうるとした。ネットワーク系資産(NW 系資産)の場合は、#16～#21 の脅威が発生しうるとした。今回のネットワーク系資産は無線機能を利用していないため、#18 無線妨害の脅威は発生しないこととした。

【作業 3.1②】各資産において、脅威（攻撃手法）の脅威レベルを決定すること。

- 攻撃者の想定は、「悪意のある第三者」とする（第三者の過失、内部関係者の過失、悪意のある内部関係者は資産ベースのリスク分析において除外する）。
- 「2.8 脅威レベルの判断基準」の判断基準を使い、特定の資産に対する脅威（攻撃手法）の脅威レベルを決めること。
- 脅威レベルを決定した根拠を合わせて記載すること。

【アウトプット 3.1②】

HMI（操作端末）について脅威レベルとその根拠を設定した表を以下に示す。全ての資産の脅威レベルは【アウトプット 3.1③】を参照して欲しい。

表 3-4 HMI（操作端末）の脅威レベルと根拠

#	脅威（攻撃手法）	脅威レベル	根拠
1	不正アクセス	2	無償有償を問わずハッキングツールが存在するため、一定スキルを持った攻撃者により可能。
2	物理的侵入	2	一定のソーシャルエンジニアリング能力（構内侵入等）を持った攻撃者により可能。
3	不正操作	2	スキルを問わず攻撃者によりコンソール操作が可能だが、建屋の中にあるために脅威は低い。
4	過失操作	2	制御システムと制御プロセスに精通した攻撃者により可能となるが、コントローラへの直接攻撃が可能
5	不正媒体・機器接続	3	スキルを問わず攻撃者により不正媒体や機器接続が可能。
6	プロセス不正実行	3	一定スキルを持った攻撃者により可能であるが、コントローラへの直接攻撃が可能なため脅威が高い。
7	マルウェア感染	3	汎用 OS の資産の場合、マルウェア感染の頻度は高い。
8	情報窃取	3	マルウェアに感染した場合(#7)、容易に起こり得るため脅威が高い。
9	情報改ざん	3	マルウェアに感染した場合(#7)、容易に起こり得るため脅威が高い。
10	情報破壊	3	マルウェアに感染した場合(#7)、容易に起こり得るため脅威が高い。
11	不正送信	3	マルウェアに感染した場合(#7)、容易に起こり得るため脅威が高い。
12	機能停止	3	マルウェアに感染した場合(#7)、容易に起こり得るため脅威が高い。
13	高負荷攻撃	1	高負荷であっても代替機器で運用可能であるため、脅威は低い。
14	窃盗	2	一定のソーシャルエンジニアリング能力（構内侵入等）を持った攻撃者により可能。
15	盗難・廃棄時の分解による情報窃取	2	窃盗（#14）により起こり得る。
16	経路遮断	―	ネットワーク資産ではないため対象外。
17	通信輻輳	―	ネットワーク資産ではないため対象外。
18	無線妨害	―	ネットワーク資産ではない、無線機能がないため対象外。
19	盗聴	―	ネットワーク資産ではないため対象外。
20	通信データ改ざん	―	ネットワーク資産ではないため対象外。
21	不正機器接続	―	ネットワーク資産ではないため対象外。

【作業 3.1③】分析対象の全資産で脅威レベルを検討し、それらを一覧表にまとめること。

- 資産と脅威の種類の組み合わせにおける、脅威レベルの分布の把握や見直しができる。

【アウトプット 3.1③】

資産の脅威レベルまとめ表を以下に示す。

表 3-5 資産の脅威レベルまとめ表

脅威＼資産	監視端末	ファイアウォール	DMZ	データヒストリアン（中継）	データヒストリアン	制御NW(情)	EWS	制御サーバ	HMI(操作端末)	制御NW(フ)	フィールドネットワーク	コントローラ（マスター）	コントローラ（スレーブ）
機器	○			○	○		○	○	○			○	○
NW系資産（通信制御機能有）		○	○			○							
NW系資産（通信制御機能無）										○	○		
不正アクセス	3	3	3	3	2	2	2	2	2			2	2
物理的侵入	2	1	1	1	1	1	1	1	2			2	3
不正操作	2	2	2	2	2	2	2	2	2			2	3
過失操作	3	2	2	2	2	2	2	2	2			2	2
不正媒体・機器接続	3	2	2	2	2	2	3	2	3			2	2
プロセス不正実行	3	2	2	2	2	1	3	3	3			2	2
マルウェア感染	3	1	1	3	3	1	3	3	3			1	1
情報窃取	3	1	1	3	3	1	3	3	3			3	3
情報改ざん	2	3	3	3	3	2	3	3	3			3	3
情報破壊	2	2	2	3	3	2	3	3	3			3	3
不正送信	2	1	1	3	3	1	3	3	3			3	3
機能停止	2	2	2	3	3	2	3	3	3			2	3
高負荷攻撃　DDOS	1	3	3	1	1	3	1	1	1			3	3
窃盗	2	1	1	1	1	1	2	1	2			2	3
盗難・廃棄時	2	1	1	1	1	1	2	1	2			2	3
経路遮断			2			2				3	3		
通信輻輳			2			2				2	2		
無線妨害													
盗聴			2			2				2	2		
通信データ改ざん			2			2				2	2		
不正機器接続			3			3				2	2		

3.2. 資産ベースのリスク分析シートへの記入

ガイド本体「*5 章* 資産ベースのリスク分析」で解説された手順に基づき、分析対象システムの資産ベースのリスク分析を実施する。詳細な手順はガイド本体を参照するものとして、ここでは作業の大きな流れを説明する。

【作業 3.2①】資産ベースの分析シートに重要度を記載すること。

- 「表 2-6 資産の重要度」で定義した数値を分析シートに記載する。

【作業 3.2②】資産ベースの分析シートに脅威レベルを記載すること。また、想定しない脅威はグレーアウトすること。

- 「表 3-3 分析対象の資産に想定される脅威一覧表」を参照し、資産に対して想定する脅威に脅威レベルを記載する。また想定しない脅威はグレーアウトする。

【作業 3.2③】脅威に対する対策状況を確認し、実施している対策に〇を記入すること。対策の実施内容について補足があれば追記すること。また、必要に応じて対策項目の追記すること。

- 「表 2-3 資産一覧表」のセキュリティ対策項目と資産ベースの分析シートの対策状況を比較し、該当する対策状況に〇を記入する。

【作業 3.2④】対策内容から対策レベルを評価し、対策レベルと脆弱性レベルを分析シートに記入すること。

- ガイド本体「*5.5.1 項 表 5-7*」を基準として採用し、対策レベルと脆弱性レベルを記載する。

【作業 3.2⑤】重要度レベル、脅威レベル、脆弱性レベルからリスク値を決定し、分析シートに記入すること。

【アウトプット 3.2】

資産ベースのリスク分析シートの記入例について、43 頁以降に示す（表 3-6）。

このページは空白です。

表 3-6 資産ベースのリスク分析シート

凡例: ○ 対策実施　グレーアウト行：該当資産で考慮しない脅威　対策の緑字：対策の補足情報

項番	資産種別	対象装置	評価指標				脅威(攻撃手法)	説明	対策						対策レベル
									防御				検知/被害把握	事業継続	
			脅威レベル	脆弱性レベル	資産の重要度	リスク値			侵入/拡散段階		目的遂行段階				脅威毎
1	情報系資産	**監視端末**	**3**	**2**		**D**	不正アクセス	ネットワーク経由で機器に侵入し、攻撃を実行する。	FW（パケットフィルタリング型） FW（アプリケーションゲートウェイ型） 一方向ゲートウェイ プロキシサーバ WAF 通信相手の認証 ○ IPS／IDS パッチ適用 ○ 脆弱性回避				IPS／IDS ログ収集・分析 統合ログ管理システム		2
2			**2**	**2**		**D**	物理的侵入	入室が制限された区画・領域（機器が設置された場所等）に不正侵入する。あるいは、物理的アクセスが制限された機器（ラックや箱内に設置された機器等）の制限を解除する。	入退管理　（ICカード） ○ 施錠管理 ○				監視カメラ 侵入センサ		2
3			**2**	**2**		**D**	不正操作	機器のコンソール等の直接操作で侵入し、攻撃を実行する。	操作者認証 ○						2
4			**3**	**2**		**D**	過失操作	内部関係者（社員や協力者の内、当該機器へのアクセス権を有する者）の過失操作を誘発し、攻撃を実行する。 機器に対して、正規の媒体・機器を接続した結果、攻撃に相当する行為が実行される。	URLフィルタリング／Webレピュテーション ○ メールフィルタリング ○						2
5			**3**	**2**		**D**	不正媒体・機器接続	機器に対して、不正に持ち込んだ媒体・機器（CD/DVDやUSB機器等）を接続し、攻撃を実行する。	デバイス接続・利用制限 ○	（同左）			（同左） ログ収集・分析 統合ログ管理システム		2
6			**3**	**3**		**C**	プロセス不正実行	攻撃対象機器上に存在する正規のプログラムやコマンド、サービス等のプロセスを、不正に実行する。	権限管理 アクセス制御 ホワイトリストによるプロセスの起動制限 重要操作の承認	（同左） （同左） （同左） （同左）			機器異常検知 機器死活監視 ログ収集・分析 統合ログ管理システム		1
7			**3**	**2**		**D**	マルウェア感染	攻撃対象機器にマルウェア（不正プログラム）を感染・動作させる。	アンチウイルス ○ ホワイトリストによるプロセスの起動制限 パッチ適用 ○ 脆弱性回避 データ署名				機器異常検知 機器死活監視 ログ収集・分析 統合ログ管理システム		2
8			**3**	**3**		**C**	情報窃取	機器内に格納されている情報（ソフトウェア、認証情報、構成設定情報、暗号鍵等の機密情報）を窃取する。	権限管理 アクセス制御 データ暗号化 DLP	（同左） （同左） （同左） （同左）			ログ収集・分析 統合ログ管理システム		1
9			**2**	**3**		**D**	情報改ざん	機器内に格納されている情報（ソフトウェア、認証情報、構成設定情報、暗号鍵等の機密情報）を改ざんする。	権限管理 アクセス制御 データ署名	（同左） （同左） （同左）			機器異常検知 ログ収集・分析 統合ログ管理システム	データバックアップ	1
10			**2**	**3**		**D**	情報破壊	機器内に格納されている情報（ソフトウェア、認証情報、構成設定情報、暗号鍵等の機密情報）を破壊する。		権限管理 アクセス制御			機器異常検知 ログ収集・分析 統合ログ管理システム	データバックアップ	1
11			**2**	**3**	**1**	**D**	不正送信	他の機器に対して、不正な制御コマンド（設定値変更、電源断等）や不正なデータを送信する。	セグメント分割／ゾーニング データ署名 重要操作の承認	（同左） （同左） （同左）			ログ収集・分析 統合ログ管理システム		1
12			**2**	**3**		**D**	機能停止	機器の機能を停止する。					機器異常検知 機器死活監視 ログ収集・分析 統合ログ管理システム	冗長化 フェールセーフ設計	1
13			**1**	**3**		**E**	高負荷攻撃	DDoS攻撃等によって、機器の処理能力以上の処理を要求し、機器の正常動作を妨害する。	DDoS対策				機器異常検知 機器死活監視 ログ収集・分析 統合ログ管理システム	冗長化 フェールセーフ設計	1
14			**2**	**2**		**D**	窃盗	機器を窃盗する。	施錠管理 ○	（同左）			（同左）		2
15			**2**	**2**		**D**	盗難・廃棄時の分解による情報窃取	盗難にあった機器や廃棄した機器が分解され、機器内部に保存されていた情報（ソフトウェア、認証情報、構成設定情報、暗号鍵等の機密情報）が窃取される。	耐タンパー 難読化 セキュア消去 ○	（同左） （同左） （同左）					2
16							経路遮断	通信ケーブルを切断し、通信を遮断する。あるいは、機器から通信ケーブルを引き抜き、通信を遮断する。	入退管理　（ICカード） 施錠管理				機器異常検知 機器死活監視 ログ収集・分析 統合ログ管理システム 監視カメラ 侵入センサ	冗長化	
17							通信輻輳	容量以上の通信トラフィックを発生させ、輻輳状態とする。	FW（パケットフィルタリング型） FW（アプリケーションゲートウェイ型） WAF IPS／IDS DDoS対策				機器異常検知 機器死活監視 ログ収集・分析 統合ログ管理システム	冗長化	
18	対象外（機能なし）						無線妨害	無線通信を妨害する。					機器異常検知 機器死活監視 ログ収集・分析 統合ログ管理システム	冗長化	
19							盗聴	ネットワーク上を流れる情報を盗聴する。	通信路暗号化 データ暗号化 専用線						
20							通信データ改ざん	ネットワーク上を流れる情報を改ざんする。	通信路暗号化 データ署名 専用線				ログ収集・分析 統合ログ管理システム		
21							不正機器接続	ネットワーク上に不正機器を接続する。	デバイス接続・利用制限				デバイス接続・利用制限 ログ収集・分析 統合ログ管理システム		

表 3-6 資産ベースのリスク分析シート

凡例: ○ 対策実施　グレーアウト行: 該当資産で考慮しない脅威　　対策の緑字:　対策の補足情報

項番	資産種別	対象装置	評価指標				脅威(攻撃手法)	説明	対策								対策レベル
									防御				検知/被害把握		事業継続		
			脅威レベル	脆弱性レベル	資産の重要度	リスク値			侵入/拡散段階		目的遂行段階						脅威毎
1	ネットワーク資産	**ファイアウォール**	3	2	3	A	不正アクセス	ネットワーク経由で機器に侵入し、攻撃を実行する。	FW(パケットフィルタリング型) FW(アプリケーションゲートウェイ型) 一方向ゲートウェイ プロキシサーバ WAF 通信相手の認証 IPS／IDS パッチ適用 脆弱性回避	○ ○ ○ 			IPS／IDS ログ収集・分析 統合ログ管理システム				2
2			1	1		C	物理的侵入	入室が制限された区画・領域(機器が設置された場所等)に不正侵入する。あるいは、物理的アクセスが制限された機器(ラックや箱内に設置された機器等)の制限を解除する。	入退管理　(ICカード、生体認証) 施錠管理	○ ○			監視カメラ 侵入センサ	○ ○			3
3			2	2		B	不正操作	機器のコンソール等の直接操作で侵入し、攻撃を実行する。	操作者認証 (ID/Pass)	○							2
4			2	3		A	過失操作	内部関係者(社員や協力者の内、当該機器へのアクセス権を有する者)の過失操作を誘発し、攻撃を実行する。 機器に対して、正規の媒体・機器を接続した結果、攻撃に相当する行為が実行される。	URLフィルタリング／Webレピュテーション メールフィルタリング								1
5			2	3		A	不正媒体・機器接続	機器に対して、不正に持ち込んだ媒体・機器(CD/DVDやUSB機器等)を接続し、攻撃を実行する。	デバイス接続・利用制限		(同左)		(同左) ログ収集・分析 統合ログ管理システム				1
6			2	2		B	プロセス不正実行	攻撃対象機器上に存在する正規のプログラムやコマンド、サービス等のプロセスを、不正に実行する。	権限管理 アクセス制御 ホワイトリストによるプロセスの起動制限 重要操作の承認	○	(同左) (同左) (同左) (同左)		機器異常検知 機器死活監視 ログ収集・分析 統合ログ管理システム				2
7			1	3		B	マルウェア感染	攻撃対象機器にマルウェア(不正プログラム)を感染・動作させる。	アンチウイルス ホワイトリストによるプロセスの起動制限 パッチ適用 脆弱性回避 データ署名				機器異常検知 機器死活監視 ログ収集・分析 統合ログ管理システム				1
8			1	2		C	情報窃取	機器内に格納されている情報(ソフトウェア、認証情報、構成設定情報、暗号鍵等の機密情報)を窃取する。	権限管理 アクセス制御 データ暗号化 DLP	○	(同左) (同左) (同左) (同左)		ログ収集・分析 統合ログ管理システム				2
9			3	2		A	情報改ざん	機器内に格納されている情報(ソフトウェア、認証情報、構成設定情報、暗号鍵等の機密情報)を改ざんする。	権限管理 アクセス制御 データ署名	○	(同左) (同左) (同左)		機器異常検知 ログ収集・分析 統合ログ管理システム		データバックアップ		2
10			2	2		B	情報破壊	機器内に格納されている情報(ソフトウェア、認証情報、構成設定情報、暗号鍵等の機密情報)を破壊する。			権限管理 アクセス制御	 ○	機器異常検知 ログ収集・分析 統合ログ管理システム		データバックアップ		2
11			1	3	3	B	不正送信	他の機器に対して、不正な制御コマンド(設定値変更、電源断等)や不正なデータを送信する。	セグメント分割／ゾーニング データ署名 重要操作の承認		(同左) (同左) (同左)		ログ収集・分析 統合ログ管理システム				1
12			2	3		A	機能停止	機器の機能を停止する。					機器異常検知 機器死活監視 ログ収集・分析 統合ログ管理システム		冗長化 フェールセーフ設計		1
13			3	3		A	高負荷攻撃	DDoS攻撃等によって、機器の処理能力以上の処理を要求し、機器の正常動作を妨害する。	DDoS対策				機器異常検知 機器死活監視 ログ収集・分析 統合ログ管理システム		冗長化 フェールセーフ設計		1
14			1	2		C	窃盗	機器を窃盗する。	施錠管理	○	(同左)		(同左)				2
15			1	2		C	盗難・廃棄時の分解による情報窃取	盗難にあった機器や廃棄した機器が分解され、機器内部に保存されていた情報(ソフトウェア、認証情報、構成設定情報、暗号鍵等の機密情報)が窃取される。	耐タンパー 難読化 セキュア消去	 ○	(同左) (同左) (同左)						2
16							経路遮断	通信ケーブルを切断し、通信を遮断する。あるいは、機器から通信ケーブルを引き抜き、通信を遮断する。	入退管理　(ICカード、生体認証) 施錠管理	○ ○			機器異常検知 機器死活監視 ログ収集・分析 統合ログ管理システム 監視カメラ 侵入センサ	 ○ ○	冗長化		
17							通信輻輳	容量以上の通信トラフィックを発生させ、輻輳状態とする。	FW(パケットフィルタリング型) FW(アプリケーションゲートウェイ型) WAF IPS／IDS DDoS対策	○			機器異常検知 機器死活監視 ログ収集・分析 統合ログ管理システム		冗長化		
18	対象外(機能なし)						無線妨害	無線通信を妨害する。					機器異常検知 機器死活監視 ログ収集・分析 統合ログ管理システム		冗長化		
19							盗聴	ネットワーク上を流れる情報を盗聴する。	通信路暗号化 データ暗号化 専用線								
20							通信データ改ざん	ネットワーク上を流れる情報を改ざんする。	通信路暗号化 データ署名 専用線				ログ収集・分析 統合ログ管理システム				
21							不正機器接続	ネットワーク上に不正機器を接続する。	デバイス接続・利用制限				デバイス接続・利用制限 ログ収集・分析 統合ログ管理システム				

表 3-6 資産ベースのリスク分析シート

凡例: ○ 対策実施　グレーアウト行: 該当資産で考慮しない脅威　　対策の緑字:　対策の補足情報

項番	資産種別	対象装置	評価指標				脅威(攻撃手法)	説明	対策								対策レベル
									防御				検知/被害把握		事業継続		
			脅威レベル	脆弱性レベル	資産の重要度	リスク値			侵入/拡散段階		目的遂行段階						脅威毎
1	ネットワーク資産	**スイッチ(DMZ内)** **DMZ**	**3**	**2**		**B**	不正アクセス	ネットワーク経由で機器に侵入し、攻撃を実行する。	FW(パケットフィルタリング型) FW(アプリケーションゲートウェイ型) 一方向ゲートウェイ プロキシサーバ WAF 通信相手の認証 IPS／IDS パッチ適用 脆弱性回避	 ○ ○ 			IPS／IDS ログ収集・分析 統合ログ管理システム				2
2			**1**	**1**		**D**	物理的侵入	入室が制限された区画・領域(機器が設置された場所等)に不正侵入する。あるいは、物理的アクセスが制限された機器(ラックや箱内に設置された機器等)の制限を解除する。	入退管理　(ICカード、生体認証) 施錠管理	○ ○			監視カメラ 侵入センサ	○ ○			3
3			**2**	**2**		**C**	不正操作	機器のコンソール等の直接操作で侵入し、攻撃を実行する。	操作者認証 (ID/Pass)	○							2
4			**2**	**3**		**B**	過失操作	内部関係者(社員や協力者の内、当該機器へのアクセス権を有する者)の過失操作を誘発し、攻撃を実行する。 機器に対して、正規の媒体・機器を接続した結果、攻撃に相当する行為が実行される。	URLフィルタリング／Webレピュテーション メールフィルタリング								1
5			**2**	**3**		**B**	不正媒体・機器接続	機器に対して、不正に持ち込んだ媒体・機器(CD/DVDやUSB機器等)を接続し、攻撃を実行する。	デバイス接続・利用制限		(同左)		(同左) ログ収集・分析 統合ログ管理システム				1
6			**2**	**2**		**C**	プロセス不正実行	攻撃対象機器上に存在する正規のプログラムやコマンド、サービス等のプロセスを、不正に実行する。	権限管理 アクセス制御 ホワイトリストによるプロセスの起動制限 重要操作の承認	○	(同左) (同左) (同左) (同左)		機器異常検知 機器死活監視 ログ収集・分析 統合ログ管理システム				2
7			**1**	**3**		**C**	マルウェア感染	攻撃対象機器にマルウェア(不正プログラム)を感染・動作させる。	アンチウイルス ホワイトリストによるプロセスの起動制限 パッチ適用 脆弱性回避 データ署名				機器異常検知 機器死活監視 ログ収集・分析 統合ログ管理システム				1
8			**1**	**2**		**D**	情報窃取	機器内に格納されている情報(ソフトウェア、認証情報、構成設定情報、暗号鍵等の機密情報)を窃取する。	権限管理 アクセス制御 データ暗号化 DLP	○	(同左) (同左) (同左) (同左)		ログ収集・分析 統合ログ管理システム				2
9			**3**	**2**		**B**	情報改ざん	機器内に格納されている情報(ソフトウェア、認証情報、構成設定情報、暗号鍵等の機密情報)を改ざんする。	権限管理 アクセス制御 データ署名	○	(同左) (同左) (同左)		機器異常検知 ログ収集・分析 統合ログ管理システム		データバックアップ		2
10			**2**	**2**		**C**	情報破壊	機器内に格納されている情報(ソフトウェア、認証情報、構成設定情報、暗号鍵等の機密情報)を破壊する。			権限管理 アクセス制御	○	機器異常検知 ログ収集・分析 統合ログ管理システム		データバックアップ		2
11			**1**	**3**	**2**	**C**	不正送信	他の機器に対して、不正な制御コマンド(設定値変更、電源断等)や不正なデータを送信する。	セグメント分割／ゾーニング データ署名 重要操作の承認		(同左) (同左) (同左)		ログ収集・分析 統合ログ管理システム				1
12			**2**	**3**		**B**	機能停止	機器の機能を停止する。					機器異常検知 機器死活監視 ログ収集・分析 統合ログ管理システム		冗長化 フェールセーフ設計		1
13			**3**	**3**		**B**	高負荷攻撃	DDoS攻撃等によって、機器の処理能力以上の処理を要求し、機器の正常動作を妨害する。	DDoS対策				機器異常検知 機器死活監視 ログ収集・分析 統合ログ管理システム		冗長化 フェールセーフ設計		1
14			**1**	**2**		**D**	窃盗	機器を窃盗する。	施錠管理	○	(同左)		(同左)				2
15			**1**	**2**		**D**	盗難・廃棄時の分解による情報窃取	盗難にあった機器や廃棄した機器が分解され、機器内部に保存されていた情報(ソフトウェア、認証情報、構成設定情報、暗号鍵等の機密情報)が窃取される。	耐タンパー 難読化 セキュア消去	 ○	(同左) (同左) (同左)						2
16			**2**	**1**		**D**	経路遮断	通信ケーブルを切断し、通信を遮断する。あるいは、機器から通信ケーブルを引き抜き、通信を遮断する。	入退管理　(ICカード、生体認証) 施錠管理	○ ○			機器異常検知 機器死活監視 ログ収集・分析 統合ログ管理システム 監視カメラ 侵入センサ	 ○ ○	冗長化		3
17			**2**	**3**		**B**	通信輻輳	容量以上の通信トラフィックを発生させ、輻輳状態とする。	FW(パケットフィルタリング型) FW(アプリケーションゲートウェイ型) WAF IPS／IDS DDoS対策				機器異常検知 機器死活監視 ログ収集・分析 統合ログ管理システム		冗長化		1
18	対象外(機能なし)						無線妨害	無線通信を妨害する。					機器異常検知 機器死活監視 ログ収集・分析 統合ログ管理システム		冗長化		
19			**2**	**3**		**B**	盗聴	ネットワーク上を流れる情報を盗聴する。	通信路暗号化 データ暗号化 専用線								1
20			**2**	**3**		**B**	通信データ改ざん	ネットワーク上を流れる情報を改ざんする。	通信路暗号化 データ署名 専用線				ログ収集・分析 統合ログ管理システム				1
21			**3**	**3**		**B**	不正機器接続	ネットワーク上に不正機器を接続する。	デバイス接続・利用制限				デバイス接続・利用制限 ログ収集・分析 統合ログ管理システム				1

表 3-6 資産ベースのリスク分析シート

凡例: ○ 対策実施　グレーアウト行: 該当資産で考慮しない脅威　　対策の緑字:　対策の補足情報

項番	資産種別	対象装置	評価指標				脅威(攻撃手法)	説明	対策								対策レベル
									防御				検知/被害把握		事業継続		
			脅威レベル	脆弱性レベル	資産の重要度	リスク値			侵入/拡散段階		目的遂行段階						脅威毎
1	制御系資産	**データヒストリアン(中継)**	**3**	**2**		**B**	不正アクセス	ネットワーク経由で機器に侵入し、攻撃を実行する。	FW(パケットフィルタリング型) FW(アプリケーションゲートウェイ型) 一方向ゲートウェイ プロキシサーバ WAF 通信相手の認証 IPS／IDS パッチ適用　(Webサーバのみ) 脆弱性回避	 ○ ○ 	 		IPS／IDS ログ収集・分析 統合ログ管理システム				2
2			**1**	**1**		**D**	物理的侵入	入室が制限された区画・領域(機器が設置された場所等)に不正侵入する。あるいは、物理的アクセスが制限された機器(ラックや箱内に設置された機器等)の制限を解除する。	入退管理　(ICカード、生体認証) 施錠管理	○ ○			監視カメラ 侵入センサ	○ ○			3
3			**2**	**2**		**C**	不正操作	機器のコンソール等の直接操作で侵入し、攻撃を実行する。	操作者認証 (ID/Pass)	○							2
4			**2**	**3**		**B**	過失操作	内部関係者(社員や協力者の内、当該機器へのアクセス権を有する者)の過失操作を誘発し、攻撃を実行する。 機器に対して、正規の媒体・機器を接続した結果、攻撃に相当する行為が実行される。	URLフィルタリング／Webレピュテーション メールフィルタリング								1
5			**2**	**3**		**B**	不正媒体・機器接続	機器に対して、不正に持ち込んだ媒体・機器(CD/DVDやUSB機器等)を接続し、攻撃を実行する。	デバイス接続・利用制限		(同左)		デバイス接続・利用制限 ログ収集・分析 統合ログ管理システム				1
6			**2**	**2**		**C**	プロセス不正実行	攻撃対象機器上に存在する正規のプログラムやコマンド、サービス等のプロセスを、不正に実行する。	権限管理 アクセス制御 ホワイトリストによるプロセスの起動制限 重要操作の承認	○	(同左) (同左) (同左) (同左)		機器異常検知 機器死活監視 ログ収集・分析 統合ログ管理システム				2
7			**3**	**2**		**B**	マルウェア感染	攻撃対象機器にマルウェア(不正プログラム)を感染・動作させる。	アンチウイルス ホワイトリストによるプロセスの起動制限 パッチ適用 脆弱性回避 データ署名	○			機器異常検知 機器死活監視 ログ収集・分析 統合ログ管理システム				2
8			**3**	**2**		**B**	情報窃取	機器内に格納されている情報(ソフトウェア、認証情報、構成設定情報、暗号鍵等の機密情報)を窃取する。	権限管理 アクセス制御 データ暗号化 DLP	○	(同左) (同左) (同左) (同左)		ログ収集・分析 統合ログ管理システム				2
9			**3**	**2**		**B**	情報改ざん	機器内に格納されている情報(ソフトウェア、認証情報、構成設定情報、暗号鍵等の機密情報)を改ざんする。	権限管理 アクセス制御 データ署名	○	(同左) (同左) (同左)		機器異常検知 ログ収集・分析 統合ログ管理システム		データバックアップ	○	2
10			**3**	**2**		**B**	情報破壊	機器内に格納されている情報(ソフトウェア、認証情報、構成設定情報、暗号鍵等の機密情報)を破壊する。			権限管理 アクセス制御	○ ○	機器異常検知 ログ収集・分析 統合ログ管理システム		データバックアップ	○	2
11			**3**	**3**	**2**	**B**	不正送信	他の機器に対して、不正な制御コマンド(設定値変更、電源断等)や不正なデータを送信する。	セグメント分割／ゾーニング データ署名 重要操作の承認		(同左) (同左) (同左)		ログ収集・分析 統合ログ管理システム				1
12			**3**	**3**		**B**	機能停止	機器の機能を停止する。					機器異常検知 機器死活監視 ログ収集・分析 統合ログ管理システム		冗長化 フェールセーフ設計		1
13			**1**	**3**		**C**	高負荷攻撃	DDoS攻撃等によって、機器の処理能力以上の処理を要求し、機器の正常動作を妨害する。	DDoS対策				機器異常検知 機器死活監視 ログ収集・分析 統合ログ管理システム		冗長化 フェールセーフ設計		1
14			**1**	**2**		**D**	窃盗	機器を窃盗する。	施錠管理	○	(同左)		(同左)				2
15			**1**	**2**		**D**	盗難・廃棄時の分解による情報窃取	盗難にあった機器や廃棄した機器が分解され、機器内部に保存されていた情報(ソフトウェア、認証情報、構成設定情報、暗号鍵等の機密情報)が窃取される。	耐タンパー 難読化 セキュア消去	 ○	(同左) (同左) (同左)						2
16							経路遮断	通信ケーブルを切断し、通信を遮断する。あるいは、機器から通信ケーブルを引き抜き、通信を遮断する。	入退管理 施錠管理				機器異常検知 機器死活監視 ログ収集・分析 統合ログ管理システム 監視カメラ 侵入センサ		冗長化		
17							通信輻輳	容量以上の通信トラフィックを発生させ、輻輳状態とする。	FW(パケットフィルタリング型) FW(アプリケーションゲートウェイ型) WAF IPS／IDS DDoS対策				機器異常検知 機器死活監視 ログ収集・分析 統合ログ管理システム		冗長化		
18							無線妨害	無線通信を妨害する。					機器異常検知 機器死活監視 ログ収集・分析 統合ログ管理システム		冗長化		
19	対象外(機能なし)						盗聴	ネットワーク上を流れる情報を盗聴する。	通信路暗号化 データ暗号化 専用線								
20							通信データ改ざん	ネットワーク上を流れる情報を改ざんする。	通信路暗号化 データ署名 専用線				ログ収集・分析 統合ログ管理システム				
21							不正機器接続	ネットワーク上に不正機器を接続する。	デバイス接続・利用制限				デバイス接続・利用制限 ログ収集・分析 統合ログ管理システム				

表 3-6 資産ベースのリスク分析シート

凡例: ○ 対策実施　グレーアウト行：該当資産で考慮しない脅威　　対策の緑字：　対策の補足情報

項番	資産種別	対象装置	評価指標				脅威(攻撃手法)	説明	対策								対策レベル
									防御				検知/被害把握		事業継続		
			脅威レベル	脆弱性レベル	資産の重要度	リスク値			侵入/拡散段階		目的遂行段階						脅威毎
1	制御系資産	**データヒストリアン**	**2**	**2**		**C**	不正アクセス	ネットワーク経由で機器に侵入し、攻撃を実行する。	FW（パケットフィルタリング型） FW（アプリケーションゲートウェイ型） 一方向ゲートウェイ プロキシサーバ WAF 通信相手の認証 IPS／IDS パッチ適用 脆弱性回避	 ○ 			IPS／IDS ログ収集・分析 統合ログ管理システム				2
2			**1**	**1**		**D**	物理的侵入	入室が制限された区画・領域（機器が設置された場所等）に不正侵入する。あるいは、物理的アクセスが制限された機器（ラックや箱内に設置された機器等）の制限を解除する。	入退管理　（ICカード、生体認証） 施錠管理	○ ○			監視カメラ 侵入センサ	○ ○			3
3			**2**	**2**		**C**	不正操作	機器のコンソール等の直接操作で侵入し、攻撃を実行する。	操作者認証（ID/Pass）	○							2
4			**2**	**3**		**B**	過失操作	内部関係者（社員や協力者の内、当該機器へのアクセス権を有する者）の過失操作を誘発し、攻撃を実行する。 機器に対して、正規の媒体・機器を接続した結果、攻撃に相当する行為が実行される。	URLフィルタリング／Webレピュテーション メールフィルタリング								1
5			**2**	**3**		**B**	不正媒体・機器接続	機器に対して、不正に持ち込んだ媒体・機器（CD/DVDやUSB機器等）を接続し、攻撃を実行する。	デバイス接続・利用制限		（同左）		（同左） ログ収集・分析 統合ログ管理システム				1
6			**2**	**2**		**C**	プロセス不正実行	攻撃対象機器上に存在する正規のプログラムやコマンド、サービス等のプロセスを、不正に実行する。	権限管理 アクセス制御 ホワイトリストによるプロセスの起動制限 重要操作の承認	○ ○ 	（同左） （同左） （同左） （同左）		機器異常検知 機器死活監視 ログ収集・分析 統合ログ管理システム				2
7			**3**	**2**		**B**	マルウェア感染	攻撃対象機器にマルウェア（不正プログラム）を感染・動作させる。	アンチウイルス ホワイトリストによるプロセスの起動制限 パッチ適用 脆弱性回避 データ署名	 ○ 			機器異常検知 機器死活監視 ログ収集・分析 統合ログ管理システム				2
8			**3**	**2**		**B**	情報窃取	機器内に格納されている情報（ソフトウェア、認証情報、構成設定情報、暗号鍵等の機密情報）を窃取する。	権限管理 アクセス制御 データ暗号化 DLP	○ 	（同左） （同左） （同左） （同左）		ログ収集・分析 統合ログ管理システム				2
9			**3**	**2**		**B**	情報改ざん	機器内に格納されている情報（ソフトウェア、認証情報、構成設定情報、暗号鍵等の機密情報）を改ざんする。	権限管理 アクセス制御 データ署名	○ 	（同左） （同左） （同左）		機器異常検知 ログ収集・分析 統合ログ管理システム		データバックアップ	○	2
10			**3**	**2**		**B**	情報破壊	機器内に格納されている情報（ソフトウェア、認証情報、構成設定情報、暗号鍵等の機密情報）を破壊する。			権限管理 アクセス制御	○	機器異常検知 ログ収集・分析 統合ログ管理システム		データバックアップ	○	2
11			**3**	**3**	**2**	**B**	不正送信	他の機器に対して、不正な制御コマンド（設定値変更、電源断等）や不正なデータを送信する。	セグメント分割／ゾーニング データ署名 重要操作の承認		（同左） （同左） （同左）		ログ収集・分析 統合ログ管理システム				1
12			**3**	**3**		**B**	機能停止	機器の機能を停止する。					機器異常検知 機器死活監視 ログ収集・分析 統合ログ管理システム		冗長化 フェールセーフ設計		1
13			**1**	**3**		**C**	高負荷攻撃	DDoS攻撃等によって、機器の処理能力以上の処理を要求し、機器の正常動作を妨害する。	DDoS対策				機器異常検知 機器死活監視 ログ収集・分析 統合ログ管理システム		冗長化 フェールセーフ設計		1
14			**1**	**2**		**D**	窃盗	機器を窃盗する。	施錠管理	○	（同左）		（同左）				2
15			**1**	**2**		**D**	盗難・廃棄時の分解による情報窃取	盗難にあった機器や廃棄した機器が分解され、機器内部に保存されていた情報（ソフトウェア、認証情報、構成設定情報、暗号鍵等の機密情報）が窃取される。	耐タンパー 難読化 セキュア消去	 ○	（同左） （同左） （同左）						2
16							経路遮断	通信ケーブルを切断し、通信を遮断する。あるいは、機器から通信ケーブルを引き抜き、通信を遮断する。	入退管理 施錠管理				機器異常検知 機器死活監視 ログ収集・分析 統合ログ管理システム 監視カメラ 侵入センサ		冗長化		
17							通信輻輳	容量以上の通信トラフィックを発生させ、輻輳状態とする。	FW（パケットフィルタリング型） FW（アプリケーションゲートウェイ型） WAF IPS／IDS DDoS対策				機器異常検知 機器死活監視 ログ収集・分析 統合ログ管理システム		冗長化		
18	対象外（機能なし）						無線妨害	無線通信を妨害する。					機器異常検知 機器死活監視 ログ収集・分析 統合ログ管理システム		冗長化		
19							盗聴	ネットワーク上を流れる情報を盗聴する。	通信路暗号化 データ暗号化 専用線								
20							通信データ改ざん	ネットワーク上を流れる情報を改ざんする。	通信路暗号化 データ署名 専用線				ログ収集・分析 統合ログ管理システム				
21							不正機器接続	ネットワーク上に不正機器を接続する。	デバイス接続・利用制限				デバイス接続・利用制限 ログ収集・分析 統合ログ管理システム				

表 3-6 資産ベースのリスク分析シート

凡例: ○ 対策実施　グレーアウト行：該当資産で考慮しない脅威　　対策の緑字：　対策の補足情報

項番	資産種別	対象装置	評価指標				脅威(攻撃手法)	説明	対策								対策レベル
									防御				検知/被害把握		事業継続		
			脅威レベル	脆弱性レベル	資産の重要度	リスク値			侵入/拡散段階		目的遂行段階						脅威毎
1	ネットワーク資産	**スイッチ(制御ネットワーク(情報側)内) 制御ネットワーク(情報側)**	**2**	**2**		**C**	不正アクセス	ネットワーク経由で機器に侵入し、攻撃を実行する。	FW(パケットフィルタリング型) FW(アプリケーションゲートウェイ型) 一方向ゲートウェイ プロキシサーバ WAF 通信相手の認証 IPS／IDS パッチ適用 脆弱性回避	 ○ 			IPS／IDS ログ収集・分析 統合ログ管理システム				2
2			**1**	**2**		**D**	物理的侵入	入室が制限された区画・領域(機器が設置された場所等)に不正侵入する。あるいは、物理的アクセスが制限された機器(ラックや箱内に設置された機器等)の制限を解除する。	入退管理　(ICカード) 施錠管理	○ ○			監視カメラ 侵入センサ	○ ○			2
3			**2**	**2**		**C**	不正操作	機器のコンソール等の直接操作で侵入し、攻撃を実行する。	操作者認証 (ID/Pass)	○							2
4			**2**	**3**		**B**	過失操作	内部関係者(社員や協力者の内、当該機器へのアクセス権を有する者)の過失操作を誘発し、攻撃を実行する。 機器に対して、正規の媒体・機器を接続した結果、攻撃に相当する行為が実行される。	URLフィルタリング／Webレピュテーション メールフィルタリング								1
5			**2**	**3**		**B**	不正媒体・機器接続	機器に対して、不正に持ち込んだ媒体・機器(CD/DVDやUSB機器等)を接続し、攻撃を実行する。	デバイス接続・利用制限		(同左)		(同左) ログ収集・分析 統合ログ管理システム				1
6			**1**	**2**		**D**	プロセス不正実行	攻撃対象機器上に存在する正規のプログラムやコマンド、サービス等のプロセスを、不正に実行する。	権限管理 アクセス制御 ホワイトリストによるプロセスの起動制限 重要操作の承認	○	(同左) (同左) (同左) (同左)		機器異常検知 機器死活監視 ログ収集・分析 統合ログ管理システム				2
7			**1**	**3**		**C**	マルウェア感染	攻撃対象機器にマルウェア(不正プログラム)を感染・動作させる。	アンチウイルス ホワイトリストによるプロセスの起動制限 パッチ適用 脆弱性回避 データ署名				機器異常検知 機器死活監視 ログ収集・分析 統合ログ管理システム				1
8			**1**	**2**		**D**	情報窃取	機器内に格納されている情報(ソフトウェア、認証情報、構成設定情報、暗号鍵等の機密情報)を窃取する。	権限管理 アクセス制御 データ暗号化 DLP	○	(同左) (同左) (同左) (同左)		ログ収集・分析 統合ログ管理システム				2
9			**2**	**2**		**C**	情報改ざん	機器内に格納されている情報(ソフトウェア、認証情報、構成設定情報、暗号鍵等の機密情報)を改ざんする。	権限管理 アクセス制御 データ署名	○	(同左) (同左) (同左)		機器異常検知 ログ収集・分析 統合ログ管理システム		データバックアップ		2
10			**2**	**2**		**C**	情報破壊	機器内に格納されている情報(ソフトウェア、認証情報、構成設定情報、暗号鍵等の機密情報)を破壊する。			権限管理 アクセス制御	 ○	機器異常検知 ログ収集・分析 統合ログ管理システム		データバックアップ		2
11			**1**	**3**	**2**	**C**	不正送信	他の機器に対して、不正な制御コマンド(設定値変更、電源断等)や不正なデータを送信する。	セグメント分割／ゾーニング データ署名 重要操作の承認		(同左) (同左) (同左)		ログ収集・分析 統合ログ管理システム				1
12			**2**	**3**		**B**	機能停止	機器の機能を停止する。					機器異常検知 機器死活監視 ログ収集・分析 統合ログ管理システム		冗長化 フェールセーフ設計		1
13			**3**	**3**		**B**	高負荷攻撃	DDoS攻撃等によって、機器の処理能力以上の処理を要求し、機器の正常動作を妨害する。	DDoS対策				機器異常検知 機器死活監視 ログ収集・分析 統合ログ管理システム		冗長化 フェールセーフ設計		1
14			**1**	**2**		**D**	窃盗	機器を窃盗する。	施錠管理	○	(同左)		施錠管理	○			2
15			**1**	**2**		**D**	盗難・廃棄時の分解による情報窃取	盗難にあった機器や廃棄した機器が分解され、機器内部に保存されていた情報(ソフトウェア、認証情報、構成設定情報、暗号鍵等の機密情報)が窃取される。	耐タンパー 難読化 セキュア消去	 ○	(同左) (同左) (同左)						2
16			**2**	**2**		**C**	経路遮断	通信ケーブルを切断し、通信を遮断する。あるいは、機器から通信ケーブルを引き抜き、通信を遮断する。	入退管理　(ICカード) 施錠管理	○ ○			機器異常検知 機器死活監視 ログ収集・分析 統合ログ管理システム 監視カメラ 侵入センサ	 ○ ○	冗長化		2
17			**2**	**3**		**B**	通信輻輳	容量以上の通信トラフィックを発生させ、輻輳状態とする。	FW(パケットフィルタリング型) FW(アプリケーションゲートウェイ型) WAF IPS／IDS DDoS対策				機器異常検知 機器死活監視 ログ収集・分析 統合ログ管理システム		冗長化		1
18	対象外(機能なし)						無線妨害	無線通信を妨害する。					機器異常検知 機器死活監視 ログ収集・分析 統合ログ管理システム		冗長化		
19			**2**	**3**		**B**	盗聴	ネットワーク上を流れる情報を盗聴する。	通信路暗号化 データ暗号化 専用線								1
20			**2**	**3**		**B**	通信データ改ざん	ネットワーク上を流れる情報を改ざんする。	通信路暗号化 データ署名 専用線				ログ収集・分析 統合ログ管理システム				1
21			**3**	**3**		**B**	不正機器接続	ネットワーク上に不正機器を接続する。	デバイス接続・利用制限				デバイス接続・利用制限 ログ収集・分析 統合ログ管理システム				1

表 3-6 資産ベースのリスク分析シート

凡例: ○ 対策実施　グレーアウト行：該当資産で考慮しない脅威　　対策の緑字：　対策の補足情報

項番	資産種別	対象装置	評価指標				脅威(攻撃手法)	説明	対策								対策レベル
									防御				検知/被害把握		事業継続		
			脅威レベル	脆弱性レベル	資産の重要度	リスク値			侵入/拡散段階		目的遂行段階						脅威毎
1	制御系資産	EWS	2	2		B	不正アクセス	ネットワーク経由で機器に侵入し、攻撃を実行する。	FW（パケットフィルタリング型） FW（アプリケーションゲートウェイ型） 一方向ゲートウェイ プロキシサーバ WAF 通信相手の認証 IPS／IDS パッチ適用 脆弱性回避	 ○ 			IPS／IDS ログ収集・分析 統合ログ管理システム			2
2			1	1		C	物理的侵入	入室が制限された区画・領域（機器が設置された場所等）に不正侵入する。あるいは、物理的アクセスが制限された機器（ラックや箱内に設置された機器等）の制限を解除する。	入退管理　（ICカード、生体認証） 施錠管理	○ ○			監視カメラ 侵入センサ	○ ○			3
3			2	2		B	不正操作	機器のコンソール等の直接操作で侵入し、攻撃を実行する。	操作者認証（ID/Pass）	○							2
4			2	3		A	過失操作	内部関係者（社員や協力者の内、当該機器へのアクセス権を有する者）の過失操作を誘発し、攻撃を実行する。 機器に対して、正規の媒体・機器を接続した結果、攻撃に相当する行為が実行される。	URLフィルタリング／Webレピュテーション メールフィルタリング								1
5			3	3		A	不正媒体・機器接続	機器に対して、不正に持ち込んだ媒体・機器（CD/DVDやUSB機器等）を接続し、攻撃を実行する。	デバイス接続・利用制限		（同左）		（同左） ログ収集・分析 統合ログ管理システム				1
6			3	3		A	プロセス不正実行	攻撃対象機器上に存在する正規のプログラムやコマンド、サービス等のプロセスを、不正に実行する。	権限管理 アクセス制御 ホワイトリストによるプロセスの起動制限 重要操作の承認		（同左） （同左） （同左） （同左）		機器異常検知 機器死活監視 ログ収集・分析 統合ログ管理システム				1
7			3	3		A	マルウェア感染	攻撃対象機器にマルウェア（不正プログラム）を感染・動作させる。	アンチウイルス ホワイトリストによるプロセスの起動制限 パッチ適用 脆弱性回避 データ署名				機器異常検知 機器死活監視 ログ収集・分析 統合ログ管理システム				1
8			3	3		A	情報窃取	機器内に格納されている情報（ソフトウェア、認証情報、構成設定情報、暗号鍵等の機密情報）を窃取する。	権限管理 アクセス制御 データ暗号化 DLP		（同左） （同左） （同左） （同左）		ログ収集・分析 統合ログ管理システム				1
9			3	3		A	情報改ざん	機器内に格納されている情報（ソフトウェア、認証情報、構成設定情報、暗号鍵等の機密情報）を改ざんする。	権限管理 アクセス制御 データ署名		（同左） （同左） （同左）		機器異常検知 ログ収集・分析 統合ログ管理システム		データバックアップ		1
10			3	3		A	情報破壊	機器内に格納されている情報（ソフトウェア、認証情報、構成設定情報、暗号鍵等の機密情報）を破壊する。			権限管理 アクセス制御		機器異常検知 ログ収集・分析 統合ログ管理システム		データバックアップ		1
11			3	3	3	A	不正送信	他の機器に対して、不正な制御コマンド（設定値変更、電源断等）や不正なデータを送信する。	セグメント分割／ゾーニング データ署名 重要操作の承認		（同左） （同左） （同左）		ログ収集・分析 統合ログ管理システム				1
12			3	3		A	機能停止	機器の機能を停止する。					機器異常検知 機器死活監視 ログ収集・分析 統合ログ管理システム		冗長化 フェールセーフ設計		1
13			1	3		B	高負荷攻撃	DDoS攻撃等によって、機器の処理能力以上の処理を要求し、機器の正常動作を妨害する。	DDoS対策				機器異常検知 機器死活監視 ログ収集・分析 統合ログ管理システム		冗長化 フェールセーフ設計		1
14			2	2		B	窃盗	機器を窃盗する。	施錠管理	○	（同左）		（同左）				2
15			2	2		B	盗難・廃棄時の分解による情報窃取	盗難にあった機器や廃棄した機器が分解され、機器内部に保存されていた情報（ソフトウェア、認証情報、構成設定情報、暗号鍵等の機密情報）が窃取される。	耐タンパー 難読化 セキュア消去	 ○	（同左） （同左） （同左）						2
16							経路遮断	通信ケーブルを切断し、通信を遮断する。あるいは、機器から通信ケーブルを引き抜き、通信を遮断する。	入退管理 施錠管理				機器異常検知 機器死活監視 ログ収集・分析 統合ログ管理システム 監視カメラ 侵入センサ		冗長化		
17							通信輻輳	容量以上の通信トラフィックを発生させ、輻輳状態とする。	FW（パケットフィルタリング型） FW（アプリケーションゲートウェイ型） WAF IPS／IDS DDoS対策				機器異常検知 機器死活監視 ログ収集・分析 統合ログ管理システム		冗長化		
18	対象外（機能なし）						無線妨害	無線通信を妨害する。					機器異常検知 機器死活監視 ログ収集・分析 統合ログ管理システム		冗長化		
19							盗聴	ネットワーク上を流れる情報を盗聴する。	通信路暗号化 データ暗号化 専用線								
20							通信データ改ざん	ネットワーク上を流れる情報を改ざんする。	通信路暗号化 データ署名 専用線				ログ収集・分析 統合ログ管理システム				
21							不正機器接続	ネットワーク上に不正機器を接続する。	デバイス接続・利用制限				デバイス接続・利用制限 ログ収集・分析 統合ログ管理システム				

表 3-6 資産ベースのリスク分析シート

凡例: ○ 対策実施　グレーアウト行：該当資産で考慮しない脅威　　対策の緑字：　対策の補足情報

項番	資産種別	対象装置	評価指標				脅威(攻撃手法)	説明	対策								対策レベル
									防御				検知/被害把握		事業継続		
			脅威レベル	脆弱性レベル	資産の重要度	リスク値			侵入/拡散段階		目的遂行段階						脅威毎
1	制御系資産	**制御サーバ**	**2**	**2**		**B**	不正アクセス	ネットワーク経由で機器に侵入し、攻撃を実行する。	FW（パケットフィルタリング型） FW（アプリケーションゲートウェイ型） 一方向ゲートウェイ プロキシサーバ WAF 通信相手の認証 IPS／IDS パッチ適用 脆弱性回避	 ○ 			IPS／IDS ログ収集・分析 統合ログ管理システム				2
2			**1**	**1**		**C**	物理的侵入	入室が制限された区画・領域（機器が設置された場所等）に不正侵入する。あるいは、物理的アクセスが制限された機器（ラックや箱内に設置された機器等）の制限を解除する。	入退管理　（ICカード、生体認証） 施錠管理	○ ○			監視カメラ 侵入センサ	○ ○			3
3			**2**	**2**		**B**	不正操作	機器のコンソール等の直接操作で侵入し、攻撃を実行する。	操作者認証（ID/Pass）	○							2
4			**2**	**3**		**A**	過失操作	内部関係者（社員や協力者の内、当該機器へのアクセス権を有する者）の過失操作を誘発し、攻撃を実行する。 機器に対して、正規の媒体・機器を接続した結果、攻撃に相当する行為が実行される。	URLフィルタリング／Webレピュテーション メールフィルタリング								1
5			**2**	**3**		**A**	不正媒体・機器接続	機器に対して、不正に持ち込んだ媒体・機器（CD/DVDやUSB機器等）を接続し、攻撃を実行する。	デバイス接続・利用制限		（同左）		（同左） ログ収集・分析 統合ログ管理システム				1
6			**3**	**2**		**A**	プロセス不正実行	攻撃対象機器上に存在する正規のプログラムやコマンド、サービス等のプロセスを、不正に実行する。	権限管理 アクセス制御 ホワイトリストによるプロセスの起動制限 重要操作の承認	○ ○ 	（同左） （同左） （同左） （同左）		機器異常検知 機器死活監視 ログ収集・分析 統合ログ管理システム				2
7			**3**	**2**		**A**	マルウェア感染	攻撃対象機器にマルウェア（不正プログラム）を感染・動作させる。	アンチウイルス ホワイトリストによるプロセスの起動制限 パッチ適用 脆弱性回避 データ署名	 ○ 			機器異常検知 機器死活監視 ログ収集・分析 統合ログ管理システム				2
8			**3**	**2**		**A**	情報窃取	機器内に格納されている情報（ソフトウェア、認証情報、構成設定情報、暗号鍵等の機密情報）を窃取する。	権限管理 アクセス制御 データ暗号化 DLP	○ 	（同左） （同左） （同左） （同左）		ログ収集・分析 統合ログ管理システム				2
9			**3**	**2**		**A**	情報改ざん	機器内に格納されている情報（ソフトウェア、認証情報、構成設定情報、暗号鍵等の機密情報）を改ざんする。	権限管理 アクセス制御 データ署名	○ 	（同左） （同左） （同左）		機器異常検知 ログ収集・分析 統合ログ管理システム		データバックアップ	○	2
10			**3**	**2**		**A**	情報破壊	機器内に格納されている情報（ソフトウェア、認証情報、構成設定情報、暗号鍵等の機密情報）を破壊する。			権限管理 アクセス制御	○	機器異常検知 ログ収集・分析 統合ログ管理システム		データバックアップ	○	2
11			**3**	**3**	**3**	**A**	不正送信	他の機器に対して、不正な制御コマンド（設定値変更、電源断等）や不正なデータを送信する。	セグメント分割／ゾーニング データ署名 重要操作の承認		（同左） （同左） （同左）		ログ収集・分析 統合ログ管理システム				1
12			**3**	**3**		**A**	機能停止	機器の機能を停止する。					機器異常検知 機器死活監視 ログ収集・分析 統合ログ管理システム		冗長化 フェールセーフ設計		1
13			**1**	**3**		**B**	高負荷攻撃	DDoS攻撃等によって、機器の処理能力以上の処理を要求し、機器の正常動作を妨害する。	DDoS対策				機器異常検知 機器死活監視 ログ収集・分析 統合ログ管理システム		冗長化 フェールセーフ設計		1
14			**1**	**2**		**C**	窃盗	機器を窃盗する。	施錠管理	○	（同左）		（同左）				2
15			**1**	**2**		**C**	盗難・廃棄時の分解による情報窃取	盗難にあった機器や廃棄した機器が分解され、機器内部に保存されていた情報（ソフトウェア、認証情報、構成設定情報、暗号鍵等の機密情報）が窃取される。	耐タンパー 難読化 セキュア消去	 ○	（同左） （同左） （同左）						2
16							経路遮断	通信ケーブルを切断し、通信を遮断する。あるいは、機器から通信ケーブルを引き抜き、通信を遮断する。	入退管理 施錠管理				機器異常検知 機器死活監視 ログ収集・分析 統合ログ管理システム 監視カメラ 侵入センサ		冗長化		
17							通信輻輳	容量以上の通信トラフィックを発生させ、輻輳状態とする。	FW（パケットフィルタリング型） FW（アプリケーションゲートウェイ型） WAF IPS／IDS DDoS対策				機器異常検知 機器死活監視 ログ収集・分析 統合ログ管理システム		冗長化		
18	対象外（機能なし）						無線妨害	無線通信を妨害する。					機器異常検知 機器死活監視 ログ収集・分析 統合ログ管理システム		冗長化		
19							盗聴	ネットワーク上を流れる情報を盗聴する。	通信路暗号化 データ暗号化 専用線								
20							通信データ改ざん	ネットワーク上を流れる情報を改ざんする。	通信路暗号化 データ署名 専用線				ログ収集・分析 統合ログ管理システム				
21							不正機器接続	ネットワーク上に不正機器を接続する。	デバイス接続・利用制限				デバイス接続・利用制限 ログ収集・分析 統合ログ管理システム				

表 3-6 資産ベースのリスク分析シート

凡例: ○ 対策実施　グレーアウト行：該当資産で考慮しない脅威　　対策の緑字：　対策の補足情報

項番	資産種別	対象装置	評価指標				脅威(攻撃手法)	説明	対策								対策レベル
									防御				検知/被害把握		事業継続		
			脅威レベル	脆弱性レベル	資産の重要度	リスク値			侵入/拡散段階		目的遂行段階						脅威毎
1	制御系資産	**HMI(操作端末)**	**2**	**2**		**B**	不正アクセス	ネットワーク経由で機器に侵入し、攻撃を実行する。	FW（パケットフィルタリング型）				IPS／IDS				
									FW（アプリケーションゲートウェイ型）				ログ収集・分析				
									一方向ゲートウェイ				統合ログ管理システム				
									プロキシサーバ								
									WAF								
									通信相手の認証	○							2
									IPS／IDS								
									パッチ適用								
									脆弱性回避								
2			**2**	**2**		**B**	物理的侵入	入室が制限された区画・領域（機器が設置された場所等）に不正侵入する。あるいは、物理的アクセスが制限された機器（ラックや箱内に設置された機器等）の制限を解除する。	入退管理　（ICカード）	○			監視カメラ	○			
									施錠管理	○			侵入センサ	○			2
3			**2**	**3**		**A**	不正操作	機器のコンソール等の直接操作で侵入し、攻撃を実行する。	操作者認証								1
4			**2**	**3**		**A**	過失操作	内部関係者（社員や協力者の内、当該機器へのアクセス権を有する者）の過失操作を誘発し、攻撃を実行する。 機器に対して、正規の媒体・機器を接続した結果、攻撃に相当する行為が実行される。	URLフィルタリング／Webレピュテーション								
									メールフィルタリング								1
5			**3**	**3**		**A**	不正媒体・機器接続	機器に対して、不正に持ち込んだ媒体・機器（CD/DVDやUSB機器等）を接続し、攻撃を実行する。	デバイス接続・利用制限		（同左）		（同左）				1
6			**3**	**3**		**A**	プロセス不正実行	攻撃対象機器上に存在する正規のプログラムやコマンド、サービス等のプロセスを、不正に実行する。	権限管理		（同左）		機器異常検知				1
									アクセス制御		（同左）		機器死活監視				
									ホワイトリストによるプロセスの起動制限		（同左）		ログ収集・分析				
									重要操作の承認		（同左）		統合ログ管理システム				
7			**3**	**3**		**A**	マルウェア感染	攻撃対象機器にマルウェア（不正プログラム）を感染・動作させる。	アンチウイルス				機器異常検知				1
									ホワイトリストによるプロセスの起動制限				機器死活監視				
									パッチ適用				ログ収集・分析				
									脆弱性回避				統合ログ管理システム				
									データ署名								
8			**3**	**3**		**A**	情報窃取	機器内に格納されている情報（ソフトウェア、認証情報、構成設定情報、暗号鍵等の機密情報）を窃取する。	権限管理		（同左）		ログ収集・分析				1
									アクセス制御		（同左）		統合ログ管理システム				
									データ暗号化		（同左）						
									DLP		（同左）						
9			**3**	**3**		**A**	情報改ざん	機器内に格納されている情報（ソフトウェア、認証情報、構成設定情報、暗号鍵等の機密情報）を改ざんする。	権限管理		（同左）		機器異常検知		データバックアップ		1
									アクセス制御		（同左）		ログ収集・分析				
									データ署名		（同左）		統合ログ管理システム				
10			**3**	**3**		**A**	情報破壊	機器内に格納されている情報（ソフトウェア、認証情報、構成設定情報、暗号鍵等の機密情報）を破壊する。			権限管理		機器異常検知		データバックアップ		1
											アクセス制御		ログ収集・分析				
													統合ログ管理システム				
11			**3**	**3**	**3**	**A**	不正送信	他の機器に対して、不正な制御コマンド（設定値変更、電源断等）や不正なデータを送信する。	セグメント分割／ゾーニング		（同左）		ログ収集・分析				1
									データ署名		（同左）		統合ログ管理システム				
									重要操作の承認		（同左）						
12			**3**	**3**		**A**	機能停止	機器の機能を停止する。					機器異常検知		冗長化		1
													機器死活監視		フェールセーフ設計		
													ログ収集・分析				
													統合ログ管理システム				
13			**1**	**3**		**B**	高負荷攻撃	DDoS攻撃等によって、機器の処理能力以上の処理を要求し、機器の正常動作を妨害する。	DDoS対策				機器異常検知		冗長化		1
													機器死活監視		フェールセーフ設計		
													ログ収集・分析				
													統合ログ管理システム				
14			**2**	**2**		**B**	窃盗	機器を窃盗する。	施錠管理	○	（同左）		（同左）				2
15			**2**	**2**		**B**	盗難・廃棄時の分解による情報窃取	盗難にあった機器や廃棄した機器が分解され、機器内部に保存されていた情報（ソフトウェア、認証情報、構成設定情報、暗号鍵等の機密情報）が窃取される。	耐タンパー		（同左）						2
									難読化		（同左）						
									セキュア消去	○	（同左）						
16							経路遮断	通信ケーブルを切断し、通信を遮断する。あるいは、機器から通信ケーブルを引き抜き、通信を遮断する。	入退管理				機器異常検知		冗長化		
									施錠管理				機器死活監視				
													ログ収集・分析				
													統合ログ管理システム				
													監視カメラ				
													侵入センサ				
17							通信輻輳	容量以上の通信トラフィックを発生させ、輻輳状態とする。	FW（パケットフィルタリング型）				機器異常検知		冗長化		
									FW（アプリケーションゲートウェイ型）				機器死活監視				
									WAF				ログ収集・分析				
									IPS／IDS				統合ログ管理システム				
									DDoS対策								
18	対象外（機能なし）						無線妨害	無線通信を妨害する。					機器異常検知		冗長化		
													機器死活監視				
													ログ収集・分析				
													統合ログ管理システム				
19							盗聴	ネットワーク上を流れる情報を盗聴する。	通信路暗号化								
									データ暗号化								
									専用線								
20							通信データ改ざん	ネットワーク上を流れる情報を改ざんする。	通信路暗号化				ログ収集・分析				
									データ署名				統合ログ管理システム				
									専用線								
21							不正機器接続	ネットワーク上に不正機器を接続する。	デバイス接続・利用制限				デバイス接続・利用制限				
													ログ収集・分析				
													統合ログ管理システム				

表 3-6 資産ベースのリスク分析シート

凡例: ○ 対策実施　グレーアウト行：該当資産で考慮しない脅威　　対策の緑字：　対策の補足情報

項番	資産種別	対象装置	評価指標				脅威(攻撃手法)	説明	対策								対策レベル
									防御				検知/被害把握		事業継続		
			脅威レベル	脆弱性レベル	資産の重要度	リスク値			侵入/拡散段階		目的遂行段階						脅威毎
1	ネットワーク資産	**制御ネットワーク(フィールド側)**					不正アクセス	ネットワーク経由で機器に侵入し、攻撃を実行する。	FW(パケットフィルタリング型) FW(アプリケーションゲートウェイ型) 一方向ゲートウェイ プロキシサーバ WAF 通信相手の認証 IPS／IDS パッチ適用 脆弱性回避				IPS／IDS ログ収集・分析 統合ログ管理システム				
2							物理的侵入	入室が制限された区画・領域(機器が設置された場所等)に不正侵入する。あるいは、物理的アクセスが制限された機器(ラックや箱内に設置された機器等)の制限を解除する。	入退管理 施錠管理				監視カメラ 侵入センサ				
3							不正操作	機器のコンソール等の直接操作で侵入し、攻撃を実行する。	操作者認証								
4							過失操作	内部関係者(社員や協力者の内、当該機器へのアクセス権を有する者)の過失操作を誘発し、攻撃を実行する。 機器に対して、正規の媒体・機器を接続した結果、攻撃に相当する行為が実行される。	URLフィルタリング／Webレピュテーション メールフィルタリング								
5							不正媒体・機器接続	機器に対して、不正に持ち込んだ媒体・機器(CD/DVDやUSB機器等)を接続し、攻撃を実行する。	デバイス接続・利用制限		(同左)		デバイス接続・利用制限 ログ収集・分析 統合ログ管理システム				
6							プロセス不正実行	攻撃対象機器上に存在する正規のプログラムやコマンド、サービス等のプロセスを、不正に実行する。	権限管理 アクセス制御 ホワイトリストによるプロセスの起動制限 重要操作の承認		(同左) (同左) (同左) (同左)		機器異常検知 機器死活監視 ログ収集・分析 統合ログ管理システム				
7							マルウェア感染	攻撃対象機器にマルウェア(不正プログラム)を感染・動作させる。	アンチウイルス ホワイトリストによるプロセスの起動制限 パッチ適用 脆弱性回避 データ署名				機器異常検知 機器死活監視 ログ収集・分析 統合ログ管理システム				
8							情報窃取	機器内に格納されている情報(ソフトウェア、認証情報、構成設定情報、暗号鍵等の機密情報)を窃取する。	権限管理 アクセス制御 データ暗号化 DLP		(同左) (同左) (同左) (同左)		ログ収集・分析 統合ログ管理システム				
9							情報改ざん	機器内に格納されている情報(ソフトウェア、認証情報、構成設定情報、暗号鍵等の機密情報)を改ざんする。	権限管理 アクセス制御 データ署名		(同左) (同左) (同左)		機器異常検知 ログ収集・分析 統合ログ管理システム		データバックアップ		
10							情報破壊	機器内に格納されている情報(ソフトウェア、認証情報、構成設定情報、暗号鍵等の機密情報)を破壊する。			権限管理 アクセス制御		機器異常検知 ログ収集・分析 統合ログ管理システム		データバックアップ		
11					3		不正送信	他の機器に対して、不正な制御コマンド(設定値変更、電源断等)や不正なデータを送信する。	セグメント分割／ゾーニング データ署名 重要操作の承認		(同左) (同左) (同左)		ログ収集・分析 統合ログ管理システム				
12							機能停止	機器の機能を停止する。					機器異常検知 機器死活監視 ログ収集・分析 統合ログ管理システム		冗長化 フェールセーフ設計		
13							高負荷攻撃	DDoS攻撃等によって、機器の処理能力以上の処理を要求し、機器の正常動作を妨害する。	DDoS対策				機器異常検知 機器死活監視 ログ収集・分析 統合ログ管理システム		冗長化 フェールセーフ設計		
14							窃盗	機器を窃盗する。	施錠管理	○	(同左)		(同左)				
15							盗難・廃棄時の分解による情報窃取	盗難にあった機器や廃棄した機器が分解され、機器内部に保存されていた情報(ソフトウェア、認証情報、構成設定情報、暗号鍵等の機密情報)が窃取される。	耐タンパー 難読化 セキュア消去		(同左) (同左) (同左)						
16			**3**	**2**		**A**	経路遮断	通信ケーブルを切断し、通信を遮断する。あるいは、機器から通信ケーブルを引き抜き、通信を遮断する。	入退管理 (ICカード、生体認証) 施錠管理	○ ○			機器異常検知 機器死活監視 ログ収集・分析 統合ログ管理システム 監視カメラ 侵入センサ		冗長化		2
17			**2**	**3**		**A**	通信輻輳	容量以上の通信トラフィックを発生させ、輻輳状態とする。	FW(パケットフィルタリング型) FW(アプリケーションゲートウェイ型) WAF IPS／IDS DDoS対策				機器異常検知 機器死活監視 ログ収集・分析 統合ログ管理システム		冗長化		1
18	対象外(機能なし)						無線妨害	無線通信を妨害する。					機器異常検知 機器死活監視 ログ収集・分析 統合ログ管理システム		冗長化		
19			**2**	**3**		**A**	盗聴	ネットワーク上を流れる情報を盗聴する。	通信路暗号化 データ暗号化 専用線								1
20			**2**	**3**		**A**	通信データ改ざん	ネットワーク上を流れる情報を改ざんする。	通信路暗号化 データ署名 専用線				ログ収集・分析 統合ログ管理システム				1
21			**2**	**3**		**A**	不正機器接続	ネットワーク上に不正機器を接続する。	デバイス接続・利用制限				デバイス接続・利用制限 ログ収集・分析 統合ログ管理システム				1

表 3-6 資産ベースのリスク分析シート

凡例: ○ 対策実施　グレーアウト行：該当資産で考慮しない脅威　　対策の緑字：　対策の補足情報

項番	資産種別	対象装置	評価指標				脅威(攻撃手法)	説明	対策								対策レベル
									防御				検知/被害把握		事業継続		
			脅威レベル	脆弱性レベル	資産の重要度	リスク値			侵入/拡散段階		目的遂行段階						脅威毎
1	ネットワーク資産	**フィールドネットワーク**					不正アクセス	ネットワーク経由で機器に侵入し、攻撃を実行する。	FW（パケットフィルタリング型） FW（アプリケーションゲートウェイ型） 一方向ゲートウェイ プロキシサーバ WAF 通信相手の認証 IPS／IDS パッチ適用 脆弱性回避				IPS／IDS ログ収集・分析 統合ログ管理システム				
2							物理的侵入	入室が制限された区画・領域（機器が設置された場所等）に不正侵入する。あるいは、物理的アクセスが制限された機器（ラックや箱内に設置された機器等）の制限を解除する。	入退管理 施錠管理				監視カメラ 侵入センサ				
3							不正操作	機器のコンソール等の直接操作で侵入し、攻撃を実行する。	操作者認証								
4							過失操作	内部関係者（社員や協力者の内、当該機器へのアクセス権を有する者）の過失操作を誘発し、攻撃を実行する。 機器に対して、正規の媒体・機器を接続した結果、攻撃に相当する行為が実行される。	URLフィルタリング／Webレピュテーション メールフィルタリング								
5							不正媒体・機器接続	機器に対して、不正に持ち込んだ媒体・機器（CD/DVDやUSB機器等）を接続し、攻撃を実行する。	デバイス接続・利用制限		（同左）		デバイス接続・利用制限 ログ収集・分析 統合ログ管理システム				
6							プロセス不正実行	攻撃対象機器上に存在する正規のプログラムやコマンド、サービス等のプロセスを、不正に実行する。	権限管理 アクセス制御 ホワイトリストによるプロセスの起動制限 重要操作の承認		（同左） （同左） （同左） （同左）		機器異常検知 機器死活監視 ログ収集・分析 統合ログ管理システム				
7							マルウェア感染	攻撃対象機器にマルウェア（不正プログラム）を感染・動作させる。	アンチウイルス ホワイトリストによるプロセスの起動制限 パッチ適用 脆弱性回避 データ署名				機器異常検知 機器死活監視 ログ収集・分析 統合ログ管理システム				
8							情報窃取	機器内に格納されている情報（ソフトウェア、認証情報、構成設定情報、暗号鍵等の機密情報）を窃取する。	権限管理 アクセス制御 データ暗号化 DLP		（同左） （同左） （同左） （同左）		ログ収集・分析 統合ログ管理システム				
9							情報改ざん	機器内に格納されている情報（ソフトウェア、認証情報、構成設定情報、暗号鍵等の機密情報）を改ざんする。	権限管理 アクセス制御 データ署名		（同左） （同左） （同左）		機器異常検知 ログ収集・分析 統合ログ管理システム		データバックアップ		
10							情報破壊	機器内に格納されている情報（ソフトウェア、認証情報、構成設定情報、暗号鍵等の機密情報）を破壊する。			権限管理 アクセス制御		機器異常検知 ログ収集・分析 統合ログ管理システム		データバックアップ		
11					3		不正送信	他の機器に対して、不正な制御コマンド（設定値変更、電源断等）や不正なデータを送信する。	セグメント分割／ゾーニング データ署名 重要操作の承認		（同左） （同左） （同左）		ログ収集・分析 統合ログ管理システム				
12							機能停止	機器の機能を停止する。					機器異常検知 機器死活監視 ログ収集・分析 統合ログ管理システム		冗長化 フェールセーフ設計		
13							高負荷攻撃	DDoS攻撃等によって、機器の処理能力以上の処理を要求し、機器の正常動作を妨害する。	DDoS対策				機器異常検知 機器死活監視 ログ収集・分析 統合ログ管理システム		冗長化 フェールセーフ設計		
14							窃盗	機器を窃盗する。	施錠管理		（同左）		（同左）				
15							盗難・廃棄時の分解による情報窃取	盗難にあった機器や廃棄した機器が分解され、機器内部に保存されていた情報（ソフトウェア、認証情報、構成設定情報、暗号鍵等の機密情報）が窃取される。	耐タンパー 難読化 セキュア消去		（同左） （同左） （同左）						
16			**3**	**2**		**A**	経路遮断	通信ケーブルを切断し、通信を遮断する。あるいは、機器から通信ケーブルを引き抜き、通信を遮断する。	入退管理（敷地内のみ） 施錠管理	○ ○			機器異常検知 機器死活監視 ログ収集・分析 統合ログ管理システム 監視カメラ 侵入センサ		冗長化		2
17			**2**	**3**		**A**	通信輻輳	容量以上の通信トラフィックを発生させ、輻輳状態とする。	FW（パケットフィルタリング型） FW（アプリケーションゲートウェイ型） WAF IPS／IDS DDoS対策				機器異常検知 機器死活監視 ログ収集・分析 統合ログ管理システム		冗長化		1
18	対象外（機能なし）						無線妨害	無線通信を妨害する。					機器異常検知 機器死活監視 ログ収集・分析 統合ログ管理システム		冗長化		
19			**2**	**3**		**A**	盗聴	ネットワーク上を流れる情報を盗聴する。	通信路暗号化 データ暗号化 専用線								1
20			**2**	**3**		**A**	通信データ改ざん	ネットワーク上を流れる情報を改ざんする。	通信路暗号化 データ署名 専用線				ログ収集・分析 統合ログ管理システム				1
21			**2**	**3**		**A**	不正機器接続	ネットワーク上に不正機器を接続する。	デバイス接続・利用制限				デバイス接続・利用制限 ログ収集・分析 統合ログ管理システム				1

表 3-6 資産ベースのリスク分析シート

凡例: ○ 対策実施　グレーアウト行：該当資産で考慮しない脅威　　対策の緑字：　対策の補足情報

項番	資産種別	対象装置	評価指標				脅威(攻撃手法)	説明	対策								対策レベル
									防御				検知/被害把握		事業継続		
			脅威レベル	脆弱性レベル	資産の重要度	リスク値			侵入/拡散段階		目的遂行段階						脅威毎
1	制御系資産	**コントローラ コントローラ(マスター)**	**2**	**3**		**A**	不正アクセス	ネットワーク経由で機器に侵入し、攻撃を実行する。	FW(パケットフィルタリング型) FW(アプリケーションゲートウェイ型) 一方向ゲートウェイ プロキシサーバ WAF 通信相手の認証 IPS／IDS パッチ適用 脆弱性回避				IPS／IDS ログ収集・分析 統合ログ管理システム				1
2			**2**	**2**		**B**	物理的侵入	入室が制限された区画・領域(機器が設置された場所等)に不正侵入する。あるいは、物理的アクセスが制限された機器(ラックや箱内に設置された機器等)の制限を解除する。	入退管理　(ICカード) 施錠管理	○ ○			監視カメラ 侵入センサ	○ ○			2
3			**2**	**2**		**B**	不正操作	機器のコンソール等の直接操作で侵入し、攻撃を実行する。	操作者認証 (ID/Pass)	○							2
4			**2**	**3**		**A**	過失操作	内部関係者(社員や協力者の内、当該機器へのアクセス権を有する者)の過失操作を誘発し、攻撃を実行する。 機器に対して、正規の媒体・機器を接続した結果、攻撃に相当する行為が実行される。	URLフィルタリング／Webレピュテーション メールフィルタリング								1
5			**2**	**3**		**A**	不正媒体・機器接続	機器に対して、不正に持ち込んだ媒体・機器(CD/DVDやUSB機器等)を接続し、攻撃を実行する。	デバイス接続・利用制限		(同左)		(同左) ログ収集・分析 統合ログ管理システム				1
6			**2**	**3**		**A**	プロセス不正実行	攻撃対象機器上に存在する正規のプログラムやコマンド、サービス等のプロセスを、不正に実行する。	権限管理 アクセス制御 ホワイトリストによるプロセスの起動制限 重要操作の承認		(同左) (同左) (同左) (同左)		機器異常検知 機器死活監視 ログ収集・分析 統合ログ管理システム				1
7			**1**	**3**		**B**	マルウェア感染	攻撃対象機器にマルウェア(不正プログラム)を感染・動作させる。	アンチウイルス ホワイトリストによるプロセスの起動制限 パッチ適用 脆弱性回避 データ署名				機器異常検知 機器死活監視 ログ収集・分析 統合ログ管理システム				1
8			**3**	**3**		**A**	情報窃取	機器内に格納されている情報(ソフトウェア、認証情報、構成設定情報、暗号鍵等の機密情報)を窃取する。	権限管理 アクセス制御 データ暗号化 DLP		(同左) (同左) (同左) (同左)		ログ収集・分析 統合ログ管理システム				1
9			**3**	**3**		**A**	情報改ざん	機器内に格納されている情報(ソフトウェア、認証情報、構成設定情報、暗号鍵等の機密情報)を改ざんする。	権限管理 アクセス制御 データ署名		(同左) (同左) (同左)		機器異常検知 ログ収集・分析 統合ログ管理システム		データバックアップ		1
10			**3**	**3**		**A**	情報破壊	機器内に格納されている情報(ソフトウェア、認証情報、構成設定情報、暗号鍵等の機密情報)を破壊する。			権限管理 アクセス制御		機器異常検知 ログ収集・分析 統合ログ管理システム		データバックアップ		1
11			**3**	**3**	**3**	**A**	不正送信	他の機器に対して、不正な制御コマンド(設定値変更、電源断等)や不正なデータを送信する。	セグメント分割／ゾーニング データ署名 重要操作の承認		(同左) (同左) (同左)		ログ収集・分析 統合ログ管理システム				1
12			**2**	**3**		**A**	機能停止	機器の機能を停止する。					機器異常検知 機器死活監視 ログ収集・分析 統合ログ管理システム		冗長化 フェールセーフ設計		1
13			**3**	**3**		**A**	高負荷攻撃	DDoS攻撃等によって、機器の処理能力以上の処理を要求し、機器の正常動作を妨害する。	DDoS対策				機器異常検知 機器死活監視 ログ収集・分析 統合ログ管理システム		冗長化 フェールセーフ設計		1
14			**2**	**2**		**B**	窃盗	機器を窃盗する。	施錠管理	○	(同左)		(同左)				2
15			**2**	**2**		**B**	盗難・廃棄時の分解による情報窃取	盗難にあった機器や廃棄した機器が分解され、機器内部に保存されていた情報(ソフトウェア、認証情報、構成設定情報、暗号鍵等の機密情報)が窃取される。	耐タンパー 難読化 セキュア消去		(同左) (同左) (同左)						2
16							経路遮断	通信ケーブルを切断し、通信を遮断する。あるいは、機器から通信ケーブルを引き抜き、通信を遮断する。	入退管理 施錠管理				機器異常検知 機器死活監視 ログ収集・分析 統合ログ管理システム 監視カメラ 侵入センサ		冗長化		
17							通信輻輳	容量以上の通信トラフィックを発生させ、輻輳状態とする。	FW(パケットフィルタリング型) FW(アプリケーションゲートウェイ型) WAF IPS／IDS DDoS対策				機器異常検知 機器死活監視 ログ収集・分析 統合ログ管理システム		冗長化		
18	対象外(機能なし)						無線妨害	無線通信を妨害する。					機器異常検知 機器死活監視 ログ収集・分析 統合ログ管理システム		冗長化		
19							盗聴	ネットワーク上を流れる情報を盗聴する。	通信路暗号化 データ暗号化 専用線								
20							通信データ改ざん	ネットワーク上を流れる情報を改ざんする。	通信路暗号化 データ署名 専用線				ログ収集・分析 統合ログ管理システム				
21							不正機器接続	ネットワーク上に不正機器を接続する。	デバイス接続・利用制限				デバイス接続・利用制限 ログ収集・分析 統合ログ管理システム				

表 3-6 資産ベースのリスク分析シート

凡例: ○ 対策実施　グレーアウト行：該当資産で考慮しない脅威　　対策の緑字：　対策の補足情報

項番	資産種別	対象装置	評価指標				脅威(攻撃手法)	説明	対策								対策レベル
									防御				検知/被害把握		事業継続		
			脅威レベル	脆弱性レベル	資産の重要度	リスク値			侵入/拡散段階		目的遂行段階						脅威毎
1	制御系資産	**コントローラ(スレーブ)**	**2**	**3**		**A**	不正アクセス	ネットワーク経由で機器に侵入し、攻撃を実行する。	FW（パケットフィルタリング型）				IPS／IDS				
									FW（アプリケーションゲートウェイ型）				ログ収集・分析				
									一方向ゲートウェイ				統合ログ管理システム				
									プロキシサーバ								
									WAF								
									通信相手の認証								1
									IPS／IDS								
									パッチ適用								
									脆弱性回避								
2			**3**	**2**		**A**	物理的侵入	入室が制限された区画・領域（機器が設置された場所等）に不正侵入する。あるいは、物理的アクセスが制限された機器（ラックや箱内に設置された機器等）の制限を解除する。	入退管理				監視カメラ				2
3			**3**	**2**		**A**	不正操作	機器のコンソール等の直接操作で侵入し、攻撃を実行する。	施錠管理	○			侵入センサ				2
									操作者認証（ID/Pass）	○							
4			**2**	**3**		**A**	過失操作	内部関係者（社員や協力者の内、当該機器へのアクセス権を有する者）の過失操作を誘発し、攻撃を実行する。 機器に対して、正規の媒体・機器を接続した結果、攻撃に相当する行為が実行される。	URLフィルタリング／Webレピュテーション								1
									メールフィルタリング								
5			**2**	**3**		**A**	不正媒体・機器接続	機器に対して、不正に持ち込んだ媒体・機器（CD/DVDやUSB機器等）を接続し、攻撃を実行する。	デバイス接続・利用制限		(同左)		(同左)				1
													ログ収集・分析				
													統合ログ管理システム				
6			**2**	**3**		**A**	プロセス不正実行	攻撃対象機器上に存在する正規のプログラムやコマンド、サービス等のプロセスを、不正に実行する。	権限管理		(同左)		機器異常検知				1
									アクセス制御		(同左)		機器死活監視				
									ホワイトリストによるプロセスの起動制限		(同左)		ログ収集・分析				
									重要操作の承認		(同左)		統合ログ管理システム				
7			**1**	**3**		**B**	マルウェア感染	攻撃対象機器にマルウェア（不正プログラム）を感染・動作させる。	アンチウイルス				機器異常検知				1
									ホワイトリストによるプロセスの起動制限				機器死活監視				
									パッチ適用				ログ収集・分析				
									脆弱性回避				統合ログ管理システム				
									データ署名								
8			**3**	**3**		**A**	情報窃取	機器内に格納されている情報（ソフトウェア、認証情報、構成設定情報、暗号鍵等の機密情報）を窃取する。	権限管理		(同左)		ログ収集・分析				1
									アクセス制御		(同左)		統合ログ管理システム				
									データ暗号化		(同左)						
									DLP		(同左)						
9			**3**	**3**		**A**	情報改ざん	機器内に格納されている情報（ソフトウェア、認証情報、構成設定情報、暗号鍵等の機密情報）を改ざんする。	権限管理		(同左)		機器異常検知		データバックアップ		1
									アクセス制御		(同左)		ログ収集・分析				
									データ署名		(同左)		統合ログ管理システム				
10			**3**	**3**		**A**	情報破壊	機器内に格納されている情報（ソフトウェア、認証情報、構成設定情報、暗号鍵等の機密情報）を破壊する。			権限管理		機器異常検知		データバックアップ		1
											アクセス制御		ログ収集・分析				
													統合ログ管理システム				
11			**3**	**3**	**3**	**A**	不正送信	他の機器に対して、不正な制御コマンド（設定値変更、電源断等）や不正なデータを送信する。	セグメント分割／ゾーニング		(同左)		ログ収集・分析				1
									データ署名		(同左)		統合ログ管理システム				
									重要操作の承認		(同左)						
12			**3**	**3**		**A**	機能停止	機器の機能を停止する。					機器異常検知		冗長化	○	1
													機器死活監視		フェールセーフ設計	○	
													ログ収集・分析				
													統合ログ管理システム				
13			**3**	**3**		**A**	高負荷攻撃	DDoS攻撃等によって、機器の処理能力以上の処理を要求し、機器の正常動作を妨害する。	DDoS対策				機器異常検知		冗長化	○	1
													機器死活監視		フェールセーフ設計	○	
													ログ収集・分析				
													統合ログ管理システム				
14			**3**	**2**		**A**	窃盗	機器を窃盗する。	施錠管理	○	(同左)		(同左)				2
15			**3**	**2**		**A**	盗難・廃棄時の分解による情報窃取	盗難にあった機器や廃棄した機器が分解され、機器内部に保存されていた情報（ソフトウェア、認証情報、構成設定情報、暗号鍵等の機密情報）が窃取される。	耐タンパー		(同左)						2
									難読化		(同左)						
									セキュア消去	○	(同左)						
16							経路遮断	通信ケーブルを切断し、通信を遮断する。あるいは、機器から通信ケーブルを引き抜き、通信を遮断する。	入退管理				機器異常検知		冗長化		
									施錠管理				機器死活監視				
													ログ収集・分析				
													統合ログ管理システム				
													監視カメラ				
													侵入センサ				
17							通信輻輳	容量以上の通信トラフィックを発生させ、輻輳状態とする。	FW（パケットフィルタリング型）				機器異常検知		冗長化		
									FW（アプリケーションゲートウェイ型）				機器死活監視				
									WAF				ログ収集・分析				
									IPS／IDS				統合ログ管理システム				
									DDoS対策								
18	対象外（機能なし）						無線妨害	無線通信を妨害する。					機器異常検知		冗長化		
													機器死活監視				
													ログ収集・分析				
													統合ログ管理システム				
19							盗聴	ネットワーク上を流れる情報を盗聴する。	通信路暗号化								
									データ暗号化								
									専用線								
20							通信データ改ざん	ネットワーク上を流れる情報を改ざんする。	通信路暗号化				ログ収集・分析				
									データ署名				統合ログ管理システム				
									専用線								
21							不正機器接続	ネットワーク上に不正機器を接続する。	デバイス接続・利用制限				デバイス接続・利用制限				
													ログ収集・分析				
													統合ログ管理システム				

このページは空白です。

3.3. リスク値のまとめ

【作業 3.3①】脆弱性レベルのまとめ表を作成すること。

- 資産と脅威の種類の組み合わせにおける、脆弱性レベルの分布の把握や見直しができる。

【アウトプット 3.3①】

脆弱性レベルのまとめ表を以下に示す（表 3-7）。

表 3-7 資産ベースのリスク分析 脆弱性レベルまとめ表

脅威＼資産	監視端末	ファイアウォール	DMZ	データヒストリアン（中継）	データヒストリアン	制御NW(情)	EWS	制御サーバ	HMI(操作端末)	制御NW(フ)	フィールドネットワーク	コントローラ（マスター）	コントローラ（スレーブ）
不正アクセス	2	2	2	2	2	2	2	2	2			3	3
物理的侵入	2	1	1	1	1	2	1	1	2			2	2
不正操作	2	2	2	2	2	2	2	2	3			2	2
過失操作	2	3	3	3	3	3	3	3	3			3	3
不正媒体・機器接続	2	3	3	3	3	3	3	3	3			3	3
プロセス不正実行	3	2	2	2	2	2	3	2	3			3	3
マルウェア感染	2	3	3	2	2	3	3	2	3			3	3
情報窃取	3	2	2	2	2	2	3	2	3			3	3
情報改ざん	3	2	2	2	2	2	3	2	3			3	3
情報破壊	3	2	2	2	2	2	3	2	3			3	3
不正送信	3	3	3	3	3	3	3	3	3			3	3
機能停止	3	3	3	3	3	3	3	3	3			3	3
高負荷攻撃 DDOS	3	3	3	3	3	3	3	3	3			3	3
窃盗	2	2	2	2	2	2	2	2	2			2	2
盗難・廃棄時	2	2	2	2	2	2	2	2	2			2	2
経路遮断			1			2				2	2		
通信輻輳			3			3				3	3		
無線妨害													
盗聴			3			3				3	3		
通信データ改ざん			3			3				3	3		
不正機器接続			3			3				3	3		

【作業 3.3②】リスク値まとめ表を作成すること。

【アウトプット 3.3②】

リスク値のまとめ表を以下に示す（表 3-8）。

表 3-8 資産ベースのリスク分析 リスク値まとめ表

脅威＼資産	監視端末	ファイアウォール	DMZ	データヒストリアン（中継）	データヒストリアン	制御NW(情)	EWS	制御サーバ	HMI(操作端末)	制御NW(フ)	フィールドネットワーク	コントローラ（マスター）	コントローラ（スレーブ）
不正アクセス	D	A	B	B	C	C	B	B	B			A	A
物理的侵入	D	C	D	D	D	D	C	C	B			B	A
不正操作	D	B	C	C	C	C	B	B	A			B	A
過失操作	D	A	B	B	B	B	A	A	A			A	A
不正媒体・機器接続	D	A	B	B	B	B	A	A	A			A	A
プロセス不正実行	C	B	C	C	C	D	A	A	A			A	A
マルウェア感染	D	B	C	B	B	C	A	A	A			B	B
情報窃取	C	C	D	B	B	D	A	A	A			A	A
情報改ざん	D	A	B	B	B	C	A	A	A			A	A
情報破壊	D	B	C	B	B	C	A	A	A			A	A
不正送信	D	B	C	B	B	C	A	A	A			A	A
機能停止	D	A	B	B	B	B	A	A	A			A	A
高負荷攻撃　DDOS	E	A	B	C	C	B	B	B	B			A	A
窃盗	D	C	D	D	D	D	B	C	B			B	A
盗難・廃棄時	D	C	D	D	D	D	B	C	B			B	A
経路遮断			D			C				A	A		
通信輻輳			B			B				A	A		
無線妨害													
盗聴			B			B				A	A		
通信データ改ざん			B			B				A	A		
不正機器接続			B			B				A	A		

4. 事業被害ベースのリスク分析

事業被害ベースのリスク分析では、事前準備で作成した下記のアウトプットを利用して、リスク分析作業を実施する。

表 4-1 利用する事前準備のアウトプット

別冊見出し	事前準備のアウトプット	ガイド本体
2.1.	資産一覧	*3.1.5. 表 3-9*
2.2.	システム構成図	*3.2.3. 図 3-8*
2.3.①	データフローマトリクス	*3.3.1. 表 3-10*
2.3.②	データフロー図	*3.3.2. 図 3-14*
2.6.	事業被害レベルの判断基準	*4.3.2. 表 4-11*
2.7.	事業被害及び各事業被害に対する事業被害レベル一覧	*4.3.3. 表 4-12*
2.8.	脅威レベルの判断基準	*4.4.5. 表 4-20～表 4-24*

事業被害ベースのリスク分析作業で新たに作成するアウトプット一覧を下記に示す。

表 4-2 事業被害ベースのリスク分析作業で作成するアウトプット

別冊見出し	資産ベース アウトプット	ガイド本体
4.1.	攻撃シナリオ一覧	*6.2.2. 表 6-6*
4.2.	攻撃ルート一覧	*6.5.1. 表 6-11～表 6-12*
4.3.	攻撃ルート図	*6.5.1. 図 6-9*
4.4.	事業被害ベースのリスク分析シート	*6.6.4.~ 6.11.*
4.5.	リスク値まとめ	*6.11.3.*

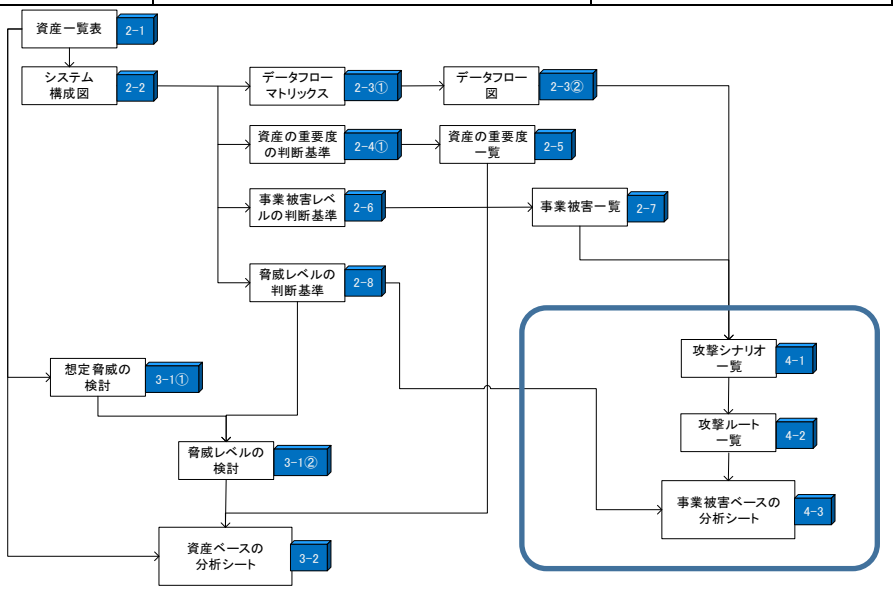


図 4-1 事業被害ベースのリスク分析作業の流れ

4.1. 攻撃シナリオ一覧の作成

ここでは、2.7 節で作成した「表 2-8 事業被害の一覧表」を基に、具体的な攻撃シナリオを作成する。

【作業 4.1①】当該事業被害の原因となるサイバー攻撃（攻撃シナリオの概要）を検討すること。
【作業 4.1②】攻撃シナリオの攻撃対象を列挙すること。
【作業 4.1③】攻撃シナリオの攻撃拠点を列挙すること。

- 2.3 節で作成したデータフローマトリクスを参照し、攻撃対象とデータフローが発生している攻撃拠点を必ず含めること。

【作業 4.1④】攻撃シナリオの具体的な攻撃手法を記載すること。

表 4-3 攻撃シナリオフォーマット

#	事業被害	事業被害の概要、攻撃シナリオ				事業被害レベル
1	広域でのエネルギー供給停止	供給設備へのサイバー攻撃により、正規の供給停止機能を悪用され、広域でエネルギーの供給が停止し、社会に多大な影響を及ぼし、当社への信頼が大きく低下する。				3
		1-1	① 広域供給停止操作の実行により、広域で供給が停止する。			
			攻撃拠点	攻撃対象	最終攻撃	
			③ HMI	② コントローラ	④ 広域供給停止操作を実行する。	

【アウトプット 4.1】

攻撃シナリオ一覧を以下に示す(表 4-4)。表中の注釈*1～*5 については次頁参照。

表 4-4 攻撃シナリオ一覧表

項番	事業被害	事業被害の概要と攻撃シナリオ (*1)					事業被害レベル
1	広域での燃料供給停止	供給設備へのサイバー攻撃により、正規の供給停止機能を悪用され、広域で燃料の供給が停止し、社会に多大な影響を及ぼし、当社への信頼が大きく低下する。					3 (*2)
		シナリオ#	攻撃シナリオ	攻撃拠点	攻撃対象	最終攻撃	
		1-1	広域供給停止操作の実行により、広域で供給が停止する。	HMI	コントローラ	広域供給停止操作を実行する。	
		1-2	複数コントローラへの供給停止コマンドの送信により、広域で供給が停止する。	コントローラ(マスター)	コントローラ(スレーブ)	供給停止コマンドを不正送信する。	
2	火災・爆発事故の発生	製造設備へのサイバー攻撃により、危険物取扱い設備の制御異常や操作監視不能が発生し、火災・爆発等が発生する。近隣住民や環境に影響を及ぼし、賠償費用等の損失が発生するとともに、当社への信頼が大きく低下する。 (*3)					3
		項番	攻撃シナリオ	攻撃拠点	攻撃対象	最終攻撃	
		2-1	適切でない目標値の入力により、危険物取扱い設備の制御が異常となり、火災・爆発等が発生する。	HMI	コントローラ	コントローラに不適切な目標値を設定する。	
				制御サーバ	コントローラ	コントローラに不適切な目標値を設定する。	
		2-2	設定(閾値等)やプログラムの改ざんにより、危険物取扱い設備の制御が異常となり、火災・爆発等が発生する。	EWS	コントローラ	コントローラの設定(閾値等)やプログラムを改ざんする。	
		2-3	データやプログラムの改ざんにより、危険物取扱い設備が異常な動作をするようになり、正しい操作を行っても正しい反応が得られず、火災・爆発等が発生する。	HMI	HMI	HMIのデータやプログラムを改ざんする。	
				制御サーバ	制御サーバ	制御サーバのデータやプログラムを改ざんする。	
		2-4	制御ネットワーク(フィールド側)の輻輳により、危険物取扱い設備が監視操作不能となり、監視制御ができなくなり火災・爆発等が発生する。	制御ネットワーク(フィールド側)接続機器	制御ネットワーク(フィールド側)	ネットワーク設定を改ざんし、通信不能にする。	
						マルウェアに感染させて不正通信を発生させ、通信不能にする。	
3	仕様不良燃料の供給	製造設備へのサイバー攻撃により、品質基準を満たさない燃料が製造・供給され、顧客に多大な迷惑を掛け、賠償費用等の損失が発生するとともに、当社への信頼が大きく低下する。					2 (*4)
		項番	攻撃シナリオ	攻撃拠点	攻撃対象	最終攻撃	
		3-1	適切でない目標値の入力により、製造設備の制御が異常となり、品質基準を満たさない燃料が製造される。	HMI	コントローラ	コントローラに不適切な目標値を設定する。	
				制御サーバ	コントローラ	コントローラに不適切な目標値を設定する。	
		3-2	設定(閾値等)やプログラムの改ざんにより、製造設備の制御が異常となり、品質基準を満たさない燃料が製造される。	EWS	コントローラ	コントローラの設定(閾値等)やプログラムを改ざんする。	
		3-3	データやプログラムの改ざんにより、製造設備が異常な動作をするようになり、品質基準を満たさない燃料が製造される。	HMI	HMI	HMIのデータやプログラムを改ざんする。	
				制御サーバ	制御サーバ	制御サーバのデータやプログラムを改ざんする。	
4	製造停止の発生	製造設備へのサイバー攻撃により、プロセスの制御異常や操作監視不能が発生し、プロセス停止を余儀なくされて製造が停止し、損害が発生する。					1 (*5)
		項番	攻撃シナリオ	攻撃拠点	攻撃対象	最終攻撃	
		4-1	適切でない目標値の入力により、製造設備の制御が異常となり、安全のためプロセスを停止する。	HMI	コントローラ	コントローラに不適切な目標値を設定する。	
				制御サーバ	コントローラ	コントローラに不適切な目標値を設定する。	
		4-2	設定(閾値等)やプログラムの改ざんにより、製造設備の制御が異常となり、安全のためプロセスを停止する。	EWS	コントローラ	コントローラの設定(閾値等)やプログラムを改ざんする。	
		4-3	データやプログラムの改ざんにより、製造設備が異常な動作をするようになり、安全のためプロセスを停止する。	HMI	HMI	HMIのデータやプログラムを改ざんする。	
				制御サーバ	制御サーバ	制御サーバのデータやプログラムを改ざんする。	
		4-4	破壊型マルウェアやランサムウェアへの感染により、製造設備が監視操作不能となり、監視制御ができなくなり安全のためプロセスを停止する。	HMI	HMI	破壊型マルウェアやランサムウェアに感染させ、監視操作を不能にする。	
5	機密情報の漏洩	制御システムへのサイバー攻撃により、製造に関わる企業機密が外部に漏洩し、競合他社との差別化に影響を及ぼし、競争力が低下する。					3
		項番	攻撃シナリオ	攻撃拠点	攻撃対象	最終攻撃	
		5-1	制御システムに保存されている製造に関わる企業機密が窃取され、外部に漏洩する。	EWS	EWS	EWSに保存されている機密情報を窃取する。	
				制御サーバ	制御サーバ	制御サーバに保存されている機密情報を窃取する。	

*1：本例で記載している設備や操作機能等は、説明のために仮定している。

*2：本例では事業被害レベル＝3 としているが、供給停止が実行されても一定時間であれば供給が継続でき、顧客に影響が及ぶ前に供給停止解除（供給再開）が可能な供給構造であれば、「2」や「1」もあり得る。

*3：実際に爆発・火災の発生に至るには、サイバー攻撃以外の要因が絡む可能性がある。

*4：本例では、製造工程へのサイバー攻撃により品質基準を満たさない製品が製造されても、当該ロットの廃棄など被害の自社内での食い止め、検査工程での発見、仮に供給が為されてしまっても引き戻し／回収等の対応等により、
大規模な損失には至らないと仮定し、事業被害レベル＝2 とする。

*5：本例では、監視操作不能（監視制御不能）によって安全のためプロセス停止が行われるため、事業被害レベル＝1 とする。

4.2. 攻撃ルートの作成

ここでは 4.1 で作成した攻撃シナリオ一覧を元に、攻撃ルートを作成する。

【作業 4.2①】攻撃シナリオ 1-1 の攻撃拠点「HMI」への侵入口を列挙すること。

【作業 4.2②】侵入口から攻撃拠点までの経由資産を列挙すること。また、侵入口から攻撃拠点までの攻撃ルートをシステム構成図上に示すこと。

- 2.3 節で作成したデータフローマトリクスを参照し、経由となる資産から攻撃対象・攻撃対象までデータフローがあるものを含めること。

【作業 4.2③】攻撃者を決定すること。

【作業 4.2④】全ての攻撃シナリオについて①～③を実施すること。

表 4-5 攻撃ルート一覧表のフォーマット

攻撃シナリオ	誰が	どこから	どうやって			攻撃拠点	攻撃対象	最終攻撃
	攻撃者	侵入口	経由 1	経由 2	経由 3			
1-1	悪意のある第三者	監視端末	データヒストリアン(中継)	データヒストリアン		HMI	コントローラ	広域供給停止操作を実行する。
1-1	悪意のある第三者	情報 NW	FW			HMI	コントローラ	広域供給停止操作を実行する。
1-1	内部関係者（過失）	HMI（物理的侵入）				HMI	コントローラ	広域供給停止操作を実行する。
1-2	③	①			②	コントローラ（M）	コントローラ（S）	供給停止コマンドを不正送信する。
1-2						コントローラ（M）	コントローラ（S）	供給停止コマンドを不正送信する。
1-2						コントローラ（M）	コントローラ（S）	供給停止コマンドを不正送信する。

このページは空白です。

【アウトプット 4.2】

シナリオ番号でまとめた攻撃ルート一覧表(表 4-6)と、攻撃の侵入口でまとめた攻撃ルート一覧表(表 4-7)の 2 つを示す。

表 4-6 攻撃ルート一覧表(シナリオソート版)

攻撃ツリー番号#	シナリオ番号#	誰が	どこから	どうやって					
		攻撃者	侵入口	経由1	経由2	経由3	攻撃拠点	攻撃対象	最終攻撃
1-1	1-1	悪意のある第三者	情報NW	FW			HMI	コントローラ	広域供給停止操作を実行する。
1-2	1-1	悪意のある第三者	監視端末	データヒストリアン(中継)	データヒストリアン		HMI	コントローラ	広域供給停止操作を実行する。
1-3	1-1	内部関係者(過失)	HMI(物理的侵入)				HMI	コントローラ	広域供給停止操作を実行する。
1-4	1-2	悪意のある第三者	情報NW	FW	EWS		コントローラ(M)	コントローラ(S)	供給停止コマンドを不正送信する。
1-5	1-2	悪意のある第三者	監視端末	データヒストリアン(中継)	データヒストリアン	EWS	コントローラ(M)	コントローラ(S)	供給停止コマンドを不正送信する。
1-6	1-2	内部関係者(過失)	EWS(物理的侵入)				コントローラ(M)	コントローラ(S)	供給停止コマンドを不正送信する。
ツリー#	シナリオ#	攻撃者	侵入口	経由1	経由2	経由3	攻撃拠点	攻撃対象	最終攻撃
2-1	2-1	悪意のある第三者	情報NW	FW			HMI	コントローラ	コントローラに不適切な目標値を設定する。
2-2	2-1	悪意のある第三者	情報NW	FW			制御サーバ	コントローラ	コントローラに不適切な目標値を設定する。
2-3	2-1	悪意のある第三者	監視端末	データヒストリアン(中継)	データヒストリアン		HMI	コントローラ	コントローラに不適切な目標値を設定する。
2-4	2-1	悪意のある第三者	監視端末	データヒストリアン(中継)	データヒストリアン		制御サーバ	コントローラ	コントローラに不適切な目標値を設定する。
2-5	2-1	内部関係者(過失)	HMI(物理的侵入)				HMI	コントローラ	コントローラに不適切な目標値を設定する。
2-6	2-1	内部関係者(過失)	制御サーバ(物理的侵入)				制御サーバ	コントローラ	コントローラに不適切な目標値を設定する。
2-7	2-2	悪意のある第三者	情報NW	FW			EWS	コントローラ	コントローラの設定(閾値等)やプログラムを改ざんする。
2-8	2-2	悪意のある第三者	監視端末	データヒストリアン(中継)	データヒストリアン		EWS	コントローラ	コントローラの設定(閾値等)やプログラムを改ざんする。
2-9	2-2	内部関係者(過失)	EWS(物理的侵入)				EWS	コントローラ	コントローラの設定(閾値等)やプログラムを改ざんする。
2-10	2-3	悪意のある第三者	情報NW	FW			HMI	HMI	HMIのデータやプログラムを改ざんする。
2-11	2-3	悪意のある第三者	情報NW	FW			制御サーバ	制御サーバ	制御サーバのデータやプログラムを改ざんする。
2-12	2-3	悪意のある第三者	監視端末	データヒストリアン(中継)	データヒストリアン		HMI	HMI	HMIのデータやプログラムを改ざんする。
2-13	2-3	悪意のある第三者	監視端末	データヒストリアン(中継)	データヒストリアン		制御サーバ	制御サーバ	制御サーバのデータやプログラムを改ざんする。
2-14	2-3	内部関係者(過失)	HMI(物理的侵入)				HMI	HMI	HMIのデータやプログラムを改ざんする。
2-15	2-3	内部関係者(過失)	制御サーバ(物理的侵入)				制御サーバ	制御サーバ	制御サーバのデータやプログラムを改ざんする。
2-16	2-4	悪意のある第三者	情報NW	FW			HMI	制御NW(フ)	ネットワーク設定を改ざんし、通信不能にする。
2-17	2-4	悪意のある第三者	情報NW	FW			HMI	制御NW(フ)	マルウェアに感染させて不正通信を発生させ、通信不能にする。
2-18	2-4	悪意のある第三者	監視端末	データヒストリアン(中継)	データヒストリアン		HMI	制御NW(フ)	ネットワーク設定を改ざんし、通信不能にする。
2-19	2-4	悪意のある第三者	監視端末	データヒストリアン(中継)	データヒストリアン		HMI	制御NW(フ)	マルウェアに感染させて不正通信を発生させ、通信不能にする。
2-20	2-4	内部関係者(過失)	HMI(物理的侵入)				HMI	制御NW(フ)	ネットワーク設定を改ざんし、通信不能にする。
2-21	2-4	内部関係者(過失)	HMI(物理的侵入)				HMI	制御NW(フ)	マルウェアに感染させて不正通信を発生させ、通信不能にする。
2-22	2-4	内部関係者(過失)	EWS(物理的侵入)				EWS	制御NW(フ)	ネットワーク設定を改ざんし、通信不能にする。
2-23	2-4	内部関係者(過失)	EWS(物理的侵入)				EWS	制御NW(フ)	マルウェアに感染させて不正通信を発生させ、通信不能にする。
ツリー#	シナリオ#	攻撃者	侵入口	経由1	経由2	経由3	攻撃拠点	攻撃対象	最終攻撃
3-1	3-1	悪意のある第三者	情報NW	FW			HMI	コントローラ	コントローラに不適切な目標値を設定する。
3-2	3-1	悪意のある第三者	情報NW	FW			制御サーバ	コントローラ	コントローラに不適切な目標値を設定する。
3-3	3-1	悪意のある第三者	監視端末	データヒストリアン(中継)	データヒストリアン		HMI	コントローラ	コントローラに不適切な目標値を設定する。
3-4	3-1	悪意のある第三者	監視端末	データヒストリアン(中継)	データヒストリアン		制御サーバ	コントローラ	コントローラに不適切な目標値を設定する。
3-5	3-1	内部関係者(過失)	HMI(物理的侵入)				HMI	コントローラ	コントローラに不適切な目標値を設定する。
3-6	3-1	内部関係者(過失)	制御サーバ(物理的侵入)				制御サーバ	コントローラ	コントローラに不適切な目標値を設定する。
3-7	3-2	悪意のある第三者	情報NW	FW			EWS	コントローラ	コントローラの設定(閾値等)やプログラムを改ざんする。
3-8	3-2	悪意のある第三者	監視端末	データヒストリアン(中継)	データヒストリアン		EWS	コントローラ	コントローラの設定(閾値等)やプログラムを改ざんする。
3-9	3-2	内部関係者(過失)	EWS(物理的侵入)				EWS	コントローラ	コントローラの設定(閾値等)やプログラムを改ざんする。
3-10	3-3	悪意のある第三者	情報NW	FW			HMI	HMI	HMIのデータやプログラムを改ざんする。
3-11	3-3	悪意のある第三者	情報NW	FW			制御サーバ	制御サーバ	制御サーバのデータやプログラムを改ざんする。
3-12	3-3	悪意のある第三者	監視端末	データヒストリアン(中継)	データヒストリアン		HMI	HMI	HMIのデータやプログラムを改ざんする。
3-13	3-3	悪意のある第三者	監視端末	データヒストリアン(中継)	データヒストリアン		制御サーバ	制御サーバ	制御サーバのデータやプログラムを改ざんする。
3-14	3-3	内部関係者(過失)	HMI(物理的侵入)				HMI	HMI	HMIのデータやプログラムを改ざんする。
3-15	3-3	内部関係者(過失)	制御サーバ(物理的侵入)				制御サーバ	制御サーバ	制御サーバのデータやプログラムを改ざんする。
ツリー#	シナリオ#	攻撃者	侵入口	経由1	経由2	経由3	攻撃拠点	攻撃対象	最終攻撃
4-1	4-1	悪意のある第三者	情報NW	FW			HMI	コントローラ	コントローラに不適切な目標値を設定する。
4-2	4-1	悪意のある第三者	情報NW	FW			制御サーバ	コントローラ	コントローラに不適切な目標値を設定する。
4-3	4-1	悪意のある第三者	監視端末	データヒストリアン(中継)	データヒストリアン		HMI	コントローラ	コントローラに不適切な目標値を設定する。
4-4	4-1	悪意のある第三者	監視端末	データヒストリアン(中継)	データヒストリアン		制御サーバ	コントローラ	コントローラに不適切な目標値を設定する。
4-5	4-1	内部関係者(過失)	HMI(物理的侵入)				HMI	コントローラ	コントローラに不適切な目標値を設定する。
4-6	4-1	内部関係者(過失)	制御サーバ(物理的侵入)				制御サーバ	コントローラ	コントローラに不適切な目標値を設定する。
4-7	4-2	悪意のある第三者	情報NW	FW			EWS	コントローラ	コントローラの設定(閾値等)やプログラムを改ざんする。
4-8	4-2	悪意のある第三者	監視端末	データヒストリアン(中継)	データヒストリアン		EWS	コントローラ	コントローラの設定(閾値等)やプログラムを改ざんする。
4-9	4-2	内部関係者(過失)	EWS(物理的侵入)				EWS	コントローラ	コントローラの設定(閾値等)やプログラムを改ざんする。
4-10	4-3	悪意のある第三者	情報NW	FW			HMI	HMI	HMIのデータやプログラムを改ざんする。
4-11	4-3	悪意のある第三者	情報NW	FW			制御サーバ	制御サーバ	制御サーバのデータやプログラムを改ざんする。
4-12	4-3	悪意のある第三者	監視端末	データヒストリアン(中継)	データヒストリアン		HMI	HMI	HMIのデータやプログラムを改ざんする。
4-13	4-3	悪意のある第三者	監視端末	データヒストリアン(中継)	データヒストリアン		制御サーバ	制御サーバ	制御サーバのデータやプログラムを改ざんする。
4-14	4-3	内部関係者(過失)	HMI(物理的侵入)				HMI	HMI	HMIのデータやプログラムを改ざんする。
4-15	4-3	内部関係者(過失)	制御サーバ(物理的侵入)				制御サーバ	制御サーバ	制御サーバのデータやプログラムを改ざんする。
4-16	4-4	悪意のある第三者	情報NW	FW			HMI	HMI	破壊型マルウェアやランサムウェアに感染させ、監視操作を不能にする。
4-17	4-4	悪意のある第三者	監視端末	データヒストリアン(中継)	データヒストリアン		HMI	HMI	破壊型マルウェアやランサムウェアに感染させ、監視操作を不能にする。
4-18	4-4	内部関係者(過失)	HMI(物理的侵入)				HMI	HMI	破壊型マルウェアやランサムウェアに感染させ、監視操作を不能にする。
4-19	4-4	内部関係者(過失)	EWS(物理的侵入)				HMI	HMI	破壊型マルウェアやランサムウェアに感染させ、監視操作を不能にする。
ツリー#	シナリオ#	攻撃者	侵入口	経由1	経由2	経由3	攻撃拠点	攻撃対象	最終攻撃
5-1	5-1	悪意のある第三者	情報NW	FW			制御サーバ	制御サーバ	制御サーバに保存されている機密情報を窃取する。
5-2	5-1	悪意のある第三者	情報NW	FW			EWS	EWS	EWSに保存されている機密情報を窃取する。
5-3	5-1	悪意のある第三者	監視端末	データヒストリアン(中継)	データヒストリアン		制御サーバ	制御サーバ	制御サーバに保存されている機密情報を窃取する。
5-4	5-1	悪意のある第三者	監視端末	データヒストリアン(中継)	データヒストリアン		EWS	EWS	EWSに保存されている機密情報を窃取する。

表 4-7 攻撃ルート一覧表（侵入口ソート版）

攻撃ツリー番号#	シナリオ番号#	誰が	どこから	どうやって					
		攻撃者	侵入口	経由1	経由2	経由3	攻撃拠点	攻撃対象	最終攻撃
1-1	2-3	悪意のある第三者	情報NW	FW			HMI	HMI	HMIのデータやプログラムを改ざんする。
1-2	3-3	悪意のある第三者	情報NW	FW			HMI	HMI	HMIのデータやプログラムを改ざんする。
1-3	4-3	悪意のある第三者	情報NW	FW			HMI	HMI	HMIのデータやプログラムを改ざんする。
1-4	4-4	悪意のある第三者	情報NW	FW			HMI	HMI	破壊型マルウェアやランサムウェアに感染させ、監視操作を不能にする。
1-5	1-1	悪意のある第三者	情報NW	FW			HMI	コントローラ	広域供給停止操作を実行する。
1-6	2-1	悪意のある第三者	情報NW	FW			HMI	コントローラ	コントローラに不適切な目標値を設定する。
1-7	3-1	悪意のある第三者	情報NW	FW			HMI	コントローラ	コントローラに不適切な目標値を設定する。
1-8	4-1	悪意のある第三者	情報NW	FW			HMI	コントローラ	コントローラに不適切な目標値を設定する。
1-9	2-4	悪意のある第三者	情報NW	FW			HMI	制御NW(フ)	ネットワーク設定を改ざんし、通信不能にする。
1-10	2-4	悪意のある第三者	情報NW	FW			HMI	制御NW(フ)	マルウェアに感染させて不正通信を発生させ、通信不能にする。
1-11	2-3	悪意のある第三者	情報NW	FW			制御サーバ	制御サーバ	制御サーバのデータやプログラムを改ざんする。
1-12	3-3	悪意のある第三者	情報NW	FW			制御サーバ	制御サーバ	制御サーバのデータやプログラムを改ざんする。
1-13	4-3	悪意のある第三者	情報NW	FW			制御サーバ	制御サーバ	制御サーバのデータやプログラムを改ざんする。
1-14	5-1	悪意のある第三者	情報NW	FW			制御サーバ	制御サーバ	制御サーバに保存されている機密情報を窃取する。
1-15	2-1	悪意のある第三者	情報NW	FW			制御サーバ	コントローラ	コントローラに不適切な目標値を設定する。
1-16	3-1	悪意のある第三者	情報NW	FW			制御サーバ	コントローラ	コントローラに不適切な目標値を設定する。
1-17	4-1	悪意のある第三者	情報NW	FW			制御サーバ	コントローラ	コントローラに不適切な目標値を設定する。
1-18	5-1	悪意のある第三者	情報NW	FW			EWS	EWS	EWSに保存されている機密情報を窃取する。
1-19	2-2	悪意のある第三者	情報NW	FW			EWS	コントローラ	コントローラの設定（閾値等）やプログラムを改ざんする。
1-20	3-2	悪意のある第三者	情報NW	FW			EWS	コントローラ	コントローラの設定（閾値等）やプログラムを改ざんする。
1-21	4-2	悪意のある第三者	情報NW	FW			EWS	コントローラ	コントローラの設定（閾値等）やプログラムを改ざんする。
1-22	1-2	悪意のある第三者	情報NW	FW	EWS		コントローラ(M)	コントローラ(S)	供給停止コマンドを不正送信する。
ツリー#	シナリオ#	攻撃者	侵入口	経由1	経由2	経由3	攻撃拠点	攻撃対象	最終攻撃
2-1	2-3	悪意のある第三者	監視端末	データヒストリアン(中継)	データヒストリアン		HMI	HMI	HMIのデータやプログラムを改ざんする。
2-2	3-3	悪意のある第三者	監視端末	データヒストリアン(中継)	データヒストリアン		HMI	HMI	HMIのデータやプログラムを改ざんする。
2-3	4-3	悪意のある第三者	監視端末	データヒストリアン(中継)	データヒストリアン		HMI	HMI	HMIのデータやプログラムを改ざんする。
2-4	4-4	悪意のある第三者	監視端末	データヒストリアン(中継)	データヒストリアン		HMI	HMI	破壊型マルウェアやランサムウェアに感染させ、監視操作を不能にする。
2-5	1-1	悪意のある第三者	監視端末	データヒストリアン(中継)	データヒストリアン		HMI	コントローラ	広域供給停止操作を実行する。
2-6	2-1	悪意のある第三者	監視端末	データヒストリアン(中継)	データヒストリアン		HMI	コントローラ	コントローラに不適切な目標値を設定する。
2-7	3-1	悪意のある第三者	監視端末	データヒストリアン(中継)	データヒストリアン		HMI	コントローラ	コントローラに不適切な目標値を設定する。
2-8	4-1	悪意のある第三者	監視端末	データヒストリアン(中継)	データヒストリアン		HMI	コントローラ	コントローラに不適切な目標値を設定する。
2-9	2-4	悪意のある第三者	監視端末	データヒストリアン(中継)	データヒストリアン		HMI	制御NW(フ)	ネットワーク設定を改ざんし、通信不能にする。
2-10	2-4	悪意のある第三者	監視端末	データヒストリアン(中継)	データヒストリアン		HMI	制御NW(フ)	マルウェアに感染させて不正通信を発生させ、通信不能にする。
2-11	2-3	悪意のある第三者	監視端末	データヒストリアン(中継)	データヒストリアン		制御サーバ	制御サーバ	制御サーバのデータやプログラムを改ざんする。
2-12	3-3	悪意のある第三者	監視端末	データヒストリアン(中継)	データヒストリアン		制御サーバ	制御サーバ	制御サーバのデータやプログラムを改ざんする。
2-13	4-3	悪意のある第三者	監視端末	データヒストリアン(中継)	データヒストリアン		制御サーバ	制御サーバ	制御サーバのデータやプログラムを改ざんする。
2-14	5-1	悪意のある第三者	監視端末	データヒストリアン(中継)	データヒストリアン		制御サーバ	制御サーバ	制御サーバに保存されている機密情報を窃取する。
2-15	2-1	悪意のある第三者	監視端末	データヒストリアン(中継)	データヒストリアン		制御サーバ	コントローラ	コントローラに不適切な目標値を設定する。
2-16	3-1	悪意のある第三者	監視端末	データヒストリアン(中継)	データヒストリアン		制御サーバ	コントローラ	コントローラに不適切な目標値を設定する。
2-17	4-1	悪意のある第三者	監視端末	データヒストリアン(中継)	データヒストリアン		制御サーバ	コントローラ	コントローラに不適切な目標値を設定する。
2-18	5-1	悪意のある第三者	監視端末	データヒストリアン(中継)	データヒストリアン		EWS	EWS	EWSに保存されている機密情報を窃取する。
2-19	2-2	悪意のある第三者	監視端末	データヒストリアン(中継)	データヒストリアン		EWS	コントローラ	コントローラの設定（閾値等）やプログラムを改ざんする。
2-20	3-2	悪意のある第三者	監視端末	データヒストリアン(中継)	データヒストリアン		EWS	コントローラ	コントローラの設定（閾値等）やプログラムを改ざんする。
2-21	4-2	悪意のある第三者	監視端末	データヒストリアン(中継)	データヒストリアン		EWS	コントローラ	コントローラの設定（閾値等）やプログラムを改ざんする。
2-22	1-2	悪意のある第三者	監視端末	データヒストリアン(中継)	データヒストリアン	EWS	コントローラ(M)	コントローラ(S)	供給停止コマンドを不正送信する。
ツリー#	シナリオ#	攻撃者	侵入口	経由1	経由2	経由3	攻撃拠点	攻撃対象	最終攻撃
3-1	2-3	内部関係者（過失）	HMI（物理的侵入）				HMI	HMI	HMIのデータやプログラムを改ざんする。
3-2	3-3	内部関係者（過失）	HMI（物理的侵入）				HMI	HMI	HMIのデータやプログラムを改ざんする。
3-3	4-3	内部関係者（過失）	HMI（物理的侵入）				HMI	HMI	HMIのデータやプログラムを改ざんする。
3-4	4-4	内部関係者（過失）	HMI（物理的侵入）				HMI	HMI	破壊型マルウェアやランサムウェアに感染させ、監視操作を不能にする。
3-5	1-1	内部関係者（過失）	HMI（物理的侵入）				HMI	コントローラ	広域供給停止操作を実行する。
3-6	2-1	内部関係者（過失）	HMI（物理的侵入）				HMI	コントローラ	コントローラに不適切な目標値を設定する。
3-7	3-1	内部関係者（過失）	HMI（物理的侵入）				HMI	コントローラ	コントローラに不適切な目標値を設定する。
3-8	4-1	内部関係者（過失）	HMI（物理的侵入）				HMI	コントローラ	コントローラに不適切な目標値を設定する。
3-9	2-4	内部関係者（過失）	HMI（物理的侵入）				HMI	制御NW(フ)	ネットワーク設定を改ざんし、通信不能にする。
3-10	2-4	内部関係者（過失）	HMI（物理的侵入）				HMI	制御NW(フ)	マルウェアに感染させて不正通信を発生させ、通信不能にする。
3-11	2-3	内部関係者（過失）	制御サーバ（物理的侵入）				制御サーバ	制御サーバ	制御サーバのデータやプログラムを改ざんする。
3-12	3-3	内部関係者（過失）	制御サーバ（物理的侵入）				制御サーバ	制御サーバ	制御サーバのデータやプログラムを改ざんする。
3-13	4-3	内部関係者（過失）	制御サーバ（物理的侵入）				制御サーバ	制御サーバ	制御サーバのデータやプログラムを改ざんする。
3-15	2-1	内部関係者（過失）	制御サーバ（物理的侵入）				制御サーバ	コントローラ	コントローラに不適切な目標値を設定する。
3-16	3-1	内部関係者（過失）	制御サーバ（物理的侵入）				制御サーバ	コントローラ	コントローラに不適切な目標値を設定する。
3-17	4-1	内部関係者（過失）	制御サーバ（物理的侵入）				制御サーバ	コントローラ	コントローラに不適切な目標値を設定する。
3-18	4-4	内部関係者（過失）	EWS（物理的侵入）				HMI	HMI	破壊型マルウェアやランサムウェアに感染させ、監視操作を不能にする。
3-20	2-2	内部関係者（過失）	EWS（物理的侵入）				EWS	コントローラ	コントローラの設定（閾値等）やプログラムを改ざんする。
3-21	3-2	内部関係者（過失）	EWS（物理的侵入）				EWS	コントローラ	コントローラの設定（閾値等）やプログラムを改ざんする。
3-22	4-2	内部関係者（過失）	EWS（物理的侵入）				EWS	コントローラ	コントローラの設定（閾値等）やプログラムを改ざんする。
3-23	2-4	内部関係者（過失）	EWS（物理的侵入）				EWS	制御NW(フ)	ネットワーク設定を改ざんし、通信不能にする。
3-24	2-4	内部関係者（過失）	EWS（物理的侵入）				EWS	制御NW(フ)	マルウェアに感染させて不正通信を発生させ、通信不能にする。
3-25	1-2	内部関係者（過失）	EWS（物理的侵入）				コントローラ(M)	コントローラ(S)	供給停止コマンドを不正送信する。

侵入口から攻撃拠点までの攻撃ルートをシステム構成図上で表現した攻撃ルート図を以下に示す。

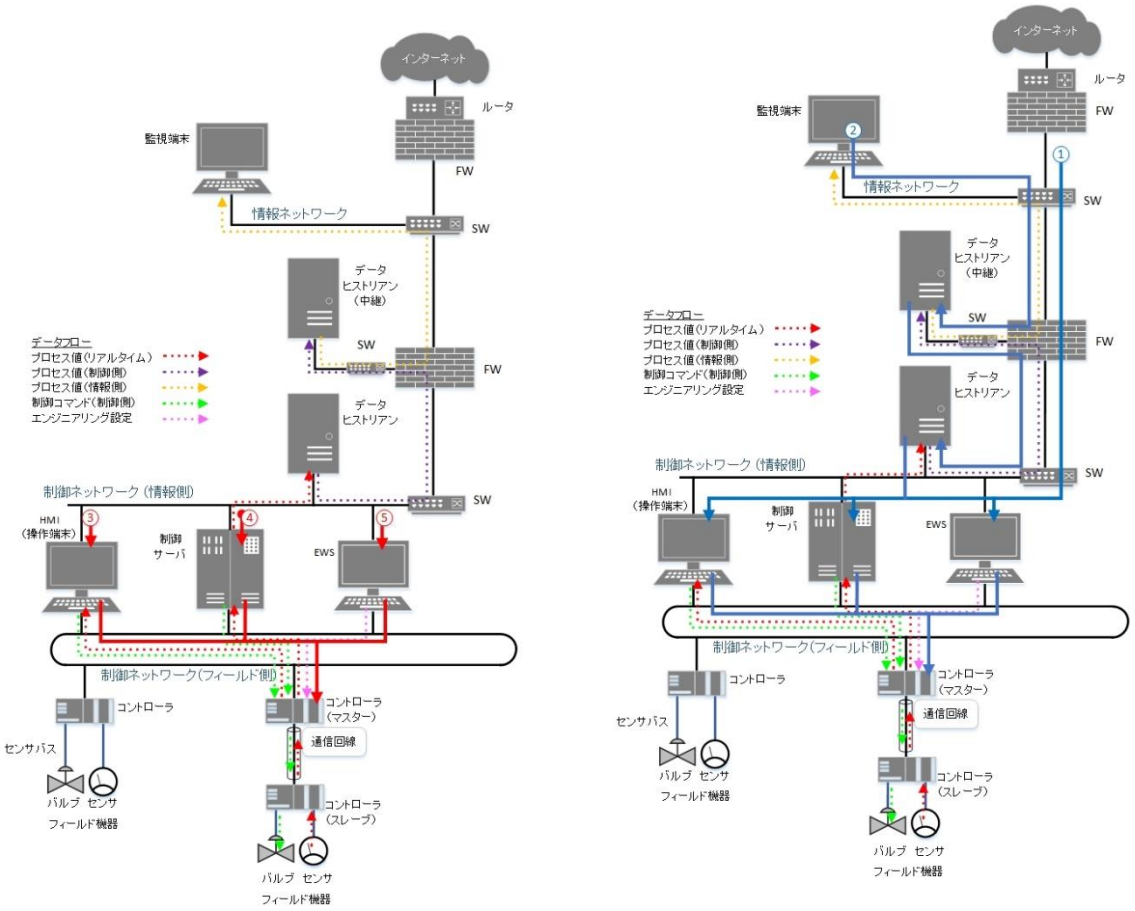


図 4-2 攻撃ルート図

4.3. リスク分析シートの作成

ガイド本体「*6 章* 事業被害ベースのリスク分析」で解説された手順に基づき、分析対象システムの事業被害ベースのリスク分析を実施する。詳細な手順はガイド本体を参照するものとして、ここでは作業の大きな流れを説明する。

【作業 4.3①】「4.2 節 表 4-6 攻撃ルート一覧表」を元に、攻撃ツリーを作成し、分析シートに記載すること。

- ガイド本体「*6.6.2 項* 攻撃ツリーの記入」を参考にして攻撃ツリーを作成する。

【作業 4.3②】攻撃ツリーの脅威レベルを検討し、分析シートに記載すること。

- ガイド本体「*6.8 節* 脅威レベルの評価」を参考にして、攻撃ツリーの脅威レベルの評価方法を決定する。
- 個々の攻撃ツリーは「表 2-10 脅威レベルの判断基準」を利用して脅威レベルを決定する。

【作業 4.3③】攻撃ツリーの事業被害レベルを、分析シートに記載すること。

- 「表 4-4 攻撃シナリオ一覧表」で攻撃シナリオの事業被害レベルが定義されているので、それらを分析シートに記載する。

【作業 4.3④】攻撃ツリーの各ステップで想定する攻撃に対する、対策状況を調査し、対策状況を分析シートに記載すること。

- ガイド本体「*6.9 節* セキュリティ対策状況の記入」を参考にして、対策状況を分析シートに記載する。

【作業 4.3⑤】攻撃ツリーの対策レベル／脆弱性レベルを評価し、分析シートに記載すること。

- ガイド本体「*6.10 節* 対策レベル／脆弱性レベルの評価」を参考にして、攻撃ツリーの対策レベルと脆弱性レベルを評価し、分析シートに記載する。

【作業 4.3⑥】攻撃ツリーのリスク値を評価し、分析シートに記載すること。

- ガイド本体「*6.11 項* リスク値の評価」を参考にして、リスク値を評価する。

【アウトプット 4.3】

事業被害のリスク分析シートを、71 頁以降に「表 4-8 事業被害ベースのリスク分析シート(シナリオソート版)」として示す。また、参考資料としてまとめ方が異なる 2 種類(計 3 種類)の分析シートを表 4-9、表 4-10 に示す。

【解説 4.3】

・3 種類の分析シートの形式（記入例）の特徴

表 4-6 攻撃ルート一覧表を基に、攻撃ツリーを検討して整理したものが、表 4-8 事業被害ベースのリスク分析シート（シナリオソート版）である。このシートでは、各事業被害の項目ごとに、攻撃シナリオに対応した攻撃ツリーをまとめた上で、侵入口でソートした攻撃ツリーの配置となっている。この整理方法では、攻撃シナリオとの対比が容易であり、分析の初期の段階での整理方法としては分かり易い。ただし、この方法ではシートに記述する攻撃ステップの数が多くなる（冗長な記述が多くなる）デメリットがある。

一方、表 4-9 事業被害ベースのリスク分析シート（侵入口ソート版）は、侵入口を起点とした攻撃ツリーの配置となっており、ATA アプローチでの整理方法となっている。この整理方法では、全体像が見えない時点では整理し難いため、分析の初期段階での整理方法としては向かないが、分析結果の評価の段階では、強化すべき共通的な攻撃ステップの確認等が容易である利点がある。なお、この方式ではシートに記述する攻撃ステップの数は最小となる。

また、表 4-10 事業被害ベースのリスク分析シート（ハイブリット版）は、前述の 2 つの方法の折衷案的なアプローチとなっている。いくつかの事業被害の項目をまとめて、攻撃ツリーを整理した上で、侵入口でソートした攻撃ツリーの配置となっている。事業被害／事業被害の項目ごとに区分した上で、重要度の高い事業被害／事業被害の項目から分析を開始し、この方式で整理するのも一つの進め方である。

・制御システムのセーフティ機能やアラーム(*)

分析シートの記入例では、対策欄において制御システムのセーフティ機能や制御システムのアラームを考慮していない。例えば、表 4-8 シナリオ#1-1、#1-2 において、サイバー攻撃で供給停止操作を行われても、制御システムのアラーム等ですぐに気付き、事業被害となる前に供給を復旧できるという場合もある。事業者の制御システムでリスク分析をする際は、制御システムのセーフティ機能やアラームと運用による復旧等と合わせて、脆弱性レベルの評価を変更して欲しい。

*アラーム：制御システムのアラーム、システムアラート、イベントを指す。情報セキュリティの警告イベントではない。

このページは空白です。

表 4-8 事業被害ベースのリスク分析シート（シナリオソート版）

1. 広域での製品供給停止

項番	攻撃シナリオ	攻撃ツリー／攻撃ステップ	評価指標 脅威レベル	脆弱性レベル	事業被害レベル	リスク値	対策 防御 侵入／拡散段階		防御 目的遂行段階		検知／被害把握		事業継続		対策レベル 攻撃ステップ	攻撃ツリー	攻撃ツリー番号	構成ステップ（項番）
	1-1	広域供給停止操作の実行により、広域で供給が停止する。																
1	1-1	**侵入口=情報NW** 悪意ある第三者が、情報NWからFWに不正アクセスする。 ※不正アクセスは「プロセス不正実行」(特権昇格)を含む。対策も2つの脅威への対策をマージ。斜体が「プロセス不正実行」のもの。					FW	○			IPS/IDS				2 ※1			
							通信相手の認証	○			ログ収集・分析							
							パッチ適用	○			統合ログ管理システム							
							脆弱性回避				*機器死活監視*							
							権限管理	○	（同左）									
2	1-1	悪意ある第三者が、FWを経由してHMIへ不正にアクセスする。 ※不正アクセスは「プロセス不正実行」を含む。					通信相手の認証	○			IPS/IDS				2			
							パッチ適用				ログ収集・分析							
							脆弱性回避				統合ログ管理システム							
							権限管理				*機器死活監視*							
3	1-1	悪意ある第三者が、HMIからコントローラーの広域供給停止操作をして、広域に及ぶ供給が停止する。	2	2	3	B	セグメント分割／ゾーニング		（同左）		ログ収集・分析				1	2	#1-1	1,2,3
							データ署名		（同左）		統合ログ管理システム							
							重要操作の承認		（同左）									
4	1-1	**侵入口=監視端末** 悪意ある第三者が、監視端末からデータヒストリアン（中継）に不正アクセスする。 ※不正アクセスは「プロセス不正実行」(特権昇格)を含む。対策も2つの脅威への対策をマージ。斜体が「プロセス不正実行」のもの。					通信相手の認証	○			IPS/IDS				2 ※1			
							パッチ適用	○			ログ収集・分析							
							脆弱性回避				統合ログ管理システム							
							権限管理	○	（同左）		*機器死活監視*							
5	1-1	悪意ある第三者が、データヒストリアン（中継）からデータヒストリアンへ不正にアクセスする。 ※不正アクセスは「プロセス不正実行」を含む。					通信相手の認証	○			IPS/IDS				2			
							パッチ適用				ログ収集・分析							
							脆弱性回避				統合ログ管理システム							
							権限管理	○			*機器死活監視*							
6	1-1	悪意ある第三者が、データヒストリアンからHMIへ不正にアクセスする。 ※不正アクセスは「プロセス不正実行」を含む。					通信相手の認証	○			IPS/IDS				2			
							パッチ適用				ログ収集・分析							
							脆弱性回避				統合ログ管理システム							
							権限管理				*機器死活監視*							
7	1-1	悪意ある第三者が、HMIからコントローラーの広域供給停止操作をして、広域に及ぶ供給が停止する。	2	2	3	B	項番3と同じ								1	2	#1-2	4,5,6,7
8	1-1	**侵入口=HMI** 内部者の過失により、マルウェアに感染したUSB媒体をHMIに接続して、HMIがマルウェアに感染する。 ※内部者のため故意の「不正媒体接続」の脅威はない前提。					アンチウイルス				機器異常検知				1 ※2			
							ホワイトリストによるプロセスの起動制限				機器死活監視							
							パッチ適用				ログ収集・分析							
							脆弱性回避				統合ログ管理システム							
							データ署名											
9	1-1	マルウェアが、HMIから広域供給停止操作をして、広域に及ぶ供給が停止する。	2	3	3	A	セグメント分割／ゾーニング		（同左）		ログ収集・分析				1	1	#1-3	8,9
							データ署名		（同左）		統合ログ管理システム							
							重要操作の承認		（同左）									
	1-2	複数コントローラへの供給停止コマンドの送信により、広域で供給が停止する。																
10	1-2	**侵入口=情報NW** 悪意ある第三者が、情報NWからFWに不正アクセスする。 ※不正アクセスは「プロセス不正実行」(特権昇格)を含む。対策も2つの脅威への対策をマージ。斜体が「プロセス不正実行」のもの。					項番1と同じ								2 ※1			
11	1-2	悪意ある第三者が、FWを経由してEWSへ不正にアクセスする。 ※不正アクセスは「プロセス不正実行」(特権昇格)を含む。					通信相手の認証	○			IPS/IDS				1			
							パッチ適用				ログ収集・分析							
							権限管理		（同左）		統合ログ管理システム							
							ホワイトリストによるプロセスの起動制限		（同左）		*機器死活監視*							
12	1-2	悪意ある第三者が、EWSからコントローラ(M)のプログラムを改ざんする。					権限管理		（同左）		機器異常検知		データバックアップ		1			
							アクセス制御		（同左）		ログ収集・分析							
							データ署名		（同左）		統合ログ管理システム							
13	1-2	悪意ある第三者が、コントローラ(M)を経由して、コントローラ(S)を停止させるコマンドを発行する。広域に及ぶ供給が停止する。	2	2	3	B	セグメント分割／ゾーニング		（同左）		ログ収集・分析				1	2	#1-4	10,11,12,13
							データ署名		（同左）		統合ログ管理システム							
							重要操作の承認		（同左）									
14	1-2	**侵入口=監視端末** 悪意ある第三者が、監視端末からデータヒストリアン（中継）に不正アクセスする。 ※不正アクセスは「プロセス不正実行」(特権昇格)を含む。対策も2つの脅威への対策をマージ。斜体が「プロセス不正実行」のもの。					項番4と同じ								2 ※1			
15	1-2	悪意ある第三者が、データヒストリアン（中継）からデータヒストリアンへ不正にアクセスする。 ※不正アクセスは「プロセス不正実行」を含む。					項番5と同じ								2			
16	1-2	悪意ある第三者が、データヒストリアンからEWSへ不正にアクセスする。 ※不正アクセスは「プロセス不正実行」を含む。					通信相手の認証	○			IPS/IDS				2			
							パッチ適用				ログ収集・分析							
							権限管理		（同左）		統合ログ管理システム							
							ホワイトリストによるプロセスの起動制限		（同左）		*機器死活監視*							
17	1-2	悪意ある第三者が、EWSからコントローラ(M)のプログラムを改ざんする。					項番12と同じ								1			
18	1-2	悪意ある第三者が、コントローラ(M)を経由して、コントローラ(S)を停止させるコマンドを発行する。広域に及ぶ供給が停止する。	2	2	3	B	項番13と同じ								1	2	#1-5	14,15,16,17,18
19	1-2	**侵入口=EWS** 内部者の過失により、マルウェアに感染したUSB媒体をEWSに接続して、EWSがマルウェアに感染する。 ※内部者のため故意の「不正媒体接続」の脅威はない前提。					アンチウイルス				機器異常検知				1 ※2			
							ホワイトリストによるプロセスの起動制限				機器死活監視							
							パッチ適用				ログ収集・分析							
							脆弱性回避				統合ログ管理システム							
							データ署名											
20	1-2	マルウェアが、EWSからコントローラ(M)のプログラムを改ざんする。					権限管理		（同左）		機器異常検知		データバックアップ		1			
							アクセス制御		（同左）		ログ収集・分析							
							データ署名		（同左）		統合ログ管理システム							
21	1-2	マルウェアが、コントローラ(M)を経由して、コントローラ(S)を停止させるコマンドを発行する。広域に及ぶ供給が停止する。	2	3	3	A	セグメント分割／ゾーニング		（同左）		ログ収集・分析				1	1	#1-6	19,20,21
							データ署名		（同左）		統合ログ管理システム							
							重要操作の承認		（同左）									
X																		

【注】
※1
対策の評価においては、「9.4節 ゾーニング対策における各種設定」を参照して実施することが望ましい。
※2
対策の評価においては、「9.5節 外部記憶媒体におけるセキュリティ対策」を参照して実施することが望ましい。

表 4-8 事業被害ベースのリスク分析シート(シナリオソート版)

2. 火災・爆発事故の発生

項番	攻撃シナリオ	攻撃ツリー／攻撃ステップ	評価指標				対策				対策レベル		攻撃ツリー番号	
			脅威レベル	脆弱性レベル	事業被害レベル	リスク値	防御		検知／被害把握	事業継続	攻撃ステップ	攻撃ツリー	攻撃ツリー番号	構成ステップ（項番）
							侵入／拡散段階	目的遂行段階						
	2-1	適切でない目標値の入力により、危険物取扱い設備の制御が異常となり、火災・爆発等が発生する。												
22		**侵入口=情報NW** 悪意ある第三者が、情報NWからFWに不正アクセスする。 ※不正アクセスは「プロセス不正実行」(特権昇格)を含む。対策も2つの脅威への対策をマージ。斜体が「プロセス不正実行」のもの。					項番1と同じ				2 ※1			
23		悪意ある第三者が、FWを経由してHMIへ不正にアクセスする。 ※不正アクセスは「プロセス不正実行」を含む。					項番2と同じ				2			
24	2-1	悪意ある第三者が、HMIからコントローラへ不適切な目標値を設定し、危険物取扱い設備の制御が異常となる。	2	2	3	B	セグメント分割／ゾーニング データ署名 重要操作の承認	(同左) (同左) (同左)	ログ収集・分析 統合ログ管理システム		1	2	#2-1	22,23,24
25		悪意ある第三者が、FWを経由して制御サーバへ不正にアクセスする。 ※不正アクセスは「プロセス不正実行」(特権昇格)を含む。					通信相手の認証 パッチ適用 *権限管理* *ホワイトリストによるプロセスの起動制限*	○ ○ ○ (同左)	IPS/IDS ログ収集・分析 統合ログ管理システム *機器死活監視*		2			
26	2-1	悪意ある第三者が、制御サーバからコントローラへ不適切な目標値を設定し、危険物取扱い設備の制御が異常となる。	2	2	3	B	セグメント分割／ゾーニング データ署名 重要操作の承認	(同左) (同左) (同左)	ログ収集・分析 統合ログ管理システム		1	2	#2-2	22,25,26
27		**侵入口=監視端末** 悪意ある第三者が、監視端末からデータヒストリアン(中継)に不正アクセスする。 ※不正アクセスは「プロセス不正実行」(特権昇格)を含む。対策も2つの脅威への対策をマージ。斜体が「プロセス不正実行」のもの。					項番4と同じ				2 ※1			
28		悪意ある第三者が、データヒストリアン(中継)からデータヒストリアンへ不正にアクセスする。 ※不正アクセスは「プロセス不正実行」を含む。					項番5と同じ				2			
29		悪意ある第三者が、データヒストリアンからHMIへ不正にアクセスする。 ※不正アクセスは「プロセス不正実行」を含む。					項番6と同じ				2			
30	2-1	悪意ある第三者が、HMIからコントローラへ不適切な目標値を設定し、危険物取扱い設備の制御が異常となる。	2	2	3	B	項番24と同じ				1	2	#2-3	27,28,29,30
31		悪意ある第三者が、データヒストリアンから制御サーバへ不正にアクセスする。 ※不正アクセスは「プロセス不正実行」を含む。					通信相手の認証 パッチ適用 脆弱性回避 *権限管理*	○ ○	IPS/IDS ログ収集・分析 統合ログ管理システム *機器死活監視*		2			
32	2-1	悪意ある第三者が、制御サーバからコントローラへ不適切な目標値を設定し、危険物取扱い設備の制御が異常となる。	2	2	3	B	項番26と同じ				1	2	#2-4	27,28,31,32
33		**侵入口=HMI** 内部者の過失により、マルウェアに感染したUSB媒体をHMIに接続して、HMIがマルウェアに感染する。 ※内部者のため故意の「不正媒体接続」の脅威はない前提。					項番8と同じ				1 ※2			
34	2-1	マルウェアが、HMIからコントローラへ不適切な目標値を設定し、危険物取扱い設備の制御が異常となる。	2	3	3	A	項番24と同じ				1	1	#2-5	33,34
35		**侵入口=制御サーバ** 内部者の過失により、マルウェアに感染したUSB媒体を制御サーバに接続して、制御サーバがマルウェアに感染する。 ※内部者のため故意の「不正媒体接続」の脅威はない前提。					アンチウイルス ホワイトリストによるプロセスの起動制限 パッチ適用 脆弱性回避 データ署名	 ○ 	機器異常検知 機器死活監視 ログ収集・分析 統合ログ管理システム		2 ※2			
36	2-1	マルウェアが、制御サーバからコントローラへ不適切な目標値を設定し、危険物取扱い設備の制御が異常となる。	2	2	3	B	セグメント分割／ゾーニング データ署名 重要操作の承認	(同左) (同左) (同左)	ログ収集・分析 統合ログ管理システム		1	2	#2-6	35,36
	2-2	設定(閾値等)やプログラムの改ざんにより、危険物取扱い設備の制御が異常となり、火災・爆発等が発生する。												
37		**侵入口=情報NW** 悪意ある第三者が、情報NWからFWに不正アクセスする。 ※不正アクセスは「プロセス不正実行」(特権昇格)を含む。対策も2つの脅威への対策をマージ。斜体が「プロセス不正実行」のもの。					項番1と同じ				2 ※1			
38		悪意ある第三者が、FWを経由してEWSへ不正にアクセスする。 ※不正アクセスは「プロセス不正実行」(特権昇格)を含む。					項番11と同じ				1			
39	2-2	悪意ある第三者が、EWSからコントローラの設定(閾値等)やプログラムを改ざんする。	2	2	3	B	権限管理 アクセス制御 データ署名	(同左) (同左) (同左)	機器異常検知 ログ収集・分析 統合ログ管理システム	データバックアップ	1	2	#2-7	37,38,39
40		**侵入口=監視端末** 悪意ある第三者が、監視端末からデータヒストリアン(中継)に不正アクセスする。 ※不正アクセスは「プロセス不正実行」(特権昇格)を含む。対策も2つの脅威への対策をマージ。斜体が「プロセス不正実行」のもの。					項番4と同じ				2 ※1			
41		悪意ある第三者が、データヒストリアン(中継)からデータヒストリアンへ不正にアクセスする。 ※不正アクセスは「プロセス不正実行」を含む。					項番5と同じ				2			
42		悪意ある第三者が、データヒストリアンからEWSへ不正にアクセスする。 ※不正アクセスは「プロセス不正実行」を含む。					項番16と同じ				2			
43	2-2	悪意ある第三者が、EWSからコントローラの設定(閾値等)やプログラムを改ざんする。	2	2	3	B	項番39と同じ				1	2	#2-8	40,41,42,43
44		**侵入口=EWS** 内部者の過失により、マルウェアに感染したUSB媒体をEWSに接続して、EWSがマルウェアに感染する。 ※内部者のため故意の「不正媒体接続」の脅威はない前提。					項番19と同じ				1 ※2			
45	2-2	マルウェアが、EWSからコントローラの設定(閾値等)やプログラムを改ざんする。	2	3	3	A	権限管理 アクセス制御 データ署名	(同左) (同左) (同左)	機器異常検知 ログ収集・分析 統合ログ管理システム	データバックアップ	1	1	#2-9	44,45

表 4-8 事業被害ベースのリスク分析シート(シナリオソート版)

項番	攻撃シナリオ	攻撃ツリー／攻撃ステップ	評価指標				対策				対策レベル		攻撃ツリー番号	
			脅威レベル	脆弱性レベル	事業被害レベル	リスク値	防御		検知／被害把握	事業継続	攻撃ステップ	攻撃ツリー	攻撃ツリー番号	構成ステップ(項番)
							侵入／拡散段階	目的遂行段階						
	2-3	データやプログラムの改ざんにより、危険物取扱い設備が異常な動作をするようになり、正しい操作を行っても正しい反応が得られず、火災・爆発等が発生する。												
46		**侵入口=情報NW** 悪意ある第三者が、情報NWからFWに不正アクセスする。 ※不正アクセスは「プロセス不正実行」(特権昇格)を含む。対策も2つの脅威への対策をマージ。斜体が「プロセス不正実行」のもの。					項番1と同じ				2 ※1			
47		悪意ある第三者が、FWを経由してHMIへ不正にアクセスする。 ※不正アクセスは「プロセス不正実行」を含む。					項番2と同じ				2			
48	2-3	悪意ある第三者が、HMIのプログラムやデータを改ざんする。	2	2	3	B	権限管理 アクセス制御 データ署名	○ 	(同左) (同左) (同左)	機器異常検知 ログ収集・分析 統合ログ管理システム	データバックアップ	1	2	#2-10	46,47,48
49		悪意ある第三者が、FWを経由して制御サーバへ不正にアクセスする。 ※不正アクセスは「プロセス不正実行」(特権昇格)を含む。					項番25と同じ				2			
50	2-3	悪意ある第三者が、制御サーバのプログラムやデータを改ざんする。	2	2	3	B	権限管理 アクセス制御 データ署名	○ 	(同左) (同左) (同左)	機器異常検知 ログ収集・分析 統合ログ管理システム	データバックアップ	2	2	#2-11	46,49,50
51		**侵入口=監視端末** 悪意ある第三者が、監視端末からデータヒストリアン(中継)に不正アクセスする。 ※不正アクセスは「プロセス不正実行」(特権昇格)を含む。対策も2つの脅威への対策をマージ。斜体が「プロセス不正実行」のもの。					項番4と同じ				2 ※1			
52		悪意ある第三者が、データヒストリアン(中継)からデータヒストリアンへ不正にアクセスする。 ※不正アクセスは「プロセス不正実行」を含む。					項番28と同じ				2			
53		悪意ある第三者が、データヒストリアンからHMIへ不正にアクセスする。 ※不正アクセスは「プロセス不正実行」を含む。					項番6と同じ				2			
54	2-3	悪意ある第三者が、HMIのプログラムやデータを改ざんする。	2	2	3	B	項番48と同じ				1	2	#2-12	51,52,53,54
55		悪意ある第三者が、データヒストリアンから制御サーバへ不正にアクセスする。 ※不正アクセスは「プロセス不正実行」を含む。					項番31と同じ				2			
56	2-3	悪意ある第三者が、制御サーバのプログラムやデータを改ざんする。	2	2	3	B	項番50と同じ				1	2	#2-13	51,52,55,56
57		**侵入口=HMI** 内部者の過失により、マルウェアに感染したUSB媒体をHMIに接続して、HMIがマルウェアに感染する。 ※内部者のため故意の「不正媒体接続」の脅威はない前提。					項番8と同じ				1 ※2			
58	2-3	マルウェアが、HMIのプログラムやデータを改ざんする。	2	3	3	A	権限管理 アクセス制御 データ署名	 	(同左) (同左) (同左)	機器異常検知 ログ収集・分析 統合ログ管理システム	データバックアップ	1	1	#2-14	57,58
59		**侵入口=制御サーバ** 内部者の過失により、マルウェアに感染したUSB媒体を制御サーバに接続して、制御サーバがマルウェアに感染する。 ※内部者のため故意の「不正媒体接続」の脅威はない前提。					項番35と同じ				2 ※2			
60	2-3	マルウェアが、制御サーバのプログラムやデータを改ざんする。	2	2	3	B	権限管理 アクセス制御 データ署名	○ 	(同左) (同左) (同左)	機器異常検知 ログ収集・分析 統合ログ管理システム	データバックアップ	2	2	#2-15	59,60
	2-4	制御ネットワーク(フィールド側)の輻輳により、危険物取扱い設備が監視操作不能となり、監視制御ができなくなり火災・爆発等が発生する。												
61		**侵入口=情報NW** 悪意ある第三者が、情報NWからFWに不正アクセスする。 ※不正アクセスは「プロセス不正実行」(特権昇格)を含む。対策も2つの脅威への対策をマージ。斜体が「プロセス不正実行」のもの。					項番1と同じ				2 ※1			
62		悪意ある第三者が、FWを経由してHMIへ不正にアクセスする。 ※不正アクセスは「プロセス不正実行」を含む。					項番2と同じ				2			
63	2-4	悪意ある第三者が、HMIから制御NW(フ)の設定を改ざんし、制御NWの通信が輻輳する。制御システムの監視操作ができなくなる。	2	2	3	B	権限管理 アクセス制御 データ署名	 	(同左) (同左) (同左)	機器異常検知 ログ収集・分析 統合ログ管理システム	データバックアップ	1	2	#2-16	61,62,63
64	2-4	悪意ある第三者が、HMIにマルウェアを感染させて、制御NW(フ)に不正通信を発生させ、制御NWを通信不能にする。制御システムの監視操作ができなくなる。	2	2	3	B	アンチウイルス ホワイトリストによるプロセスの起動制限 パッチ適用 脆弱性回避 データ署名			機器異常検知 機器死活監視 ログ収集・分析 統合ログ管理システム		1	2	#2-17	61,62,64
65		**侵入口=監視端末** 悪意ある第三者が、監視端末からデータヒストリアン(中継)に不正アクセスする。 ※不正アクセスは「プロセス不正実行」(特権昇格)を含む。対策も2つの脅威への対策をマージ。斜体が「プロセス不正実行」のもの。					項番4と同じ				2 ※1			
66		悪意ある第三者が、データヒストリアン(中継)からデータヒストリアンへ不正にアクセスする。 ※不正アクセスは「プロセス不正実行」を含む。					項番5と同じ				2			
67		悪意ある第三者が、データヒストリアンからHMIへ不正にアクセスする。 ※不正アクセスは「プロセス不正実行」を含む。					項番6と同じ				2			
68	2-4	悪意ある第三者が、HMIから制御NW(フ)の設定を改ざんし、制御NWの通信が輻輳する。制御システムの監視操作ができなくなる。	2	2	3	B	項番63と同じ				1	2	#2-18	65,66,67,68
69	2-4	悪意ある第三者が、HMIにマルウェアを感染させて、制御NW(フ)に不正通信を発生させ、制御NWを通信不能にする。制御システムの監視操作ができなくなる。	2	2	3	B	項番64と同じ				1	2	#2-19	65,66,67,69
70		**侵入口=HMI** 内部者の過失により、マルウェアに感染したUSB媒体をHMIに接続して、HMIがマルウェアに感染する。 ※内部者のため故意の「不正媒体接続」の脅威はない前提。					項番8と同じ				1 ※2			
71	2-4	マルウェアが、HMIから制御NW(フ)の設定を改ざんし、制御NWの通信が輻輳する。制御システムの監視操作ができなくなる。	2	3	3	A	項番63と同じ				1	1	#2-20	70,71
72	2-4	マルウェアが、制御NW(フ)に不正通信を発生させ、制御NWを通信不能にする。制御システムの監視操作ができなくなる。	2	3	3	A	項番64と同じ				1	1	#2-21	70,72
73		**侵入口=EWS** 内部者の過失により、マルウェアに感染したUSB媒体をEWSに接続して、EWSがマルウェアに感染する。 ※内部者のため故意の「不正媒体接続」の脅威はない前提。					項番19と同じ				1 ※2			
74	2-4	マルウェアが、EWSから制御NW(フ)の設定を改ざんし、制御NWの通信が輻輳する。制御システムの監視操作ができなくなる。	2	3	3	A	権限管理 アクセス制御 データ署名	 	(同左) (同左) (同左)	機器異常検知 ログ収集・分析 統合ログ管理システム	データバックアップ	1	1	#2-22	73,74
75	2-4	マルウェアが、制御NW(フ)に不正通信を発生させ、制御NWを通信不能にする。制御システムの監視操作ができなくなる。	2	3	3	A	権限管理 アクセス制御 データ署名	 	(同左) (同左) (同左)	機器異常検知 ログ収集・分析 統合ログ管理システム	データバックアップ	1	1	#2-23	73,75
X														

【注】
※1
対策の評価においては、「9.4節 ゾーニング対策における各種設定」を参照して実施することが望ましい。
※2
対策の評価においては、「9.5節 外部記憶媒体におけるセキュリティ対策」を参照して実施することが望ましい。

表 4-8 事業被害ベースのリスク分析シート(シナリオソート版)

3. 仕様不良製品の供給

項番	攻撃シナリオ	攻撃ツリー／攻撃ステップ	評価指標				対策				対策レベル		攻撃ツリー番号	
			脅威レベル	脆弱性レベル	事業被害レベル	リスク値	防御		検知／被害把握	事業継続	攻撃ステップ	攻撃ツリー	攻撃ツリー番号	構成ステップ（項番）
							侵入／拡散段階	目的遂行段階						
	3-1	適切でない目標値の入力により、製造設備の制御が異常となり、品質基準を満たさない製品が製造される。												
76	3-1	**侵入口=情報NW** 悪意ある第三者が、情報NWからFWに不正アクセスする。 ※不正アクセスは「プロセス不正実行」(特権昇格)を含む。対策も2つの脅威への対策をマージ。斜体が「プロセス不正実行」のもの。					項番1と同じ				2 ※1			
77	3-1	悪意ある第三者が、FWを経由してHMIへ不正にアクセスする。 ※不正アクセスは「プロセス不正実行」を含む。					項番2と同じ				2			
78	3-1	悪意ある第三者が、HMIからコントローラへ不適切な目標値を設定し、品質基準を満たさない製品が製造される。	2	2	2	C	セグメント分割／ゾーニング データ署名 重要操作の承認	(同左) (同左) (同左)	ログ収集・分析 統合ログ管理システム		1	2	#3-1	76,77,78
79	3-1	悪意ある第三者が、FWを経由して制御サーバへ不正にアクセスする。 ※不正アクセスは「プロセス不正実行」(特権昇格)を含む。					項番25と同じ				2			
80	3-1	悪意ある第三者が、制御サーバからコントローラへ不適切な目標値を設定し、品質基準を満たさない製品が製造される。	2	2	2	C	セグメント分割／ゾーニング データ署名 重要操作の承認	(同左) (同左) (同左)	ログ収集・分析 統合ログ管理システム		1	2	#3-2	76,79,80
81	3-1	**侵入口=監視端末** 悪意ある第三者が、監視端末からデータヒストリアン(中継)に不正アクセスする。 ※不正アクセスは「プロセス不正実行」(特権昇格)を含む。対策も2つの脅威への対策をマージ。斜体が「プロセス不正実行」のもの。					項番4と同じ				2 ※1			
82	3-1	悪意ある第三者が、データヒストリアン(中継)からデータヒストリアンへ不正にアクセスする。 ※不正アクセスは「プロセス不正実行」を含む。					項番5と同じ				2			
83	3-1	悪意ある第三者が、データヒストリアンからHMIへ不正にアクセスする。 ※不正アクセスは「プロセス不正実行」を含む。					項番6と同じ				2			
84	3-1	悪意ある第三者が、HMIからコントローラへ不適切な目標値を設定し、品質基準を満たさない製品が製造される。	2	2	2	C	項番78と同じ				1	2	#3-3	81,82,83,84
85	3-1	悪意ある第三者が、データヒストリアンから制御サーバへ不正にアクセスする。 ※不正アクセスは「プロセス不正実行」を含む。					項番31と同じ				2			
86	3-1	悪意ある第三者が、制御サーバからコントローラへ不適切な目標値を設定し、品質基準を満たさない製品が製造される。	2	2	2	C	項番80と同じ				1	2	#3-4	81,82,85,86
87	3-1	**侵入口=HMI** 内部者の過失により、マルウェアに感染したUSB媒体をHMIに接続して、HMIがマルウェアに感染する。 ※内部者のため故意の「不正媒体接続」の脅威はない前提。					項番8と同じ				1 ※2			
88	3-1	マルウェアが、HMIからコントローラへ不適切な目標値を設定し、品質基準を満たさない製品が製造される。	2	3	2	B	項番78と同じ				1	1	#3-5	87,88
89	3-1	**侵入口=制御サーバ** 内部者の過失により、マルウェアに感染したUSB媒体を制御サーバに接続して、制御サーバがマルウェアに感染する。 ※内部者のため故意の「不正媒体接続」の脅威はない前提。					項番35と同じ				2 ※2			
90	3-1	マルウェアが、制御サーバからコントローラへ不適切な目標値を設定し、品質基準を満たさない製品が製造される。	2	2	2	C	項番80と同じ				1	2	#3-6	89,90
	3-2	設定(閾値等)やプログラムの改ざんにより、製造設備の制御が異常となり、品質基準を満たさない製品が製造される。												
91	3-2	**侵入口=情報NW** 悪意ある第三者が、情報NWからFWに不正アクセスする。 ※不正アクセスは「プロセス不正実行」(特権昇格)を含む。対策も2つの脅威への対策をマージ。斜体が「プロセス不正実行」のもの。					項番1と同じ				2 ※1			
92	3-2	悪意ある第三者が、FWを経由してEWSへ不正にアクセスする。 ※不正アクセスは「プロセス不正実行」(特権昇格)を含む。					項番11と同じ				1			
93	3-2	悪意ある第三者が、EWSからコントローラの設定(閾値等)やプログラムを改ざんする。	2	2	2	C	権限管理 アクセス制御 データ署名	(同左) (同左) (同左)	機器異常検知 ログ収集・分析 統合ログ管理システム	データバックアップ	1	2	#3-7	91,92,93
94	3-2	**侵入口=監視端末** 悪意ある第三者が、監視端末からデータヒストリアン(中継)に不正アクセスする。 ※不正アクセスは「プロセス不正実行」(特権昇格)を含む。対策も2つの脅威への対策をマージ。斜体が「プロセス不正実行」のもの。					項番4と同じ				2 ※1			
95	3-2	悪意ある第三者が、データヒストリアン(中継)からデータヒストリアンへ不正にアクセスする。 ※不正アクセスは「プロセス不正実行」を含む。					項番5と同じ				2			
96	3-2	悪意ある第三者が、データヒストリアンからEWSへ不正にアクセスする。 ※不正アクセスは「プロセス不正実行」を含む。					項番16と同じ				2			
97	3-2	悪意ある第三者が、EWSからコントローラの設定(閾値等)やプログラムを改ざんする。	2	2	2	C	項番93と同じ				1	2	#3-8	94,95,96,97
98	3-2	**侵入口=EWS** 内部者の過失により、マルウェアに感染したUSB媒体をEWSに接続して、EWSがマルウェアに感染する。 ※内部者のため故意の「不正媒体接続」の脅威はない前提。					項番19と同じ				1 ※2			
99	3-2	マルウェアが、EWSからコントローラの設定(閾値等)やプログラムを改ざんする。	2	3	2	B	項番93と同じ				1	1	#3-9	98,99

表 4-8 事業被害ベースのリスク分析シート(シナリオソート版)

3. 仕様不良燃料の供給

項番	攻撃シナリオ	攻撃ツリー／攻撃ステップ	評価指標				対策				対策レベル		攻撃ツリー番号	
			脅威レベル	脆弱性レベル	事業被害レベル	リスク値	防御		検知／被害把握	事業継続	攻撃ステップ	攻撃ツリー	攻撃ツリー番号	構成ステップ（項番）
							侵入／拡散段階	目的遂行段階						
	3-3	データやプログラムの改ざんにより、製造設備が異常な動作をするようになり、品質基準を満たさない製品が製造される。												
100	3-3	**侵入口=情報NW** 悪意ある第三者が、情報NWからFWに不正アクセスする。 ※不正アクセスは「プロセス不正実行」(特権昇格)を含む。対策も2つの脅威への対策をマージ。斜体が「プロセス不正実行」のもの。					項番1と同じ				2 ※1			
101		悪意ある第三者が、FWを経由してHMIへ不正にアクセスする。 ※不正アクセスは「プロセス不正実行」を含む。					項番2と同じ				2			
102		悪意ある第三者が、HMIのプログラムやデータを改ざんする。	2	2	2	C	項番48と同じ				1	2	#3-10	100,101,102
103		悪意ある第三者が、FWを経由して制御サーバへ不正にアクセスする。 ※不正アクセスは「プロセス不正実行」(特権昇格)を含む。					項番25と同じ				2			
104		悪意ある第三者が、制御サーバのプログラムやデータを改ざんする。	2	2	2	C	項番50と同じ				2	2	#3-11	100,103,104
105		**侵入口=監視端末** 悪意ある第三者が、監視端末からデータヒストリアン(中継)に不正アクセスする。 ※不正アクセスは「プロセス不正実行」(特権昇格)を含む。対策も2つの脅威への対策をマージ。斜体が「プロセス不正実行」のもの。					項番4と同じ				2 ※1			
106		悪意ある第三者が、データヒストリアン(中継)からデータヒストリアンへ不正にアクセスする。 ※不正アクセスは「プロセス不正実行」を含む。					項番5と同じ				2			
107		悪意ある第三者が、データヒストリアンからHMIへ不正にアクセスする。 ※不正アクセスは「プロセス不正実行」を含む。					項番6と同じ				2			
108		悪意ある第三者が、HMIのプログラムやデータを改ざんする。	2	2	2	C	項番48と同じ				1	2	#3-12	105,106,107,108
109		悪意ある第三者が、データヒストリアンから制御サーバへ不正にアクセスする。 ※不正アクセスは「プロセス不正実行」を含む。					項番31と同じ				2			
110		悪意ある第三者が、制御サーバのプログラムやデータを改ざんする。	2	2	2	C	項番50と同じ				1	2	#3-13	105,106,109,110
111		**侵入口=HMI** 内部者の過失により、マルウェアに感染したUSB媒体をHMIに接続して、HMIがマルウェアに感染する。 ※内部者のため故意の「不正媒体接続」の脅威はない前提。					項番8と同じ				1 ※2			
112		マルウェアが、HMIのプログラムやデータを改ざんする。	2	3	2	B	項番58と同じ				1	1	#3-14	111,112
113		**侵入口=制御サーバ** 内部者の過失により、マルウェアに感染したUSB媒体を制御サーバに接続して、制御サーバがマルウェアに感染する。 ※内部者のため故意の「不正媒体接続」の脅威はない前提。					項番35と同じ				3 ※2			
114		マルウェアが、制御サーバのプログラムやデータを改ざんする。	2	2	2	C	項番60と同じ				2	2	#3-15	113,114
X														

【注】
※1
対策の評価においては、「9.4節 ゾーニング対策における各種設定」を参照して実施することが望ましい。
※2
対策の評価においては、「9.5節 外部記憶媒体におけるセキュリティ対策」を参照して実施することが望ましい。

表 4-8 事業被害ベースのリスク分析シート(シナリオソート版)

4. 製造停止の発生

項番	攻撃シナリオ	攻撃ツリー／攻撃ステップ	脅威レベル	脆弱性レベル	事業被害レベル	リスク値	対策				対策レベル		攻撃ツリー番号	
							防御		検知／被害把握	事業継続	攻撃ステップ	攻撃ツリー	攻撃ツリー番号	構成ステップ（項番）
							侵入／拡散段階	目的遂行段階						
	4-1	適切でない目標値の入力により、製造設備の制御が異常となり、安全のためプロセスを停止する。												
117		**侵入口=情報NW** 悪意ある第三者が、情報NWからFWに不正アクセスする。 ※不正アクセスは「プロセス不正実行」(特権昇格)を含む。対策も2つの脅威への対策をマージ。斜体が「プロセス不正実行」のもの。					項番1と同じ				2 ※1			
118		悪意ある第三者が、FWを経由してHMIへ不正にアクセスする。 ※不正アクセスは「プロセス不正実行」を含む。					項番2と同じ				2			
119	4-1	悪意ある第三者が、HMIからコントローラへ不適切な目標値を設定し、製造設備が異常となり、製造システムの非常停止が必要になる。	2	2	1	D	セグメント分割／ゾーニング データ署名 重要操作の承認	（同左） （同左） （同左）	ログ収集・分析 統合ログ管理システム		1	2	#4-1	117,118,119
120	4-1	悪意ある第三者が、制御サーバからコントローラへ不適切な目標値を設定し、製造設備が異常となり、製造システムの非常停止が必要になる。	2	2	1	D	セグメント分割／ゾーニング データ署名 重要操作の承認	（同左） （同左） （同左）	ログ収集・分析 統合ログ管理システム		1	2	#4-2	117,118,120
121		**侵入口=監視端末** 悪意ある第三者が、監視端末からデータヒストリアン(中継)に不正アクセスする。 ※不正アクセスは「プロセス不正実行」(特権昇格)を含む。対策も2つの脅威への対策をマージ。斜体が「プロセス不正実行」のもの。					項番4と同じ				2 ※1			
122		悪意ある第三者が、データヒストリアン(中継)からデータヒストリアンへ不正にアクセスする。 ※不正アクセスは「プロセス不正実行」を含む。					項番5と同じ				2			
123		悪意ある第三者が、データヒストリアンからHMIへ不正にアクセスする。 ※不正アクセスは「プロセス不正実行」を含む。					項番6と同じ				2			
124	4-1	悪意ある第三者が、HMIからコントローラへ不適切な目標値を設定し、製造設備が異常となり、製造システムの非常停止が必要になる。	2	2	1	D	項番119と同じ				1	2	#4-3	121,122,123,124
125		悪意ある第三者が、データヒストリアンから制御サーバへ不正にアクセスする。 ※不正アクセスは「プロセス不正実行」を含む。					項番31と同じ				2			
126	4-1	悪意ある第三者が、制御サーバからコントローラへ不適切な目標値を設定し、製造設備が異常となり、製造システムの非常停止が必要になる。	2	2	1	D	項番120と同じ				1	2	#4-4	121,122,125,126
127		**侵入口=HMI** 内部者の過失により、マルウェアに感染したUSB媒体をHMIに接続して、HMIがマルウェアに感染する。 ※内部者のため故意の「不正媒体接続」の脅威はない前提。					項番8と同じ				1 ※2			
128	4-1	マルウェアが、HMIからコントローラへ不適切な目標値を設定し、製造設備が異常となり、製造システムの非常停止が必要になる。	2	3	1	D	セグメント分割／ゾーニング データ署名 重要操作の承認	（同左） （同左） （同左）	ログ収集・分析 統合ログ管理システム		1	1	#4-5	127,128
129		**侵入口=制御サーバ** 内部者の過失により、マルウェアに感染したUSB媒体を制御サーバに接続して、制御サーバがマルウェアに感染する。 ※内部者のため故意の「不正媒体接続」の脅威はない前提。					項番35と同じ				2 ※2			
130	4-1	マルウェアが、制御サーバからコントローラへ不適切な目標値を設定し、製造設備が異常となり、製造システムの非常停止が必要になる。	2	2	1	D	セグメント分割／ゾーニング データ署名 重要操作の承認	（同左） （同左） （同左）	ログ収集・分析 統合ログ管理システム		1	2	#4-6	129,130
	4-2	設定(閾値等)やプログラムの改ざんにより、製造設備の制御が異常となり、安全のためプロセスを停止する。												
131		**侵入口=情報NW** 悪意ある第三者が、情報NWからFWに不正アクセスする。 ※不正アクセスは「プロセス不正実行」(特権昇格)を含む。対策も2つの脅威への対策をマージ。斜体が「プロセス不正実行」のもの。					項番1と同じ				2 ※1			
132		悪意ある第三者が、FWを経由してEWSへ不正にアクセスする。 ※不正アクセスは「プロセス不正実行」(特権昇格)を含む。					項番11と同じ				1			
133	4-2	悪意ある第三者が、EWSからコントローラの設定(閾値等)やプログラムを改ざんする。	2	2	1	D	権限管理 アクセス制御 データ署名	（同左） （同左） （同左）	機器異常検知 ログ収集・分析 統合ログ管理システム	データバックアップ	1	2	#4-7	131,132,133
134		**侵入口=監視端末** 悪意ある第三者が、監視端末からデータヒストリアン(中継)に不正アクセスする。 ※不正アクセスは「プロセス不正実行」(特権昇格)を含む。対策も2つの脅威への対策をマージ。斜体が「プロセス不正実行」のもの。					項番4と同じ				2 ※1			
135		悪意ある第三者が、データヒストリアン(中継)からデータヒストリアンへ不正にアクセスする。 ※不正アクセスは「プロセス不正実行」を含む。					項番5と同じ				2			
136		悪意ある第三者が、データヒストリアンからEWSへ不正にアクセスする。 ※不正アクセスは「プロセス不正実行」を含む。					項番16と同じ				2			
137	4-2	悪意ある第三者が、EWSからコントローラの設定(閾値等)やプログラムを改ざんする。	2	2	1	D	項番133と同じ				1	2	#4-8	134,135,136,137
138		**侵入口=EWS** 内部者の過失により、マルウェアに感染したUSB媒体をEWSに接続して、EWSがマルウェアに感染する。 ※内部者のため故意の「不正媒体接続」の脅威はない前提。					項番19と同じ				1 ※2			
139	4-2	マルウェアが、EWSからコントローラの設定(閾値等)やプログラムを改ざんする。	2	3	1	D	権限管理 アクセス制御 データ署名	（同左） （同左） （同左）	機器異常検知 ログ収集・分析 統合ログ管理システム	データバックアップ	1	1	#4-9	138,139

表 4-8 事業被害ベースのリスク分析シート(シナリオソート版)

4. 製造停止の発生

項番	攻撃シナリオ	攻撃ツリー／攻撃ステップ	評価指標 脅威レベル	脆弱性レベル	事業被害レベル	リスク値	対策 防御 侵入／拡散段階	防御 目的遂行段階	検知／被害把握	事業継続	対策レベル 攻撃ステップ	対策レベル 攻撃ツリー	攻撃ツリー番号 攻撃ツリー番号	攻撃ツリー番号 構成ステップ(項番)
	4-3	データやプログラムの改ざんにより、製造設備が異常な動作をするようになり、安全のためプロセスを停止する。												
140	4-3	**侵入口=情報NW** 悪意ある第三者が、情報NWからFWに不正アクセスする。 ※不正アクセスは「プロセス不正実行」(特権昇格)を含む。対策も2つの脅威への対策をマージ。斜体が「プロセス不正実行」のもの。					項番1と同じ				2 ※1			
141	4-3	悪意ある第三者が、FWを経由してHMIへ不正にアクセスする。 ※不正アクセスは「プロセス不正実行」を含む。					項番2と同じ				2			
142	4-3	悪意ある第三者が、HMIのプログラムやデータを改ざんする。	2	2	1	D	項番48と同じ				1	2	#4-10	140,141,142
143	4-3	悪意ある第三者が、FWを経由して制御サーバへ不正にアクセスする。 ※不正アクセスは「プロセス不正実行」(特権昇格)を含む。					項番25と同じ				2			
144	4-3	悪意ある第三者が、制御サーバのプログラムやデータを改ざんする。	2	2	1	D	項番50と同じ				2	2	#4-11	140,143,144
145	4-3	**侵入口=監視端末** 悪意ある第三者が、監視端末からデータヒストリアン(中継)に不正アクセスする。 ※不正アクセスは「プロセス不正実行」(特権昇格)を含む。対策も2つの脅威への対策をマージ。斜体が「プロセス不正実行」のもの。					項番4と同じ				2 ※1			
146	4-3	悪意ある第三者が、データヒストリアン(中継)からデータヒストリアンへ不正にアクセスする。 ※不正アクセスは「プロセス不正実行」を含む。					項番5と同じ				2			
147	4-3	悪意ある第三者が、データヒストリアンからHMIへ不正にアクセスする。 ※不正アクセスは「プロセス不正実行」を含む。					項番6と同じ				2			
148	4-3	悪意ある第三者が、HMIのプログラムやデータを改ざんする。	2	2	1	D	項番48と同じ				1	2	#4-12	145,146,147,148
149	4-3	悪意ある第三者が、データヒストリアンから制御サーバへ不正にアクセスする。 ※不正アクセスは「プロセス不正実行」を含む。					項番31と同じ				2			
150	4-3	悪意ある第三者が、制御サーバのプログラムやデータを改ざんする。	2	2	1	D	項番50と同じ				1	2	#4-13	145,146,149,150
151	4-3	**侵入口=HMI** 内部者の過失により、マルウェアに感染したUSB媒体をHMIに接続して、HMIがマルウェアに感染する。 ※内部者のため故意の「不正媒体接続」の脅威はない前提。					項番8と同じ				1 ※2			
152	4-3	マルウェアが、HMIのプログラムやデータを改ざんする。	2	3	1	D	項番58と同じ				1	1	#4-14	151,152
153	4-3	**侵入口=制御サーバ** 内部者の過失により、マルウェアに感染したUSB媒体を制御サーバに接続して、制御サーバがマルウェアに感染する。 ※内部者のため故意の「不正媒体接続」の脅威はない前提。					項番35と同じ				3 ※2			
154	4-3	マルウェアが、制御サーバのプログラムやデータを改ざんする。	2	2	1	D	項番60と同じ				1	2	#4-15	152,154
	4-4	破壊型マルウェアやランサムウェアへの感染により、製造設備が監視操作不能となり、監視制御ができなくなり安全のためプロセスを停止する。												
155	4-4	**侵入口=情報NW** 悪意ある第三者が、情報NWからFWに不正アクセスする。 ※不正アクセスは「プロセス不正実行」(特権昇格)を含む。対策も2つの脅威への対策をマージ。斜体が「プロセス不正実行」のもの。					項番1と同じ				2 ※1			
156	4-4	悪意ある第三者が、FWを経由してHMIへ不正にアクセスする。 ※不正アクセスは「プロセス不正実行」を含む。					項番2と同じ				2			
157	4-4	悪意ある第三者が、HMIに破壊型マルウェア(ランサムウェア等)を感染させる。制御システムの監視操作ができなくなる。	2	2	1	D	アンチウイルス ホワイトリストによるプロセスの起動制限 パッチ適用 脆弱性回避 データ署名	*権限管理* *アクセス制御*	機器異常検知 機器死活監視 ログ収集・分析 統合ログ管理システム	*データバックアップ*	1	2	#4-16	155,156,157
158	4-4	**侵入口=監視端末** 悪意ある第三者が、監視端末からデータヒストリアン(中継)に不正アクセスする。 ※不正アクセスは「プロセス不正実行」(特権昇格)を含む。対策も2つの脅威への対策をマージ。斜体が「プロセス不正実行」のもの。					項番4と同じ				2 ※1			
159	4-4	悪意ある第三者が、データヒストリアン(中継)からデータヒストリアンへ不正にアクセスする。 ※不正アクセスは「プロセス不正実行」を含む。					項番5と同じ				2			
160	4-4	悪意ある第三者が、データヒストリアンからHMIへ不正にアクセスする。 ※不正アクセスは「プロセス不正実行」を含む。					項番6と同じ				2			
161	4-4	悪意ある第三者が、HMIに破壊型マルウェア(ランサムウェア等)を感染させる。制御システムの監視操作ができなくなる。	2	2	1	D	項番157と同じ				1	2	#4-17	158,159,160,161
162	4-4	**侵入口=HMI** 内部者の過失により、マルウェアに感染したUSB媒体をHMIに接続して、HMIがマルウェアに感染する。 ※内部者のため故意の「不正媒体接続」の脅威はない前提。					項番8と同じ				1 ※2			
163	4-4	破壊型マルウェア(ランサムウェア等)により、データが破壊される。制御システムの監視操作ができなくなる。	2	3	1	D	アンチウイルス ホワイトリストによるプロセスの起動制限 パッチ適用 脆弱性回避 データ署名	*権限管理* *アクセス制御*	機器異常検知 機器死活監視 ログ収集・分析 統合ログ管理システム	*データバックアップ*	1	1	#4-18	162,163
164	4-4	**侵入口=EWS** 内部者の過失により、マルウェアに感染したUSB媒体をEWSに接続して、EWSがマルウェアに感染する。 ※内部者のため故意の「不正媒体接続」の脅威はない前提。					項番19と同じ				1 ※2			
165	4-4	マルウェアが、HMIに感染する。破壊型マルウェア(ランサムウェア等)により、データが破壊される。制御システムの監視操作ができなくなる。	2	3	1	D	アンチウイルス ホワイトリストによるプロセスの起動制限 パッチ適用 脆弱性回避 データ署名	*権限管理* *アクセス制御*	機器異常検知 機器死活監視 ログ収集・分析 統合ログ管理システム	*データバックアップ*	1	1	#4-19	164,165
X														

【注】
※1 対策の評価においては、「9.4節 ゾーニング対策における各種設定」を参照して実施することが望ましい。
※2 対策の評価においては、「9.5節 外部記憶媒体におけるセキュリティ対策」を参照して実施することが望ましい。

表 4-8 事業被害ベースのリスク分析シート(シナリオソート版)

5. 機密情報の漏洩

項番	攻撃シナリオ	攻撃ツリー／攻撃ステップ	評価指標				対策				対策レベル		攻撃ツリー番号	
			脅威レベル	脆弱性レベル	事業被害レベル	リスク値	防御		検知／被害把握	事業継続	攻撃ステップ	攻撃ツリー	攻撃ツリー番号	構成ステップ（項番）
							侵入／拡散段階	目的遂行段階						
	5-1	:制御システムに保存されている製造に関わる企業機密が窃取され、外部に漏洩する。												
166	5-1	**侵入口=情報NW** 悪意ある第三者が、情報NWからFWに不正アクセスする。 ※不正アクセスは「プロセス不正実行」(特権昇格)を含む。対策も2つの脅威への対策をマージ。斜体が「プロセス不正実行」のもの。					項番1と同じ				2 ※1			
167	5-1	悪意ある第三者が、FWを経由して制御サーバへ不正にアクセスする。 ※不正アクセスは「プロセス不正実行」(特権昇格)を含む。					項番25と同じ				2			
168	5-1	悪意ある第三者が、制御サーバ上のデータを窃取する。 (その後、逆ルートを辿り情報を持出す。)	2	2	3	B	権限管理 アクセス制御 データ暗号化 DLP	○ 	(同左) (同左) (同左) (同左)	ログ収集・分析 統合ログ管理システム	2	2	#5-1	166,167,168
169	5-1	悪意ある第三者が、FWを経由してEWSへ不正にアクセスする。 ※不正アクセスは「プロセス不正実行」(特権昇格)を含む。					項番11と同じ				1			
170	5-1	悪意ある第三者が、EWS上のデータを窃取する。 (その後、逆ルートを辿り情報を持出す。)	2	2	3	B	権限管理 アクセス制御 データ暗号化 DLP	 	(同左) (同左) (同左) (同左)	ログ収集・分析 統合ログ管理システム	1	2	#5-2	166,169,170
171	5-1	**侵入口=監視端末** 悪意ある第三者が、監視端末からデータヒストリアン(中継)に不正アクセスする。 ※不正アクセスは「プロセス不正実行」(特権昇格)を含む。対策も2つの脅威への対策をマージ。斜体が「プロセス不正実行」のもの。					項番4と同じ				2 ※1			
172	5-1	悪意ある第三者が、データヒストリアン(中継)からデータヒストリアンへ不正にアクセスする。 ※不正アクセスは「プロセス不正実行」を含む。					項番5と同じ				2			
173	5-1	悪意ある第三者が、データヒストリアンから制御サーバへ不正にアクセスする。 ※不正アクセスは「プロセス不正実行」を含む。					項番31と同じ				2			
174	5-1	悪意ある第三者が、制御サーバ上のデータを窃取する。 (その後、逆ルートを辿り情報を持出す。)	2	2	3	B	項番168と同じ				1	2	#5-3	171,172,173,174
175	5-1	悪意ある第三者が、データヒストリアンからEWSへ不正にアクセスする。 ※不正アクセスは「プロセス不正実行」を含む。					項番16と同じ				1			
176	5-1	悪意ある第三者が、EWS上のデータを窃取する。 (その後、逆ルートを辿り情報を持出す。)	2	2	3	B	項番170と同じ				1	2	#5-4	171,172,175,176
177	5-1	**侵入口=制御サーバ** 内部者の過失により、マルウェアに感染したUSB媒体を制御サーバに接続して、制御サーバがマルウェアに感染する。 ※内部者のため故意の「不正媒体接続」の脅威はない前提。					項番35と同じ				2 ※2			
178	5-1	マルウェアが、制御サーバ上のデータを窃取する。 (その後、逆ルートを辿り情報を持出す。)	2	2	3	B	権限管理 アクセス制御 データ暗号化 DLP	○ 	(同左) (同左) (同左) (同左)	ログ収集・分析 統合ログ管理システム	2	2	#5-5	177,178
179	5-1	**侵入口=EWS** 内部者の過失により、マルウェアに感染したUSB媒体をEWSに接続して、EWSがマルウェアに感染する。 ※内部者のため故意の「不正媒体接続」の脅威はない前提。					項番19と同じ				1 ※2			
180	5-1	マルウェアが、EWS上のデータを窃取する。 (その後、逆ルートを辿り情報を持出す。)	2	3	3	A	権限管理 アクセス制御 データ暗号化 DLP	 	(同左) (同左) (同左) (同左)	ログ収集・分析 統合ログ管理システム	1	1	#5-6	179,180
X														

【注】
※1 対策の評価においては、「9.4節 ゾーニング対策における各種設定」を参照して実施することが望ましい。
※2 対策の評価においては、「9.5節 外部記憶媒体におけるセキュリティ対策」を参照して実施することが望ましい。

表 4-9 事業被害ベースのリスク分析シート（侵入口ソート版）

1. 広域での製品供給停止、2. 火災・爆発事故の発生、3. 仕様不良製品の供給、4. 製造停止の発生、5. 機密情報の漏洩

項番	攻撃シナリオ	攻撃ツリー／攻撃ステップ	評価指標				対策				対策レベル		攻撃ツリー番号	
			脅威レベル	脆弱性レベル	事業被害レベル	リスク値	防御		検知／被害把握	事業継続	攻撃ステップ	攻撃ツリー	攻撃ツリー番号	構成ステップ（項番）
							侵入／拡散段階	目的遂行段階						
1-1		1-1:広域供給停止操作の実行により、広域で供給が停止する。												
1-2		1-2:複数コントローラへの供給停止コマンドの送信により、広域で供給が停止する。												
2-1		2-1:適切でない目標値の入力により、危険物取扱い設備の制御が異常となり、火災・爆発等が発生する。												
2-2		2-2:設定（閾値等）やプログラムの改ざんにより、危険物取扱い設備の制御が異常となり、火災・爆発等が発生する。												
2-3		2-3:データやプログラムの改ざんにより、危険物取扱い設備が異常な動作をするようになり、正しい操作を行っても正しい反応が得られず、火災・爆発等が発生する。												
2-4		2-4:制御ネットワーク（フィールド側）の輻輳により、危険物取扱い設備が監視操作不能となり、監視制御ができなくなり火災・爆発等が発生する。												
3-1		3-1:適切でない目標値の入力により、製造設備の制御が異常となり、品質基準を満たさない製品が製造される。												
3-2		3-2:設定（閾値等）やプログラムの改ざんにより、製造設備の制御が異常となり、品質基準を満たさない製品が製造される。												
3-3		3-3:データやプログラムの改ざんにより、製造設備が異常な動作をするようになり、品質基準を満たさない製品が製造される。												
4-1		4-1:適切でない目標値の入力により、製造設備の制御が異常となり、安全のためプロセスを停止する。												
4-2		4-2:設定（閾値等）やプログラムの改ざんにより、製造設備の制御が異常となり、安全のためプロセスを停止する。												
4-3		4-3:データやプログラムの改ざんにより、製造設備が異常な動作をするようになり、安全のためプロセスを停止する。												
4-4		4-4:破壊型マルウェアやランサムウェアへの感染により、製造設備が監視操作不能となり、監視制御ができなくなり安全のためプロセスを停止する。												
5-1		5-1:制御システムに保存されている製造に関わる企業機密が窃取され、外部に漏洩する。												
1		**侵入口=情報NW** 悪意ある第三者が、情報NWからFWに不正アクセスする。 ※不正アクセスは「プロセス不正実行」(特権昇格)を含む。対策も2つの脅威への対策をマージ。斜体が「プロセス不正実行」のもの。					FW 通信相手の認証 パッチ適用 脆弱性回避 *権限管理*	○ ○ ○ ○	 （同左）	IPS/IDS ログ収集・分析 統合ログ管理システム *機器死活監視*			2 ※1		
2		悪意ある第三者が、FWを経由してHMIへ不正にアクセスする。 ※不正アクセスは「プロセス不正実行」を含む。					通信相手の認証 パッチ適用 脆弱性回避 *権限管理*	○ 	 	IPS/IDS ログ収集・分析 統合ログ管理システム *機器死活監視*			2		
3	2-3	悪意ある第三者が、HMIのプログラムやデータを改ざんする。	2	2	3	B	権限管理 アクセス制御 データ署名		（同左） （同左） （同左）	機器異常検知 ログ収集・分析 統合ログ管理システム	データバックアップ		1	2	#1-1	1,2,3
4	3-3	悪意ある第三者が、HMIのプログラムやデータを改ざんする。	2	2	2	C	項番3と同じ						1	2	#1-2	1,2,4
5	4-3	悪意ある第三者が、HMIのプログラムやデータを改ざんする。	2	2	1	D	項番3と同じ						1	2	#1-3	1,2,5
6	4-4	悪意ある第三者が、HMIに破壊型マルウェア（ランサムウェア等）を感染させる。制御システムの監視操作ができなくなる。	2	2	1	D	アンチウイルス ホワイトリストによるプロセスの起動制限 パッチ適用 脆弱性回避 データ署名		*権限管理* *アクセス制御* 	機器異常検知 機器死活監視 ログ収集・分析 統合ログ管理システム 	*データバックアップ*		1	2	#1-4	1,2,6
7	1-1	悪意ある第三者が、HMIからコントローラーの広域供給停止操作をして、広域に及ぶ供給が停止する。	2	2	3	B	セグメント分割／ゾーニング データ署名 重要操作の承認		（同左） （同左） （同左）	ログ収集・分析 統合ログ管理システム			1	2	#1-5	1,2,7
8	2-1	悪意ある第三者が、HMIからコントローラへ不適切な目標値を設定し、危険物取扱い設備の制御が異常となる。	2	2	3	B	セグメント分割／ゾーニング データ署名 重要操作の承認		（同左） （同左） （同左）	ログ収集・分析 統合ログ管理システム			1	2	#1-6	1,2,8
9	3-1	悪意ある第三者が、HMIからコントローラへ不適切な目標値を設定し、品質基準を満たさない製品が製造される。	2	2	2	C	項番8と同じ						1	2	#1-7	1,2,9
10	4-1	悪意ある第三者が、HMIからコントローラへ不適切な目標値を設定し、製造設備が異常となり、製造システムの非常停止が必要になる。	2	2	1	D	項番8と同じ						1	2	#1-8	1,2,10
11	2-4	悪意ある第三者が、HMIから制御NW(フ)の設定を改ざんし、制御NWの通信が輻輳する。制御システムの監視操作ができなくなる。	2	2	3	B	権限管理 アクセス制御 データ署名		（同左） （同左） （同左）	機器異常検知 ログ収集・分析 統合ログ管理システム	データバックアップ		1	2	#1-9	1,2,11
12	2-4	悪意ある第三者が、HMIにマルウェアを感染させて、制御NW(フ)に不正通信を発生させ、制御NWを通信不能にする。制御システムの監視操作ができなくなる。	2	2	3	B	アンチウイルス ホワイトリストによるプロセスの起動制限 パッチ適用 脆弱性回避 データ署名		 	機器異常検知 機器死活監視 ログ収集・分析 統合ログ管理システム 			1	2	#1-10	1,2,12
13		悪意ある第三者が、FWを経由して制御サーバへ不正にアクセスする。 ※不正アクセスは「プロセス不正実行」(特権昇格)を含む。					通信相手の認証 パッチ適用 *権限管理* *ホワイトリストによるプロセスの起動制限*	○ ○	 （同左） （同左）	IPS/IDS ログ収集・分析 統合ログ管理システム *機器死活監視*			2		
14	2-3	悪意ある第三者が、制御サーバのプログラムやデータを改ざんする。	2	2	3	B	権限管理 アクセス制御 データ署名	○	（同左） （同左） （同左）	機器異常検知 ログ収集・分析 統合ログ管理システム	データバックアップ		2	2	#1-11	1,13,14
15	3-3	悪意ある第三者が、制御サーバのプログラムやデータを改ざんする。	2	2	2	C	項番14と同じ						2	2	#1-12	1,13,15
16	4-3	悪意ある第三者が、制御サーバのプログラムやデータを改ざんする。	2	2	1	D	項番14と同じ						2	2	#1-13	1,13,16
17	5-1	悪意ある第三者が、制御サーバ上のデータを窃取する。 （その後、逆ルートを辿り情報を持出す。）	2	2	3	B	権限管理 アクセス制御 データ暗号化 DLP		（同左） （同左） （同左） （同左）	ログ収集・分析 統合ログ管理システム			1	2	#1-14	1,13,17
18	2-1	悪意ある第三者が、制御サーバからコントローラへ不適切な目標値を設定し、危険物取扱い設備の制御が異常となる。	2	2	3	B	セグメント分割／ゾーニング データ署名 重要操作の承認		（同左） （同左） （同左）	ログ収集・分析 統合ログ管理システム			1	2	#1-15	1,13,18
19	3-1	悪意ある第三者が、制御サーバからコントローラへ不適切な目標値を設定し、品質基準を満たさない製品が製造される。	2	2	2	C	項番18と同じ						1	2	#1-16	1,13,19
20	4-1	悪意ある第三者が、制御サーバからコントローラへ不適切な目標値を設定し、製造設備が異常となり、製造システムの非常停止が必要になる。	2	2	1	D	項番18と同じ						1	2	#1-17	1,13,20
21		悪意ある第三者が、FWを経由してEWSへ不正にアクセスする。 ※不正アクセスは「プロセス不正実行」(特権昇格)を含む。					通信相手の認証 パッチ適用 *権限管理* *ホワイトリストによるプロセスの起動制限*	○ 	 （同左） （同左）	IPS/IDS ログ収集・分析 統合ログ管理システム *機器死活監視*			1		
22	5-1	悪意ある第三者が、EWS上のデータを窃取する。 （その後、逆ルートを辿り情報を持出す。）	2	2	3	B	権限管理 アクセス制御 データ暗号化 DLP		（同左） （同左） （同左） （同左）	ログ収集・分析 統合ログ管理システム			1	2	#1-18	1,21,22
23	2-2	悪意ある第三者が、EWSからコントローラの設定（閾値等）やプログラムを改ざんする。	2	2	3	B	権限管理 アクセス制御 データ署名		（同左） （同左） （同左）	機器異常検知 ログ収集・分析 統合ログ管理システム	データバックアップ		1	2	#1-19	1,21,23
24	3-2	悪意ある第三者が、EWSからコントローラの設定（閾値等）やプログラムを改ざんする。	2	2	2	C	項番23と同じ						1	2	#1-20	1,21,24
25	4-2	悪意ある第三者が、EWSからコントローラの設定（閾値等）やプログラムを改ざんする。	2	2	1	D	項番23と同じ						1	2	#1-21	1,21,25
26		悪意ある第三者が、EWSからコントローラ(M)のプログラムを改ざんする。					権限管理 アクセス制御 データ署名		（同左） （同左） （同左）	機器異常検知 ログ収集・分析 統合ログ管理システム	データバックアップ		1			
27	1-2	悪意ある第三者が、コントローラ(M)を経由して、コントローラ(S)を停止させるコマンドを発行する。広域に及ぶ供給が停止する。	2	2	3	B	セグメント分割／ゾーニング データ署名 重要操作の承認		（同左） （同左） （同左）	ログ収集・分析 統合ログ管理システム			1	2	#1-22	1,21,26,27
X																

【注】
※1　対策の評価においては、「9.4節 ゾーニング対策における各種設定」を参照して実施することが望ましい。

表 4-9 事業被害ベースのリスク分析シート(侵入口ソート版)

1. 広域での製品供給停止、2. 火災・爆発事故の発生、3. 仕様不良製品の供給、4. 製造停止の発生、5. 機密情報の漏洩

項番	攻撃シナリオ	攻撃ツリー／攻撃ステップ	評価指標 脅威レベル	脆弱性レベル	事業被害レベル	リスク値	対策 防御 侵入／拡散段階	防御 目的遂行段階	検知／被害把握	事業継続	対策レベル 攻撃ステップ	対策レベル 攻撃ツリー	攻撃ツリー番号 攻撃ツリー番号	攻撃ツリー番号 構成ステップ(項番)
1-1		1-1:広域供給停止操作の実行により、広域で供給が停止する。												
1-2		1-2:複数コントローラへの供給停止コマンドの送信により、広域で供給が停止する。												
2-1		2-1:適切でない目標値の入力により、危険物取扱い設備の制御が異常となり、火災・爆発等が発生する。												
2-2		2-2:設定(閾値等)やプログラムの改ざんにより、危険物取扱い設備の制御が異常となり、火災・爆発等が発生する。												
2-3		2-3:データやプログラムの改ざんにより、危険物取扱い設備が異常な動作をするようになり、正しい操作を行っても正しい反応が得られず、火災・爆発等が発生する。												
2-4		2-4:制御ネットワーク(フィールド側)の輻輳により、危険物取扱い設備が監視操作不能となり、監視制御ができなくなり火災・爆発等が発生する。												
3-1		3-1:適切でない目標値の入力により、製造設備の制御が異常となり、品質基準を満たさない製品が製造される。												
3-2		3-2:設定(閾値等)やプログラムの改ざんにより、製造設備の制御が異常となり、品質基準を満たさない製品が製造される。												
3-3		3-3:データやプログラムの改ざんにより、製造設備が異常な動作をするようになり、品質基準を満たさない製品が製造される。												
4-1		4-1:適切でない目標値の入力により、製造設備の制御が異常となり、安全のためプロセスを停止する。												
4-2		4-2:設定(閾値等)やプログラムの改ざんにより、製造設備の制御が異常となり、安全のためプロセスを停止する。												
4-3		4-3:データやプログラムの改ざんにより、製造設備が異常な動作をするようになり、安全のためプロセスを停止する。												
4-4		4-4:破壊型マルウェアやランサムウェアへの感染により、製造設備が監視操作不能となり、監視制御ができなくなり安全のためプロセスを停止する。												
5-1		5-1:制御システムに保存されている製造に関わる企業機密が窃取され、外部に漏洩する。												
28		**侵入口=監視端末** 悪意ある第三者が、監視端末からデータヒストリアン(中継)に不正アクセスする。 ※不正アクセスは「プロセス不正実行」(特権昇格)を含む。対策も2つの脅威への対策をマージ。斜体が「プロセス不正実行」のもの。					通信相手の認証 ○ パッチ適用 ○ 脆弱性回避 *権限管理* ○	(同左)	IPS/IDS ログ収集・分析 統合ログ管理システム *機器死活監視*		2 ※1			
29		悪意ある第三者が、データヒストリアン(中継)からデータヒストリアンへ不正にアクセスする。 ※不正アクセスは「プロセス不正実行」を含む。					通信相手の認証 ○ パッチ適用 脆弱性回避 *権限管理* ○		IPS/IDS ログ収集・分析 統合ログ管理システム *機器死活監視*		2			
30		悪意ある第三者が、データヒストリアンからHMIへ不正にアクセスする。 ※不正アクセスは「プロセス不正実行」を含む。					通信相手の認証 ○ パッチ適用 脆弱性回避 *権限管理*		IPS/IDS ログ収集・分析 統合ログ管理システム *機器死活監視*		2			
31	2-3	悪意ある第三者が、HMIのプログラムやデータを改ざんする。	2	2	3	B	項番3と同じ				1	2	#2-1	28,29,30,31
32	3-3	悪意ある第三者が、HMIのプログラムやデータを改ざんする。	2	2	2	C	項番3と同じ				1	2	#2-2	28,29,30,32
33	4-3	悪意ある第三者が、HMIのプログラムやデータを改ざんする。	2	2	1	D	項番3と同じ				1	2	#2-3	28,29,30,33
34	4-4	悪意ある第三者が、HMIに破壊型マルウェア(ランサムウェア等)を感染させる。制御システムの監視操作ができなくなる。	2	2	1	D	項番6と同じ				1	2	#2-4	28,29,30,34
35	1-1	悪意ある第三者が、HMIからコントローラーの広域供給停止操作をして、広域に及ぶ供給が停止する。	2	2	3	B	項番7と同じ				1	2	#2-5	28,29,30,35
36	2-1	悪意ある第三者が、HMIからコントローラへ不適切な目標値を設定し、危険物取扱い設備の制御が異常となる。	2	2	3	B	項番8と同じ				1	2	#2-6	28,29,30,36
37	3-1	悪意ある第三者が、HMIからコントローラへ不適切な目標値を設定し、品質基準を満たさない製品が製造される。	2	2	2	C	項番8と同じ				1	2	#2-7	28,29,30,37
38	4-1	悪意ある第三者が、HMIからコントローラへ不適切な目標値を設定し、製造設備が異常となり、製造システムの非常停止が必要になる。	2	2	1	D	項番8と同じ				1	2	#2-8	28,29,30,38
39	2-4	悪意ある第三者が、HMIから制御NW(フ)の設定を改ざんし、制御NWの通信が輻輳する。制御システムの監視操作ができなくなる。	2	2	3	B	項番11と同じ				1	2	#2-9	28,29,30,39
40	2-4	悪意ある第三者が、HMIにマルウェアを感染させて、制御NW(フ)に不正通信を発生させ、制御NWを通信不能にする。制御システムの監視操作ができなくなる。	2	2	3	B	項番12と同じ				1	2	#2-10	28,29,30,40
41		悪意ある第三者が、データヒストリアンから制御サーバへ不正にアクセスする。 ※不正アクセスは「プロセス不正実行」を含む。					通信相手の認証 ○ パッチ適用 脆弱性回避 *権限管理*		IPS/IDS ログ収集・分析 統合ログ管理システム *機器死活監視*		1			
42	2-3	悪意ある第三者が、制御サーバのプログラムやデータを改ざんする。	2	2	3	B	項番14と同じ				1	2	#2-11	28,29,41,42
43	3-3	悪意ある第三者が、制御サーバのプログラムやデータを改ざんする。	2	2	2	C	項番14と同じ				1	2	#2-12	28,29,41,43
44	4-3	悪意ある第三者が、制御サーバのプログラムやデータを改ざんする。	2	2	1	D	項番14と同じ				1	2	#2-13	28,29,41,44
45	5-1	悪意ある第三者が、制御サーバ上のデータを窃取する。 (その後、逆ルートを辿り情報を持出す。)	2	2	3	B	項番17と同じ				1	2	#2-14	28,29,41,45
46	2-1	悪意ある第三者が、制御サーバからコントローラへ不適切な目標値を設定し、危険物取扱い設備の制御が異常となる。	2	2	3	B	項番18と同じ				1	2	#2-15	28,29,41,46
47	3-1	悪意ある第三者が、制御サーバからコントローラへ不適切な目標値を設定し、品質基準を満たさない製品が製造される。	2	2	2	C	項番18と同じ				1	2	#2-16	28,29,41,47
48	4-1	悪意ある第三者が、制御サーバからコントローラへ不適切な目標値を設定し、製造設備が異常となり、製造システムの非常停止が必要になる。	2	2	1	D	項番18と同じ				1	2	#2-17	28,29,41,48
49		悪意ある第三者が、データヒストリアンからEWSへ不正にアクセスする。 ※不正アクセスは「プロセス不正実行」を含む。					項番21と同じ				2			
50	5-1	悪意ある第三者が、EWS上のデータを窃取する。 (その後、逆ルートを辿り情報を持出す。)	2	2	3	B	項番22と同じ				1	2	#2-18	28,29,49,50
51	2-2	悪意ある第三者が、EWSからコントローラの設定(閾値等)やプログラムを改ざんする。	2	2	3	B	項番23と同じ				1	2	#2-19	28,29,49,51
52	3-2	悪意ある第三者が、EWSからコントローラの設定(閾値等)やプログラムを改ざんする。	2	2	2	C	項番23と同じ				1	2	#2-20	28,29,49,52
53	4-2	悪意ある第三者が、EWSからコントローラの設定(閾値等)やプログラムを改ざんする。	2	2	1	D	項番23と同じ				1	2	#2-21	28,29,49,53
54		悪意ある第三者が、EWSからコントローラ(M)のプログラムを改ざんする。					項番26と同じ				1			
55	1-2	悪意ある第三者が、コントローラ(M)を経由して、コントローラ(S)を停止させるコマンドを発行する。広域に及ぶ供給が停止する。	2	2	3	B	項番27と同じ				1	2	#2-22	28,29,49,54,55
X														

【注】
※1 対策の評価においては、「9.4節 ゾーニング対策における各種設定」を参照して実施することが望ましい。

表 4-9 事業被害ベースのリスク分析シート(侵入口ソート版)

1. 広域での製品供給停止、2. 火災・爆発事故の発生、3. 仕様不良製品の供給、4. 製造停止の発生、5. 機密情報の漏洩

項番	攻撃シナリオ		攻撃ツリー／攻撃ステップ	評価指標				対策				対策レベル		攻撃ツリー番号	
				脅威レベル	脆弱性レベル	事業被害レベル	リスク値	防御		検知／被害把握	事業継続	攻撃ステップ	攻撃ツリー	攻撃ツリー番号	構成ステップ（項番）
								侵入／拡散段階	目的遂行段階						
項番	1-1		1-1:広域供給停止操作の実行により、広域で供給が停止する。 1-2:複数コントローラへの供給停止コマンドの送信により、広域で供給が停止する。 2-1:適切でない目標値の入力により、危険物取扱い設備の制御が異常となり、火災・爆発等が発生する。 2-2:設定（閾値等）やプログラムの改ざんにより、危険物取扱い設備の制御が異常となり、火災・爆発等が発生する。 2-3:データやプログラムの改ざんにより、危険物取扱い設備が異常な動作をするようになり、正しい操作を行っても正しい反応が得られず、火災・爆発等が発生する。 2-4:制御ネットワーク（フィールド側）の輻輳により、危険物取扱い設備が監視操作不能となり、監視制御ができなくなり火災・爆発等が発生する。 3-1:適切でない目標値の入力により、製造設備の制御が異常となり、品質基準を満たさない製品が製造される。 3-2:設定（閾値等）やプログラムの改ざんにより、製造設備の制御が異常となり、品質基準を満たさない製品が製造される。 3-3:データやプログラムの改ざんにより、製造設備が異常な動作をするようになり、品質基準を満たさない製品が製造される。 4-1:適切でない目標値の入力により、製造設備の制御が異常となり、安全のためプロセスを停止する。 4-2:設定（閾値等）やプログラムの改ざんにより、製造設備の制御が異常となり、安全のためプロセスを停止する。 4-3:データやプログラムの改ざんにより、製造設備が異常な動作をするようになり、安全のためプロセスを停止する。 4-4:破壊型マルウェアやランサムウェアへの感染により、製造設備が監視操作不能となり、監視制御ができなくなり安全のためプロセスを停止する。 5-1:制御システムに保存されている製造に関わる企業機密が窃取され、外部に漏洩する。												
56		**侵入口=HMI** 内部者の過失により、マルウェアに感染したUSB媒体をHMIに接続して、HMIがマルウェアに感染する。 ※内部者のため故意の「不正媒体接続」の脅威はない前提。					アンチウイルス			機器異常検知		1 ※2			
							ホワイトリストによるプロセスの起動制限			機器死活監視					
							パッチ適用			ログ収集・分析					
							脆弱性回避			統合ログ管理システム					
							データ署名								
57	2-3	マルウェアが、HMIのプログラムやデータを改ざんする。		2	3	3	A	項番3と同じ				1	1	#3-1	56,57
58	3-3	マルウェアが、HMIのプログラムやデータを改ざんする。		2	3	2	B	項番3と同じ				1	1	#3-2	56,58
59	4-3	マルウェアが、HMIのプログラムやデータを改ざんする。		2	3	1	D	項番3と同じ				1	1	#3-3	56,59
60	4-4	破壊型マルウェア（ランサムウェア等）により、データが破壊される。制御システムの監視操作ができなくなる。		2	3	1	D	項番6と同じ				1	1	#3-4	56,60
61	1-1	マルウェアが、HMIから広域供給停止操作をして、広域に及ぶ供給が停止する。		2	3	3	A	項番7と同じ				1	1	#3-5	56,61
62	2-1	マルウェアが、HMIからコントローラへ不適切な目標値を設定し、危険物取扱い設備の制御が異常となる。		2	3	3	A	項番7と同じ				1	1	#3-6	56,62
63	3-1	マルウェアが、HMIからコントローラへ不適切な目標値を設定し、品質基準を満たさない製品が製造される。		2	3	2	B	項番7と同じ				1	1	#3-7	56,63
64	4-1	マルウェアが、HMIからコントローラへ不適切な目標値を設定し、製造設備が異常となり、製造システムの非常停止が必要になる。		2	3	1	D	項番7と同じ				1	1	#3-8	56,64
65	2-4	マルウェアが、HMIから制御NW(フ)の設定を改ざんし、制御NWの通信が輻輳する。制御システムの監視操作ができなくなる。		2	3	3	A	項番11と同じ				1	1	#3-9	56,65
66	2-4	マルウェアが、制御NW(フ)に不正通信を発生させ、制御NWを通信不能にする。制御システムの監視操作ができなくなる。		2	3	3	A	項番12と同じ				1	1	#3-10	56,66
67		**侵入口=制御サーバ** 内部者の過失により、マルウェアに感染したUSB媒体を制御サーバに接続して、制御サーバがマルウェアに感染する。 ※内部者のため故意の「不正媒体接続」の脅威はない前提。					アンチウイルス			機器異常検知		2 ※2			
							ホワイトリストによるプロセスの起動制限	○		機器死活監視					
							パッチ適用			ログ収集・分析					
							脆弱性回避			統合ログ管理システム					
							データ署名								
68	2-3	マルウェアが、制御サーバのプログラムやデータを改ざんする。		2	2	3	B	項番14と同じ				1	2	#3-11	67,68
69	3-3	マルウェアが、制御サーバのプログラムやデータを改ざんする。		2	2	2	C	項番14と同じ				1	2	#3-12	67,69
70	4-3	マルウェアが、制御サーバのプログラムやデータを改ざんする。		2	2	1	D	項番14と同じ				1	2	#3-13	67,70
71	2-1	マルウェアが、制御サーバからコントローラへ不適切な目標値を設定し、危険物取扱い設備の制御が異常となる。		2	2	3	B	項番18と同じ				1	2	#3-14	67,71
72	3-1	マルウェアが、制御サーバからコントローラへ不適切な目標値を設定し、品質基準を満たさない製品が製造される。		2	2	2	C	項番18と同じ				1	2	#3-15	67,72
73	4-1	マルウェアが、制御サーバからコントローラへ不適切な目標値を設定し、製造設備が異常となり、製造システムの非常停止が必要になる。		2	2	1	D	項番18と同じ				1	2	#3-16	67,73
74		**侵入口=EWS** 内部者の過失により、マルウェアに感染したUSB媒体をEWSに接続して、EWSがマルウェアに感染する。 ※内部者のため故意の「不正媒体接続」の脅威はない前提。					アンチウイルス			機器異常検知		1 ※2			
							ホワイトリストによるプロセスの起動制限			機器死活監視					
							パッチ適用			ログ収集・分析					
							脆弱性回避			統合ログ管理システム					
							データ署名								
75	4-4	マルウェアが、HMIに感染する。破壊型マルウェア（ランサムウェア等）により、データが破壊される。制御システムの監視操作ができなくなる。		2	3	1	D	項番6と同じ				1	1	#3-17	74,75
76	2-2	マルウェアが、EWSからコントローラの設定（閾値等）やプログラムを改ざんする。		2	3	3	A	項番23と同じ				1	1	#3-18	74,76
77	3-2	マルウェアが、EWSからコントローラの設定（閾値等）やプログラムを改ざんする。		2	3	2	B	項番23と同じ				1	1	#3-19	74,77
78	4-2	マルウェアが、EWSからコントローラの設定（閾値等）やプログラムを改ざんする。		2	3	1	D	項番23と同じ				1	1	#3-20	74,78
79	2-4	マルウェアが、EWSから制御NW(フ)の設定を改ざんし、制御NWの通信が輻輳する。制御システムの監視操作ができなくなる。		2	3	3	A	権限管理	（同左）	機器異常検知	データバックアップ	1	1	#3-21	74,79
								アクセス制御	（同左）	ログ収集・分析					
								データ署名	（同左）	統合ログ管理システム					
80	2-4	マルウェアが、制御NW(フ)に不正通信を発生させ、制御NWを通信不能にする。制御システムの監視操作ができなくなる。		2	3	3	A	権限管理	（同左）	機器異常検知	データバックアップ	1	1	#3-22	74,80
								アクセス制御	（同左）	ログ収集・分析					
								データ署名	（同左）	統合ログ管理システム					
81		マルウェアが、EWSからコントローラ(M)のプログラムを改ざんする。						項番26と同じ				1			
82	1-2	マルウェアが、コントローラ(M)を経由して、コントローラ(S)を停止させるコマンドを発行する。広域に及ぶ供給が停止する。		2	3	3	A	項番27と同じ				1	1	#3-23	74,81,82
X															

【注】
※1 対策の評価においては、「9.4節 ゾーニング対策における各種設定」を参照して実施することが望ましい。
※2 対策の評価においては、「9.5節 外部記憶媒体におけるセキュリティ対策」を参照して実施することが望ましい。

表 4-10 事業被害ベースのリスク分析シート（ハイブリット版）

1. 広域での製品供給停止

項番	攻撃シナリオ	攻撃ツリー／攻撃ステップ	評価指標				対策				対策レベル		攻撃ツリー番号	
			脅威レベル	脆弱性レベル	事業被害レベル	リスク値	防御		検知／被害把握	事業継続	攻撃ステップ	攻撃ツリー	攻撃ツリー番号	構成ステップ（項番）
							侵入／拡散段階	目的遂行段階						
	1-1 1-2	1-1:広域供給停止操作の実行により、広域で供給が停止する。 1-2:複数コントローラへの供給停止コマンドの送信により、広域で供給が停止する。												
1	1-1	**侵入口=情報NW** 悪意ある第三者が、情報NWからFWに不正アクセスする。 ※不正アクセスは「プロセス不正実行」(特権昇格)を含む。対策も2つの脅威への対策をマージ。斜体が「プロセス不正実行」のもの。					FW 通信相手の認証 パッチ適用 脆弱性回避 *権限管理*	○ ○ ○ ○	 (同左)	IPS/IDS ログ収集・分析 統合ログ管理システム *機器死活監視*		2 ※1		
2	1-1	悪意ある第三者が、FWを経由してHMIへ不正にアクセスする。 ※不正アクセスは「プロセス不正実行」を含む。					通信相手の認証 パッチ適用 脆弱性回避 *権限管理*	○ 	 	IPS/IDS ログ収集・分析 統合ログ管理システム *機器死活監視*		2		
3	1-1	悪意ある第三者が、HMIからコントローラーの広域供給停止操作をして、広域に及ぶ供給が停止する。	2	2	3	B	セグメント分割／ゾーニング データ署名 重要操作の承認	 (同左) (同左) (同左)	ログ収集・分析 統合ログ管理システム		1	2	#1-1	1,2,3
4	1-1	悪意ある第三者が、FWを経由してEWSへ不正にアクセスする。 ※不正アクセスは「プロセス不正実行」(特権昇格)を含む。					通信相手の認証 パッチ適用 *権限管理* *ホワイトリストによるプロセスの起動制限*	○ (同左) (同左)	IPS/IDS ログ収集・分析 統合ログ管理システム *機器死活監視*		2			
5	1-1	悪意ある第三者が、EWSからコントローラ(M)のプログラムを改ざんする。					権限管理 アクセス制御 データ署名	(同左) (同左) (同左)	機器異常検知 ログ収集・分析 統合ログ管理システム	データバックアップ	1			
6	1-2	悪意ある第三者が、コントローラ(M)を経由して、コントローラ(S)を停止させるコマンドを発行する。広域に及ぶ供給が停止する。	2	2	3	B	セグメント分割／ゾーニング データ署名 重要操作の承認	(同左) (同左) (同左)	ログ収集・分析 統合ログ管理システム		1	2	#1-2	1,4,5,6
7	1-1	**侵入口=監視端末** 悪意ある第三者が、監視端末からデータヒストリアン（中継）に不正アクセスする。 ※不正アクセスは「プロセス不正実行」(特権昇格)を含む。対策も2つの脅威への対策をマージ。斜体が「プロセス不正実行」のもの。					通信相手の認証 パッチ適用 脆弱性回避 *権限管理*	○ ○ ○	 (同左)	IPS/IDS ログ収集・分析 統合ログ管理システム *機器死活監視*		2 ※1		
8	1-1	悪意ある第三者が、データヒストリアン（中継）からデータヒストリアンへ不正にアクセスする。 ※不正アクセスは「プロセス不正実行」を含む。					通信相手の認証 パッチ適用 脆弱性回避 *権限管理*	○ ○	 	IPS/IDS ログ収集・分析 統合ログ管理システム *機器死活監視*		2		
9	1-1	悪意ある第三者が、データヒストリアンからHMIへ不正にアクセスする。 ※不正アクセスは「プロセス不正実行」を含む。					通信相手の認証 パッチ適用 脆弱性回避 *権限管理*	○ 	 	IPS/IDS ログ収集・分析 統合ログ管理システム *機器死活監視*		2		
10	1-1	悪意ある第三者が、HMIからコントローラーの広域供給停止操作をして、広域に及ぶ供給が停止する。	2	2	3	B	項番3と同じ				1	2	#1-3	7,8,9,10
11	1-1	悪意ある第三者が、データヒストリアンからEWSへ不正にアクセスする。 ※不正アクセスは「プロセス不正実行」を含む。					通信相手の認証 パッチ適用 *権限管理* *ホワイトリストによるプロセスの起動制限*	○ (同左) (同左)	IPS/IDS ログ収集・分析 統合ログ管理システム *機器死活監視*		2			
12	1-1	悪意ある第三者が、EWSからコントローラ(M)のプログラムを改ざんする。					権限管理 アクセス制御 データ署名	(同左) (同左) (同左)	機器異常検知 ログ収集・分析 統合ログ管理システム	データバックアップ	1			
13	1-2	悪意ある第三者が、コントローラ(M)を経由して、コントローラ(S)を停止させるコマンドを発行する。広域に及ぶ供給が停止する。	2	2	3	B	項番6と同じ				1	2	#1-4	7,8,11,12,13
14	1-1	**侵入口=HMI** 内部者の過失により、マルウェアに感染したUSB媒体をHMIに接続して、HMIがマルウェアに感染する。 ※内部者のため故意の「不正媒体接続」の脅威はない前提。					アンチウイルス ホワイトリストによるプロセスの起動制限 パッチ適用 脆弱性回避 データ署名	 	機器異常検知 機器死活監視 ログ収集・分析 統合ログ管理システム		1 ※2			
15	1-1	マルウェアが、HMIから広域供給停止操作をして、広域に及ぶ供給が停止する。	2	3	3	A	セグメント分割／ゾーニング データ署名 重要操作の承認	(同左) (同左) (同左)	ログ収集・分析 統合ログ管理システム		1	1	#1-5	14,15
16	1-1	**侵入口=EWS** 内部者の過失により、マルウェアに感染したUSB媒体をEWSに接続して、EWSがマルウェアに感染する。 ※内部者のため故意の「不正媒体接続」の脅威はない前提。					アンチウイルス ホワイトリストによるプロセスの起動制限 パッチ適用 脆弱性回避 データ署名	 	機器異常検知 機器死活監視 ログ収集・分析 統合ログ管理システム		1 ※2			
17	1-1	マルウェアが、EWSからコントローラ(M)のプログラムを改ざんする。					権限管理 アクセス制御 データ署名	(同左) (同左) (同左)	機器異常検知 ログ収集・分析 統合ログ管理システム	データバックアップ	1			
18	1-2	マルウェアが、コントローラ(M)を経由して、コントローラ(S)を停止させるコマンドを発行する。広域に及ぶ供給が停止する。	2	3	3	A	セグメント分割／ゾーニング データ署名 重要操作の承認	(同左) (同左) (同左)	ログ収集・分析 統合ログ管理システム		1	1	#1-6	16,17,18
X														

【注】
※1 対策の評価においては、「9.4節 ゾーニング対策における各種設定」を参照して実施することが望ましい。
※2 対策の評価においては、「9.5節 外部記憶媒体におけるセキュリティ対策」を参照して実施することが望ましい。

表 4-10 事業被害ベースのリスク分析シート(ハイブリット版)

2. 火災・爆発事故の発生

項番	攻撃シナリオ	攻撃ツリー／攻撃ステップ	評価指標 脅威レベル	脆弱性レベル	事業被害レベル	リスク値	対策 防御 侵入／拡散段階	防御 目的遂行段階	検知／被害把握	事業継続	対策レベル 攻撃ステップ	対策レベル 攻撃ツリー	攻撃ツリー番号 攻撃ツリー番号	攻撃ツリー番号 構成ステップ(項番)
	2-1 2-2 2-3 2-4	2-1:適切でない目標値の入力により、危険物取扱い設備の制御が異常となり、火災・爆発等が発生する。 2-2:設定(閾値等)やプログラムの改ざんにより、危険物取扱い設備の制御が異常となり、火災・爆発等が発生する。 2-3:データやプログラムの改ざんにより、危険物取扱い設備が異常な動作をするようになり、正しい操作を行っても正しい反応が得られず、火災・爆発等が発生する。 2-4:制御ネットワーク(フィールド側)の輻輳により、危険物取扱い設備が監視操作不能となり、監視制御ができなくなり火災・爆発等が発生する。												
19		**侵入口=情報NW** 悪意ある第三者が、情報NWからFWに不正アクセスする。 ※不正アクセスは「プロセス不正実行」(特権昇格)を含む。対策も2つの脅威への対策をマージ。斜体が「プロセス不正実行」のもの。					項番1と同じ				2 ※1			
20		悪意ある第三者が、FWを経由してHMIへ不正にアクセスする。 ※不正アクセスは「プロセス不正実行」を含む。					項番2と同じ				2			
21	2-1	悪意ある第三者が、HMIからコントローラへ不適切な目標値を設定し、危険物取扱い設備の制御が異常となる。	2	2	3	B	セグメント分割／ゾーニング データ署名 重要操作の承認	(同左) (同左) (同左)	ログ収集・分析 統合ログ管理システム		1	2	#2-1	19,20,21
22	2-3	悪意ある第三者が、HMIのプログラムやデータを改ざんする。	2	2	3	B	権限管理 アクセス制御 データ署名	(同左) (同左) (同左)	機器異常検知 ログ収集・分析 統合ログ管理システム	データバックアップ	1	2	#2-2	19,20,22
23	2-4	悪意ある第三者が、HMIから制御NW(フ)の設定を改ざんし、制御NWの通信が輻輳する。制御システムの監視操作ができなくなる。	2	2	3	B	権限管理 アクセス制御 データ署名	(同左) (同左) (同左)	機器異常検知 ログ収集・分析 統合ログ管理システム	データバックアップ	1	2	#2-3	19,20,23
24	2-4	悪意ある第三者が、HMIにマルウェアを感染させて、制御NW(フ)に不正通信を発生させ、制御NWを通信不能にする。制御システムの監視操作ができなくなる。	2	2	3	B	アンチウイルス ホワイトリストによるプロセスの起動制限 パッチ適用 脆弱性回避 データ署名		機器異常検知 機器死活監視 ログ収集・分析 統合ログ管理システム		1	2	#2-4	19,20,24
25		悪意ある第三者が、FWを経由して制御サーバへ不正にアクセスする。 ※不正アクセスは「プロセス不正実行」(特権昇格)を含む。					通信相手の認証 パッチ適用 *権限管理* *ホワイトリストによるプロセスの起動制限*	○ ○ ○	 (同左) (同左)	IPS/IDS ログ収集・分析 統合ログ管理システム *機器死活監視*	2			
26	2-1	悪意ある第三者が、制御サーバからコントローラへ不適切な目標値を設定し、危険物取扱い設備の制御が異常となる。	2	2	3	B	セグメント分割／ゾーニング データ署名 重要操作の承認	(同左) (同左) (同左)	ログ収集・分析 統合ログ管理システム		1	2	#2-5	19,25,26
27	2-3	悪意ある第三者が、制御サーバのプログラムやデータを改ざんする。	2	2	3	B	権限管理 アクセス制御 データ署名	○ (同左) (同左)	機器異常検知 ログ収集・分析 統合ログ管理システム	データバックアップ	2	2	#2-6	19,25,27
28		悪意ある第三者が、FWを経由してEWSへ不正にアクセスする。 ※不正アクセスは「プロセス不正実行」(特権昇格)を含む。					項番4と同じ				2			
29	2-2	悪意ある第三者が、EWSからコントローラの設定(閾値等)やプログラムを改ざんする。	2	2	3	B	権限管理 アクセス制御 データ署名	(同左) (同左) (同左)	機器異常検知 ログ収集・分析 統合ログ管理システム	データバックアップ	1	2	#2-7	19,28,29
30		**侵入口=監視端末** 悪意ある第三者が、監視端末からデータヒストリアン(中継)に不正アクセスする。 ※不正アクセスは「プロセス不正実行」(特権昇格)を含む。対策も2つの脅威への対策をマージ。斜体が「プロセス不正実行」のもの。					項番7と同じ				2 ※1			
31		悪意ある第三者が、データヒストリアン(中継)からデータヒストリアンへ不正にアクセスする。 ※不正アクセスは「プロセス不正実行」を含む。					項番8と同じ				2			
32		悪意ある第三者が、データヒストリアンからHMIへ不正にアクセスする。 ※不正アクセスは「プロセス不正実行」を含む。					項番9と同じ				2			
33	2-1	悪意ある第三者が、HMIからコントローラへ不適切な目標値を設定し、危険物取扱い設備の制御が異常となる。	2	2	3	B	項番21と同じ				1	2	#2-8	30,31,32,33
34	2-3	悪意ある第三者が、HMIのプログラムやデータを改ざんする。	2	2	3	B	項番22と同じ				1	2	#2-9	30,31,32,34
35	2-4	悪意ある第三者が、HMIから制御NW(フ)の設定を改ざんし、制御NWの通信が輻輳する。制御システムの監視操作ができなくなる。	2	2	3	B	項番23と同じ				1	2	#2-10	30,31,32,35
36	2-4	悪意ある第三者が、HMIにマルウェアを感染させて、制御NW(フ)に不正通信を発生させ、制御NWを通信不能にする。制御システムの監視操作ができなくなる。	2	2	3	B	項番24と同じ				1	2	#2-11	30,31,32,36
37		悪意ある第三者が、データヒストリアンから制御サーバへ不正にアクセスする。 ※不正アクセスは「プロセス不正実行」を含む。					通信相手の認証 パッチ適用 脆弱性回避 *権限管理*	○ ○	 *機器死活監視*	IPS/IDS ログ収集・分析 統合ログ管理システム 	2			
38	2-1	悪意ある第三者が、制御サーバからコントローラへ不適切な目標値を設定し、危険物取扱い設備の制御が異常となる。	2	2	3	B	項番26と同じ				1	2	#2-12	30,31,37,38
39	2-3	悪意ある第三者が、制御サーバのプログラムやデータを改ざんする。	2	2	3	B	項番27と同じ				1	2	#2-13	30,31,37,39
40		悪意ある第三者が、データヒストリアンからEWSへ不正にアクセスする。 ※不正アクセスは「プロセス不正実行」を含む。					項番11と同じ				2			
41	2-2	悪意ある第三者が、EWSからコントローラの設定(閾値等)やプログラムを改ざんする。	2	2	3	B	項番29と同じ				1	2	#2-14	30,31,40,41

表 4-10 事業被害ベースのリスク分析シート(ハイブリット版)

2. 火災・爆発事故の発生

項番	攻撃シナリオ	攻撃ツリー／攻撃ステップ	評価指標 脅威レベル	脆弱性レベル	事業被害レベル	リスク値	対策 防御 侵入／拡散段階	防御 目的遂行段階	検知／被害把握	事業継続	対策レベル 攻撃ステップ	対策レベル 攻撃ツリー	攻撃ツリー番号 攻撃ツリー番号	攻撃ツリー番号 構成ステップ(項番)
	2-1 2-2 2-3 2-4	2-1:適切でない目標値の入力により、危険物取扱い設備の制御が異常となり、火災・爆発等が発生する。 2-2:設定(閾値等)やプログラムの改ざんにより、危険物取扱い設備の制御が異常となり、火災・爆発等が発生する。 2-3:データやプログラムの改ざんにより、危険物取扱い設備が異常な動作をするようになり、正しい操作を行っても正しい反応が得られず、火災・爆発等が発生する。 2-4:制御ネットワーク(フィールド側)の輻輳により、危険物取扱い設備が監視操作不能となり、監視制御ができなくなり火災・爆発等が発生する。												
42		侵入口=HMI 内部者の過失により、マルウェアに感染したUSB媒体をHMIに接続して、HMIがマルウェアに感染する。 ※内部者のため故意の「不正媒体接続」の脅威はない前提。					項番14と同じ				1 ※2			
43	2-1	マルウェアが、HMIからコントローラへ不適切な目標値を設定し、危険物取扱い設備の制御が異常となる。	2	3	3	A	セグメント分割／ゾーニング	(同左)	ログ収集・分析		1	1	#2-15	42,43
							データ署名	(同左)	統合ログ管理システム					
							重要操作の承認	(同左)						
44	2-3	マルウェアが、HMIのプログラムやデータを改ざんする。	2	3	3	A	権限管理	(同左)	機器異常検知	データバックアップ	1	1	#2-16	42,44
							アクセス制御	(同左)	ログ収集・分析					
							データ署名	(同左)	統合ログ管理システム					
45	2-4	マルウェアが、HMIから制御NW(フ)の設定を改ざんし、制御NWの通信が輻輳する。制御システムの監視操作ができなくなる。	2	3	3	A	権限管理	(同左)	機器異常検知	データバックアップ	1	1	#2-17	42,45
							アクセス制御	(同左)	ログ収集・分析					
							データ署名	(同左)	統合ログ管理システム					
46	2-4	マルウェアが、制御NW(フ)に不正通信を発生させ、制御NWを通信不能にする。制御システムの監視操作ができなくなる。	2	3	3	A	アンチウイルス		機器異常検知		1	1	#2-18	42,46
							ホワイトリストによるプロセスの起動制限		機器死活監視					
							パッチ適用		ログ収集・分析					
							脆弱性回避		統合ログ管理システム					
							データ署名							
47		侵入口=制御サーバ 内部者の過失により、マルウェアに感染したUSB媒体を制御サーバに接続して、制御サーバがマルウェアに感染する。 ※内部者のため故意の「不正媒体接続」の脅威はない前提。					アンチウイルス		機器異常検知		2 ※2			
							ホワイトリストによるプロセスの起動制限	○	機器死活監視					
							パッチ適用		ログ収集・分析					
							脆弱性回避		統合ログ管理システム					
							データ署名							
48	2-1	マルウェアが、制御サーバからコントローラへ不適切な目標値を設定し、危険物取扱い設備の制御が異常となる。	2	2	3	B	セグメント分割／ゾーニング	(同左)	ログ収集・分析		1	2	#2-19	47,48
							データ署名	(同左)	統合ログ管理システム					
							重要操作の承認	(同左)						
49	2-3	マルウェアが、制御サーバのプログラムやデータを改ざんする。	2	2	3	B	権限管理	○ (同左)	機器異常検知	データバックアップ	2	2	#2-20	47,49
							アクセス制御	(同左)	ログ収集・分析					
							データ署名	(同左)	統合ログ管理システム					
50		侵入口=EWS 内部者の過失により、マルウェアに感染したUSB媒体をEWSに接続して、EWSがマルウェアに感染する。 ※内部者のため故意の「不正媒体接続」の脅威はない前提。					項番16と同じ				1 ※2			
51	2-2	マルウェアが、EWSからコントローラの設定(閾値等)やプログラムを改ざんする。	2	3	3	A	権限管理	(同左)	機器異常検知	データバックアップ	1	1	#2-21	50,51
							アクセス制御	(同左)	ログ収集・分析					
							データ署名	(同左)	統合ログ管理システム					
52	2-4	マルウェアが、EWSから制御NW(フ)の設定を改ざんし、制御NWの通信が輻輳する。制御システムの監視操作ができなくなる。	2	3	3	A	権限管理	(同左)	機器異常検知	データバックアップ	1	1	#2-22	50,52
							アクセス制御	(同左)	ログ収集・分析					
							データ署名	(同左)	統合ログ管理システム					
53	2-4	マルウェアが、制御NW(フ)に不正通信を発生させ、制御NWを通信不能にする。制御システムの監視操作ができなくなる。	2	3	3	A	権限管理	(同左)	機器異常検知	データバックアップ	1	1	#2-23	50,53
							アクセス制御	(同左)	ログ収集・分析					
							データ署名	(同左)	統合ログ管理システム					
X														

【注】
※1 対策の評価においては、「9.4節 ゾーニング対策における各種設定」を参照して実施することが望ましい。
※2 対策の評価においては、「9.5節 外部記憶媒体におけるセキュリティ対策」を参照して実施することが望ましい。

表 4-10 事業被害ベースのリスク分析シート(ハイブリット版)

3. 仕様不良製品の供給

項番	攻撃シナリオ	攻撃ツリー／攻撃ステップ	評価指標 脅威レベル	脆弱性レベル	事業被害レベル	リスク値	対策 防御 侵入／拡散段階	防御 目的遂行段階	検知／被害把握	事業継続	対策レベル 攻撃ステップ	対策レベル 攻撃ツリー	攻撃ツリー番号 攻撃ツリー番号	攻撃ツリー番号 構成ステップ(項番)
	3-1 3-2 3-3	3-1:適切でない目標値の入力により、製造設備の制御が異常となり、品質基準を満たさない製品が製造される。 3-2:設定(閾値等)やプログラムの改ざんにより、製造設備の制御が異常となり、品質基準を満たさない製品が製造される。 3-3:データやプログラムの改ざんにより、製造設備が異常な動作をするようになり、品質基準を満たさない製品が製造される。												
54		**侵入口=情報NW** 悪意ある第三者が、情報NWからFWに不正アクセスする。 ※不正アクセスは「プロセス不正実行」(特権昇格)を含む。対策も2つの脅威への対策をマージ。斜体が「プロセス不正実行」のもの。					項番1と同じ				2 ※1			
55		悪意ある第三者が、FWを経由してHMIへ不正にアクセスする。 ※不正アクセスは「プロセス不正実行」を含む。					項番2と同じ				2			
56	3-1	悪意ある第三者が、HMIからコントローラへ不適切な目標値を設定し、品質基準を満たさない製品が製造される。	2	2	2	C	セグメント分割／ゾーニング データ署名 重要操作の承認	(同左) (同左) (同左)	ログ収集・分析 統合ログ管理システム		1	2	#3-1	54,55,56
57	3-3	悪意ある第三者が、HMIのプログラムやデータを改ざんする。	2	2	2	C	権限管理 アクセス制御 データ署名	(同左) (同左) (同左)	機器異常検知 ログ収集・分析 統合ログ管理システム	データバックアップ	1	2	#3-2	54,55,57
58		悪意ある第三者が、FWを経由して制御サーバへ不正にアクセスする。 ※不正アクセスは「プロセス不正実行」(特権昇格)を含む。					項番25と同じ				2			
59	3-1	悪意ある第三者が、制御サーバからコントローラへ不適切な目標値を設定し、品質基準を満たさない製品が製造される。	2	2	2	C	セグメント分割／ゾーニング データ署名 重要操作の承認	(同左) (同左) (同左)	ログ収集・分析 統合ログ管理システム		1	2	#3-3	54,58,59
60	3-3	悪意ある第三者が、制御サーバのプログラムやデータを改ざんする。	2	2	2	C	権限管理 アクセス制御 データ署名	○ (同左) (同左)	機器異常検知 ログ収集・分析 統合ログ管理システム	データバックアップ	2	2	#3-4	54,58,60
61		悪意ある第三者が、FWを経由してEWSへ不正にアクセスする。 ※不正アクセスは「プロセス不正実行」(特権昇格)を含む。					項番4と同じ				2			
62	3-2	悪意ある第三者が、EWSからコントローラの設定(閾値等)やプログラムを改ざんする。	2	2	2	C	権限管理 アクセス制御 データ署名	(同左) (同左) (同左)	機器異常検知 ログ収集・分析 統合ログ管理システム	データバックアップ	1	2	#3-5	54,61,62
63		**侵入口=監視端末** 悪意ある第三者が、監視端末からデータヒストリアン(中継)に不正アクセスする。 ※不正アクセスは「プロセス不正実行」(特権昇格)を含む。対策も2つの脅威への対策をマージ。斜体が「プロセス不正実行」のもの。					項番7と同じ				2 ※1			
64		悪意ある第三者が、データヒストリアン(中継)からデータヒストリアンへ不正にアクセスする。 ※不正アクセスは「プロセス不正実行」を含む。					項番8と同じ				2			
65		悪意ある第三者が、データヒストリアンからHMIへ不正にアクセスする。 ※不正アクセスは「プロセス不正実行」を含む。					項番9と同じ				2			
66	3-1	悪意ある第三者が、HMIからコントローラへ不適切な目標値を設定し、品質基準を満たさない製品が製造される。	2	2	2	C	項番56と同じ				1	2	#3-6	63,64,65,66
67	3-3	悪意ある第三者が、HMIのプログラムやデータを改ざんする。	2	2	2	C	項番57と同じ				1	2	#3-7	63,64,65,67
68		悪意ある第三者が、データヒストリアンから制御サーバへ不正にアクセスする。 ※不正アクセスは「プロセス不正実行」を含む。					項番37と同じ				2			
69	3-1	悪意ある第三者が、制御サーバからコントローラへ不適切な目標値を設定し、品質基準を満たさない製品が製造される。	2	2	2	C	項番59と同じ				1	2	#3-8	63,64,68,69
70	3-3	悪意ある第三者が、制御サーバのプログラムやデータを改ざんする。	2	2	2	C	項番60と同じ				1	2	#3-9	63,64,68,70
71		悪意ある第三者が、データヒストリアンからEWSへ不正にアクセスする。 ※不正アクセスは「プロセス不正実行」を含む。					項番11と同じ				2			
72	3-2	悪意ある第三者が、EWSからコントローラの設定(閾値等)やプログラムを改ざんする。	2	2	2	C	項番62と同じ				1	2	#3-10	63,64,71,72
73		**侵入口=HMI** 内部者の過失により、マルウェアに感染したUSB媒体をHMIに接続して、HMIがマルウェアに感染する。 ※内部者のため故意の「不正媒体接続」の脅威はない前提。					項番14と同じ				1 ※2			
74	3-1	マルウェアが、HMIからコントローラへ不適切な目標値を設定し、品質基準を満たさない製品が製造される。	2	3	2	B	項番56と同じ				1	1	#3-11	73,74
75	3-3	マルウェアが、HMIのプログラムやデータを改ざんする。	2	3	2	B	項番57と同じ				1	1	#3-12	73,75
76		**侵入口=制御サーバ** 内部者の過失により、マルウェアに感染したUSB媒体を制御サーバに接続して、制御サーバがマルウェアに感染する。 ※内部者のため故意の「不正媒体接続」の脅威はない前提。					項番47と同じ				2 ※2			
77	3-1	マルウェアが、制御サーバからコントローラへ不適切な目標値を設定し、品質基準を満たさない製品が製造される。	2	2	2	C	項番59と同じ				1	2	#3-13	76,77
78	3-3	マルウェアが、制御サーバのプログラムやデータを改ざんする。	2	2	2	C	項番60と同じ				1	2	#3-14	76,78
79		**侵入口=EWS** 内部者の過失により、マルウェアに感染したUSB媒体をEWSに接続して、EWSがマルウェアに感染する。 ※内部者のため故意の「不正媒体接続」の脅威はない前提。					項番16と同じ				1 ※2			
80	3-2	マルウェアが、EWSからコントローラの設定(閾値等)やプログラムを改ざんする。	2	3	2	B	項番62と同じ				1	1	#3-15	79,80
X														

【注】
※1 対策の評価においては、「9.4節 ゾーニング対策における各種設定」を参照して実施することが望ましい。
※2 対策の評価においては、「9.5節 外部記憶媒体におけるセキュリティ対策」を参照して実施することが望ましい。

表 4-10 事業被害ベースのリスク分析シート(ハイブリット版)

4. 製造停止の発生

項番	攻撃シナリオ	攻撃ツリー／攻撃ステップ	評価指標 脅威レベル	脆弱性レベル	事業被害レベル	リスク値	対策 防御 侵入／拡散段階	防御 目的遂行段階	検知／被害把握	事業継続	対策レベル 攻撃ステップ	対策レベル 攻撃ツリー	攻撃ツリー番号 攻撃ツリー番号	攻撃ツリー番号 構成ステップ(項番)
	4-1 4-2 4-3 4-4	4-1:適切でない目標値の入力により、製造設備の制御が異常となり、安全のためプロセスを停止する。 4-2:設定(閾値等)やプログラムの改ざんにより、製造設備の制御が異常となり、安全のためプロセスを停止する。 4-3:データやプログラムの改ざんにより、製造設備が異常な動作をするようになり、安全のためプロセスを停止する。 4-4:破壊型マルウェアやランサムウェアへの感染により、製造設備が監視操作不能となり、監視制御ができなくなり安全のためプロセスを停止する。												
81		**侵入口=情報NW** 悪意ある第三者が、情報NWからFWに不正アクセスする。 ※不正アクセスは「プロセス不正実行」(特権昇格)を含む。対策も2つの脅威への対策をマージ。斜体が「プロセス不正実行」のもの。					項番1と同じ				2 ※1			
82		悪意ある第三者が、FWを経由してHMIへ不正にアクセスする。 ※不正アクセスは「プロセス不正実行」を含む。					項番2と同じ				2			
83	4-1	悪意ある第三者が、HMIからコントローラへ不適切な目標値を設定し、製造設備が異常となり、製造システムの非常停止が必要になる。	2	2	1	D	セグメント分割／ゾーニング データ署名 重要操作の承認	(同左) (同左) (同左)	ログ収集・分析 統合ログ管理システム		1	2	#4-1	81,82,83
84	4-3	悪意ある第三者が、HMIのプログラムやデータを改ざんする。	2	2	1	D	権限管理 アクセス制御 データ署名	(同左) (同左) (同左)	機器異常検知 ログ収集・分析 統合ログ管理システム	データバックアップ	1	2	#4-2	81,82,84
85	4-4	悪意ある第三者が、HMIに破壊型マルウェア(ランサムウェア等)を感染させる。制御システムの監視操作ができなくなる。	2	2	1	D	アンチウイルス ホワイトリストによるプロセスの起動制限 パッチ適用 脆弱性回避 データ署名	*権限管理* *アクセス制御*	機器異常検知 機器死活監視 ログ収集・分析 統合ログ管理システム	*データバックアップ*	1	2	#4-3	81,82,85
86		悪意ある第三者が、FWを経由して制御サーバへ不正にアクセスする。 ※不正アクセスは「プロセス不正実行」(特権昇格)を含む。					項番25と同じ				2			
87	4-1	悪意ある第三者が、制御サーバからコントローラへ不適切な目標値を設定し、製造設備が異常となり、製造システムの非常停止が必要になる。	2	2	1	D	セグメント分割／ゾーニング データ署名 重要操作の承認	(同左) (同左) (同左)	ログ収集・分析 統合ログ管理システム		1	2	#4-4	81,86,87
88	4-3	悪意ある第三者が、制御サーバのプログラムやデータを改ざんする。	2	2	1	D	権限管理 アクセス制御 データ署名	○ (同左) (同左) (同左)	機器異常検知 ログ収集・分析 統合ログ管理システム	データバックアップ	2	2	#4-5	81,86,88
89		悪意ある第三者が、FWを経由してEWSへ不正にアクセスする。 ※不正アクセスは「プロセス不正実行」(特権昇格)を含む。					項番4と同じ				1			
90	4-2	悪意ある第三者が、EWSからコントローラの設定(閾値等)やプログラムを改ざんする。	2	2	1	D	権限管理 アクセス制御 データ署名	(同左) (同左) (同左)	機器異常検知 ログ収集・分析 統合ログ管理システム	データバックアップ	1	2	#4-6	81,89,90
91		**侵入口=監視端末** 悪意ある第三者が、監視端末からデータヒストリアン(中継)に不正アクセスする。 ※不正アクセスは「プロセス不正実行」(特権昇格)を含む。対策も2つの脅威への対策をマージ。斜体が「プロセス不正実行」のもの。					項番7と同じ				2 ※1			
92		悪意ある第三者が、データヒストリアン(中継)からデータヒストリアンへ不正にアクセスする。 ※不正アクセスは「プロセス不正実行」を含む。					項番8と同じ				2			
93		悪意ある第三者が、データヒストリアンからHMIへ不正にアクセスする。 ※不正アクセスは「プロセス不正実行」を含む。					項番9と同じ				2			
94	4-1	悪意ある第三者が、HMIからコントローラへ不適切な目標値を設定し、製造設備が異常となり、製造システムの非常停止が必要になる。	2	2	1	D	項番83と同じ				1	2	#4-7	91,92,93,94
95	4-3	悪意ある第三者が、HMIのプログラムやデータを改ざんする。	2	2	1	D	項番84と同じ				1	2	#4-8	91,92,93,95
96	4-4	悪意ある第三者が、HMIに破壊型マルウェア(ランサムウェア等)を感染させる。制御システムの監視操作ができなくなる。	2	2	1	D	項番85と同じ				1	2	#4-9	91,92,93,96
97		悪意ある第三者が、データヒストリアンから制御サーバへ不正にアクセスする。 ※不正アクセスは「プロセス不正実行」を含む。					項番37と同じ				2			
98	4-1	悪意ある第三者が、制御サーバからコントローラへ不適切な目標値を設定し、製造設備が異常となり、製造システムの非常停止が必要になる。	2	2	1	D	項番87と同じ				1	2	#4-10	91,92,97,98
99	4-3	悪意ある第三者が、制御サーバのプログラムやデータを改ざんする。	2	2	1	D	項番88と同じ				1	2	#4-11	91,92,97,99
100		悪意ある第三者が、データヒストリアンからEWSへ不正にアクセスする。 ※不正アクセスは「プロセス不正実行」を含む。					項番11と同じ				2			
101	4-2	悪意ある第三者が、EWSからコントローラの設定(閾値等)やプログラムを改ざんする。	2	2	1	D	項番90と同じ				1	2	#4-12	91,92,100,101
102		**侵入口=HMI** 内部者の過失により、マルウェアに感染したUSB媒体をHMIに接続して、HMIがマルウェアに感染する。 ※内部者のため故意の「不正媒体接続」の脅威はない前提。					項番14と同じ				1 ※2			
103	4-1	マルウェアが、HMIからコントローラへ不適切な目標値を設定し、製造設備が異常となり、製造システムの非常停止が必要になる。	2	3	1	D	セグメント分割／ゾーニング データ署名 重要操作の承認	(同左) (同左) (同左)	ログ収集・分析 統合ログ管理システム		1	1	#4-13	102,103
104	4-3	マルウェアが、HMIのプログラムやデータを改ざんする。	2	3	1	D	権限管理 アクセス制御 データ署名	(同左) (同左) (同左)	機器異常検知 ログ収集・分析 統合ログ管理システム	データバックアップ	1	1	#4-14	102,104
105	4-4	破壊型マルウェア(ランサムウェア等)により、データが破壊される。制御システムの監視操作ができなくなる。	2	3	1	D	アンチウイルス ホワイトリストによるプロセスの起動制限 パッチ適用 脆弱性回避 データ署名	*権限管理* *アクセス制御*	機器異常検知 機器死活監視 ログ収集・分析 統合ログ管理システム	*データバックアップ*	1	1	#4-15	102,105
106		**侵入口=制御サーバ** 内部者の過失により、マルウェアに感染したUSB媒体を制御サーバに接続して、制御サーバがマルウェアに感染する。 ※内部者のため故意の「不正媒体接続」の脅威はない前提。					項番47と同じ				2 ※2			
107	4-1	マルウェアが、制御サーバからコントローラへ不適切な目標値を設定し、製造設備が異常となり、製造システムの非常停止が必要になる。	2	2	1	D	セグメント分割／ゾーニング データ署名 重要操作の承認	(同左) (同左) (同左)	ログ収集・分析 統合ログ管理システム		1	2	#4-16	106,107
108	4-3	マルウェアが、制御サーバのプログラムやデータを改ざんする。	2	2	1	D	権限管理 アクセス制御 データ署名	○ (同左) (同左) (同左)	機器異常検知 ログ収集・分析 統合ログ管理システム	データバックアップ	1	2	#4-17	106,108
109		**侵入口=EWS** 内部者の過失により、マルウェアに感染したUSB媒体をEWSに接続して、EWSがマルウェアに感染する。 ※内部者のため故意の「不正媒体接続」の脅威はない前提。					項番16と同じ				1 ※2			
110	4-2	マルウェアが、EWSからコントローラの設定(閾値等)やプログラムを改ざんする。	2	3	1	D	権限管理 アクセス制御 データ署名	(同左) (同左) (同左)	機器異常検知 ログ収集・分析 統合ログ管理システム	データバックアップ	1	1	#4-18	109,110
111	4-4	マルウェアが、HMIに感染する。破壊型マルウェア(ランサムウェア等)により、データが破壊される。制御システムの監視操作ができなくなる。	2	3	1	D	アンチウイルス ホワイトリストによるプロセスの起動制限 パッチ適用 脆弱性回避 データ署名	*権限管理* *アクセス制御*	機器異常検知 機器死活監視 ログ収集・分析 統合ログ管理システム	*データバックアップ*	1	1	#4-19	109,111
X														

【注】
※1 対策の評価においては、「9.4節 ゾーニング対策における各種設定」を参照して実施することが望ましい。
※2 対策の評価においては、「9.5節 外部記憶媒体におけるセキュリティ対策」を参照して実施することが望ましい。

表 4-10 事業被害ベースのリスク分析シート(ハイブリット版)

5. 機密情報の漏洩

項番	攻撃シナリオ	攻撃ツリー／攻撃ステップ	評価指標				対策				対策レベル		攻撃ツリー番号	
			脅威レベル	脆弱性レベル	事業被害レベル	リスク値	防御		検知／被害把握	事業継続	攻撃ステップ	攻撃ツリー	攻撃ツリー番号	構成ステップ（項番）
							侵入／拡散段階	目的遂行段階						
	5-1	5-1:制御システムに保存されている製造に関わる企業機密が窃取され、外部に漏洩する。												
112	5-1	**侵入口=情報NW** 悪意ある第三者が、情報NWからFWに不正アクセスする。 ※不正アクセスは「プロセス不正実行」(特権昇格)を含む。対策も2つの脅威への対策をマージ。斜体が「プロセス不正実行」のもの。					項番1と同じ				2 ※1			
113	5-1	悪意ある第三者が、FWを経由して制御サーバへ不正にアクセスする。 ※不正アクセスは「プロセス不正実行」(特権昇格)を含む。					項番25と同じ				2			
114	5-1	悪意ある第三者が、制御サーバ上のデータを窃取する。 (その後、逆ルートを辿り情報を持出す。)	2	2	3	B	権限管理 ○ (同左) アクセス制御 (同左) データ暗号化 (同左) DLP (同左)		ログ収集・分析 統合ログ管理システム		2	2	#5-1	112,113,114
115	5-1	悪意ある第三者が、FWを経由してEWSへ不正にアクセスする。 ※不正アクセスは「プロセス不正実行」(特権昇格)を含む。					項番4と同じ				1			
116	5-1	悪意ある第三者が、EWS上のデータを窃取する。 (その後、逆ルートを辿り情報を持出す。)	2	2	3	B	権限管理 (同左) アクセス制御 (同左) データ暗号化 (同左) DLP (同左)		ログ収集・分析 統合ログ管理システム		1	2	#5-2	112,115,116
117	5-1	**侵入口=監視端末** 悪意ある第三者が、監視端末からデータヒストリアン(中継)に不正アクセスする。 ※不正アクセスは「プロセス不正実行」(特権昇格)を含む。対策も2つの脅威への対策をマージ。斜体が「プロセス不正実行」のもの。					項番7と同じ				2 ※1			
118	5-1	悪意ある第三者が、データヒストリアン(中継)からデータヒストリアンへ不正にアクセスする。 ※不正アクセスは「プロセス不正実行」を含む。					項番8と同じ				2			
119	5-1	悪意ある第三者が、データヒストリアンから制御サーバへ不正にアクセスする。 ※不正アクセスは「プロセス不正実行」を含む。					項番37と同じ				2			
120	5-1	悪意ある第三者が、制御サーバ上のデータを窃取する。 (その後、逆ルートを辿り情報を持出す。)	2	2	3	B	項番114と同じ				1	2	#5-3	117,118,119,120
121	5-1	悪意ある第三者が、データヒストリアンからEWSへ不正にアクセスする。 ※不正アクセスは「プロセス不正実行」を含む。					項番11と同じ				2			
122	5-1	悪意ある第三者が、EWS上のデータを窃取する。 (その後、逆ルートを辿り情報を持出す。)	2	2	3	B	項番116と同じ				1	2	#5-4	117,118,121,122
X														

【注】
※1 対策の評価においては、「9.4節 ゾーニング対策における各種設定」を参照して実施することが望ましい。
※2 対策の評価においては、「9.5節 外部記憶媒体におけるセキュリティ対策」を参照して実施することが望ましい。

このページは空白です。

4.4. リスク値のまとめ

【作業 4.4】事業被害ベースのリスク分析で分析した攻撃ツリーのリスク値をまとめること。

【アウトプット 4.4】

事業被害ベースのリスク分析結果をまとめた例を以下に示す（表 4-11）。

表 4-11 事業被害ベースのリスク分析結果 リスク値まとめ表

リスク値	合計 攻撃ツリー数	事業被害シナリオ		攻撃ツリー数 （事業シナリオ毎）
A	10	1	広域での製品供給停止	2
		2	火災・爆発事故の発生	7
B	29	1	広域での製品供給停止	4
		2	火災・爆発事故の発生	16
		3	仕様不良製品の供給	3
		5	機密情報の漏洩	4
C	12	3	仕様不良製品の供給	12
D	19	4	製造停止の発生	19
E	0	-		0

侵入口ベースでリスク値（A,B）をまとめた例を以下に示す（表 4-12）。

表 4-12 事業被害ベースのリスク分析結果 リスク値まとめ表（侵入口ベース）

#	リスク値	侵入口	攻撃ツリー数	合計 攻撃ツリー数
1	A	HMI（物理的侵入）	4	9
2		EWS（物理的侵入）	5	
3	B	情報 NW〔→FW〕	11	29
4		監視端末→〔データヒストリアン（中継）〕	11	
5		HMI（物理的侵入）	1	
6		EWS（物理的侵入）	2	
7		制御サーバ（物理的侵入）	2	
8	C	（省略）	12	12
9	D	（省略）	19	19
10	E	（省略）	0	0

5. リスク分析の活用

5.1. 制御システムのリスク分析結果（リスク低減のための改善策）

【作業 5.1①】事業被害ベースのリスク分析結果から、リスク値 A と B の攻撃ツリーのリスクを低減するための対策を検討すること。

- ガイド本体「*7 章* リスク分析結果の解釈と活用法」で制御システムのリスクを効果的に低減する方法を解説している。

【アウトプット 5.1①】

リスク低減のための改善策を整理したものを次頁に示す（表 5-1）。

表 5-1 リスク低減のための改善策

#	対策資産	対象攻撃ステップ	現状の攻撃ツリーリスク値 (表 4-12 と対応)	現状の対策 （対象となる脅威への対策）	追加対策（対策の改善案、強化策）	追加対策後の 攻撃ツリー リスク値
1	HMI	内部者の過失により、マルウェアに感染した USB 媒体を HMI に接続して、HMI がマルウェアに感染する。	A 対象ツリー数=4 (表 4-12#1)	なし	・ホワイトリストの適用 （脆弱性レベル 3→2）	B 対象ツリー数=4
2			B 対象ツリー数=1 (表 4-12#6)			C 対象ツリー数=1
3	EWS	内部者の過失により、マルウェアに感染した USB 媒体を EWS に接続して、EWS がマルウェアに感染する。	A 対象ツリー数=5 (表 4-12#2)	なし	・ホワイトリストの適用 （脆弱性レベル 3→2）	B 対象ツリー数=5
4			B 対象ツリー数=2 (表 4-12#5)			C 対象ツリー数=2
5	ファイアウォール（FW）	悪意ある第三者が、ファイアウォールに不正アクセスする。	B 対象ツリー数=11 (表 4-12#3)	・セキュリティパッチの適用 ・利用者の認証(パスワード)	（案 1） ・ファイアウォールの管理者認証の強化。 画面へのアクセスを踏み台サーバ経由に限定する、2 要素認証を利用するといった追加対策を講じる。 （脆弱性レベル 2→1） （案 2） ・管理 I/F を情報 NW から制御 NW へ変更し、情報 NW からの FW アクセスを不能にする。 （脆弱性レベル 2→1） ※FW のパッチ更新がオフラインで可能であることを前提とする。	C 対象ツリー数=11
6		悪意ある第三者が、DMZ 上のデータヒストリアン（中継）を経由して、制御 NW 上の資産に不正アクセスする。	B 対象ツリー数=11 (表 4-12#4)	・必要最低限の通信先の制限 （IP パケットレベルの制限）	「*9.4 節* ゾーニング対策における各種設定」を参照して、強化策を検討する。具体的には、一方向ゲートウェイを導入すれば、対象ツリー全てのリスク値を B から C へ低減可能。 （脆弱性レベル 2→1）	C 対象ツリー数=11
7	制御サーバ	内部者の過失により、マルウェアに感染した USB 媒体を制御サーバに接続して、制御サーバがマルウェアに感染する。	B 対象ツリー数=2 (表 4-12#7)	・ホワイトリストによる不正プロセスの実行抑止。	（追加対策無し）	B 対象ツリー数=2

【作業 5.1②】対策実施前と実施後でリスク値がどのように変わったかをまとめること。

【アウトプット 5.1②】

対策実施前と後でのツリーのリスク値の分布を以下に示す（表 5-2）。また、攻撃ルート一覧表とリスク値の変化をまとめたシートを次頁に示す（表 5-3）。

表 5-2 対策実施前と後でのツリーのリスク値の分布

リスク値	現状 攻撃ツリー数	改善後 攻撃ツリー数
A	9	0
B	27	11
C	12	27
D	19	17
E	0	12

表 5-3 攻撃ルート一覧表と対策前・対策後リスク値の変化（抜粋）

		誰が	どこから	どうやって						対策前				対策後			
攻撃ツリー番号#	シナリオ番号#	攻撃者	侵入口	経由1	経由2	経由3	攻撃拠点	攻撃対象	最終攻撃	脅威	脆弱性	事業被害	リスク値	脅威	脆弱性	事業被害	リスク値
1-1	1-1	悪意のある第三者	情報NW	FW			HMI	コントローラ	広域供給停止操作を実行する。	2	2	3	B	2	1	3	C
1-2	1-1	悪意のある第三者	監視端末	データヒストリアン(中継)	データヒストリアン		HMI	コントローラ	広域供給停止操作を実行する。	2	2	3	B	2	1	3	C
1-3	1-1	内部関係者(過失)	HMI(物理的侵入)				HMI	コントローラ	広域供給停止操作を実行する。	2	3	3	A	2	2	3	B
1-4	1-2	悪意のある第三者	情報NW	FW	EWS		コントローラ(M)	コントローラ(S)	供給停止コマンドを不正送信する。	2	2	3	B	2	1	3	C
1-5	1-2	悪意のある第三者	監視端末	データヒストリアン(中継)	データヒストリアン	EWS	コントローラ(M)	コントローラ(S)	供給停止コマンドを不正送信する。	2	2	3	B	2	1	3	C
1-6	1-2	内部関係者(過失)	EWS(物理的侵入)				コントローラ(M)	コントローラ(S)	供給停止コマンドを不正送信する。	2	3	3	A	2	2	3	B
2-1	2-1	悪意のある第三者	情報NW	FW			HMI	コントローラ	コントローラに不適切な目標値を設定する。	2	2	3	B	2	1	3	C
2-2	2-1	悪意のある第三者	情報NW	FW			制御サーバ	コントローラ	コントローラに不適切な目標値を設定する。	2	2	3	B	2	1	3	C
2-3	2-1	悪意のある第三者	監視端末	データヒストリアン(中継)	データヒストリアン		HMI	コントローラ	コントローラに不適切な目標値を設定する。	2	2	3	B	2	1	3	C
2-4	2-1	悪意のある第三者	監視端末	データヒストリアン(中継)	データヒストリアン		制御サーバ	コントローラ	コントローラに不適切な目標値を設定する。	2	2	3	B	2	1	3	C
2-5	2-1	内部関係者(過失)	HMI(物理的侵入)				HMI	コントローラ	コントローラに不適切な目標値を設定する。	2	3	3	A	2	2	3	B
2-6	2-1	内部関係者(過失)	制御サーバ(物理的侵入)				制御サーバ	コントローラ	コントローラに不適切な目標値を設定する。	2	2	3	B	2	2	3	B
2-7	2-2	悪意のある第三者	情報NW	FW			EWS	コントローラ	コントローラの設定(閾値等)やプログラムを改ざんする。	2	2	3	B	2	1	3	C
2-8	2-2	悪意のある第三者	監視端末	データヒストリアン(中継)	データヒストリアン		EWS	コントローラ	コントローラの設定(閾値等)やプログラムを改ざんする。	2	2	3	B	2	1	3	C
2-9	2-2	内部関係者(過失)	EWS(物理的侵入)				EWS	コントローラ	コントローラの設定(閾値等)やプログラムを改ざんする。	2	3	3	A	2	2	3	B
2-10	2-3	悪意のある第三者	情報NW	FW			HMI	HMI	HMIのデータやプログラムを改ざんする。	2	2	3	B	2	1	3	C
2-11	2-3	悪意のある第三者	情報NW	FW			制御サーバ	制御サーバ	制御サーバのデータやプログラムを改ざんする。	2	2	3	B	2	1	3	C
2-12	2-3	悪意のある第三者	監視端末	データヒストリアン(中継)	データヒストリアン		HMI	HMI	HMIのデータやプログラムを改ざんする。	2	2	3	B	2	1	3	C
2-13	2-3	悪意のある第三者	監視端末	データヒストリアン(中継)	データヒストリアン		制御サーバ	制御サーバ	制御サーバのデータやプログラムを改ざんする。	2	2	3	B	2	1	3	C
2-14	2-3	内部関係者(過失)	HMI(物理的侵入)				HMI	HMI	HMIのデータやプログラムを改ざんする。	2	3	3	A	2	2	3	B
2-15	2-3	内部関係者(過失)	制御サーバ(物理的侵入)				制御サーバ	制御サーバ	制御サーバのデータやプログラムを改ざんする。	2	2	3	B	2	2	3	B
2-16	2-4	悪意のある第三者	情報NW	FW			HMI	制御NW(フ)	ネットワーク設定を改ざんし、通信不能にする。	2	2	3	B	2	1	3	C
2-17	2-4	悪意のある第三者	情報NW	FW			HMI	制御NW(フ)	マルウェアに感染させて不正通信を発生させ、通信不能にする。	2	2	3	B	2	1	3	C
2-18	2-4	悪意のある第三者	監視端末	データヒストリアン(中継)	データヒストリアン		HMI	制御NW(フ)	ネットワーク設定を改ざんし、通信不能にする。	2	2	3	B	2	1	3	C
2-19	2-4	悪意のある第三者	監視端末	データヒストリアン(中継)	データヒストリアン		HMI	制御NW(フ)	マルウェアに感染させて不正通信を発生させ、通信不能にする。	2	2	3	B	2	1	3	C
2-20	2-4	内部関係者(過失)	HMI(物理的侵入)				HMI	制御NW(フ)	ネットワーク設定を改ざんし、通信不能にする。	2	3	3	A	2	2	3	B
2-21	2-4	内部関係者(過失)	HMI(物理的侵入)				HMI	制御NW(フ)	マルウェアに感染させて不正通信を発生させ、通信不能にする。	2	3	3	A	2	2	3	B
2-22	2-4	内部関係者(過失)	EWS(物理的侵入)				EWS	制御NW(フ)	ネットワーク設定を改ざんし、通信不能にする。	2	3	3	A	2	2	3	B
2-23	2-4	内部関係者(過失)	EWS(物理的侵入)				EWS	制御NW(フ)	マルウェアに感染させて不正通信を発生させ、通信不能にする。	2	3	3	A	2	2	3	B

このページは空白です。

更新履歴

2017 年 10 月 2 日	初版
2018 年 10 月 15 日	第 2 版
2018 年 10 月 31 日	誤字修正
2020 年 3 月 31 日	第 2 版(2020 年 3 月版) P10. 表 1-1、P93. 表 5-4 追加

本書は、以下の URL からダウンロード可能です。

https://www.ipa.go.jp/security/controlsystem/riskanalysis.html

IPA 独立行政法人情報処理推進機構
セキュリティセンター

〒113-6591
東京都文京区本駒込二丁目 28 番 8 号
文京グリーンコート　センターオフィス
TEL: 03-5978-7527　FAX: 03-5978-7552
https://www.ipa.go.jp/security/