制御システムに対する
リスク分析の実施例

～制御システムのセキュリティリスク分析ガイド　別冊～

2017 年 10 月

IPA 独立行政法人情報処理推進機構
技術本部 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」では、セキュリティリスク分析の本質の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完全な実施事例を解説、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、多くの制御システム事業者が、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	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

1. 本書の構成

本書では、「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）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いる。

- **本書のリスク分析対象システム**
  ガイド本体の 3 章 図 3-6 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。

  - 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 3 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 2 章で示すアウトップットを丸数字(①～⑫)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。

  また、図中の【アウトプット】に示された①～⑫について 2 章で例示するが、それらの一覧を表 1-1 に示す。

このページは空白です。

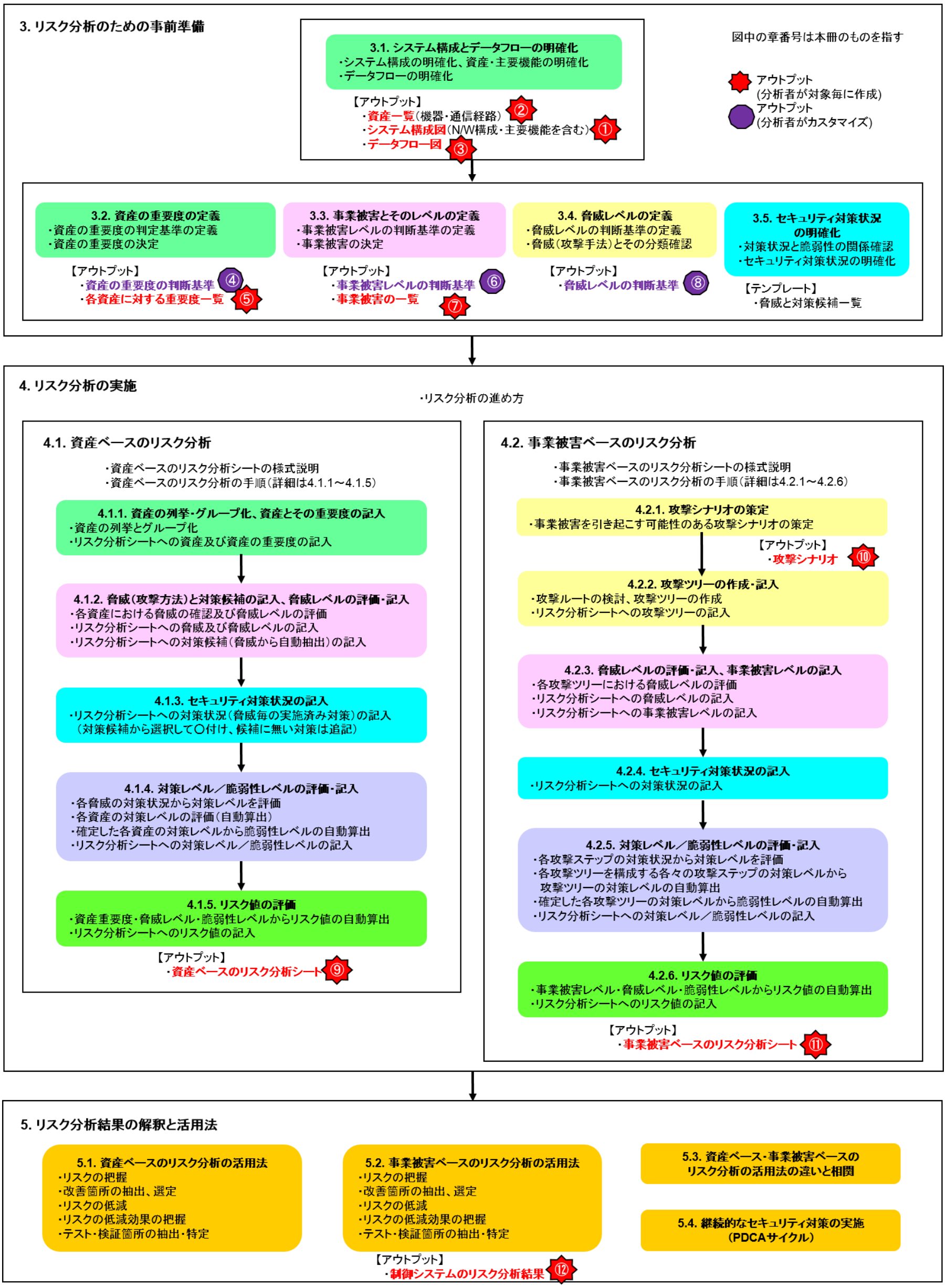

図 1-1 リスク分析の流れと成果物

このページは空白です。

表 1-1 アウトプットの一覧

番号[1]	アウトプット	ガイド本体の図表との関係
①	システム構成図	ガイド本体「図 3-6 典型的な制御システムの構成図（分類 3：DMZ）」を基に作成。
②	資産一覧	ガイド本体「表 3-8 典型的な制御システム構成における資産とその役割（1/2）、表 3-9 典型的な制御システム構成における資産とその役割（2/2）、ガイド本体「4.2 節【補足 1】システム構成資産の追加調査結果」を基に作成。
③	データフロー図	ガイド本体「図 3-11 典型的な制御システム（分類 3：DMZ）におけるデータフローの例」を基に作成。
④	資産の重要度の判断基準	ガイド本体「表 3-10 資産の重要度の判断基準の定義例（1）」を基に作成。
⑤	各資産に対する重要度一覧	各資産の重要度は、ガイド本体「表 3-15 資産の重要度の検討例（1/3）、表 3-16 資産の重要度の検討例（2/3）、表 3-17 資産の重要度の検討例（3/3）」を基に作成。
⑥	事業被害レベルの判断基準	本冊「表 3-18 事業被害レベルの判断基準の定義例」を基に作成。
⑦	事業被害の一覧	新規提示資料。
⑧	脅威レベルの判断基準	ガイド本体「表 3-21 脅威レベルの判断基準の定義例」を基に作成。
⑨	資産ベースのリスク分析シート	新規提示資料。
⑩	攻撃シナリオ	新規提示資料。
⑪	事業被害ベースのリスク分析シート	新規提示資料。
⑫	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）	新規提示資料。

[1] 図 1-1 のアウトプットの丸数字、2 章の丸数字の見出しと対応している。

2. リスク分析のアウトプット例

図 1-1 で説明したリスク分析の各ステップで作成するアウトプット例を、以下①～⑫に示す。

① システム構成図

リスク分析を行う対象であるモデルシステムのシステム構成図を図 2-1 に示す。分析対象のモデルシステムは、ガイド本体 3.1.2 節における典型的な制御システム構成の中から、DMZ 構成を用いた分類 3 のシステム構成としている。

図中の各資産は、常時稼働している定常時稼働機器と、通常は稼働せず一時的にしか稼働しない非定常稼働機器に分けられている。本書では、ガイド本体と同様に非定常稼働機器（パッチサーバ、EWS、保守用 PC）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。

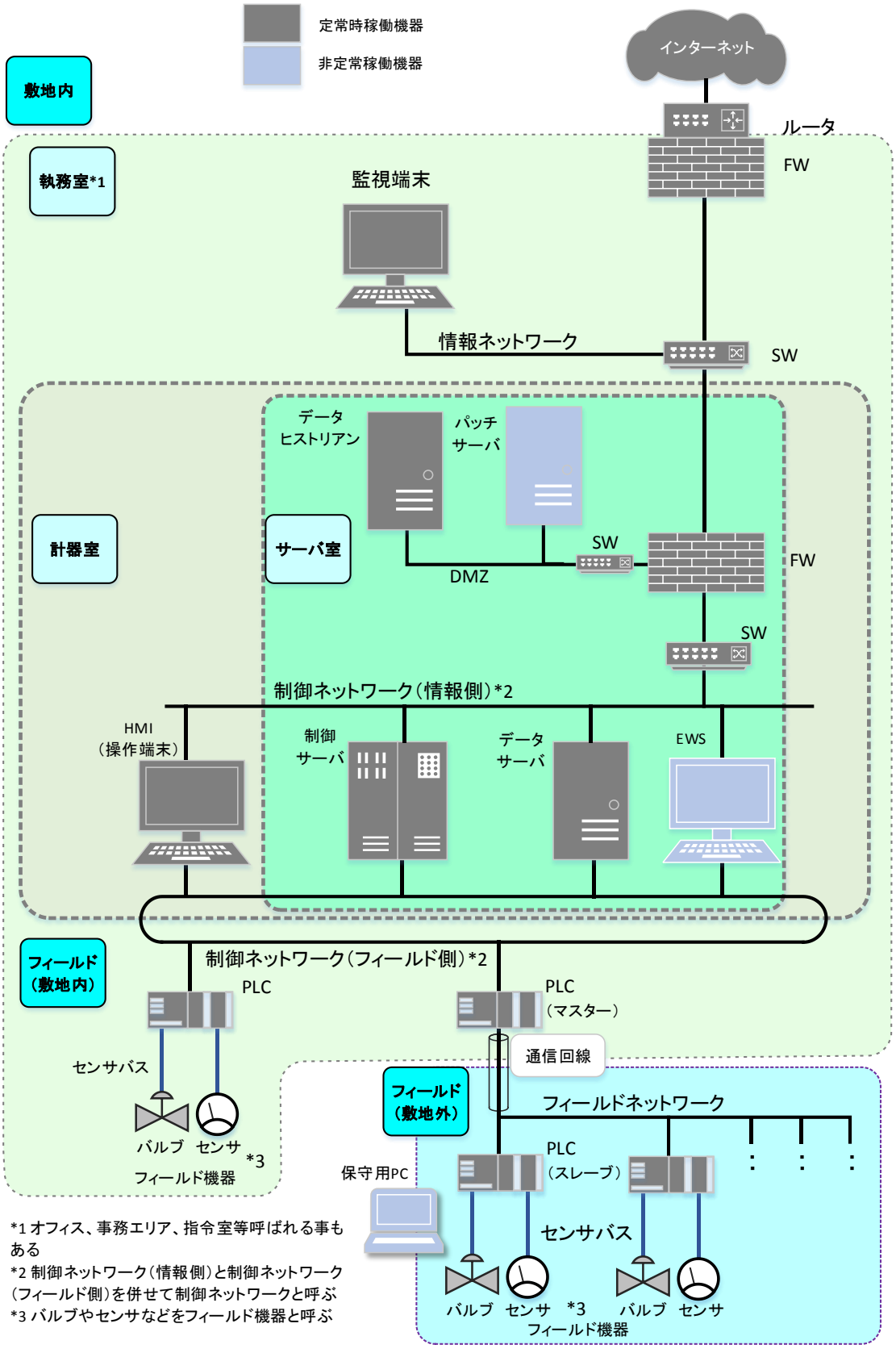
定常時稼働機器
非定常稼働機器
敷地内
インターネット
ルータ
FW
執務室*1
監視端末
情報ネットワーク
SW
データ
ヒストリアン
パッチ
サーバ
計器室
サーバ室
SW
DMZ
FW
SW
制御ネットワーク（情報側）*2
HMI
（操作端末）
制御
サーバ
データ
サーバ
EWS
フィールド
（敷地内）
制御ネットワーク（フィールド側）*2
PLC
PLC
（マスター）
通信回線
センサバス
フィールド
（敷地外）
フィールドネットワーク
PLC
（スレーブ）
保守用PC
センサバス
バルブ
センサ
*3
フィールド機器
バルブ
センサ
*3
バルブ
センサ
フィールド機器
*1 オフィス、事務エリア、指令室等呼ばれる事もある
*2 制御ネットワーク（情報側）と制御ネットワーク（フィールド側）を併せて制御ネットワークと呼ぶ
*3 バルブやセンサなどをフィールド機器と呼ぶ

図 2-1 システム構成図

このページは空白です。

②　資産一覧

図 2-1 システム構成図に登場する定常時稼働資産（定常時稼働機器）の一覧と、その資産の役割と機能、影響範囲と事業継続への影響、セキュリティ対策を説明したものを、表 2-1 に示す。

表 2-1 資産一覧、役割・機能、影響範囲・事業継続への影響、セキュリティ対策

資産		役割・機能	影響範囲・事業継続への影響	物理的・運用的セキュリティ対策	技術的セキュリティ対策
1	監視端末	・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。	・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。		・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。
2	HMI（操作端末）	・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（発行自体は制御サーバ経由）。	・機能停止しても、制御サーバや設備・機器の直接操作により事業継続が可能。	・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。	・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。
3	ファイアウォール、スイッチ（DMZ 内）、DMZ	・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（ファイアウォール）。 ・複数のネットワークを集線、中継する機器（スイッチ）。	・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（ファイアウォール）。 ・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（ファイアウォール、スイッチ）。	・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。	・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（ファイアウォール、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。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、スイッチ）。 ・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。 情報ネットワーク ⇔ データヒストリアン（DMZ） データヒストリアン（DMZ） ⇔ データサーバ（制御ネットワーク（情報側）） ・ファイアウォールや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。

資産		役割・機能	影響範囲・事業継続への影響	物理的・運用的セキュリティ対策	技術的セキュリティ対策
4	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）	・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。 ・IP 系プロトコルを利用している。	・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（スイッチ）。	・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。	・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）。
5	データヒストリアン	・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。 ・データサーバより静的なデータを扱う。	・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。	・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。	・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。 ・Web サーバが稼動しており、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。
6	制御サーバ	・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。 ・広域供給停止コマンドを発行可能。	・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。	・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。	・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。

資産		役割・機能	影響範囲・事業継続への影響	物理的・運用的セキュリティ対策	技術的セキュリティ対策
7	データサーバ	・制御ネットワーク上にありプロセス値を収集するサーバ。 ・更に PLC から届いたプロセス値を転送する。 ・営業秘密（レシピ）をサーバ上（DB 上）に保存している。 ・外部記憶媒体（主に USB メモリ）をデータサーバに接続して外部からデータを持ち込む運用がある。	・改ざんされると、不正なデータが HMI（操作端末）に表示され、オペレータが誤って広域供給停止コマンドを発行する可能性のある、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。	・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。	・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。 ・バックアップ間隔は週次、3 世代分を保管。
8	制御ネットワーク（フィールド側）	・自ネットワーク及びフィールドネットワーク上の機器（PLC）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。		・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。	・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、スイッチへのリモート管理機能は禁止されている。 ・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。
9	フィールドネットワーク	・PLC（マスター）と PLC（スレーブ）間のネットワーク。		・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。	
10	PLC、PLC（マスター）	・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フィールド機器。 ・制御サーバやデータサーバと PLC との間の通信を中継する PLC も存在し、中継する側を「PLC（マスター）」、中継される側を「PLC（スレーブ）」と示す。 ・PLC（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 PLC（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、イーサネット以外の方法で接続している。	・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。 ・PLC（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 PLC（スレーブ）が存在。	・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。	・OS は独自 OS とし、PLC 用のアンチウィルス対策製品は存在しない。 ・PLC 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。

資産		役割・機能	影響範囲・事業継続への影響	物理的・運用的セキュリティ対策	技術的セキュリティ対策
11	PLC（スレーブ）	・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フィールド機器。 ・PLC（マスター）の下位システムで、PLC（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。	・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。	・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。	・OS は独自 OS とし、PLC 用のアンチウィルス対策製品は存在しない。 ・PLC 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。

③ データフロー図

モデルシステムのデータフローを図 2-2 に示す（ガイド本体「図 3-11 典型的な制御システム（分類 3：DMZ）におけるデータフローの例」と同一）。具体的なデータフローの説明については、ガイド本体「3.1.3.節 データフローの明確化」を参照すること。

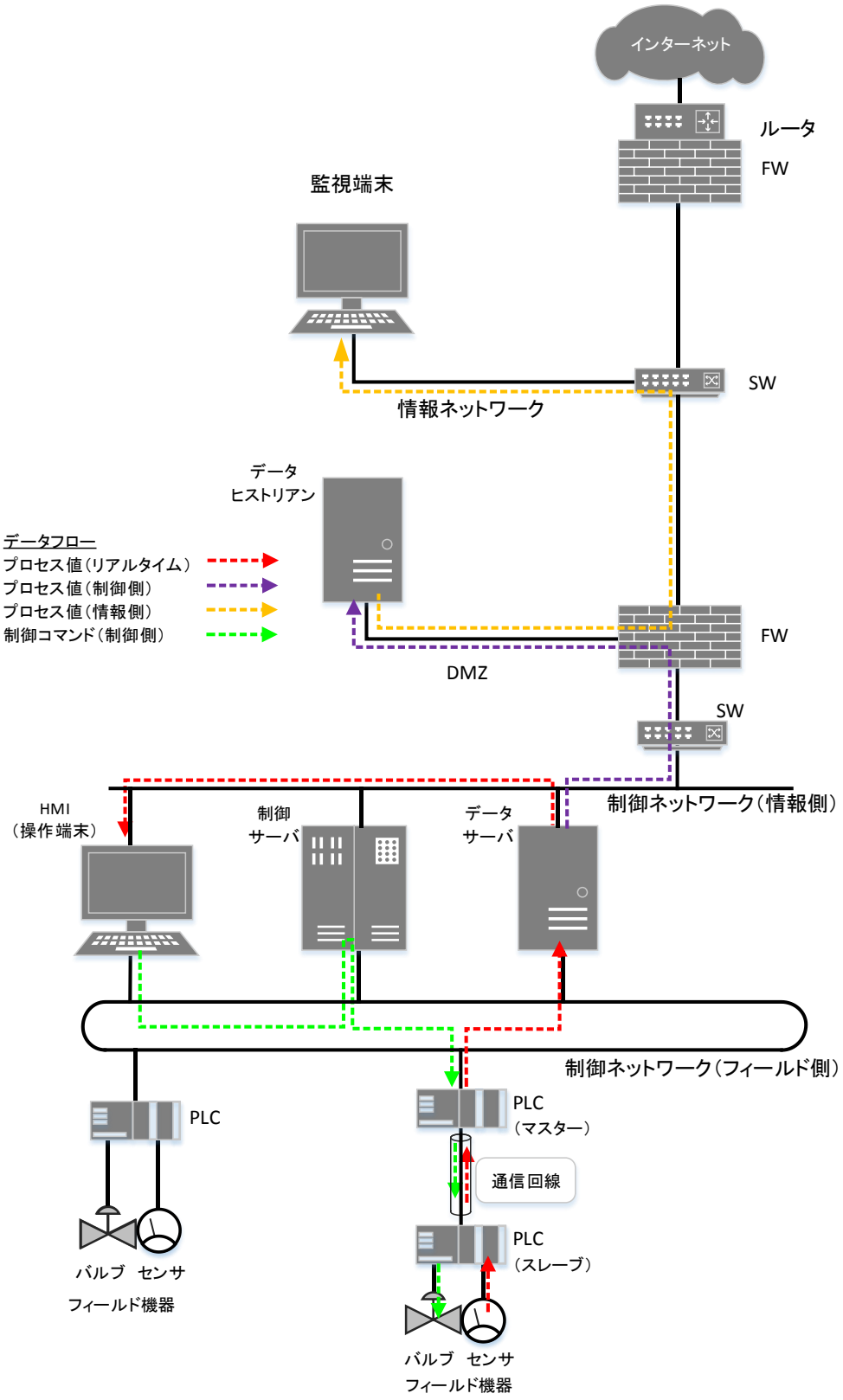
インターネット
ルータ
FW
監視端末
SW
情報ネットワーク
データ
ヒストリアン
データフロー
プロセス値（リアルタイム）
プロセス値（制御側）
プロセス値（情報側）
制御コマンド（制御側）
FW
DMZ
SW
制御ネットワーク（情報側）
HMI
（操作端末）
制御
サーバ
データ
サーバ
制御ネットワーク（フィールド側）
PLC
PLC
（マスター）
通信回線
PLC
（スレーブ）
バルブ センサ
フィールド機器
バルブ センサ
フィールド機器

図 2-2 データフロー図

④ 資産の重要度の判断基準

資産の重要度の判断基準を検討した結果を表 2-2 に示す(ガイド本体「表 3-10 資産の重要度の判断基準の定義例(1)」を基に作成している)。資産が異なる評価点となる判断基準に該当する場合は、重要度の高い評価点とする。

表 2-2 資産の重要度の判断基準の定義

評価点	判断基準
3	・資産が攻撃された場合、システムが長期間停止する恐れがある。 ・資産から情報が漏えいした場合、巨額の損失が発生する恐れがある。 ・資産が攻撃された場合、大規模の人的／環境被害が発生する恐れがある。
2	・資産が攻撃された場合、システムが一定期間停止する恐れがある。 ・資産から情報が漏えいした場合、ある程度の損失が発生する恐れがある。 ・資産が攻撃された場合、中規模の人的／環境被害が発生する恐れがある。
1	・資産が攻撃された場合、システムが短期間停止する恐れがある。 ・資産から情報が漏えいした場合、小額の損失が発生する恐れがある。 ・資産が攻撃された場合、小規模の人的／環境被害が発生する恐れがある。

⑤ 各資産に対する重要度一覧

表 2-2 資産の重要度の判断基準の定義に従い資産に対して重要度を検討した結果を表 2-3 に示す。個々の資産についてはガイド本体と同じ重要度を設定している。重要度をどのように評価したかの具体的な説明については、ガイド本体「3.2.節【補足】CIA 要件及び HSE 要件を考慮した資産の重要度の評価例」を参照すること。

表 2-3 資産一覧と重要度

資産		重要度
1	監視端末	2
2	HMI（操作端末）	3
3	ファイアウォール、スイッチ（DMZ 内）、DMZ	3
4	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）	3
5	データヒストリアン	2
6	制御サーバ	3
7	データサーバ	3
8	制御ネットワーク（フィールド側）	3
9	フィールドネットワーク	3
10	PLC、PLC（マスター）	3
11	PLC（スレーブ）	3

⑥ 事業被害レベルの判断基準

事業被害レベルの判断基準を検討した結果を表 2-4 に示す(ガイド本体「表 3-18 事業被害レベルの判断基準の定義例」を基に作成している)。事業被害が異なる評価点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(事業被害レベルが深刻な)評価点とする。

表 2-4 事業被害レベルの判断基準

評価点	判断基準
3	・発生した場合、被害範囲はシステム全体に及ぶ。 ・会社の経営上、致命的もしくは永続的な打撃を与える可能性がある。
2	・発生した場合、被害範囲がシステムの一部に限定される。 ・会社の経営上、大きなもしくは長期的な打撃を与える可能性がある。
1	・発生した場合、被害範囲はシステムの極一部に限定される。 ・会社の経営上、中程度以下もしくは一時的な打撃を与える可能性がある。

⑦ 事業被害の一覧

モデルシステムの事業被害を検討し、それぞれに事業被害レベルを設定したものを表 2-5 に示す。

表 2-5 事業被害の一覧表

#	事業被害	事業被害の概要		事業被害レベル
1	広域でのエネルギー供給停止	エネルギー製造・供給設備等へのサイバー攻撃により、広域において供給停止が発生し、社会に多大な影響を及ぼし、賠償費用等の高額な損失が生じると共に、当社の信頼が大きく低下する。		3
		1-1	制御 NW[2]が輻輳し、PLC に制御情報を伝える事ができなくなり、広域に及ぶ供給停止が発生する。	
		1-2	PLC に対して不正なコマンド（広域供給停止コマンド等）が送信され、広域に及ぶ供給停止が発生する。	
		1-3	重要な資産のデータやプログラムが改ざんされ資産の動作が異常となり、広域に及ぶ供給停止が発生する。	
		1-4	重要な資産の停止により、広域に及ぶ供給停止が発生する。	
2	限定地域でのエネルギー供給停止	エネルギー製造・供給設備等へのサイバー攻撃により、限定地域において供給停止が発生し、社会に影響を及ぼし、賠償費用等の損失が生じると共に、当社の信頼が低下する。		2
		2-1	フィールド NW[3]の輻輳により、PLC に制御情報を伝える事ができなくなり、限定地域において供給停止が発生する。	
		2-2	フィールド NW 上の資産のデータやプログラムが改ざんされ機器の動作が異常となり、限定地域において供給停止が発生する。	
		2-3	フィールド NW 上の重要な資産が停止し、限定地域において供給停止が発生する。	
3	営業秘密の漏洩	エネルギー製造設備等へのサイバー攻撃により、製造に関わる営業秘密が社外へ漏洩し、競合他社との差異化に影響を及ぼし、当社の競争力が低下する。		1
		3-1	データサーバ上の機密データが窃取され、情報漏洩が発生する。	

[2] 制御 NW：制御ネットワーク（フィールド側）
[3] フィールド NW：フィールドネットワーク

⑧ 脅威レベルの判断基準

モデルシステムを対象とした脅威レベルの判断基準の検討結果を表 2-6 に示す（ガイド本体「表 3-21　脅威レベルの判断基準の定義例」を基に作成している）。脅威の判断基準（攻撃の容易性、発生頻度等）で異なる評価点となる脅威に対しては、脅威レベルの高い（より深刻な脅威の）評価点とする。

表 2-6 脅威レベルの判断基準

評価点	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。 ・近未来に発生することが予想される。
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。 ・将来に渡って発生することが想定される。
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。 ・未来永劫に渡って発生することが想像しがたい。

⑨ 資産ベースのリスク分析シート

ガイド本体「4.1.節 資産ベースのリスク分析」で解説された手順に基づき、モデルシステムの資産ベースのリスク分析を実施した。アウトプットである資産ベースのリスク分析シートを表 2-7 に示す。

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。

- 分析対象の資産の重要度を分析シートに記載する。
  表 2-3 資産一覧と重要度 で定義済みである。

- 分析対象の資産にどのような脅威が想定されるか検討し、分析シートの脅威（攻撃手法）の列に記載する。
  ガイド本体 4.1.2.節（1）で示された脅威一覧のうち、分析対象の資産に発生する脅威を選択する。ここでの選択基準は、ガイド本体 4.1.2.節（2）（3）（4）での記載に準じている。

- 脅威に対する対策候補の一覧を分析シートに記載し、分析対象の資産での実施状況を分析シートに記載する。
  ガイド本体 4.1.2.節（5）で IPA の実績を基に脅威に対して有効と思われる対策候補の一覧を提示しているため、対策候補はそれを参照している。

- 分析対象の資産に対する脅威（攻撃方法）の脅威レベルを分析シートに記載する。
  表 2-6 脅威レベルの判断基準 に従い脅威レベルを記載する。

- 挙げられた対策候補に対して、実際のシステム（資産）を検証し、実施している対策は分析シートに“○”をつけ、対策の状況を把握する。また、対策候補の一覧にない対策を実施している場合は、それを分析シートに追記して“○”をつける。

- 分析対象の各脅威（攻撃方法）に対して対策レベル／脆弱性レベルを分析シートに記載する。
  ガイド本体 「表 4-23 対策レベルの具体的な判断基準（指針）の例」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。

- 分析対象の各脅威（攻撃方法）に対してリスク値を算出し、分析シートに記載する。

表 2-7 資産ベースのリスク分析シート

凡例: ○ 対策実施　× 対策未実施　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	—	**監視端末**	**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			**3**	**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			**3**	**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	○							2
4			**3**	**2**		**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レビュテーション メールフィルタリング	○ ○							2
5			**3**	**2**		**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				2
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					**2**		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			**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			**2**	**2**		**C**	窃盗	機器を窃盗する。	施錠管理	○	(同左)		(同左)				2
15			**3**	**3**		**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)						1
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			**3**	**2**		**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	○			2

表 2-7 資産ベースのリスク分析シート

凡例: ○ 対策実施　×　対策未実施　　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	—	**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) 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**		**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**	**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			**3**	**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							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**	**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							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			**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			**3**	**3**		**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 難読化 セキュア消去		(同左) (同左) (同左)						1
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		2
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		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							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							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**		**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 2-7 資産ベースのリスク分析シート

凡例: ○ 対策実施　×　対策未実施　　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 スイッチ(DMZ内) DMZ**	**3**	**2**		**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			**2**	**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**	**1**		**C**	窃盗	機器を窃盗する。	施錠管理	○	(同左)		(同左)				3
15			**3**	**3**		**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 難読化 セキュア消去		(同左) (同左) (同左)						1
16			**2**	**1**		**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、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**	**2**		**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		2
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			**3**	**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 2-7 資産ベースのリスク分析シート

凡例: ○ 対策実施　×　対策未実施　　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**		**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			**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			**1**	**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**		**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			**2**	**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**		**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)		施錠管理	○			2
15			**3**	**3**		**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 難読化 セキュア消去		(同左) (同左) (同左)						1
16			**2**	**2**		**B**	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**		**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			**3**	**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 2-7 資産ベースのリスク分析シート

凡例: ○ 対策実施　× 対策未実施　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	**データヒストリアン**	**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			**2**	**2**		**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	○ ○			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)		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			**3**	**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							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			**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**	**3**		**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	○	1
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			**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			**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			**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			**3**	**3**		**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)						1
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			**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 2-7 資産ベースのリスク分析シート

凡例: ○ 対策実施　×　対策未実施　　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	**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			**2**	**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**	**1**		**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				3
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**	**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			**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			**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			**2**	**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			**3**	**3**		**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 難読化 セキュア消去		(同左) (同左) (同左)						1
16			**2**	**2**		**B**	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			**3**	**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 2-7 資産ベースのリスク分析シート

凡例: ○ 対策実施　×　対策未実施　　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	**データサーバ**	**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			**2**	**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**	**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**	**1**		**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				3
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**	**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			**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			**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			**2**	**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			**3**	**3**		**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 難読化 セキュア消去		(同左) (同左) (同左)						1
16			**2**	**2**		**B**	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			**3**	**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 2-7 資産ベースのリスク分析シート

凡例: ○ 対策実施　×　対策未実施　　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			**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							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			**2**	**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			**3**	**3**		**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 難読化 セキュア消去		(同左) (同左) (同左)						1
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							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 2-7 資産ベースのリスク分析シート

凡例: ○ 対策実施　×　対策未実施　　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			**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)		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							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			**2**	**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			**3**	**3**		**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 難読化 セキュア消去		(同左) (同左) (同左)						1
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							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 2-7 資産ベースのリスク分析シート

凡例: ○ 対策実施　×　対策未実施　　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	PLC PLC(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			3	3		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 難読化 セキュア消去		(同左) (同左) (同左)						1
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 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			1	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		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			3	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 2-7 資産ベースのリスク分析シート

凡例: ○ 対策実施　× 対策未実施　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	PLC(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) 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			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 施錠管理	 ○			監視カメラ 侵入センサ				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。	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							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			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			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			3	2		A	窃盗	機器を窃盗する。	施錠管理	○	(同左)		(同左)				2
15			3	3		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 難読化 セキュア消去		(同左) (同左) (同左)						1
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 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			1	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		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			3	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

このページは空白です。

⑩ 攻撃シナリオ

ガイド本体「4.2.節 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、モデルシステムの事業被害を引き起こす攻撃シナリオを検討した。事業被害と攻撃シナリオの一覧（表 2-8）は、事業被害の一覧（表 2-5）を基に、各事業被害の項目ごとに、攻撃シナリオを整理したものであり、攻撃拠点、攻撃対象、最終攻撃の内容を記載している。さらに、各攻撃シナリオのリスク分析シート上の攻撃ツリー番号は、事業被害ベースのリスク分析シート（表 2-9）上の攻撃ツリーを示す攻撃ツリー番号との対応を示している。

表 2-8 事業被害を引き起こす攻撃シナリオ

<table>
<tr><th>#</th><th>事業被害</th><th colspan="5">事業被害の概要、攻撃シナリオ</th><th>事業被害レベル</th></tr>
<tr><td rowspan="5">1</td><td rowspan="5">広域でのエネルギー供給停止</td><td colspan="5">エネルギー製造・供給設備等へのサイバー攻撃により、広域において供給停止が発生し、社会に多大な影響を及ぼし、賠償費用等の高額な損失が生じると共に、当社の信頼が大きく低下する。</td><td rowspan="5">3</td></tr>
<tr><td rowspan="4">1-1</td><td colspan="4">制御 NW が輻輳し、PLC に制御情報を伝える事ができなくなり、広域に及ぶ供給停止が発生する。</td></tr>
<tr><td>攻撃拠点</td><td>攻撃対象</td><td>最終攻撃</td><td>リスク分析シート上の攻撃ツリー番号</td></tr>
<tr><td>HMI</td><td>制御 NW</td><td>攻撃者が、HMI から不正なコマンドにて制御 NW を輻輳させ、PLC への制御情報の伝達をできなくし、広域に及ぶ供給を停止させる。</td><td>#1-1,#1-5,#1-8</td></tr>
<tr><td>制御サーバ</td><td>制御 NW</td><td>攻撃者が、制御サーバから不正なコマンドにて制御 NW を輻輳させ、PLC への制御情報の伝達をできなくし、広域に及ぶ供給を停止させる。</td><td>#1-2,#1-6,#1-9</td></tr>
<tr><td>データサーバ</td><td>制御 NW</td><td>攻撃者が、データサーバから不正なコマンドにて制御 NW を輻輳させ、PLC への制御情報の伝達をできなくし、広域に及ぶ供給を停止させる。</td><td>#1-3,#1-4,#1-7,#1-10</td></tr>
</table>

#	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	1-2	PLC に対して不正なコマンド（広域供給停止コマンド等）が送信され、広域に及ぶ供給停止が発生する。			
			攻撃拠点	攻撃対象	最終攻撃	リスク分析シート上の攻撃ツリー番号
			HMI	PLC	攻撃者が、HMI から多数の PLC へ不正なコマンド（広域供給停止コマンド等）を発行し、広域に及ぶ供給を停止させる。	#1-11,#1-15,#1-18
			制御サーバ	PLC	攻撃者が、制御サーバから多数の PLC へ不正なコマンド（広域供給停止コマンド等）を発行し、広域に及ぶ供給を停止させる。	#1-12,#1-16,#1-19
			PLC（マスター）	PLC（スレーブ）	攻撃者が、PLC（マスター）から多数の PLC（スレーブ）へ不正なコマンド（広域供給停止コマンド等）を発行し、広域に及ぶ供給を停止させる。	#1-13,#1-14, #1-17,#1-20
		1-3	重要な資産のデータやプログラムが改ざんされ資産の動作が異常となり、広域に及ぶ供給停止が発生する。			
			攻撃拠点	攻撃対象	最終攻撃	リスク分析シート上の攻撃ツリー番号
			制御サーバ	PLC	攻撃者が、制御サーバ上のデータやプログラムが改ざんし、多数の PLC へ不正なコマンド（広域供給停止コマンド等）を発行させ、広域に及ぶ供給を停止させる。	#1-21,#1-26,#1-29
			データサーバ	HMI	攻撃者が、データサーバ上のデータを改ざんし、HMI から多数の PLC へ適切なコマンド発行ができず（不適切なコマンドが発行され）、広域に及ぶ供給を停止させる。	#1-22,#1-24, #1-27,#1-30
			PLC（マスター）	PLC（スレーブ）	攻撃者が、PLC（マスター）上のデータやプログラムが改ざんし、PLC（マスター）から多数の PLC（スレーブ）へ不正なコマンド（広域供給停止コマンド等）を発行させ、広域に及ぶ供給を停止させる。	#1-23,#1-25,#1-28,#1-31

#	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	1-4	重要な資産の停止により、広域に及ぶ供給停止が発生する。				
			攻撃拠点	攻撃対象	最終攻撃	リスク分析シート上の攻撃ツリー番号	
			HMI	HMI	攻撃者が、HMI の機能を停止させ多数の PLC に適切なコマンドを発行できなくなり、広域に及ぶ供給を停止させる。	#1-32,#1-38,#1-42	
			制御サーバ	制御サーバ	攻撃者が、制御サーバ上の機能を停止させ多数の PLC に適切なコマンドを発行できなくなり、広域に及ぶ供給を停止させる。	#1-33,#1-39,#1-43	
			データサーバ	HMI	攻撃者が、データサーバの機能を停止させ HMI から多数の PLC へ適切なコマンド発行ができず、広域に及ぶ供給を停止させる。	#1-34,#1-36, #1-40,#1-44	
			PLC（マスター）	PLC（スレーブ）	攻撃者が、PLC（マスター）の機能を停止させ多数の PLC（スレーブ）に適切なコマンドを発行できなくなり、広域に及ぶ供給を停止させる。	#1-35,#1-37, #1-41,#1-45	
2	限定地域でのエネルギー供給停止	エネルギー製造・供給設備等へのサイバー攻撃により、限定地域において供給停止が発生し、社会に影響を及ぼし、賠償費用等の損失が生じると共に、当社の信頼が低下する。					2
		2-1	フィールド NW の輻輳により、PLC に制御情報を伝える事ができなくなり、限定地域において供給停止が発生する。				
			攻撃拠点	攻撃対象	最終攻撃	リスク分析シート上の攻撃ツリー番号	
			不正端末	フィールド NW	攻撃者が、不正端末 I から不正なコマンドにてフィールド NW を輻輳させ、PLC（スレーブ）への制御情報の伝達をできなくし、局所的な供給を停止させる。	#2-1	

<table>
<tr><th>#</th><th>事業被害</th><th colspan="5">事業被害の概要、攻撃シナリオ</th><th>事業被害レベル</th></tr>
<tr><td rowspan="6">2</td><td rowspan="6">限定地域でのエネルギー供給停止</td><td rowspan="3">2-2</td><td colspan="4">フィールド NW 上の資産のデータやプログラムが改ざんされ機器の動作が異常となり、限定地域において供給停止が発生する。</td><td rowspan="6"></td></tr>
<tr><td>攻撃拠点</td><td>攻撃対象</td><td>最終攻撃</td><td>リスク分析シート上の攻撃ツリー番号</td></tr>
<tr><td>PLC（スレーブ）</td><td>PLC（スレーブ）</td><td>攻撃者が、PLC（スレーブ）のデータやプログラムが改ざんし動作異常を発生させ、限定地域において供給を停止させる。</td><td>#2-2,#2-3</td></tr>
<tr><td rowspan="3">2-3</td><td colspan="4">フィールド NW 上の重要な資産が停止し、限定地域において供給停止が発生する。</td></tr>
<tr><td>攻撃拠点</td><td>攻撃対象</td><td>最終攻撃</td><td>リスク分析シート上の攻撃ツリー番号</td></tr>
<tr><td>PLC（スレーブ）</td><td>PLC（スレーブ）</td><td>攻撃者が、PLC（スレーブ）の機能を停止させ、局所的な供給を停止させる。</td><td>#2-4,#2-5</td></tr>
<tr><td rowspan="5">3</td><td rowspan="5">営業秘密の漏洩</td><td colspan="5">エネルギー製造設備等へのサイバー攻撃により、製造に関わる営業秘密が社外へ漏洩し、競合他社との差異化に影響を及ぼし、当社の競争力が低下する。</td><td rowspan="5">1</td></tr>
<tr><td rowspan="3">3-1</td><td colspan="4">データサーバ上の機密データが窃取され、情報漏洩が発生する。</td></tr>
<tr><td>攻撃拠点</td><td>攻撃対象</td><td>最終攻撃</td><td>リスク分析シート上の攻撃ツリー番号</td></tr>
<tr><td>データサーバ</td><td>データサーバ</td><td>攻撃者が、データサーバ上のデータを窃取し、逆ルートを辿り、情報 NW[4]上かインターネット上のサーバへ情報を持出す。</td><td>#3-1,#3-2,#3-3,#3-4</td></tr>
</table>

[4] 情報 NW：情報ネットワーク

⑪ 事業被害ベースのリスク分析シート

ガイド本体「4.2.節　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、モデルシステムの事業被害ベースのリスク分析を実施した。

ここでは、リスク分析結果である分析シートの形式（記入例）を 3 種類提示し、それぞれの形式がどのような特徴があるかを説明する。

事業被害と攻撃シナリオの一覧（表 2-8）を基に、攻撃ツリーを検討して整理したものが、表 2-9 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 2-10 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 2-11 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。

このページは空白です。

表 2-9 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. 広域でのエネルギー供給停止

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	制御NWが輻輳し、PLCに制御情報を伝える事ができなくなり、広域に及ぶ供給停止が発生する。														
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」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			
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	○			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		悪意ある第三者が、HMIから不正なコマンドにて制御NWを輻輳させ、PLC-Mへの制御情報の伝達をできなくし、広域に及ぶ供給を停止させる。	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		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」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		悪意ある第三者が、制御サーバから不正なコマンドにて制御NWを輻輳させ、PLC-Mへの制御情報の伝達をできなくし、広域に及ぶ供給を停止させる。	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		悪意ある第三者が、FWを経由してデータ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 *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			
7		悪意ある第三者が、データサーバから不正なコマンドにて制御NWを輻輳させ、PLC-Mへの制御情報の伝達をできなくし、広域に及ぶ供給を停止させる。	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	#1-3	1,6,7
8		**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に不正アクセスする。 ※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			
9		悪意ある第三者が、データヒストリアンを経由してデータ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6に同じ						2			
10		悪意ある第三者が、データサーバから不正なコマンドにて制御NWを輻輳させ、PLC-Mへの制御情報の伝達をできなくし、広域に及ぶ供給を停止させる。	2	2	3	B	項番7に同じ						1	2	#1-4	8,9,10
11		悪意ある第三者が、データヒストリアンを経由してFW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*	○ ○ ○	 （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			
12		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に同じ						2			
13		悪意ある第三者が、HMIから不正なコマンドにて制御NWを輻輳させ、PLC-Mへの制御情報の伝達をできなくし、広域に及ぶ供給を停止させる。	2	2	3	B	項番3に同じ						1	2	#1-5	10.11.12.13
14		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」を含む。					項番4に同じ						2			
15		悪意ある第三者が、制御サーバから不正なコマンドにて制御NWを輻輳させ、PLC-Mへの制御情報の伝達をできなくし、広域に及ぶ供給を停止させる。	2	2	3	B	項番5に同じ						1	2	#1-6	10,11,14,15
16		悪意ある第三者が、FWを経由してデータ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6に同じ						2			
17		悪意ある第三者が、データサーバから不正なコマンドにて制御NWを輻輳させ、PLC-Mへの制御情報の伝達をできなくし、広域に及ぶ供給を停止させる。	2	2	3	B	項番7に同じ						1	2	#1-7	10,11,16,17
18		**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			
19		マルウェアが、HMIから不正なコマンドにて制御NWを輻輳させ、PLC-Mへの制御情報の伝達をできなくし、広域に及ぶ供給を停止させる。	3	3	3	A	項番3に同じ						1	1	#1-8	18,19
20		**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		3 ※2			
21		マルウェアが、制御サーバから不正なコマンドにて制御NWを輻輳させ、PLC-Mへの制御情報の伝達をできなくし、広域に及ぶ供給を停止させる。	3	1	3	B	項番5に同じ						1	3	#1-9	20,21
22		**侵入口=データサーバ** 内部者の過失により、マルウェアに感染したUSB媒体をデータサーバに接続して、データ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		3 ※2			
23		マルウェアが、データサーバから不正なコマンドにて制御NWを輻輳させ、PLC-Mへの制御情報の伝達をできなくし、広域に及ぶ供給を停止させる。	3	1	3	B	項番7に同じ						1	3	#1-10	22,23
X																

【注】
※1
対策の評価においては、「7.4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、「7.5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 2-9 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. 広域でのエネルギー供給停止

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	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)
	1-2	PLCに対して不正なコマンド(広域供給停止コマンド等)が送信され、広域に及ぶ供給停止が発生する。												
24	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」を含む。					項番1に同じ				2 ※1			
25		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に同じ				2			
26		悪意ある第三者が、HMIから多数のPLC-Mへ不正なコマンド(広域供給停止コマンド等)を発行し、広域に及ぶ供給を停止させる。	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	#1-11	24,25,26
27		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」を含む。					項番4に同じ				2			
28		悪意ある第三者が、制御サーバから多数のPLC-Mへ不正なコマンド(広域供給停止コマンド等)を発行し、広域に及ぶ供給を停止させる。	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	#1-12	24,27,28
29		悪意ある第三者が、FWを経由してデータ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6に同じ				2			
30		悪意ある第三者が、データサーバを経由してPLC-M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*	○ ○ ○ (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			
31		悪意ある第三者が、PLC-Mから多数のPLC-Sへ不正なコマンド(広域供給停止コマンド等)を発行し、広域に及ぶ供給を停止させる。	1	2	3	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	#1-13	24,29,30,31
32	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に不正アクセスする。 ※不正アクセスは「プロセス不正実行」を含む。					項番8に同じ				2			
33		悪意ある第三者が、データヒストリアンを経由してデータ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6に同じ				2			
34		悪意ある第三者が、データサーバを経由してPLC-M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30に同じ				1			
35		悪意ある第三者が、PLC-Mから多数のPLC-Sへ不正なコマンド(広域供給停止コマンド等)を発行し、広域に及ぶ供給を停止させる。	1	2	3	C	項番31に同じ				1	2	#1-14	32,33,34,35
36		悪意ある第三者が、データヒストリアンを経由してFW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に同じ				2 ※1			
37		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に同じ				2			
38		悪意ある第三者が、HMIから多数のPLC-Mへ不正なコマンド(広域供給停止コマンド等)を発行し、広域に及ぶ供給を停止させる。	2	2	3	B	項番26に同じ				1	2	#1-15	32,36,37,38
39		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」を含む。					項番4に同じ				2			
40		悪意ある第三者が、制御サーバから多数のPLC-Mへ不正なコマンド(広域供給停止コマンド等)を発行し、広域に及ぶ供給を停止させる。	2	2	3	B	項番28に同じ				1	2	#1-16	32,36,39.40
41		悪意ある第三者が、FWを経由してデータ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6に同じ				2			
42		悪意ある第三者が、データサーバを経由してPLC-M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30に同じ				1			
43		悪意ある第三者が、PLC-Mから多数のPLC-Sへ不正なコマンド(広域供給停止コマンド等)を発行し、広域に及ぶ供給を停止させる。	1	2	3	C	項番31に同じ				1	2	#1-17	32,36,41, 42,43
44	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18に同じ				1 ※2			
45		マルウェアが、HMIから多数のPLC-Mへ不正なコマンド(広域供給停止コマンド等)を発行し、広域に及ぶ供給を停止させる。	3	3	3	A	項番26に同じ				1	1	#1-18	44,45
46	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20に同じ				3 ※2			
47		マルウェアが、制御サーバから多数のPLC-Mへ不正なコマンド(広域供給停止コマンド等)を発行し、広域に及ぶ供給を停止させる。	3	1	3	B	項番28に同じ				1	3	#1-19	46,47
48	侵入口=データサーバ	内部者の過失により、マルウェアに感染したUSB媒体をデータサーバに接続して、データ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22に同じ				3 ※2			
49		マルウェアが、データサーバから多数のPLC-Mに感染する。					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			
50		マルウェアが、PLC-Mから多数のPLC-Sへ不正なコマンド(広域供給停止コマンド等)を発行し、広域に及ぶ供給を停止させる。	1	1	3	C	項番31に同じ				1	3	#1-20	48,49,50
X														

表 2-9 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. 広域でのエネルギー供給停止

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	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)
	1-3	重要な資産のデータやプログラムが改ざんされ資産の動作が異常となり、広域に及ぶ供給停止が発生する。												
51		**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」を含む。					項番1に同じ				2 ※1			
52		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」を含む。					項番4に同じ				2			
53		悪意ある第三者が、制御サーバ上のデータやプログラムが改ざんし、多数のPLC-Mへ不正なコマンド(広域供給停止コマンド等)を発行させ、広域に及ぶ供給を停止させる。	2	2	3	B	権限管理 (同左) アクセス制御 (同左) データ署名 (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	#1-21	51,52,53
54		悪意ある第三者が、FWを経由してデータ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6に同じ				2			
55		悪意ある第三者が、データサーバ上のデータを改ざんし、HMIから多数のPLC-Mへ適切なコマンド発行ができず(不適切なコマンドが発行され)、広域に及ぶ供給を停止させる。	2	2	3	B	権限管理 (同左) アクセス制御 (同左) データ署名 (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	#1-22	51,54,55
56		悪意ある第三者が、データサーバを経由してPLC-M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30に同じ				1			
57		悪意ある第三者が、PLC-M上のデータやプログラムが改ざんし、PLC-Mから多数のPLC-Sへ不正なコマンド(広域供給停止コマンド等)を発行させ、広域に及ぶ供給を停止させる。	1	2	3	C	権限管理 (同左) アクセス制御 (同左) データ署名 (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	#1-23	51,54,56,57
58		**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に不正アクセスする。 ※不正アクセスは「プロセス不正実行」を含む。					項番8に同じ				2			
59		悪意ある第三者が、データヒストリアンを経由してデータ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6に同じ				2			
60		悪意ある第三者が、データサーバ上のデータを改ざんし、HMIから多数のPLC-Mへ適切なコマンド発行ができず(不適切なコマンドが発行され)、広域に及ぶ供給を停止させる。	2	2	3	B	項番55に同じ				1	2	#1-24	58,59,60
61		悪意ある第三者が、データサーバを経由してPLC-M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30に同じ				1			
62		悪意ある第三者が、PLC-M上のデータやプログラムが改ざんし、PLC-Mから多数のPLC-Sへ不正なコマンド(広域供給停止コマンド等)を発行させ、広域に及ぶ供給を停止させる。	1	2	3	C	項番57に同じ				1	2	#1-25	58,59,61,62
63		悪意ある第三者が、データヒストリアンを経由してFW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に同じ				2 ※1			
64		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」を含む。					項番4に同じ				2			
65		悪意ある第三者が、制御サーバ上のデータやプログラムが改ざんし、多数のPLC-Mへ不正なコマンド(広域供給停止コマンド等)を発行させ、広域に及ぶ供給を停止させる。	2	2	3	B	項番53に同じ				1	2	#1-26	58,63,64,65
66		悪意ある第三者が、FWを経由してデータ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6に同じ				2			
67		悪意ある第三者が、データサーバ上のデータを改ざんし、HMIから多数のPLC-Mへ適切なコマンド発行ができず(不適切なコマンドが発行され)、広域に及ぶ供給を停止させる。	2	2	3	B	項番55に同じ				1	2	#1-27	58,63,66,67
68		悪意ある第三者が、データサーバを経由してPLC-M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30に同じ				1			
69		悪意ある第三者が、PLC-M上のデータやプログラムが改ざんし、PLC-Mから多数のPLC-Sへ不正なコマンド(広域供給停止コマンド等)を発行させ、広域に及ぶ供給を停止させる。	1	2	3	C	項番57に同じ				1	2	#1-28	58,63,66,68,69
70		**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20に同じ				3 ※2			
71		マルウェアが、制御サーバ上のデータやプログラムが改ざんし、多数のPLC-Mへ不正なコマンド(広域供給停止コマンド等)を発行させ、広域に及ぶ供給を停止させる。	3	1	3	B	項番53に同じ				1	3	#1-29	70,71
72		**侵入口=データサーバ** 内部者の過失により、マルウェアに感染したUSB媒体をデータサーバに接続して、データ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22に同じ				3 ※2			
73		マルウェアが、データサーバ上のデータを改ざんし、HMIからPLC-Mへ適切なコマンド発行ができず(不適切なコマンドが発行され)、広域に及ぶ供給を停止させる。	3	1	3	B	項番55に同じ				1	3	#1-30	72,73
74		マルウェアが、データサーバから多数のPLC-Mに感染する。					項番49に同じ				1			
75		マルウェアが、PLC-M上のデータやプログラムが改ざんし、PLC-Mから多数のPLC-Sへ不正なコマンド(広域供給停止コマンド等)を発行させ、広域に及ぶ供給を停止させる。	1	1	3	C	項番57に同じ				1	3	#1-31	72,74,75
X														

表 2-9 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. 広域でのエネルギー供給停止

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	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)
	1-4	重要な資産の停止により、広域に及ぶ供給停止が発生する。												
76		**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」を含む。					項番1に同じ				2 ※1			
77		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に同じ				2			
78		悪意ある第三者が、HMIの機能を停止させ多数のPLC-Mに適切なコマンドを発行できなくなり、広域に及ぶ供給を停止させる。 ※HMIが停止しても、制御サーバでの機能により代替運用可能。(フェールセーフ設計)	2	1	3	C			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 ○	3	3	#1-32	76,77,78
79		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」を含む。					項番4に同じ				2			
80		悪意ある第三者が、制御サーバ上の機能を停止させ多数のPLC-Mに適切なコマンドを発行できなくなり、広域に及ぶ供給を停止させる。	2	2	3	B			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	2	#1-33	76,79,80
81		悪意ある第三者が、FWを経由してデータ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6に同じ				2			
82		悪意ある第三者が、データサーバの機能を停止させHMIから多数のPLC-Mへ適切なコマンド発行ができず(不適切なコマンドが発行され)、広域に及ぶ供給を停止させる。	2	2	3	B			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	2	#1-34	76,81,82
83		悪意ある第三者が、データサーバを経由してPLC-M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30に同じ				1			
84		悪意ある第三者が、PLC-Mの機能を停止させ多数のPLC-Sに適切なコマンドを発行できなくなり、広域に及ぶ供給を停止させる。	1	2	3	C			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	2	2	#1-35	76,81,83,84
85		**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に不正アクセスする。 ※不正アクセスは「プロセス不正実行」を含む。					項番8に同じ				2			
86		悪意ある第三者が、データヒストリアンを経由してデータ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6に同じ				2			
87		悪意ある第三者が、データサーバの機能を停止させHMIから多数のPLC-Mへ適切なコマンド発行ができず(不適切なコマンドが発行され)、広域に及ぶ供給を停止させる。	2	2	3	B	項番82に同じ				2	2	#1-36	85,86,87
88		悪意ある第三者が、データサーバを経由してPLC-M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30に同じ				1			
89		悪意ある第三者が、PLC-Mの機能を停止させ多数のPLC-Sに適切なコマンドを発行できなくなり、広域に及ぶ供給を停止させる。	1	2	3	C	項番84に同じ				2	2	#1-37	85,86,88,89
90		悪意ある第三者が、データヒストリアンを経由してFW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に同じ				2 ※1			
91		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に同じ				2			
92		悪意ある第三者が、HMIの機能を停止させ多数のPLC-Mに適切なコマンドを発行できなくなり、広域に及ぶ供給を停止させる。	2	1	3	C	項番78に同じ				3	3	#1-38	85,90,91,92
93		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」を含む。					項番4に同じ				2			
94		悪意ある第三者が、制御サーバ上の機能を停止させ多数のPLC-Mに適切なコマンドを発行できなくなり、広域に及ぶ供給を停止させる。	2	2	3	B	項番80に同じ				1	2	#1-39	85,90,93,94
95		悪意ある第三者が、FWを経由してデータ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6に同じ				2			
96		悪意ある第三者が、データサーバの機能を停止させHMIから多数のPLC-Mへ適切なコマンド発行ができず(不適切なコマンドが発行され)、広域に及ぶ供給を停止させる。	2	2	3	B	項番82に同じ				2	2	#1-40	85,90,95,96
97		悪意ある第三者が、データサーバを経由してPLC-M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30に同じ				1			
98		悪意ある第三者が、PLC-Mの機能を停止させ多数のPLC-Sに適切なコマンドを発行できなくなり、広域に及ぶ供給を停止させる。	1	2	3	C	項番84に同じ				2	2	#1-41	85,90,95,97,98
99		**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18に同じ				1 ※2			
100		マルウェアが、HMIの機能を停止させ多数のPLC-Mに適切なコマンドを発行できなくなり、広域に及ぶ供給を停止させる。	3	1	3	B	項番78に同じ				3	3	#1-42	99,100
101		**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20に同じ				3 ※2			
102		マルウェアが、制御サーバの機能を停止させ多数のPLC-Mに適切なコマンドを発行できなくなり、広域に及ぶ供給を停止させる。	3	1	3	B	項番80に同じ				1	3	#1-43	101,102
103		**侵入口=データサーバ** 内部者の過失により、マルウェアに感染したUSB媒体をデータサーバに接続して、データ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22に同じ				3 ※2			
104		マルウェアが、データサーバの機能を停止させ、HMIから多数のPLC-Mへ適切なコマンド発行ができず(不適切なコマンドが発行され)、広域に及ぶ供給を停止させる。	3	1	3	B	項番82に同じ				1	3	#1-44	103,104
105		マルウェアが、データサーバから多数のPLC-Mに感染する。					項番49に同じ				1			
106		マルウェアが、PLC-Mの機能を停止させ多数のPLC-Sに適切なコマンドを発行できなくなり、広域に及ぶ供給を停止させる。	1	1	3	C	項番84に同じ				2	3	#1-45	103,105,106
X														

表 2-9 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. 限定地域でのエネルギー供給停止

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							
	2-1	フィールドNWの輻輳により、PLCに制御情報を伝える事ができなくなり、限定地域において供給停止が発生する。														
107		侵入口=フィールドNW、PLC-S 悪意ある第三者が、フィールド機器の保管場所に物理的に侵入する。					入退管理	○			監視カメラ	○		2		
							施錠管理	○			侵入センサ	○				
108		悪意ある第三者が、フィールドNWに不正端末を接続する。					デバイス接続・利用制限		（同左）		ログ収集・分析			1		
											統合ログ管理システム					
109		悪意ある第三者が、不正端末Iから不正なコマンドにてフィールドNWを輻輳させ、PLC-Sへの制御情報の伝達をできなくし、局所的な供給を停止させる。 ※フィールドNWとしての脅威は「通信輻輳」。	2	2	2	C	DDoS対策				機器異常検知		冗長化	1	2	#2-1	107,108,109
											機器死活監視					
											ログ収集・分析					
											統合ログ管理システム					
X																

表 2-9 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. 限定地域でのエネルギー供給停止

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	評価指標 脆弱性レベル	評価指標 事業被害レベル	リスク値	対策 防御 侵入／拡散段階	対策 防御 目的遂行段階	対策 検知／被害把握	対策 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）
	2-2	フィールドNW上の資産のデータやプログラムが改ざんされ機器の動作が異常となり、限定地域において供給停止が発生する。												
110		侵入口=フィールドNW、PLC-S 悪意ある第三者が、フィールド機器の保管場所に物理的に侵入する。					項番107に同じ				2			
111		悪意ある第三者が、フィールドNWに不正端末を接続する。					項番108に同じ				1			
112		悪意ある第三者が、不正端末からPLC-Sに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*		1			
113		悪意ある第三者が、PLC-Sのデータやプログラムが改ざんし動作異常を発生させ、局所的な供給を停止させる。	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	#2-2	110,111,112,113
114		悪意ある第三者が、PLC-Sに不正端末を接続する。					デバイス接続・利用制限	（同左）	ログ収集・分析 統合ログ管理システム		1			
115		悪意ある第三者が、不正端末からPLC-Sに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112に同じ				1			
116		悪意ある第三者が、PLC-Sのデータやプログラムが改ざんし動作異常を発生させ、局所的な供給を停止させる。	2	2	2	C	項番113に同じ				1	2	#2-3	110,114,115,116
X														

表 2-9 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. 限定地域でのエネルギー供給停止

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						
	2-3	フィールドNW上の重要な資産が停止し、限定地域において供給停止が発生する。												
117		侵入口=フィールドNW、PLC-S 悪意ある第三者が、フィールド機器の保管場所に物理的に侵入する。					項番107に同じ				2			
118		悪意ある第三者が、フィールドNWに不正端末を接続する。					項番108に同じ				1			
119		悪意ある第三者が、不正端末からPLC-Sに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112に同じ				1			
120		悪意ある第三者が、PLC-Sの機能を停止させ、局所的な供給を停止させる。	2	2	2	C			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	2	#2-4	117,118,119,120
121		悪意ある第三者が、PLC-Sに不正端末を接続する。					項番114に同じ				1			
122		悪意ある第三者が、不正端末からPLC-Sに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112に同じ				1			
123		悪意ある第三者が、PLC-Sの機能を停止させ、局所的な供給を停止させる。	2	2	2	C	項番113に同じ				1	2	#2-5	117,121,122,123
X														

表 2-9 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. 営業秘密の漏洩

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						
	3-1	データサーバ上の機密データが窃取され、情報漏洩が発生する。												
124		**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」を含む。					項番1に同じ				2 ※1			
125		悪意ある第三者が、FWを経由してデータ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6に同じ				2			
126		悪意ある第三者が、データ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	1	D	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	#3-1	124,125, 126,127
127		**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に不正アクセスする。 ※不正アクセスは「プロセス不正実行」を含む。					項番8に同じ				2			
128		悪意ある第三者が、データヒストリアンを経由してデータ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6に同じ				2			
129		悪意ある第三者が、データ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	1	D	項番126に同じ				2	2	#3-2	127,128, 129
130		悪意ある第三者が、データヒストリアンを経由してFW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に同じ				2 ※1			
131		悪意ある第三者が、FWを経由してデータ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6に同じ				2			
132		悪意ある第三者が、データ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	1	D	項番126に同じ				2	2	#3-3	127,130, 131,132
133		**侵入口=データサーバ** 内部者の過失により、マルウェアに感染したUSB媒体をデータサーバに接続して、データ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22に同じ				3 ※2			
134		マルウェアが、データサーバ上のデータを窃取する。 （その後、USB媒体経由で情報が漏洩する。）	2	1	1	E	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	3	#3-4	133,134
X														

表 2-10 事業被害ベースのリスク分析シート（侵入口ソート版）

1. 広域でのエネルギー供給停止、3. 営業秘密の漏洩

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）
	1-1,2,3,4 3-1	1-1 制御NWが轢検し、PLCに制御情報を伝える事ができなくなり、広域に及ぶ供給停止が発生する。 1-2 PLCに対して不正なコマンド(広域供給停止コマンド等)が送信され、広域に及ぶ供給停止が発生する。 1-3 重要な資産のデータやプログラムが改ざんされ資産の動作が異常となり、広域に及ぶ供給停止が発生する。 1-4 重要な資産の停止により、広域に及ぶ供給停止が発生する。 3-1 データサーバ上の機密データが窃取され、情報漏洩が発生する。												
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」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） （同左） *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 ※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		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から不正なコマンドにて制御NWを輻輳させ、PLC-Mへの制御情報の伝達をできなくし、広域に及ぶ供給を停止させる。	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	1-2	悪意ある第三者が、HMIから多数のPLC-Mへ不正なコマンド(広域供給停止コマンド等)を発行し、広域に及ぶ供給を停止させる。	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	1,2,4
5	1-4	悪意ある第三者が、HMIの機能を停止させ多数のPLC-MIに適切なコマンドを発行できなくなり、広域に及ぶ供給を停止させる。 ※HMIが停止しても、制御サーバでの機能により代替運用可能。(フェールセーフ設計)	2	1	3	C			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 ○	3	3	#1-3	1,2,5
6		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」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			
7	1-1	悪意ある第三者が、制御サーバから不正なコマンドにて制御NWを輻輳させ、PLC-Mへの制御情報の伝達をできなくし、広域に及ぶ供給を停止させる。	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	#1-4	1,6,7
8	1-2	悪意ある第三者が、制御サーバから多数のPLC-Mへ不正なコマンド(広域供給停止コマンド等)を発行し、広域に及ぶ供給を停止させる。	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	1,6,8
9	1-3	悪意ある第三者が、制御サーバ上のデータやプログラムが改ざんし、多数のPLC-Mへ不正なコマンド(広域供給停止コマンド等)を発行させ、広域に及ぶ供給を停止させる。	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	#1-6	1,6,9
10	1-4	悪意ある第三者が、制御サーバ上の機能を停止させ多数のPLC-MIに適切なコマンドを発行できなくなり、広域に及ぶ供給を停止させる。	2	2	3	B			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	2	#1-7	1,6,10
11		悪意ある第三者が、FWを経由してデータ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 *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、データサーバから不正なコマンドにて制御NWを輻輳させ、PLC-Mへの制御情報の伝達をできなくし、広域に及ぶ供給を停止させる。	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	#1-8	1,11,12
13	1-3	悪意ある第三者が、データサーバ上のデータを改ざんし、HMIから多数のPLC-Mへ適切なコマンド発行ができず(不適切なコマンドが発行され)、広域に及ぶ供給を停止させる。	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	1,11,13
14	1-4	悪意ある第三者が、データサーバの機能を停止させHMIから多数のPLC-Mへ適切なコマンド発行ができず(不適切なコマンドが発行され)、広域に及ぶ供給を停止させる。	2	2	3	B			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	2	#1-10	1,11,14
15		悪意ある第三者が、データサーバを経由してPLC-M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*		1			
16	1-2	悪意ある第三者が、PLC-Mから多数のPLC-Sへ不正なコマンド(広域供給停止コマンド等)を発行し、広域に及ぶ供給を停止させる。	1	2	3	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	#1-11	1,11,15,16
17	1-3	悪意ある第三者が、PLC-M上のデータやプログラムが改ざんし、PLC-Mから多数のPLC-Sへ不正なコマンド(広域供給停止コマンド等)を発行させ、広域に及ぶ供給を停止させる。	1	2	3	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	#1-12	1,11,15,17
18	1-4	悪意ある第三者が、PLC-Mの機能を停止させ多数のPLC-Sに適切なコマンドを発行できなくなり、広域に及ぶ供給を停止させる。	1	2	3	C			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	2	2	#1-13	1,11,15,18
19	3-1	悪意ある第三者が、データ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	1	D	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	#3-1	1,11,19
20		**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に不正アクセスする。 ※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			
21		悪意ある第三者が、データヒストリアンを経由してデータ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11に同じ				2			
22	1-1	悪意ある第三者が、データサーバから不正なコマンドにて制御NWを輻輳させ、PLC-Mへの制御情報の伝達をできなくし、広域に及ぶ供給を停止させる。	2	2	3	B	項番12に同じ				1	2	#1-14	20,21,22
23	1-3	悪意ある第三者が、データサーバ上のデータを改ざんし、HMIから多数のPLC-Mへ適切なコマンド発行ができず(不適切なコマンドが発行され)、広域に及ぶ供給を停止させる。	2	2	3	B	項番13に同じ				1	2	#1-15	20,21,22
24	1-4	悪意ある第三者が、データサーバの機能を停止させHMIから多数のPLC-Mへ適切なコマンド発行ができず(不適切なコマンドが発行され)、広域に及ぶ供給を停止させる。	2	2	3	B	項番14に同じ				2	2	#1-16	20,21,24
25		悪意ある第三者が、データサーバを経由してPLC-M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15に同じ				1			
26	1-2	悪意ある第三者が、PLC-Mから多数のPLC-Sへ不正なコマンド(広域供給停止コマンド等)を発行し、広域に及ぶ供給を停止させる。	1	2	3	C	項番16に同じ				1	2	#1-17	20,21,25,26
27	1-3	悪意ある第三者が、PLC-M上のデータやプログラムが改ざんし、PLC-Mから多数のPLC-Sへ不正なコマンド(広域供給停止コマンド等)を発行させ、広域に及ぶ供給を停止させる。	1	2	3	C	項番17に同じ				1	2	#1-18	20,21,25,27
28	1-4	悪意ある第三者が、PLC-Mの機能を停止させ多数のPLC-Sに適切なコマンドを発行できなくなり、広域に及ぶ供給を停止させる。	1	2	3	C	項番18に同じ				2	2	#1-19	20,21,25,28
29	3-1	悪意ある第三者が、データ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	1	D	項番19に同じ				2	2	#3-2	20,21,29

【注】
※1
対策の評価においては、「7.4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 2-10 事業被害ベースのリスク分析シート（侵入口ソート版）

1. 広域でのエネルギー供給停止、3. 営業秘密の漏洩

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）
	1-1,2,3,4 3-1	1-1 制御NWが輻輳し、PLCに制御情報を伝える事ができなくなり、広域に及ぶ供給停止が発生する。 1-2 PLCに対して不正なコマンド(広域供給停止コマンド等)が送信され、広域に及ぶ供給停止が発生する。 1-3 重要な資産のデータやプログラムが改ざんされ資産の動作が異常となり、広域に及ぶ供給停止が発生する。 1-4 重要な資産の停止により、広域に及ぶ供給停止が発生する。 3-1 データサーバ上の機密データが窃取され、情報漏洩が発生する。												
30		悪意ある第三者が、データヒストリアンを経由してFW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* ○	（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			
31		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に同じ				2			
32	1-1	悪意ある第三者が、HMIから不正なコマンドにて制御NWを輻輳させ、PLC-Mへの制御情報の伝達をできなくし、広域に及ぶ供給を停止させる。	2	2	3	B	項番3に同じ				1	2	#1-20	20,30,31,32
33	1-2	悪意ある第三者が、HMIから多数のPLC-Mへ不正なコマンド(広域供給停止コマンド等)を発行し、広域に及ぶ供給を停止させる。	2	2	3	B	項番4に同じ				1	2	#1-21	20,30,31,33
34	1-4	悪意ある第三者が、HMIの機能を停止させ多数のPLC-MIに適切なコマンドを発行できなくなり、広域に及ぶ供給を停止させる。	2	1	3	C	項番5に同じ				3	3	#1-22	20,30,31,34
35		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」を含む。					項番6に同じ				2			
36	1-1	悪意ある第三者が、制御サーバから不正なコマンドにて制御NWを輻輳させ、PLC-Mへの制御情報の伝達をできなくし、広域に及ぶ供給を停止させる。	2	2	3	B	項番7に同じ				1	2	#1-23	20,30,35,36
37	1-2	悪意ある第三者が、制御サーバから多数のPLC-Mへ不正なコマンド(広域供給停止コマンド等)を発行し、広域に及ぶ供給を停止させる。	2	2	3	B	項番8に同じ				1	2	#1-24	20,30,35,37
38	1-3	悪意ある第三者が、制御サーバ上のデータやプログラムが改ざんし、多数のPLC-Mへ不正なコマンド(広域供給停止コマンド等)を発行させ、広域に及ぶ供給を停止させる。	2	2	3	B	項番9に同じ				1	2	#1-25	20,30,35,38
39	1-4	悪意ある第三者が、制御サーバ上の機能を停止させ多数のPLC-MIに適切なコマンドを発行できなくなり、広域に及ぶ供給を停止させる。	2	2	3	B	項番10に同じ				1	2	#1-26	20,30,35,39
40		悪意ある第三者が、FWを経由してデータ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11に同じ				2			
41	1-1	悪意ある第三者が、データサーバから不正なコマンドにて制御NWを輻輳させ、PLC-Mへの制御情報の伝達をできなくし、広域に及ぶ供給を停止させる。	2	2	3	B	項番12に同じ				1	2	#1-27	20,30,40,41
42	1-3	悪意ある第三者が、データサーバ上のデータを改ざんし、HMIから多数のPLC-Mへ適切なコマンド発行ができず(不適切なコマンドが発行され)、広域に及ぶ供給を停止させる。	2	2	3	B	項番13に同じ				1	2	#1-28	20,30,40,42
43	1-4	悪意ある第三者が、データサーバの機能を停止させHMIから多数のPLC-Mへ適切なコマンド発行ができず(不適切なコマンドが発行され)、広域に及ぶ供給を停止させる。	2	2	3	B	項番14に同じ				1	2	#1-29	20,30,40,43
44		悪意ある第三者が、データサーバを経由してPLC-M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15に同じ				1			
45	1-2	悪意ある第三者が、PLC-Mから多数のPLC-Sへ不正なコマンド(広域供給停止コマンド等)を発行し、広域に及ぶ供給を停止させる。	1	2	3	C	項番16に同じ				1	2	#1-30	20,30,40, 44,45
46	1-3	悪意ある第三者が、PLC-M上のデータやプログラムが改ざんし、PLC-Mから多数のPLC-Sへ不正なコマンド(広域供給停止コマンド等)を発行させ、広域に及ぶ供給を停止させる。	1	2	3	C	項番17に同じ				1	2	#1-31	20,30,40, 44,46
47	1-4	悪意ある第三者が、PLC-Mの機能を停止させ多数のPLC-SIに適切なコマンドを発行できなくなり、広域に及ぶ供給を停止させる。	1	2	3	C	項番18に同じ				2	2	#1-32	20,30,40, 44,47
48	3-1	悪意ある第三者が、データ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	1	D	項番19に同じ				2	2	#3-3	20,30,40,48
49		**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			
50	1-1	マルウェアが、HMIから不正なコマンドにて制御NWを輻輳させ、PLC-Mへの制御情報の伝達をできなくし、広域に及ぶ供給を停止させる。	3	3	3	A	項番3に同じ				1	1	#1-33	49,50
51	1-2	マルウェアが、HMIから多数のPLC-Mへ不正なコマンド(広域供給停止コマンド等)を発行し、広域に及ぶ供給を停止させる。	3	3	3	A	項番4に同じ				1	1	#1-34	49,51
52	1-4	マルウェアが、HMIの機能を停止させ多数のPLC-MIに適切なコマンドを発行できなくなり、広域に及ぶ供給を停止させる。	3	1	3	B	項番5に同じ				3	3	#1-35	49,52
53		**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		3 ※2			
54	1-1	マルウェアが、制御サーバから不正なコマンドにて制御NWを輻輳させ、PLC-Mへの制御情報の伝達をできなくし、広域に及ぶ供給を停止させる。	3	1	3	B	項番7に同じ				1	3	#1-36	53,54
55	1-2	マルウェアが、制御サーバから多数のPLC-Mへ不正なコマンド(広域供給停止コマンド等)を発行し、広域に及ぶ供給を停止させる。	3	1	3	B	項番8に同じ				1	3	#1-37	53,55
56	1-3	マルウェアが、制御サーバ上のデータやプログラムが改ざんし、多数のPLC-Mへ不正なコマンド(広域供給停止コマンド等)を発行させ、広域に及ぶ供給を停止させる。	3	1	3	B	項番9に同じ				1	3	#1-38	53,56
57	1-4	マルウェアが、制御サーバの機能を停止させ多数のPLC-MIに適切なコマンドを発行できなくなり、広域に及ぶ供給を停止させる。	3	1	3	B	項番10に同じ				1	3	#1-39	53,57

【注】
※1
対策の評価においては、「7.4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、「7.5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 2-10 事業被害ベースのリスク分析シート(侵入口ソート版)

1. 広域でのエネルギー供給停止、3. 営業秘密の漏洩

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)
	1-1,2,3,4 3-1	1-1 制御NWが輻輳し、PLCに制御情報を伝える事ができなくなり、広域に及ぶ供給停止が発生する。 1-2 PLCに対して不正なコマンド(広域供給停止コマンド等)が送信され、広域に及ぶ供給停止が発生する。 1-3 重要な資産のデータやプログラムが改ざんされ資産の動作が異常となり、広域に及ぶ供給停止が発生する。 1-4 重要な資産の停止により、広域に及ぶ供給停止が発生する。 3-1 データサーバ上の機密データが窃取され、情報漏洩が発生する。												
58		**侵入口=データサーバ** 内部者の過失により、マルウェアに感染したUSB媒体をデータサーバに接続して、データ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		3 ※2			
59	1-1	マルウェアが、データサーバから不正なコマンドにて制御NWを輻輳させ、PLC-Mへの制御情報の伝達をできなくし、広域に及ぶ供給を停止させる。	3	1	3	B	項番12に同じ				1	3	#1-40	58,59
60	1-3	マルウェアが、データサーバ上のデータを改ざんし、HMIからPLC-Mへ適切なコマンド発行ができず(不適切なコマンドが発行され)、広域に及ぶ供給を停止させる。	3	1	3	B	項番13に同じ				1	3	#1-41	58,60
61	1-4	マルウェアが、データサーバの機能を停止させ、HMIから多数のPLC-Mへ適切なコマンド発行ができず(不適切なコマンドが発行され)、広域に及ぶ供給を停止させる。	3	1	3	B	項番14に同じ				1	3	#1-42	58,61
62		マルウェアが、データサーバから多数のPLC-Mに感染する。					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			
63	1-2	マルウェアが、PLC-Mから多数のPLC-Sへ不正なコマンド(広域供給停止コマンド等)を発行し、広域に及ぶ供給を停止させる。	1	1	3	C	項番16に同じ				1	3	#1-43	58,62,63
64	1-3	マルウェアが、PLC-M上のデータやプログラムが改ざんし、PLC-Mから多数のPLC-Sへ不正なコマンド(広域供給停止コマンド等)を発行させ、広域に及ぶ供給を停止させる。	1	1	3	C	項番17に同じ				1	3	#1-44	58,62,64
65	1-4	マルウェアが、PLC-Mの機能を停止させ多数のPLC-Sに適切なコマンドを発行できなくなり、広域に及ぶ供給を停止させる。	1	1	3	C	項番18に同じ				2	3	#1-45	58,62,65
66	3-1	マルウェアが、データサーバ上のデータを窃取する。 (その後、USB媒体経由で情報が漏洩する。)	2	1	1	E	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	3	#3-4	58,66
X														

【注】
※2
対策の評価においては、「7.5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 2-10 事業被害ベースのリスク分析シート（侵入口ソート版）

2. 限定地域でのエネルギー供給停止

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						
	2-1,2,3	2-1 フィールドNWの輻輳により、PLCに制御情報を伝える事ができなくなり、限定地域において供給停止が発生する。 2-2 フィールドNW上の資産のデータやプログラムが改ざんされ機器の動作が異常となり、限定地域において供給停止が発生する。 2-3 フィールドNW上の重要な資産が停止し、限定地域において供給停止が発生する。													
67		**侵入口=フィールドNW、PLC-S** 悪意ある第三者が、フィールド機器の保管場所に物理的に侵入する。					入退管理 ○ 施錠管理 ○		監視カメラ ○ 侵入センサ ○		2			
68		悪意ある第三者が、フィールドNWに不正端末を接続する。					デバイス接続・利用制限	（同左）	ログ収集・分析 統合ログ管理システム		1			
69	2-1	悪意ある第三者が、不正端末Iから不正なコマンドにてフィールドNWを輻輳させ、PLC-Sへの制御情報の伝達をできなくし、局所的な供給を停止させる。 ※フィールドNWとしての脅威は「通信輻輳」。	2	2	2	C	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	2	#2-1	67,68,69
70		悪意ある第三者が、不正端末からPLC-Sに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*		1			
71	2-2	悪意ある第三者が、PLC-Sのデータやプログラムが改ざんし動作異常を発生させ、局所的な供給を停止させる。	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	#2-2	67,68,70,71
72	2-3	悪意ある第三者が、PLC-Sの機能を停止させ、局所的な供給を停止させる。	2	2	2	C			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	2	#2-3	67,68,70,72
73		悪意ある第三者が、PLC-Sに不正端末を接続する。					デバイス接続・利用制限	（同左）	ログ収集・分析 統合ログ管理システム		1			
74		悪意ある第三者が、不正端末からPLC-Sに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70に同じ				1			
75	2-2	悪意ある第三者が、PLC-Sのデータやプログラムが改ざんし動作異常を発生させ、局所的な供給を停止させる。	2	2	2	C	項番71に同じ				1	2	#2-4	67,73,74,75
76	2-3	悪意ある第三者が、PLC-Sの機能を停止させ、局所的な供給を停止させる。	2	2	2	C	項番72に同じ				1	2	#2-5	67,73,74,76
X														

表 2-11 事業被害ベースのリスク分析シート（ハイブリット版）

1. 広域でのエネルギー供給停止

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	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	制御NWが輻輳し、PLCに制御情報を伝える事ができなくなり、広域に及ぶ供給停止が発生する。													
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」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			
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		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		悪意ある第三者が、HMIから不正なコマンドにて制御NWを輻輳させ、PLC-Mへの制御情報の伝達をできなくし、広域に及ぶ供給を停止させる。	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		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」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		悪意ある第三者が、制御サーバから不正なコマンドにて制御NWを輻輳させ、PLC-Mへの制御情報の伝達をできなくし、広域に及ぶ供給を停止させる。	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		悪意ある第三者が、FWを経由してデータ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 *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			
7		悪意ある第三者が、データサーバから不正なコマンドにて制御NWを輻輳させ、PLC-Mへの制御情報の伝達をできなくし、広域に及ぶ供給を停止させる。	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	#1-3	1,6,7
8	**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に不正アクセスする。 ※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			
9		悪意ある第三者が、データヒストリアンを経由してデータ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6に同じ				2			
10		悪意ある第三者が、データサーバから不正なコマンドにて制御NWを輻輳させ、PLC-Mへの制御情報の伝達をできなくし、広域に及ぶ供給を停止させる。	2	2	3	B	項番7に同じ				1	2	#1-4	8,9,10
11		悪意ある第三者が、データヒストリアンを経由してFW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* ○	 （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			
12		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に同じ				2			
13		悪意ある第三者が、HMIから不正なコマンドにて制御NWを輻輳させ、PLC-Mへの制御情報の伝達をできなくし、広域に及ぶ供給を停止させる。	2	2	3	B	項番3に同じ				1	2	#1-5	10.11.12.13
14		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」を含む。					項番4に同じ				2			
15		悪意ある第三者が、制御サーバから不正なコマンドにて制御NWを輻輳させ、PLC-Mへの制御情報の伝達をできなくし、広域に及ぶ供給を停止させる。	2	2	3	B	項番5に同じ				1	2	#1-6	10,11,14,15
16		悪意ある第三者が、FWを経由してデータ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6に同じ				2			
17		悪意ある第三者が、データサーバから不正なコマンドにて制御NWを輻輳させ、PLC-Mへの制御情報の伝達をできなくし、広域に及ぶ供給を停止させる。	2	2	3	B	項番7に同じ				1	2	#1-7	10,11,16,17
18	**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			
19		マルウェアが、HMIから不正なコマンドにて制御NWを輻輳させ、PLC-Mへの制御情報の伝達をできなくし、広域に及ぶ供給を停止させる。	3	3	3	A	項番3に同じ				1	1	#1-8	18,19
20	**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		3 ※2			
21		マルウェアが、制御サーバから不正なコマンドにて制御NWを輻輳させ、PLC-Mへの制御情報の伝達をできなくし、広域に及ぶ供給を停止させる。	3	1	3	B	項番5に同じ				1	3	#1-9	20,21
22	**侵入口=データサーバ** 内部者の過失により、マルウェアに感染したUSB媒体をデータサーバに接続して、データ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		3 ※2			
23		マルウェアが、データサーバから不正なコマンドにて制御NWを輻輳させ、PLC-Mへの制御情報の伝達をできなくし、広域に及ぶ供給を停止させる。	3	1	3	B	項番7に同じ				1	3	#1-10	22,23
X														

【注】
※1
対策の評価においては、「7.4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、「7.5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 2-11 事業被害ベースのリスク分析シート（ハイブリット版）

1. 広域でのエネルギー供給停止

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	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）
	1-2,3,4	1-2 PLCに対して不正なコマンド(広域供給停止コマンド等)が送信され、広域に及ぶ供給停止が発生する。 1-3 重要な資産のデータやプログラムが改ざんされ資産の動作が異常となり、広域に及ぶ供給停止が発生する。 1-4 重要な資産の停止により、広域に及ぶ供給停止が発生する。												
24		**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」を含む。					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			
25		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		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	1-2	悪意ある第三者が、HMIから多数のPLC-Mへ不正なコマンド(広域供給停止コマンド等)を発行し、広域に及ぶ供給を停止させる。	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	#1-11	24,25,26
27	1-4	悪意ある第三者が、HMIの機能を停止させ多数のPLC-MIに適切なコマンドを発行できなくなり、広域に及ぶ供給を停止させる。 ※HMIが停止しても、制御サーバでの機能により代替運用可能。(フェールセーフ設計)	2	1	3	C			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 ○	3	3	#1-12	24,25,27
28		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」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			
29	1-2	悪意ある第三者が、制御サーバから多数のPLC-Mへ不正なコマンド(広域供給停止コマンド等)を発行し、広域に及ぶ供給を停止させる。	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	#1-13	24,28,29
30	1-3	悪意ある第三者が、制御サーバ上のデータやプログラムが改ざんし、多数のPLC-Mへ不正なコマンド(広域供給停止コマンド等)を発行させ、広域に及ぶ供給を停止させる。	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	#1-14	24,28,30
31	1-4	悪意ある第三者が、制御サーバ上の機能を停止させ多数のPLC-MIに適切なコマンドを発行できなくなり、広域に及ぶ供給を停止させる。	2	2	3	B			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	2	#1-15	24,28,31
32		悪意ある第三者が、FWを経由してデータ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 *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			
33	1-3	悪意ある第三者が、データサーバ上のデータを改ざんし、HMIから多数のPLC-Mへ適切なコマンド発行ができず(不適切なコマンドが発行され)、広域に及ぶ供給を停止させる。	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	#1-16	24,32,33
34	1-4	悪意ある第三者が、データサーバの機能を停止させHMIから多数のPLC-Mへ適切なコマンド発行ができず(不適切なコマンドが発行され)、広域に及ぶ供給を停止させる。	2	2	3	B			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	2	#1-17	24,32,34
35		悪意ある第三者が、データサーバを経由してPLC-M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*		1			
36	1-2	悪意ある第三者が、PLC-Mから多数のPLC-Sへ不正なコマンド(広域供給停止コマンド等)を発行し、広域に及ぶ供給を停止させる。	1	2	3	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	#1-18	24,32,35,36
37	1-3	悪意ある第三者が、PLC-M上のデータやプログラムが改ざんし、PLC-Mから多数のPLC-Sへ不正なコマンド(広域供給停止コマンド等)を発行させ、広域に及ぶ供給を停止させる。	1	2	3	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	#1-19	24,32,35,37
38	1-4	悪意ある第三者が、PLC-Mの機能を停止させ多数のPLC-Sに適切なコマンドを発行できなくなり、広域に及ぶ供給を停止させる。	1	2	3	C			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	2	2	#1-20	24,32,35,38
39		**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に不正アクセスする。 ※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			
40		悪意ある第三者が、データヒストリアンを経由してデータ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32に同じ				2			
41	1-3	悪意ある第三者が、データサーバ上のデータを改ざんし、HMIから多数のPLC-Mへ適切なコマンド発行ができず(不適切なコマンドが発行され)、広域に及ぶ供給を停止させる。	2	2	3	B	項番33に同じ				1	2	#1-21	39,40,41
42	1-4	悪意ある第三者が、データサーバの機能を停止させHMIから多数のPLC-Mへ適切なコマンド発行ができず(不適切なコマンドが発行され)、広域に及ぶ供給を停止させる。	2	2	3	B	項番34に同じ				2	2	#1-22	39,40,42
43		悪意ある第三者が、データサーバを経由してPLC-M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35に同じ				1			
44	1-2	悪意ある第三者が、PLC-Mから多数のPLC-Sへ不正なコマンド(広域供給停止コマンド等)を発行し、広域に及ぶ供給を停止させる。	1	2	3	C	項番36に同じ				1	2	#1-23	39,40,43,44
45	1-3	悪意ある第三者が、PLC-M上のデータやプログラムが改ざんし、PLC-Mから多数のPLC-Sへ不正なコマンド(広域供給停止コマンド等)を発行させ、広域に及ぶ供給を停止させる。	1	2	3	C	項番37に同じ				1	2	#1-24	39,40,43,45
46	1-4	悪意ある第三者が、PLC-Mの機能を停止させ多数のPLC-Sに適切なコマンドを発行できなくなり、広域に及ぶ供給を停止させる。	1	2	3	C	項番38に同じ				2	2	#1-25	39,40,43,46
47		悪意ある第三者が、データヒストリアンを経由してFW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* ○	（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			
48		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25に同じ				2			
49	1-2	悪意ある第三者が、HMIから多数のPLC-Mへ不正なコマンド(広域供給停止コマンド等)を発行し、広域に及ぶ供給を停止させる。	2	2	3	B	項番26に同じ				1	2	#1-26	39,47,48,49
50	1-4	悪意ある第三者が、HMIの機能を停止させ多数のPLC-MIに適切なコマンドを発行できなくなり、広域に及ぶ供給を停止させる。	2	1	3	C	項番27に同じ				3	3	#1-27	39,47,48,50

表 2-11 事業被害ベースのリスク分析シート（ハイブリット版）

1. 広域でのエネルギー供給停止

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	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）
	1-2,3,4	1-2 PLCに対して不正なコマンド(広域供給停止コマンド等)が送信され、広域に及ぶ供給停止が発生する。 1-3 重要な資産のデータやプログラムが改ざんされ資産の動作が異常となり、広域に及ぶ供給停止が発生する。 1-4 重要な資産の停止により、広域に及ぶ供給停止が発生する。												
51		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」を含む。					項番28に同じ				2			
52	1-2	悪意ある第三者が、制御サーバから多数のPLC-Mへ不正なコマンド(広域供給停止コマンド等)を発行し、広域に及ぶ供給を停止させる。	2	2	3	B	項番29に同じ				1	2	#1-28	39,47,51,52
53	1-3	悪意ある第三者が、制御サーバ上のデータやプログラムが改ざんし、多数のPLC-Mへ不正なコマンド(広域供給停止コマンド等)を発行させ、広域に及ぶ供給を停止させる。	2	2	3	B	項番30に同じ				1	2	#1-29	39,47,51,53
54	1-4	悪意ある第三者が、制御サーバ上の機能を停止させ多数のPLC-Mに適切なコマンドを発行できなくなり、広域に及ぶ供給を停止させる。	2	2	3	B	項番31に同じ				1	2	#1-30	39,47,51,54
55		悪意ある第三者が、FWを経由してデータ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32に同じ				2			
56	1-3	悪意ある第三者が、データサーバ上のデータを改ざんし、HMIから多数のPLC-Mへ適切なコマンド発行ができず(不適切なコマンドが発行され)、広域に及ぶ供給を停止させる。	2	2	3	B	項番33に同じ				1	2	#1-31	39,47,55,56
57	1-4	悪意ある第三者が、データサーバの機能を停止させHMIから多数のPLC-Mへ適切なコマンド発行ができず(不適切なコマンドが発行され)、広域に及ぶ供給を停止させる。	2	2	3	B	項番34に同じ				2	2	#1-32	39,47,55,57
58		悪意ある第三者が、データサーバを経由してPLC-M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35に同じ				1			
59	1-2	悪意ある第三者が、PLC-Mから多数のPLC-Sへ不正なコマンド(広域供給停止コマンド等)を発行し、広域に及ぶ供給を停止させる。	1	2	3	C	項番36に同じ				1	2	#1-33	39,47,55,58,59
60	1-3	悪意ある第三者が、PLC-M上のデータやプログラムが改ざんし、PLC-Mから多数のPLC-Sへ不正なコマンド(広域供給停止コマンド等)を発行させ、広域に及ぶ供給を停止させる。	1	2	3	C	項番37に同じ				1	2	#1-34	39,47,55,58,60
61	1-4	悪意ある第三者が、PLC-Mの機能を停止させ多数のPLC-Sに適切なコマンドを発行できなくなり、広域に及ぶ供給を停止させる。	1	2	3	C	項番38に同じ				2	2	#1-35	39,47,55,58,61
62		**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			
63	1-2	マルウェアが、HMIから多数のPLC-Mへ不正なコマンド(広域供給停止コマンド等)を発行し、広域に及ぶ供給を停止させる。	3	3	3	A	項番26に同じ				1	1	#1-36	62,63
64	1-4	マルウェアが、HMIの機能を停止させ多数のPLC-Mに適切なコマンドを発行できなくなり、広域に及ぶ供給を停止させる。	3	1	3	B	項番27に同じ				3	3	#1-37	62,64
65		**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		3 ※2			
66	1-2	マルウェアが、制御サーバから多数のPLC-Mへ不正なコマンド(広域供給停止コマンド等)を発行し、広域に及ぶ供給を停止させる。	3	1	3	B	項番29に同じ				1	3	#1-38	65,66
67	1-3	マルウェアが、制御サーバ上のデータやプログラムが改ざんし、多数のPLC-Mへ不正なコマンド(広域供給停止コマンド等)を発行させ、広域に及ぶ供給を停止させる。	3	1	3	B	項番30に同じ				1	3	#1-39	65,67
68	1-4	マルウェアが、制御サーバの機能を停止させ多数のPLC-Mに適切なコマンドを発行できなくなり、広域に及ぶ供給を停止させる。	3	1	3	B	項番31に同じ				1	3	#1-40	65,68
69		**侵入口=データサーバ** 内部者の過失により、マルウェアに感染したUSB媒体をデータサーバに接続して、データ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		3 ※2			
70	1-3	マルウェアが、データサーバ上のデータを改ざんし、HMIからPLC-Mへ適切なコマンド発行ができず(不適切なコマンドが発行され)、広域に及ぶ供給を停止させる。	3	1	3	B	項番33に同じ				1	3	#1-41	69,70
71	1-4	マルウェアが、データサーバの機能を停止させ、HMIから多数のPLC-Mへ適切なコマンド発行ができず(不適切なコマンドが発行され)、広域に及ぶ供給を停止させる。	3	1	3	B	項番34に同じ				1	3	#1-42	69,71
72		マルウェアが、データサーバから多数のPLC-Mに感染する。					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			
73	1-2	マルウェアが、PLC-Mから多数のPLC-Sへ不正なコマンド(広域供給停止コマンド等)を発行し、広域に及ぶ供給を停止させる。	1	1	3	C	項番36に同じ				1	3	#1-43	69,72,73
74	1-3	マルウェアが、PLC-M上のデータやプログラムが改ざんし、PLC-Mから多数のPLC-Sへ不正なコマンド(広域供給停止コマンド等)を発行させ、広域に及ぶ供給を停止させる。	1	1	3	C	項番37に同じ				1	3	#1-44	69,72,74
75	1-4	マルウェアが、PLC-Mの機能を停止させ多数のPLC-Sに適切なコマンドを発行できなくなり、広域に及ぶ供給を停止させる。	1	1	3	C	項番38に同じ				2	3	#1-45	69,72,75
X														

表 2-11 事業被害ベースのリスク分析シート（ハイブリット版）

2. 限定地域でのエネルギー供給停止

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	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）
	2-1,2,3	2-1 フィールドNWの輻輳により、PLCに制御情報を伝える事ができなくなり、限定地域において供給停止が発生する。 2-2 フィールドNW上の資産のデータやプログラムが改ざんされ機器の動作が異常となり、限定地域において供給停止が発生する。 2-3 フィールドNW上の重要な資産が停止し、限定地域において供給停止が発生する。												
76		**侵入口=フィールドNW、PLC-S** 悪意ある第三者が、フィールド機器の保管場所に物理的に侵入する。					入退管理 ○ 施錠管理 ○		監視カメラ ○ 侵入センサ ○		2			
77		悪意ある第三者が、フィールドNWに不正端末を接続する。					デバイス接続・利用制限	（同左）	ログ収集・分析 統合ログ管理システム		1			
78	2-1	悪意ある第三者が、不正端末Iから不正なコマンドにてフィールドNWを輻輳させ、PLC-Sへの制御情報の伝達をできなくし、局所的な供給を停止させる。 ※フィールドNWとしての脅威は「通信輻輳」。	2	2	2	C	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	2	#2-1	76,77,78
79		悪意ある第三者が、不正端末からPLC-Sに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*		1			
80	2-2	悪意ある第三者が、PLC-Sのデータやプログラムが改ざんし動作異常を発生させ、局所的な供給を停止させる。	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	#2-2	76,77,79,80
81	2-3	悪意ある第三者が、PLC-Sの機能を停止させ、局所的な供給を停止させる。	2	2	2	C			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	2	#2-3	76,77,79,81
82		悪意ある第三者が、PLC-Sに不正端末を接続する。					デバイス接続・利用制限	（同左）	ログ収集・分析 統合ログ管理システム		1			
83		悪意ある第三者が、不正端末からPLC-Sに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79に同じ				1			
84	2-2	悪意ある第三者が、PLC-Sのデータやプログラムが改ざんし動作異常を発生させ、局所的な供給を停止させる。	2	2	2	C	項番80に同じ				1	2	#2-4	76,82,83,84
85	2-3	悪意ある第三者が、PLC-Sの機能を停止させ、局所的な供給を停止させる。	2	2	2	C	項番81に同じ				1	2	#2-5	76,82,83,85
X														

表 2-11 事業被害ベースのリスク分析シート（ハイブリット版）

3. 営業秘密の漏洩

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						
	3-1	データサーバ上の機密データが窃取され、情報漏洩が発生する。												
86		**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」を含む。					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			
87		悪意ある第三者が、FWを経由してデータ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 *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			
88		悪意ある第三者が、データ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	1	D	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	#3-1	86,87,88
89		**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に不正アクセスする。 ※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） *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			
90		悪意ある第三者が、データヒストリアンを経由してデータ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87に同じ				2			
91		悪意ある第三者が、データ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	1	D	項番88に同じ				2	2	#3-2	89,90,91
92		悪意ある第三者が、データヒストリアンを経由してFW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* ○	 （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			
93		悪意ある第三者が、FWを経由してデータ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87に同じ				2			
94		悪意ある第三者が、データ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	1	D	項番88に同じ				2	2	#3-3	89,92,93,94
95		**侵入口=データサーバ** 内部者の過失により、マルウェアに感染したUSB媒体をデータサーバに接続して、データ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		3 ※2			
96		マルウェアが、データサーバ上のデータを窃取する。 （その後、USB媒体経由で情報が漏洩する。）	2	1	1	E	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	3	#3-4	95,96
X														

このページは空白です。

⑫ 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）

ガイド本体「5 章 リスク分析結果の解釈と活用法」では、資産ベースまたは事業被害ベースのリスク分析結果を活用し、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。事業被害ベースのリスク分析シート（表 2-9）を基に、リスク低減のための改善策を整理したものが表 2-12 である。改善策の検討対象としては、リスク評価結果でリスク値が A または B の攻撃ツリーとした。

表 2-12 リスク低減のための改善策

対策資産		対象攻撃ステップ	攻撃ツリー リスク値 （現状）	現状の対策 （対象となる脅威 への対策）	対策の改善案、強化策	攻撃ツリー リスク値 （追加対策後）
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。 ＜事業被害ベースの分析シート＞ 攻撃シナリオ 1-1 の項番 18（ツリー数=1） 攻撃シナリオ 1-2 の項番 44（ツリー数=1） 攻撃シナリオ 1-4 の項番 99（ツリー数=1）	A 対象ツリー数=2 B 対象ツリー数=1	・なし	（1） ホワイトリストの適用により、HMI での対策レベルを制御サーバやデータサーバの対策レベルに合わせる。この対策により、2 つの攻撃ツリーのリスク値を A から B へ低減可能。 （2）前項の対策により対象となる全ての攻撃ツリーの脆弱性レベルが 1 となり、資産への対策だけではさらなるリスク値の低減不可。	B 対象ツリー数=3

対策資産		対象攻撃ステップ	攻撃ツリー リスク値 （現状）	現状の対策 （対象となる脅威 への対策）	対策の改善案、強化策	攻撃ツリー リスク値 （追加対策後）
2	ファイア ウォール	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。 ＜事業被害ベースの分析シート＞ 攻撃シナリオ 1-1 の項番 1（ツリー数=3） 攻撃シナリオ 1-1 の項番 11（ツリー数=3） 攻撃シナリオ 1-2 の項番 24（ツリー数=2） 攻撃シナリオ 1-2 の項番 36（ツリー数=2） 攻撃シナリオ 1-3 の項番 51（ツリー数=2） 攻撃シナリオ 1-3 の項番 63（ツリー数=2） 攻撃シナリオ 1-4 の項番 76（ツリー数=2） 攻撃シナリオ 1-4 の項番 90（ツリー数=2） 悪意ある第三者が、データヒストリアンを経由してデータサーバに不正アクセスする。 ＜事業被害ベースの分析シート＞ 攻撃シナリオ 1-1 の項番 9（ツリー数=1） 攻撃シナリオ 1-3 の項番 59（ツリー数=1） 攻撃シナリオ 1-4 の項番 86（ツリー数=1）	B 対象ツリー数 =21	・セキュリティパッチの適用、利用者の権限管理、必要最低限の通信先の制限（IP パケットレベルの制限）。	（1）「7.4 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。	C 対象ツリー数 =21

対策資産		対象攻撃ステップ	攻撃ツリー リスク値 （現状）	現状の対策 （対象となる脅威 への対策）	対策の改善案、強化策	攻撃ツリー リスク値 （追加対策後）
3	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。 ＜事業被害ベースの分析シート＞ 攻撃シナリオ 1-1 の項番 20（ツリー数=1） 攻撃シナリオ 1-2 の項番 46（ツリー数=1） 攻撃シナリオ 1-3 の項番 70（ツリー数=1） 攻撃シナリオ 1-4 の項番 101（ツリー数=1）	B 対象ツリー数 =4	・ホワイトリストによる不正プロセスの実行抑止。	（1） 現状の対策により対象となる攻撃ツリーの脆弱性レベルが既に 1 であり、資産への対策だけではリスク値の低減不可。	B 対象ツリー数 =4
4	データ サーバ	内部者の過失により、マルウェアに感染したUSB 媒体をデータサーバに接続して、データサーバがマルウェアに感染する。 ＜事業被害ベースの分析シート＞ 攻撃シナリオ 1-1 の項番 22（ツリー数=1） 攻撃シナリオ 1-3 の項番 72（ツリー数=1） 攻撃シナリオ 1-4 の項番 103（ツリー数=1）	B 対象ツリー数 =3	・ホワイトリストによる不正プロセスの実行抑止。	（1） 現状の対策により対象となる攻撃ツリーの脆弱性レベルが既に 1 であり、資産への対策だけではリスク値の低減不可。	B 対象ツリー数 =3

表 2-12 に示したリスク低減のための改善策の実施により、リスク値の分布は表 2-13 の「改善後 1」の列の値となる。しかし、リスク値 B の攻撃ツリーが 10 個残存することになる。これらのリスク値低減のためには、攻撃ツリーの脆弱性レベルが既に最低の 1 になっているため、リスク値上は B 未満に下げることはできない。

このようなケースでは、実施する対策の強化、運用管理の強化等で、脅威レベルを下げることができるかを検討することになる（後述のコラム参照）。具体的な方法を以下に示す。

HMI および制御サーバでは USB 媒体の利用は無い前提のため、「接続の可能性のあるポートを物理的に塞ぐ」ことにより、USB 媒体を用いた攻撃の脅威レベルを 2 に低減させ、その結果リスク値を B から C へ低減させる。また、データサーバに関しては USB 媒体の利用があるが、ガイド本体「7.5 節 外部記憶媒体におけるセキュリティ対策」に基づく、

【「申請～利用」の局面】

・媒体利用おける利用可能な媒体の定義、申請、承認、報告の一連の手順をルール化する。

【「利用（媒体の端末への接続）」の局面】

・別の端末にて、事前に媒体上の不正プログラムの検知、駆除をできるようにする。

の対策を実施することで不正プログラムに感染した USB 媒体の利用を抑止し、脅威レベルを 2 に低減させ、その結果リスク値を B から C へ低減させる。

最終的には、リスク値の分布は表 2-13 の「改善後 2」の列の値となり、すべての攻撃ツリーのリスク値が C 以下となる。

表 2-13 対策実施前と後でのツリーのリスク値の分布

ツリーのリスク値	現状	改善後 1	改善後 2
A	2	0	0
B	29	10	0
C	19	40	50
D	3	3	3
E	1	1	1

【コラム】

リスク分析のパラドックス　～下げきれないリスク値～

リスク分析は、脅威、脆弱性、資産重要度／事業被害の 3 つの評価指標の下に実施して、リスク値を算出する（ステップ 1）。その分析結果を受け、脆弱性レベルの低減（対策の強化）を検討、実施することで、リスク値の低減を図ることが可能となる（ステップ 2）。

このプロセスにおいて、重要度／事業被害は、脅威や脆弱性には全く依存しないシステムや事業に固定のレベルとなる。また、脅威レベルは、評価時点でのシステムの状態に対しての攻撃の可能性や容易性を評価しており、リスク値の改善ステップにおいては、変更（操作）すべきではない。これを変えてリスク値を下げるのは本末転倒となる。しかし、脆弱性レベルの低減だけでは、リスク値をどうしても組織が要求するレベルまで下げきれないケースに直面することがある。そのケースを下表に示すが、脆弱性レベルを最低にしても（打てる対策は全て打っても）リスク値を C にできない（ケース 1）や、システムの現状で脆弱性を充分下げる実施可能な対策がない（ケース 2）などが挙げられる。

上記において、脅威レベルの変更は本末転倒と述べたが、ステップ 2（対策強化）が実施されることを前提とすると、システムの脅威に対抗する状況は大きく変化する。脅威レベルは、脅威（攻撃）発生の可能性や容易性の指標であるので、例えば対策の強化や物理セキュリティの強化や運用管理の強化等によって、その指標は自ずと変化することになる。従って、ステップ 3 では、脅威レベルの変更を考慮したリスク値の評価に合理性が出てくる。

ケース 1

プロセス 時間軸	脅威レベル	脆弱性レベル	重要度 事業被害	リスク値
ステップ 1（現状）	3	3	3	A
ステップ 2（対策強化）	3	1	3	B
↓	課題：脆弱性レベルを 1 にしてもリスクレベルは C 以下にできない			
ステップ 3	**2**	1	3	**C**

ケース 2

プロセス 時間軸	脅威レベル	脆弱性レベル	重要度 事業被害	リスク値
ステップ 1（現状）	3	3	3	A
ステップ 2（対策強化）	3	2	3	A
↓	課題：脆弱性レベルを下げる実施可能な対策がない			
ステップ 3	**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
2017 年 12 月 19 日	誤字修正

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**
技術本部 **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/