

事業被害ベースのリスク分析シート

No.	事業被害	発生頻度			発生規模			リスク	リスク	リスク	リスク	リスク	リスク
		発生頻度	発生規模	発生頻度	発生規模	発生頻度	発生規模						
1	システム障害による業務停止	2	2	3	3	3	3	3	3	3	3	3	3
2	システム障害による業務停止	2	2	3	3	3	3	3	3	3	3	3	3
3	システム障害による業務停止	2	2	3	3	3	3	3	3	3	3	3	3
4	システム障害による業務停止	2	2	3	3	3	3	3	3	3	3	3	3
5	システム障害による業務停止	2	2	3	3	3	3	3	3	3	3	3	3
6	システム障害による業務停止	2	2	3	3	3	3	3	3	3	3	3	3
7	システム障害による業務停止	2	2	3	3	3	3	3	3	3	3	3	3
8	システム障害による業務停止	2	2	3	3	3	3	3	3	3	3	3	3
9	システム障害による業務停止	2	2	3	3	3	3	3	3	3	3	3	3
10	システム障害による業務停止	2	2	3	3	3	3	3	3	3	3	3	3
11	システム障害による業務停止	2	2	3	3	3	3	3	3	3	3	3	3
12	システム障害による業務停止	2	2	3	3	3	3	3	3	3	3	3	3
13	システム障害による業務停止	2	2	3	3	3	3	3	3	3	3	3	3
14	システム障害による業務停止	2	2	3	3	3	3	3	3	3	3	3	3
15	システム障害による業務停止	2	2	3	3	3	3	3	3	3	3	3	3
16	システム障害による業務停止	2	2	3	3	3	3	3	3	3	3	3	3
17	システム障害による業務停止	2	2	3	3	3	3	3	3	3	3	3	3
18	システム障害による業務停止	2	2	3	3	3	3	3	3	3	3	3	3
19	システム障害による業務停止	2	2	3	3	3	3	3	3	3	3	3	3
20	システム障害による業務停止	2	2	3	3	3	3	3	3	3	3	3	3

早分かり

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アセスメントの実施と活用～

【活用の手引き 第2版】

独立行政法人 情報処理推進機構
セキュリティセンター

2026年4月



制御システムのセキュリティリスク分析ガイド

第2版 ガイド本編と別冊

【ガイド本編の目次】

- 1章 セキュリティ対策におけるリスク分析の位置付け
- 2章 リスク分析の全体像と作業手順
- 3章 リスク分析のための事前準備(1)
～分析対象の明確化～
- 4章 リスク分析のための事前準備(2)
～リスク値と評価指標～
- 5章 リスク分析の実施(1)
～資産ベースのリスク分析～
- 6章 リスク分析の実施(2)
～事業被害ベースのリスク分析～
- 7章 リスク分析結果の解釈と活用法
- 8章 セキュリティテスト
- 9章 特定対策に対する追加基準
- 参考文献、付録

2018年10月15日 第2版公開

2020年3月16日 同(2020年3月版)公開

2023年3月27日 同(2023年3月版)公開

2026年4月6日 同(2026年4月版)公開

ガイド本編



406頁

別冊#1



102頁

別冊#2



100頁

<https://www.ipa.go.jp/security/controlsystem/riskanalysis.html> からダウンロード可能

リスク分析の位置付けと重要性

～制御システムのセキュリティ維持・向上に有効な施策～

「リスク分析」 = ①②③を評価指標にリスクレベルを明確化するプロセス

- ① 分析対象(資産や事業)の価値(重要性)、想定される被害の規模・影響
- ② 分析対象に対して想定される脅威とその発生可能性
- ③ 想定される脅威が生じた際の受容可能性(分析対象の脆弱性)

プロセス	ISO/IEC 27000:2018(JIS Q 27000:2019)における規定
リスクアセスメント(risk assessment)	リスク特定、リスク分析及びリスク評価のプロセス全体
リスク特定(risk identification)	リスクを発見、認識及び記述するプロセス
リスク分析(risk analysis)	リスクの特質を理解し、リスクレベルを決定するプロセス
リスク評価(risk evaluation)	リスク及び／又はその大きさが受容可能か又は許容可能かを決定するために、リスク分析の結果をリスク基準と比較するプロセス
リスク対応(risk treatment)	リスクを修正するプロセス

リスク分析の重要性と有効性

- 実効的なリスクの低減の実現
- 効果的な投資の実現(追加対策、有効なテスト箇所抽出)
- PDCAサイクルの確立とセキュリティの維持向上を継続するためのベース

リスク分析の手法と課題

～様々なセキュリティリスク分析手法とその特徴、課題～

リスク分析の手法と特徴

分析手法		工数	効果	
ベースラインアプローチ		小	△	
非形式的アプローチ		小	×?	
詳細リスク分析	資産ベース	中	○	
	シナリオベース	攻撃ツリー解析(ATA)	大	○
		イベントツリー解析(ETA)	大	○
組み合わせアプローチ		大	◎	

詳細リスク分析の課題

【課題A】 リスク分析の具体的な手法や手順が分からない

【課題B】 リスク分析には膨大な工数を要する(と言われている)ので回避したい

 この課題にガイドはお答えします

2種類の詳細リスク分析を解説

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

★ 資産ベースのリスク分析

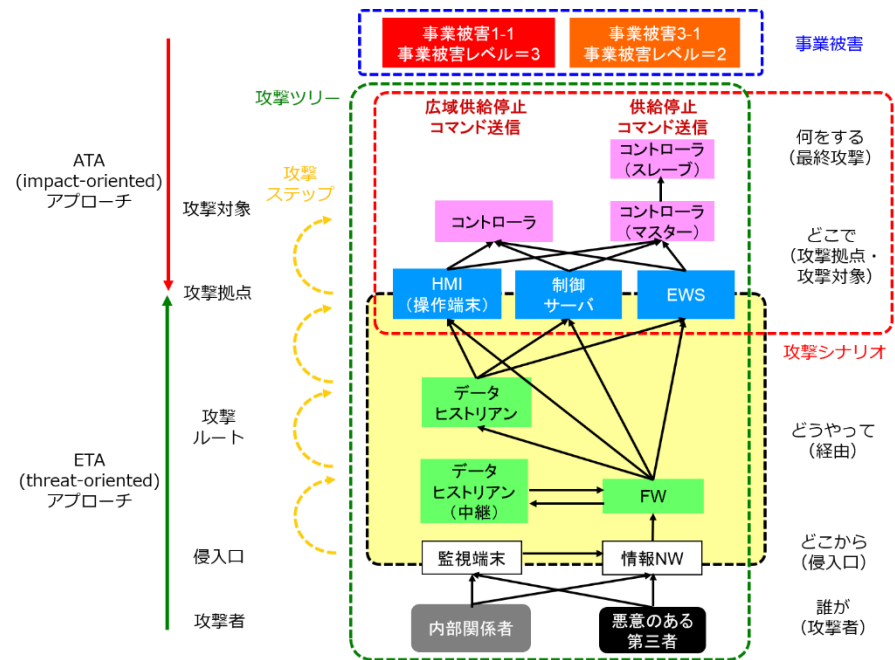
制御システムを構成する資産を対象に、各資産（サーバ、端末、通信機器等）に対して、その重要度（価値）、想定される脅威、脆弱性の3つを評価指標として、リスク分析を実施。
 ⇒ 資産に対して網羅的に脅威と対策状況を評価可能

★ 事業被害ベースのリスク分析

制御システムにおいて実現されている事業やサービスに対して、回避したい事業被害を定義し、発生した際の事業被害のレベル、その被害を起こしうる攻撃シナリオによる脅威、そのシナリオに対する脆弱性（そのシナリオの受容可能性）の3つを評価指標として、リスク分析を実施。

⇒ 一次攻撃脅威から、連鎖して事業被害に繋がる攻撃を、評価可能
 （ETAとATAの利点を融合）

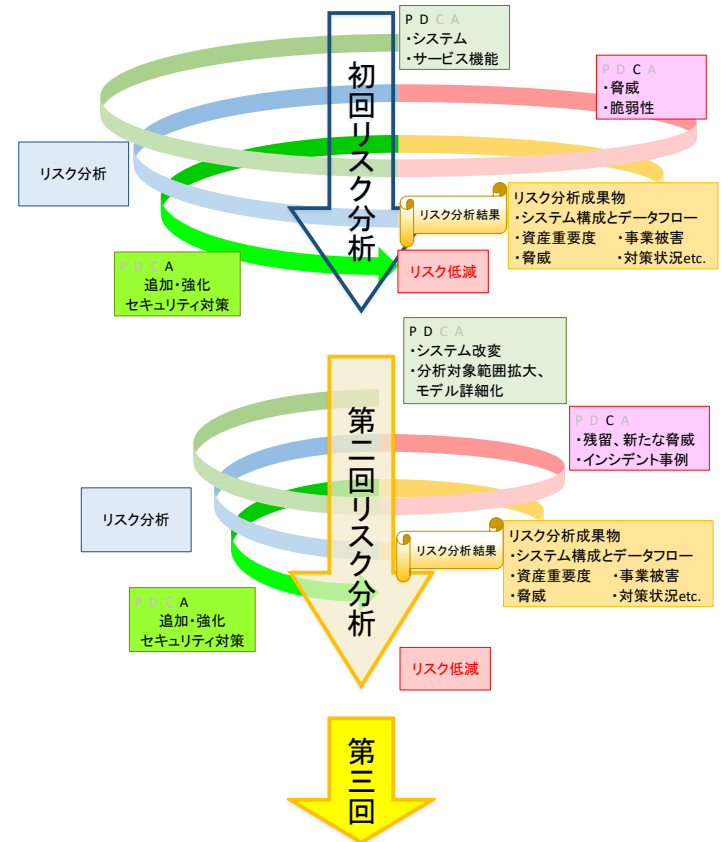
⇒机上でのペネトレーションテスト



1. セキュリティ対策における リスク分析の位置付け

制御システムのリスク分析の位置付け、重要性、必要性を説明

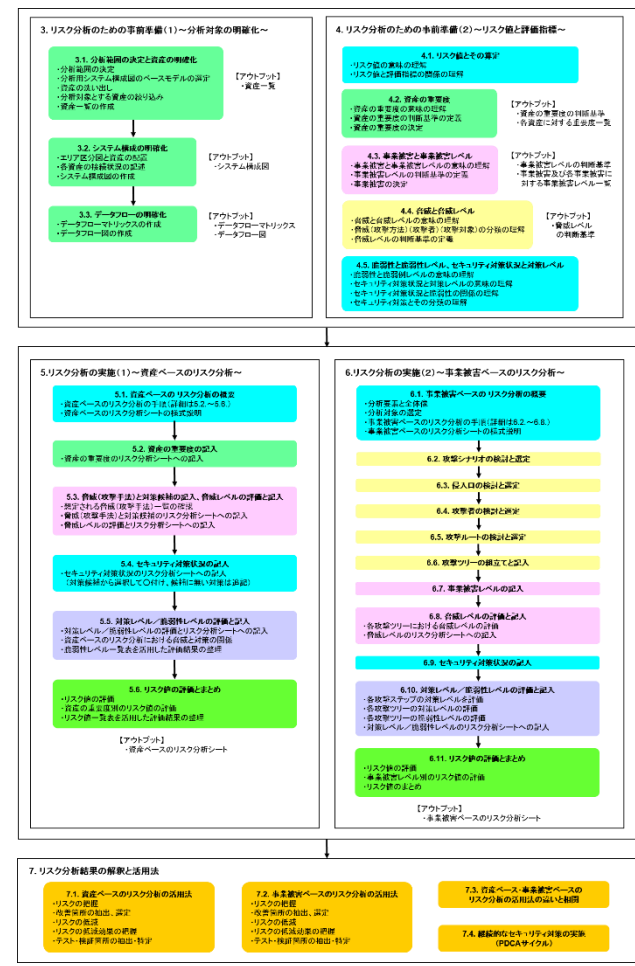
- 制御システムにおけるセキュリティ対策の必要性
 - 構成システム、コンポーネントの変化
 - 外部ネットワークとの接続、外部からの記憶媒体の持込み
 - システムの特性、位置づけ
 - 脆弱性の報告増加、標的型サイバー攻撃やマルウェア感染等の報告増加
- リスク分析の位置付けと重要性
 - 保護すべきシステムやそれによって実現している事業に対する脅威と被害のレベルを明確化するプロセス
 - セキュリティ対策上、必要不可欠



2. リスク分析の全体像と作業手順

リスク分析の手法比較、作業手順、本ガイドの利用方法を紹介

- リスク分析の全体像**
 - ベースラインアプローチ
 - 非形式的アプローチ
 - 詳細リスク分析
 - 組合せアプローチ
- リスク分析の作業手順**
 - 資産ベースのリスク分析
 - 事業被害ベースのリスク分析
- 本ガイドの構成と利用方法**
 - 本ガイドの構成
 - 実施に当たっての提言



3. リスク分析のための事前準備 (1)

～分析対象の明確化～

自組織の分析と把握 = 「己を知る最も重要なステップ」

【事前準備作業とそのアウトプット】

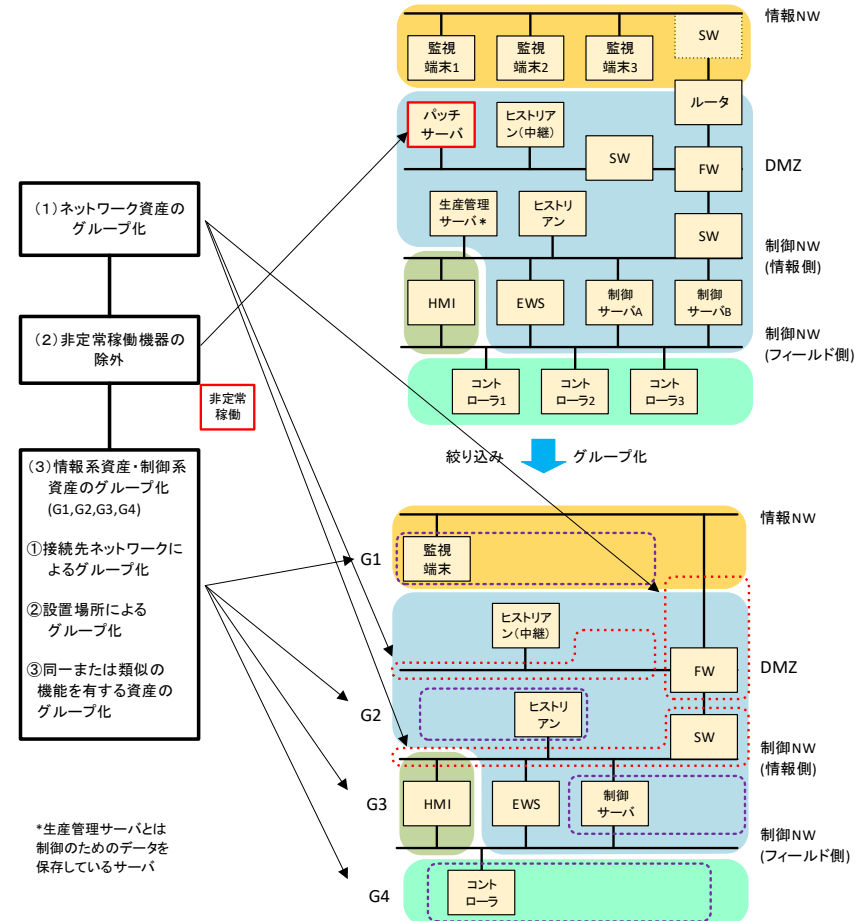
節	準備作業	アウトプット
3.1	<ul style="list-style-type: none">分析範囲の決定と資産の明確化	<ul style="list-style-type: none">資産一覧
3.2	<ul style="list-style-type: none">システム構成(ネットワーク構成を含む)の明確化	<ul style="list-style-type: none">システム構成図
3.3	<ul style="list-style-type: none">データフローの明確化	<ul style="list-style-type: none">データフローマトリックスデータフロー図

3. リスク分析のための事前準備 (1)

3.1. 分析範囲の決定と資産の明確化

- 分析範囲の決定
- 分析用システム構成図のベースモデルの選定
- 資産の洗い出し
- 分析対象とする資産の絞り込み
- 資産一覧の作成

【資産の絞り込み手順例】



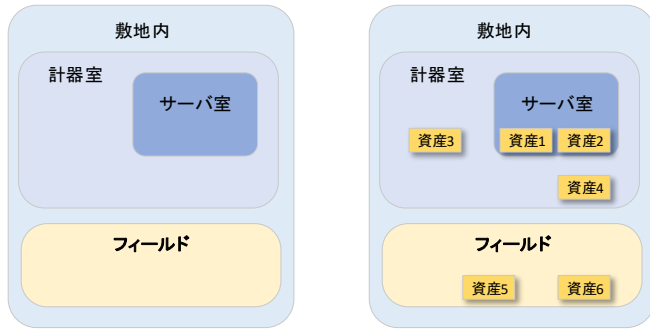
【資産一覧表】

No.	1	2	3	4	5	6	7	8
資産名	監視端末	ファイアウォール	DMZ	データヒストリアン(中継)	制御サーバ	EWS	コントローラ(マスター)	フィールドNW
資産種別	情報系資産	制御系資産	ネットワーク資産					
資産の持つ機能	入出力	データ保存	コマンド発行	ゲート				
回線種類	執務室	サーバ室	LAN	サーバ室	サーバ室	サーバ室	フィールド	専用線
接続先NW	情報NW	DMZ	制御NW(情報側)	制御NW(フィールド側)	その他			
管理ポートの接続先	x	情報NW	x	x	x	x	x	x
操作I/Fの有無	o	x		o	o	o	o	x
USBポート/通信I/Fの利用	o(USB)	o(LAN)		o(USB)	o(USB)	o(USB)	o(USB)	
媒体・機器接続の定常運用の有無	x	x	x	x	x	x	x	x
無線機能の有無	x	x	x	x	x	x	x	x
定常稼働、非定常稼働	定常稼働	定常稼働	定常稼働	定常稼働	定常稼働	定常稼働	定常稼働	定常稼働
データの種類と経路	データフローマトリックスに記載							
構築ベンダー/機器メーカー	AB/XX	AB/YY	AB/ZZ	AB/XX	AB/XX	AB/XX	AB/XX	AB/ZZ
OSの種類/バージョン	Windows	独自OS	Windows	Windows	Windows	Windows	独自OS	独自OS
使用するプロトコル	TCP, UDP	TCP, UDP	TCP, UDP	TCP, UDP	TCP,UDP:独自	TCP, UDP	独自	独自
セキュリティ対策	資産ベースのリスク分析シートに記載							

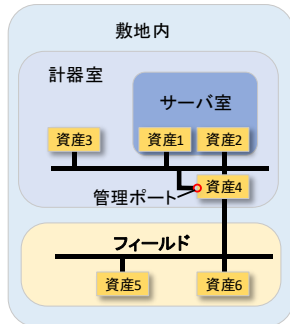
3. リスク分析のための事前準備 (1)

3.2. システム構成の明確化

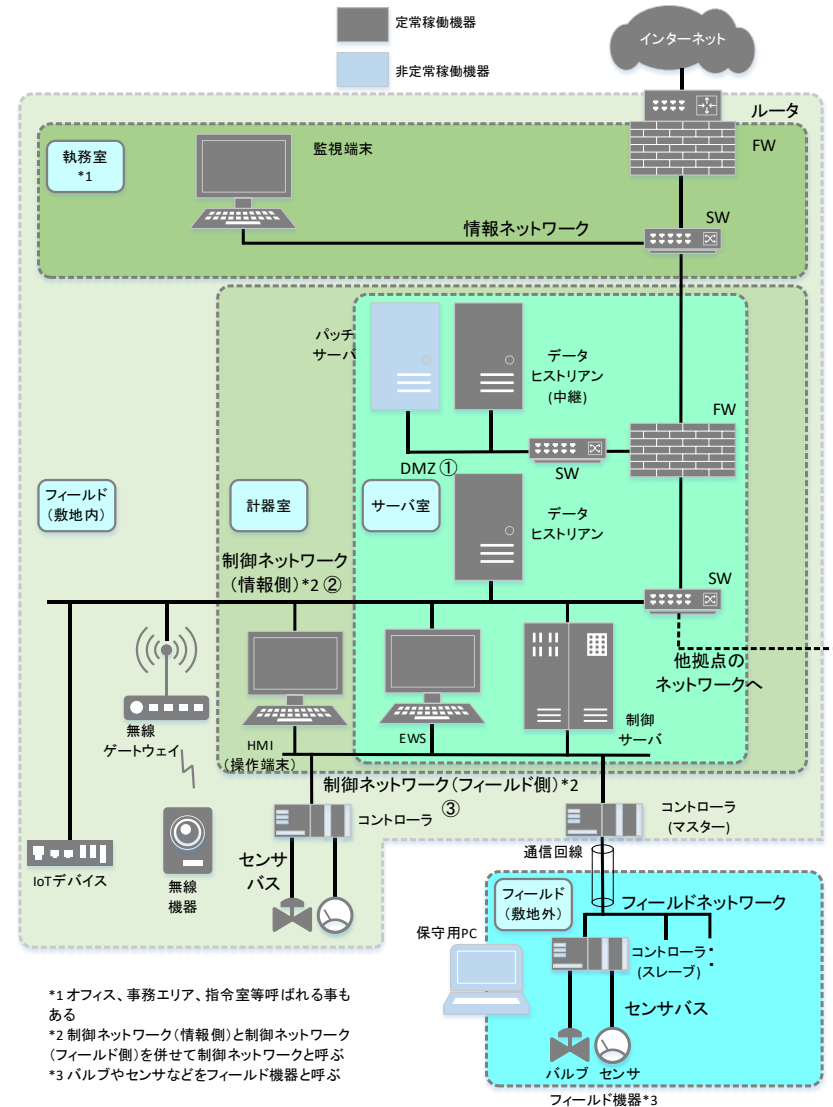
- エリア区分図と資産の配置



- 各資産の接続状況の記述



- システム構成図の作成 →



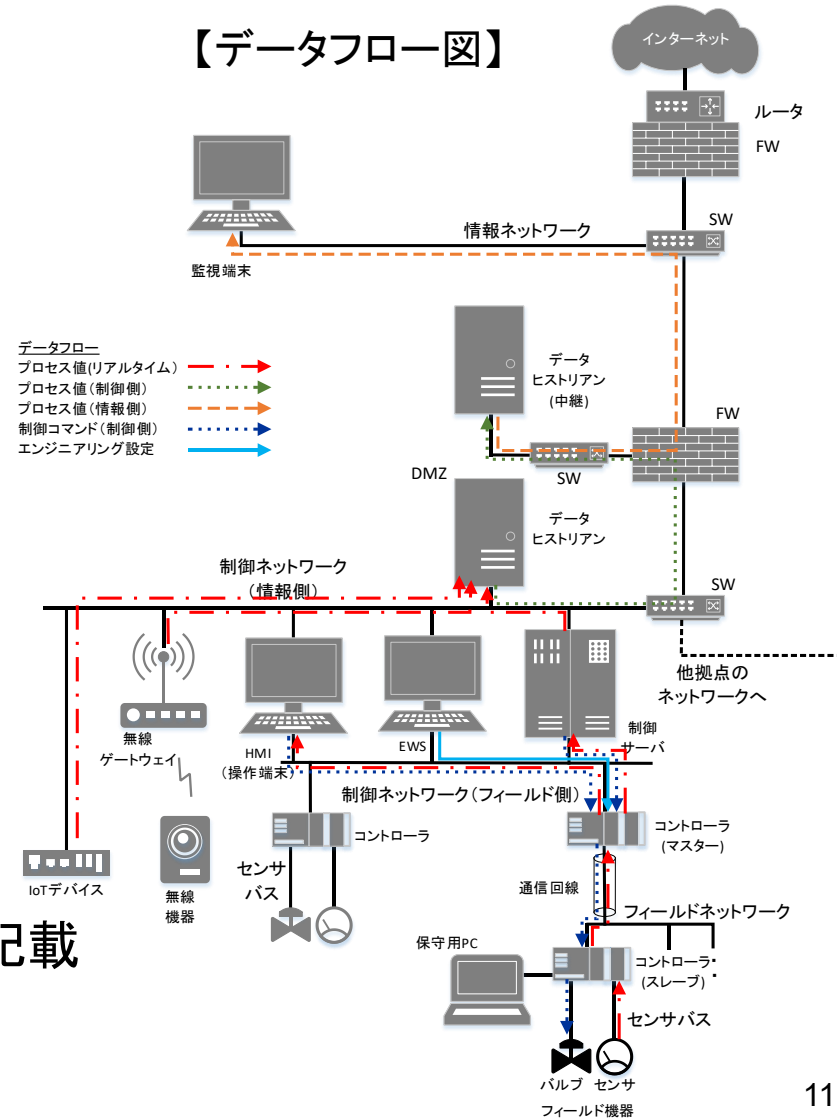
3. リスク分析のための事前準備 (1)

3.3. データフローの明確化

- データフローマトリックスの作成
 - データの流れをfrom/toで整理

To \ From	監視端末	FW	データヒストリアン (中継)	データヒストリアン	EWS	制御サーバ	HMI (操作端末)	IoTデバイス	無線ゲートウェイ	無線機器	コントローラ (マスター)	コントローラ (スレーブ)
監視端末	■											
FW		■										
データヒストリアン (中継)			■									
データヒストリアン				■								
EWS					■							S
制御サーバ						■						C
HMI (操作端末)							■					C
IoTデバイス								■				
無線ゲートウェイ									■			
無線機器										■		
コントローラ (M)											■	C
コントローラ (S)												■

- データフロー図の作成
 - データフローをシステム構成図に記載



4. リスク分析のための事前準備 (2)

～リスク値と評価指標～

リスク値と評価指標を理解し、判断基準の一部を自身で定義

【事前準備作業とそのアウトプット】

節	準備作業(抜粋)	アウトプット
4.1	<ul style="list-style-type: none"> リスク値の意味の理解 リスク値と評価指標の関係の理解 	
4.2	<ul style="list-style-type: none"> 資産の重要度の判断基準の定義 資産の重要度の決定 	<ul style="list-style-type: none"> 資産の重要度の判断基準 各資産に対する重要度一覧
4.3	<ul style="list-style-type: none"> 事業被害レベルの判断基準の定義 事業被害の決定 	<ul style="list-style-type: none"> 事業被害レベルの判断基準 事業被害及び各事業被害に対する事業被害レベル一覧
4.4	<ul style="list-style-type: none"> 脅威と脅威レベルの意味の理解 脅威レベルの判断基準の定義 	<ul style="list-style-type: none"> 脅威レベルの判断基準
4.5	<ul style="list-style-type: none"> セキュリティ対策状況と脆弱性の関係の理解 	

4. リスク分析のための事前準備 (2)

4.1. リスク値とその算定

• リスク値

- 保護対象が損なわれる各々のリスクに対して、被害の大きさと脅威の発生可能性／受容可能性を、相対評価可能な値として算定した値

【リスク値の意味】

リスク値	意味
A	リスクが非常に高い。
B	リスクが高い。
C	リスクが中程度
D	リスクが低い。
E	リスクが非常に低い。

【分析手法と評価指標の関係】

リスク分析手法	評価指標			
	資産の重要度	事業被害	脅威	脆弱性
資産ベース	○	—	○	○
事業被害ベース	—	○	○	○

4. リスク分析のための事前準備 (2)

4.2. 資産の重要度

• 資産の重要度

- 資産ベースのリスク分析における評価指標の一つ
- システム資産としての価値、攻撃によって想定される事業被害や事業継続性への影響を考慮した評価値(1:低~3:高)

【資産の重要度の判断基準の定義例】

評価値	判断基準
3	<ul style="list-style-type: none">・資産が攻撃された場合、<u>システムが長期間停止</u>する恐れがある。・資産から情報が漏えいした場合、<u>巨額の損失</u>が発生する恐れがある。・資産が攻撃された場合、<u>大規模の人的／環境被害</u>が発生する恐れがある。
2	<ul style="list-style-type: none">・資産が攻撃された場合、<u>システムが一定期間停止</u>する恐れがある。・資産から情報が漏えいした場合、<u>ある程度の損失</u>が発生する恐れがある。・資産が攻撃された場合、<u>中規模の人的／環境被害</u>が発生する恐れがある。
1	<ul style="list-style-type: none">・資産が攻撃された場合、<u>システムが短期間停止</u>する恐れがある。・資産から情報が漏えいした場合、<u>小額の損失</u>が発生する恐れがある。・資産が攻撃された場合、<u>小規模の人的／環境被害</u>が発生する恐れがある。

4. リスク分析のための事前準備 (2)

4.3. 事業被害と事業被害レベル

- 事業被害レベル
 - － 事業被害ベースのリスク分析における評価指標の一つ
 - － 脅威によって生じる事業被害の評価値(1:小～3:大)

【事業被害レベルの判断基準の定義例】

評価値	判断基準
3	事業上の被害が <u>大きい</u> 。 【例】 ・発生した場合、被害範囲は <u>システム全体に及ぶ</u> 。 ・会社の経営上、 <u>致命的もしくは永続的な打撃</u> を与える可能性がある。
2	事業上の被害が <u>中程度</u> 。 【例】 ・発生した場合、被害範囲が <u>システムの一部に限定される</u> 。 ・会社の経営上、 <u>大きなもしくは長期的な打撃</u> を与える可能性がある。
1	事業上の被害が <u>小さい</u> 。 【例】 ・発生した場合、被害範囲は <u>システムの極一部に限定される</u> 。 ・会社の経営上、 <u>中程度以下もしくは一時的な打撃</u> を与える可能性がある。

4. リスク分析のための事前準備 (2)

4.3. 事業被害と事業被害レベル

● 事業被害

- － 組織の事業の安定的な運営や継続を阻害する事象・状況
- － 発生時の被害範囲や会社経営上の打撃を基に各事業者にて定義

項番	事業被害	事業被害の概要	事業被害レベル
1	広域での 〇〇供給停止	〇〇製造設備、〇〇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
2	限定地域での 〇〇供給停止	〇〇製造設備、〇〇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
3	仕様不良 〇〇の供給	〇〇製造設備、〇〇供給設備等へのサイバー攻撃により、規定の仕様を満たさない〇〇を顧客に供給してしまい、社会に影響を及ぼし、賠償費用等の損失が生じると共に、当社の信頼が低下する。	2
4	設備の破壊	〇〇製造設備、〇〇供給設備等へのサイバー攻撃により、設備が破壊されて供給停止が発生すると共に、従業員や近隣住民の死傷者が出て、社会に多大な影響を及ぼし、賠償費用等の高額な損失が生じると共に、当社の信頼が大きく低下する。	3
5	大規模対策費用 の発生	サイバー攻撃を受け、〇〇の供給停止の被害は発生しなかったものの、現行対策の脆弱性が明らかとなり、その解消のために膨大な対策費用が発生する。	1

4. リスク分析のための事前準備 (2)

4.4. 脅威と脅威レベル

• 脅威レベル

- 2種類のリスク分析における評価指標の一つ
- それぞれのリスク分析において、
想定する脅威が発生する可能性の評価値(1:低~3:高)

【脅威レベルの判断基準の定義例】

評価値	判断基準
3	<p>脅威が発生する可能性が<u>高い</u>。</p> <p>【例】</p> <ul style="list-style-type: none"> ・<u>個人の攻撃者(スキルは問わない)</u>によって、攻撃が試みられる可能性がある。 ・<u>外部からアクセス可能なネットワーク(例:DMZ や情報ネットワーク)</u>上にある資産に対して、攻撃が試みられる可能性がある。
2	<p>脅威が発生する可能性が<u>中程度</u>である。</p> <p>【例】</p> <ul style="list-style-type: none"> ・<u>一定のスキルを持った攻撃者</u>によって、攻撃が試みられる可能性がある。 ・<u>イントラネット(例:制御ネットワーク(情報側))</u>上にある資産に対して、攻撃が試みられる可能性がある。
1	<p>脅威が発生する可能性が<u>低い</u>。</p> <p>【例】</p> <ul style="list-style-type: none"> ・<u>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)</u>によって、攻撃が試みられる可能性がある。 ・<u>特定の制限されたネットワーク(例:制御ネットワーク(制御側))</u>上にある資産に対して、攻撃が試みられる可能性がある。

4. リスク分析のための事前準備 (2)

4.4. 脅威と脅威レベル

【資産(機器)に対する脅威(攻撃手法)の抜粋】

#	脅威(攻撃手法)	説明	具体例
1	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。	<ul style="list-style-type: none"> ● 不正入手した認証情報の悪用(不正ログイン) ● 認証機構を持たない機器への侵入 ● 機器に内在する脆弱性の悪用 ● 設定不備(不要プロセス動作や不要ポート開放等)の悪用
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。	<ul style="list-style-type: none"> ● 敷地内/計器室/サーバ室への不正侵入 ● ラック/設置箱の不正開放
3	不正操作	機器のコンソール等の直接操作で侵入し、攻撃を実行する。	<ul style="list-style-type: none"> ● 不正入手した認証情報の悪用(不正ログイン) ● 認証機構を持たない機器への侵入 ● 機器に内在する脆弱性の悪用
4	過失操作	内部関係者(社員や協力者のうち、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。	<ul style="list-style-type: none"> ● メール添付ファイル開封 ● マルウェアに感染した正規媒体の持ち込み
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。	<ul style="list-style-type: none"> ● 不正媒体の接続 ● 媒体からの読み込み/媒体への書き出し
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。	<ul style="list-style-type: none"> ● プログラム/コマンドの不正実行 ● サービスの不正起動
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。	
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。	<ul style="list-style-type: none"> ● 制御パラメータの窃取
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。	<ul style="list-style-type: none"> ● 制御プログラムの改ざん ● 制御パラメータの改ざん
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。	<ul style="list-style-type: none"> ● 制御データの削除 ● 制御データの強制暗号化
11	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。	<ul style="list-style-type: none"> ● 制御コマンド/データ送信命令の不正実行 ● 送信データの改ざん
12	機能停止	機器の機能を停止する。	<ul style="list-style-type: none"> ● 停止命令の不正実行 ● 機能停止に至る脆弱性の悪用

4. リスク分析のための事前準備 (2)

4.5. 脆弱性と脆弱性レベル、セキュリティ対策状況と対策レベル

• 脆弱性レベル

- 2種類のリスク分析における評価指標の一つ
- それぞれのリスク分析において、発生した脅威を受け入れる可能性の評価値(1:低~3:高)

評価値		判断基準
脆弱性レベル	対策レベル	
3	1	<p>脅威が発生した場合、<u>受け入れる可能性が高い</u>。 <u>脅威の対策が実施されておらず</u>、攻撃が成功する可能性は高い。</p> <p>【例】</p> <ul style="list-style-type: none"> ・過去の事例において、脆弱性を利用した攻撃が発生・成功し、被害が生じたことが確認されている。
2	2	<p>脅威が発生した場合、<u>受け入れる可能性が中程度である</u>。 <u>脅威の対策が実施されているが、十分とは言えない</u>ため、攻撃が成功する可能性は中程度である。</p> <p>【例】</p> <ul style="list-style-type: none"> ・<u>一般的な対策を実施</u>しており、攻撃が成功するか否かは攻撃者のレベルに依る。 ・過去の事例において、脆弱性を利用した攻撃が発生したが、大きな被害に至らなかったことが確認されている。
1	3	<p>脅威が発生した場合、<u>受け入れる可能性が低い</u>。 <u>脅威の対策が十分実施</u>されており、攻撃が成功する可能性は低い。</p> <p>【例】</p> <ul style="list-style-type: none"> ・<u>効果的な対策や、多層的な対策を実施</u>しており、攻撃が成功する可能性は低い。 ・過去の事例において、脆弱性を利用した攻撃は発生していない。

4. リスク分析のための事前準備 (2)

4.5. 脆弱性と脆弱性レベル、セキュリティ対策状況と対策レベル

脅威、セキュリティ対策、その対応の一覧を提供

【セキュリティ対策項目一覧(全50項目)】

【脅威(攻撃手法)と技術的/物理的対策の候補一覧】

表 4-29 セキュリティ対策項目一覧(14)

#	セキュリティ対策	用途・目的			留意
		目的	効果	留意事項	
1	FW(パケットフィルタリング)	○	△	△	不正通信を遮断するために、送信元及び宛先のIPアドレス(ネットワーク層)やポート番号(トランスポート層)を識別して、通信を制御する。ファイアウォール(防火壁、壁)はファイアウォールと呼ばれることが多いが、他はファイアウォールと区別する必要がある。パケットフィルタリング型ファイアウォールは特長。
2	FW(アプリケーションゲートウェイ型)	○	△	△	アプリケーションを目的に送信元と宛先とのプロトコルレベル(アプリケーション層)やアプリケーションの種類(アプリケーション種別)を識別して、通信を制御する。ファイアウォール(防火壁、壁)とは、アプリケーションゲートウェイ型ファイアウォールと区別する必要がある。WAF(アプリケーションゲートウェイ型ファイアウォール)と呼ばれることもあるが、WAFはアプリケーションゲートウェイ型ファイアウォールと区別する必要がある。WAFはアプリケーションゲートウェイ型ファイアウォールと区別する必要がある。
3	一方向ゲートウェイ	○	△	△	不正通信を遮断するために、パケットフィルタリングやポート番号を識別して通信を制御する。ファイアウォール(防火壁、壁)とは、一方向ゲートウェイ型ファイアウォールと区別する必要がある。WAF(アプリケーションゲートウェイ型ファイアウォール)と呼ばれることもあるが、WAFはアプリケーションゲートウェイ型ファイアウォールと区別する必要がある。
4	プロキシサーバ	○	△	△	特定のサービスに対して、ネットワーク層(IP アドレス)やネットワーク層を識別して、通信を制御するために、内部ネットワークと外部ネットワークの境界を識別して、パケットフィルタリングやポート番号を識別して、通信を制御する。ウェブサーバへのアクセスを集中するWAF(ウェブフィルタリング)、電子メールを集中するSMTPプロキシサーバがある。インターネットゲートウェイ型ファイアウォールとは区別する必要がある。なお、通信を制御する機能を実現するプロキシサーバは、FW(アプリケーションゲートウェイ型)と区別する必要がある。WAF(ウェブフィルタリング)やSMTPプロキシサーバとは区別する必要がある。WAF(ウェブフィルタリング)やSMTPプロキシサーバとは区別する必要がある。
5	IPS/IDS (IDS:検知機能のみ IPS:遮断機能使用)	○	○	○	不正通信を遮断するために、ネットワーク上の通信パケットを収集・解析し、不正な通信の検知及び検知を行う「ネットワーク監視(IDS)」。また、検知された入出力データの検知結果を基に、不正な通信の検知及び検知を行う「ネットワーク監視(IPS)」。不正な通信の検知を行うIDS(検知)機能のみならず、検知した不正通信を遮断するIPS(遮断)機能も併用する必要がある。
6	DDoS対策	○	○	○	DDoS(Distributed Denial of Service)攻撃の防止。DDoS対策は、DDoS攻撃の防止に有効な手段である。DDoS対策は、DDoS攻撃の防止に有効な手段である。DDoS対策は、DDoS攻撃の防止に有効な手段である。
7	通信相手の確認	○	△	△	通信相手を確認するために、送信元と宛先を識別して、通信を制御する。ファイアウォール(防火壁、壁)とは、通信相手を確認するために、送信元と宛先を識別して、通信を制御する。ファイアウォール(防火壁、壁)とは、通信相手を確認するために、送信元と宛先を識別して、通信を制御する。
8	脆弱性診断	○	○	○	脆弱性診断は、脆弱性を検出するために、送信元と宛先を識別して、通信を制御する。脆弱性診断は、脆弱性を検出するために、送信元と宛先を識別して、通信を制御する。脆弱性診断は、脆弱性を検出するために、送信元と宛先を識別して、通信を制御する。
9	通信経路の強化	○	○	○	通信経路を強化するために、送信元と宛先を識別して、通信を制御する。通信経路を強化するために、送信元と宛先を識別して、通信を制御する。通信経路を強化するために、送信元と宛先を識別して、通信を制御する。
10	アンチウイルス (ローランニングプログラム DLL-スキャン方式)	○	○	○	ウイルスを検出するために、送信元と宛先を識別して、通信を制御する。アンチウイルスは、ウイルスを検出するために、送信元と宛先を識別して、通信を制御する。アンチウイルスは、ウイルスを検出するために、送信元と宛先を識別して、通信を制御する。
11	WAF	○	△	△	WAF(ウェブフィルタリング)は、アプリケーションゲートウェイ型ファイアウォール(防火壁、壁)とは、アプリケーションゲートウェイ型ファイアウォールと区別する必要がある。WAF(ウェブフィルタリング)は、アプリケーションゲートウェイ型ファイアウォールと区別する必要がある。WAF(ウェブフィルタリング)は、アプリケーションゲートウェイ型ファイアウォールと区別する必要がある。

表 4-33 脅威(攻撃手法)と技術的/物理的対策の候補一覧(13)

#	脅威(攻撃手法)	技術的/物理的対策の候補			
		目的	目的/対策候補	特長/留意事項	留意事項
1	不正アクセス	不正アクセス	不正アクセス対策 ・IPアドレスフィルタリング [1] ・パケットフィルタリング [2] ・一方向ゲートウェイ [3] ・パケットフィルタリング [4] ・WAF [1] ・通信相手確認 [7] ・IPS/IDS [5] ・パケット監視 [15] ・脆弱性診断 [16]	不正アクセス対策 ・ログ収集・分析 [36] ・結合型管理システム [37]	
2	物理的侵入	物理的侵入	物理的侵入対策 ・物理的侵入対策 [14] ・脆弱性診断 [16]	物理的侵入対策 ・侵入検知 [34] ・侵入防止 [35]	
3	不正操作	不正操作	不正操作対策 [14]		
4	過失操作	過失操作	過失操作対策 ・WAF/ウェブフィルタリング [12] ・メールフィルタリング [13]		
5	不正操作継続	不正操作継続	不正操作対策 ・不正アクセス対策/利用制限 [19] ・脆弱性診断 [16]	不正操作対策 ・不正アクセス対策/利用制限 [19] ・ログ収集・分析 [36] ・結合型管理システム [37]	
6	プロセス不正実行	プロセス不正実行	プロセス不正実行対策 ・プロセス監視 [23] ・プロセス監視 [24] ・プロセス監視 [25] ・脆弱性診断 [16]	プロセス不正実行対策 ・脆弱性診断 [24] ・プロセス監視 [23] ・ログ収集・分析 [36] ・結合型管理システム [37]	
7	マルウェア感染	マルウェア感染	マルウェア感染対策 ・マルウェア検出/防止/除去 の脆弱性診断 [22] ・脆弱性診断 [16] ・脆弱性診断 [16] ・脆弱性診断 [16]	マルウェア感染対策 ・脆弱性診断 [24] ・ログ収集・分析 [36] ・結合型管理システム [37]	
8	情報窃取	情報窃取	情報窃取対策 ・脆弱性診断 [23] ・プロセス監視 [24] ・脆弱性診断 [16] ・脆弱性診断 [16]	情報窃取対策 ・脆弱性診断 [24] ・ログ収集・分析 [36] ・結合型管理システム [37]	
9	情報盗竊	情報盗竊	情報盗竊対策 ・脆弱性診断 [23] ・プロセス監視 [24] ・脆弱性診断 [16]	情報盗竊対策 ・脆弱性診断 [24] ・ログ収集・分析 [36] ・結合型管理システム [37]	データバックアップ [31]
10	情報破壊	情報破壊	情報破壊対策 ・脆弱性診断 [23] ・脆弱性診断 [16]	情報破壊対策 ・脆弱性診断 [24] ・ログ収集・分析 [36] ・結合型管理システム [37]	データバックアップ [31]
11	不正送信	不正送信	不正送信対策 ・メールフィルタリング/脆弱性診断 [17] ・脆弱性診断 [16] ・脆弱性診断 [16]	不正送信対策 ・脆弱性診断 [24] ・ログ収集・分析 [36] ・結合型管理システム [37]	
12	通信停止	通信停止	通信停止対策 ・脆弱性診断 [23] ・脆弱性診断 [16]	通信停止対策 ・脆弱性診断 [24] ・ログ収集・分析 [36] ・結合型管理システム [37]	冗長化 [32] ・フェールオーバー [47]
13	制御不能 異常動作	制御不能 異常動作	制御不能 異常動作対策 ・脆弱性診断 [16] ・脆弱性診断 [16]	制御不能 異常動作対策 ・脆弱性診断 [24] ・ログ収集・分析 [36] ・結合型管理システム [37]	フェールオーバー [47]

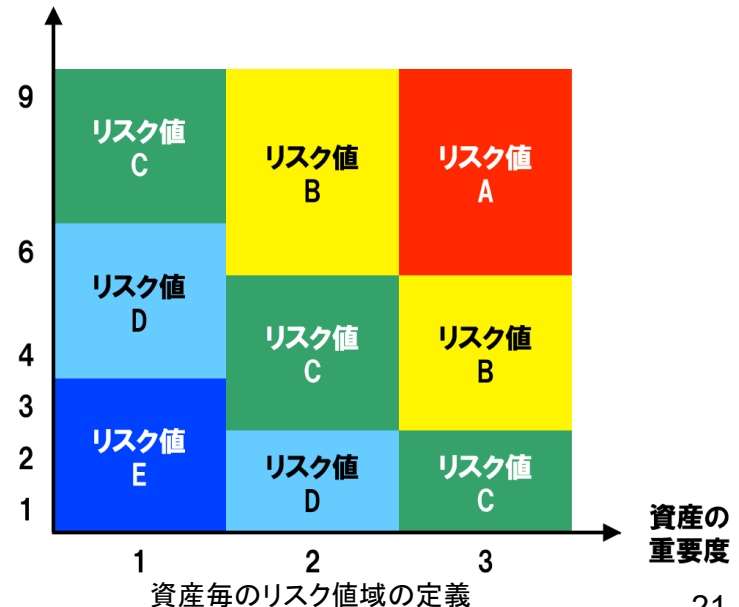
5. リスク分析の実施(1)

資産ベースのリスク分析

**制御システムを構成する資産に着目した分析手法の説明
～資産に対し想定される直接の脅威とその対策状況の十分性を評価～**

- 保護すべき制御システムを構成する資産群を対象に、
- 各資産のリスクの大きさ(リスク値)を、
 - 資産の重要度
 - 脅威レベル
(脅威の発生可能性)
 - 脆弱性レベル
(発生した脅威を受け入れる可能性)
 から算定

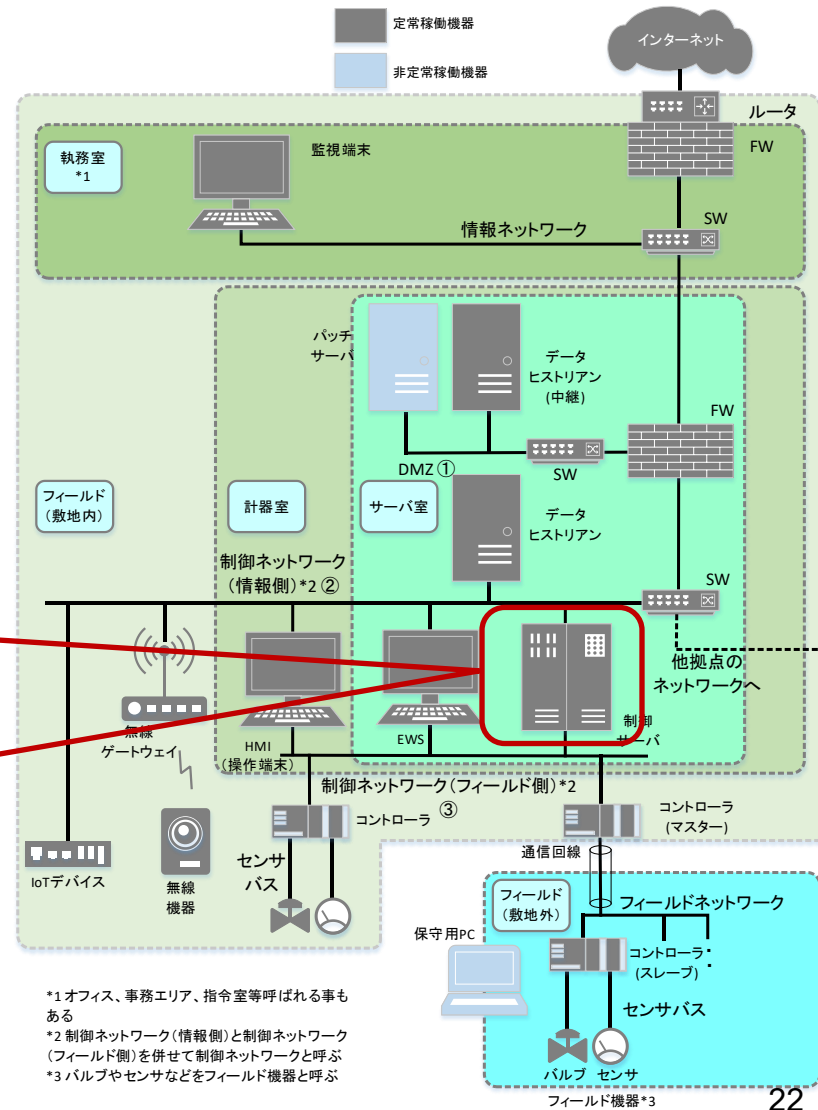
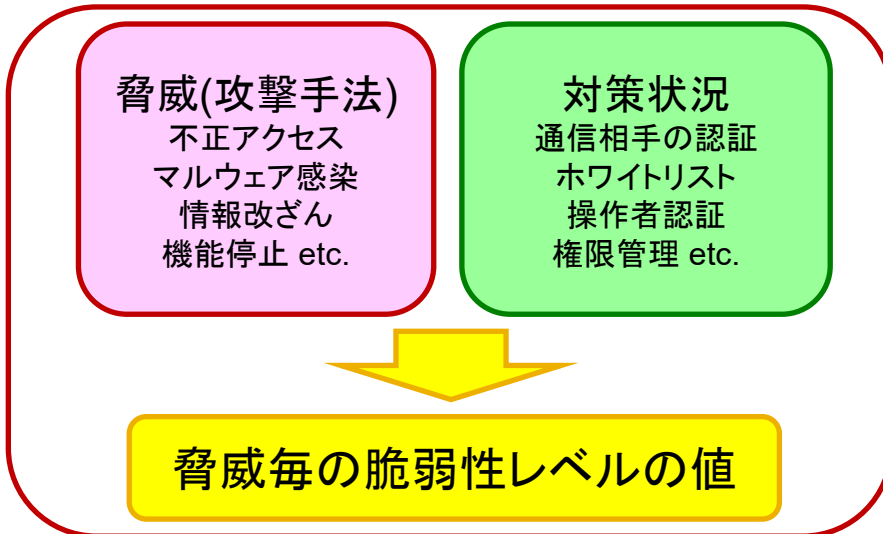
脅威レベル×脆弱性レベル



5. リスク分析の実施(1)

資産ベースのリスク分析

- 資産種別(情報系資産、制御系資産、通信経路)に基づいて脅威(攻撃手法)と対策候補をリストアップ
- 資産ごとに対策状況を記入「対策レベル」→「脆弱性レベル」



*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

5. リスク分析の実施(1)

資産ベースのリスク分析

資産ベースのリスク分析シート完成例

資産ベースのリスク分析シート

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

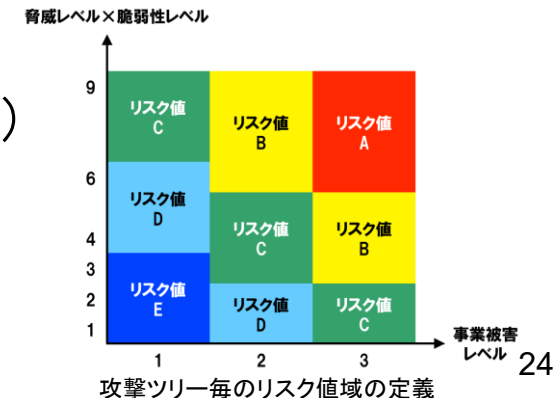
項番	資産種別	対象装置	評価指標		脅威(攻撃手法)	説明	対策				対策レベル			
			身元レベル	脆弱性レベル			侵害の重篤度	リスク値	検入/監視段階	対応		目的実行段階	検知/被害把握	事業継続
1	制御系資産	制御サーバ	2	2	B	不正アクセス	ネットワーク経由で機器に侵入し、攻撃を実行する。	ファイアウォール 通信相手の確認 IPSID パッチ適用 脆弱性診断	○			IPS/IDS ログ収集・分析 統合ログ管理システム	2	
2			2	1	C	物理的侵入	入室が制限された区域・領域(機器が設置された場所等)に不正侵入する。あるいは、物理的アクセスが制限された機器(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 施設管理	○ ○			監視カメラ 侵入センサー	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	○				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)の過失操作を誘致し、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レディケーション 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(CDDVD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		○	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	
6			3	1	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御 重要操作の承認	○ ○ ○ ○	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御 重要操作の承認	○ ○ ○ ○	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	
7			3	2	A	マルウェア感染	攻撃対象機器にマルウェア(不正プログラム)を感染・動作させる。	アンチウイルス ホワイトリストによるプロセスの起動制御 パッチ適用 脆弱性診断	○			機器異常検知 機器死活監視 ログ収集・分析 統合ログ管理システム	2	
8			3	2	A	情報窃取	機器内に格納されている情報(ソフトウェア、認証情報、構成設定情報、暗号鍵等の機密情報)を窃取する。	権限管理 アクセス制御 データ暗号化 DLP	○	権限管理 アクセス制御 データ暗号化 DLP	○	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	○	権限管理 アクセス制御 データ署名	○	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			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		セグメント分割/ゾーニング データ署名 重要操作の承認		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 安全計測システム(SIS)	1
13			1	3	B	制御不能・異常動作	機器を制御不能にする。異常動作を引き起こす。	パッチ適用 脆弱性診断				機器異常検知 ログ収集・分析 統合ログ管理システム	フェールセーフ設計 安全計測システム(SIS)	1
14			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
15			1	2	C	窃盗	機器を窃盗する。	施設管理			○	施設管理		2
16			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。	鍵管理 鍵廃止 セキュア消去				鍵管理 鍵廃止 セキュア消去		1

6. リスク分析の実施(2)

事業被害ベースのリスク分析

攻撃ツリーを用いたシナリオベースの詳細リスク分析手法の説明 ～事業に対し想定される攻撃とその対策状況の十分性を評価～

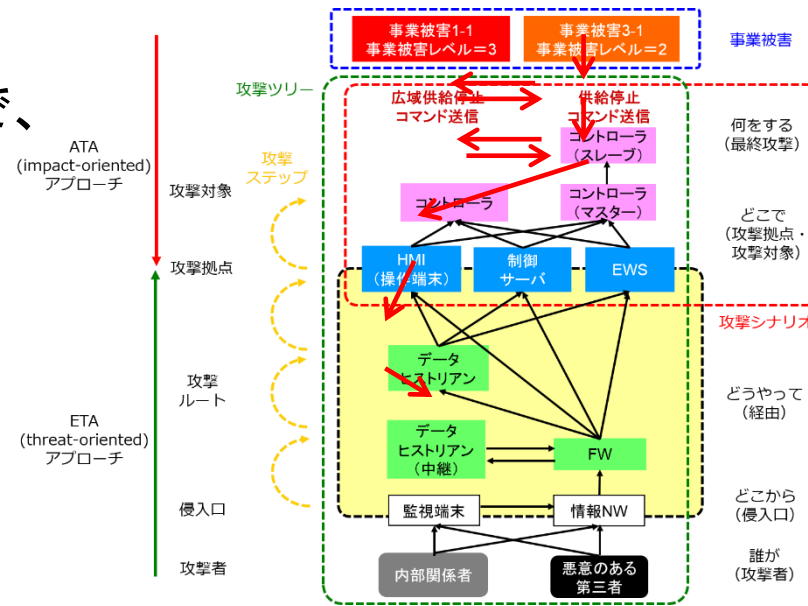
- 攻撃シナリオ
 - 回避したい事業被害を引き起こす可能性のある攻撃拠点・攻撃対象・最終攻撃を具現化したシナリオ
- 攻撃ツリー
 - 攻撃シナリオに含まれる攻撃拠点・攻撃対象・最終攻撃に加えて、攻撃シナリオを実現する攻撃者・侵入口・経路を具体化した一連の攻撃手順
- 各攻撃ツリーのリスクの大きさ(リスク値)を、
 - 脅威レベル(攻撃ツリーの発生可能性)
 - 脆弱性レベル(攻撃ツリーを受け入れる可能性)
 - 事業被害レベル(事業被害の大きさ)
 から算定



6. リスク分析の実施(2) 事業被害ベースのリスク分析

攻撃ツリーの構成

事業被害が「広域での〇〇供給停止」で、悪意のある第三者が、情報NW上の監視端末に侵入し、データヒストリアン(中継)、FW、データヒストリアンを経由して攻撃拠点のHMIに到達・侵入し、最終攻撃となる広域供給停止操作を実行する攻撃ツリーの場合



悪意のある第三者が、監視端末に不正アクセスする。	攻撃ステップ	攻撃ツリー
悪意のある第三者が、監視端末からデータヒストリアン(中継)に不正アクセスする。	攻撃ステップ	
悪意のある第三者が、データヒストリアン(中継)からデータヒストリアンに不正アクセスする。	攻撃ステップ	
悪意のある第三者が、データヒストリアンからHMIに不正アクセスする。	攻撃ステップ	
悪意のある第三者が、HMIからコントローラに、広域供給停止操作を不正実行し、広域で〇〇の供給が停止する。	最終攻撃ステップ	

6. リスク分析の実施(2) 事業被害ベースのリスク分析

分析対象の選定(1)

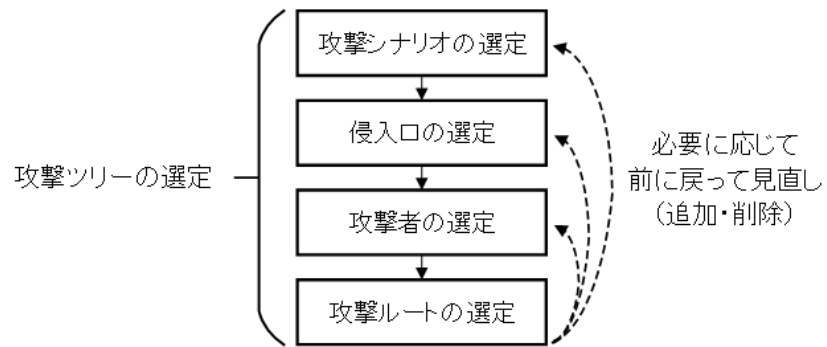
【青枠】

攻撃ツリーを選定しない場合の分析対象
→ 全ての事業被害、攻撃シナリオ、
侵入口、攻撃者、攻撃ルート进行分析

【赤枠】

攻撃ツリーを選定する場合の分析対象
→ 重要な事業被害を引き起こす
攻撃シナリオ、侵入口、攻撃者、
攻撃ルートを優先的に分析

事業被害	攻撃シナリオ	侵入口	攻撃者	攻撃ルート
事業被害 (事業被害レベル=2)	攻撃シナリオ	侵入口	悪意のある第三者	攻撃ルート
		侵入口	内部関係者	攻撃ルート
		侵入口	悪意のある第三者	攻撃ルート
		侵入口	内部関係者	攻撃ルート
	攻撃シナリオ	侵入口	悪意のある第三者	攻撃ルート
		侵入口	内部関係者	攻撃ルート
		侵入口	悪意のある第三者	攻撃ルート
		侵入口	内部関係者	攻撃ルート
	攻撃シナリオ	侵入口	悪意のある第三者	攻撃ルート
		侵入口	内部関係者	攻撃ルート
		侵入口	悪意のある第三者	攻撃ルート
		侵入口	内部関係者	攻撃ルート
事業被害 (事業被害レベル=3)	攻撃シナリオ	侵入口	悪意のある第三者	攻撃ルート
		侵入口	内部関係者	攻撃ルート
		侵入口	悪意のある第三者	攻撃ルート
		侵入口	内部関係者	攻撃ルート
	攻撃シナリオ	侵入口	悪意のある第三者	攻撃ルート
		侵入口	内部関係者	攻撃ルート
		侵入口	悪意のある第三者	攻撃ルート
		侵入口	内部関係者	攻撃ルート
	攻撃シナリオ	侵入口	悪意のある第三者	攻撃ルート
		侵入口	内部関係者	攻撃ルート
		侵入口	悪意のある第三者	攻撃ルート
		侵入口	内部関係者	攻撃ルート
事業被害 (事業被害レベル=1)	攻撃シナリオ	侵入口	悪意のある第三者	攻撃ルート
		侵入口	内部関係者	攻撃ルート
		侵入口	悪意のある第三者	攻撃ルート
		侵入口	内部関係者	攻撃ルート
	攻撃シナリオ	侵入口	悪意のある第三者	攻撃ルート
		侵入口	内部関係者	攻撃ルート
		侵入口	悪意のある第三者	攻撃ルート
		侵入口	内部関係者	攻撃ルート
	攻撃シナリオ	侵入口	悪意のある第三者	攻撃ルート
		侵入口	内部関係者	攻撃ルート
		侵入口	悪意のある第三者	攻撃ルート
		侵入口	内部関係者	攻撃ルート



6. リスク分析の実施(2)

事業被害ベースのリスク分析

- 分析対象の選定(2)

【物理アクセスによる攻撃の侵入口：優先度の判断の観点(例)】

項番	観点
1	機器にUSBポート、通信インターフェース、無線機能があり、使用可能か
2	機器にUSBメモリ、DVD、ノートPC等を接続する定常運用があるか
3	機器が攻撃拠点か
4	機器にキーボード、タッチパネル、スイッチ等の操作インターフェースがあるか
5	機器が定常機器か

【物理アクセスによる攻撃の侵入口：選定基準(例)】

<選定基準1> USBメモリやDVD等の媒体や、ノートPC等の機器を接続する定常運用がある機器

<選定基準2> 攻撃シナリオにおける攻撃拠点である機器で、操作インターフェースがある機器

6. リスク分析の実施(2)

事業被害ベースのリスク分析

事業被害ベースのリスク分析シート完成例

事業被害ベースのリスク分析シート

1. 広域での〇〇供給停止

項番	攻撃シナリオ	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	攻撃ツリー番号	構成ステップ(項番)		
						侵入/拡散段階	目的遂行段階							
1-1 広域供給停止操作の実行により、広域で供給が停止する。														
1	[D] 投入口監視漏れ 悪意ある第三者が、監視端末に不正アクセスする。					通信相手の認証 パッチ適用 脆弱性回避 権限管理	<input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/>	ログ収集・分析 統合ログ管理システム			2			
2	悪意ある第三者が、監視端末からデータベース(中絶)に不正アクセスする。					通信相手の認証 パッチ適用 脆弱性回避 権限管理	<input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/>	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			
3	悪意ある第三者が、データベース(中絶)からデータベース(中絶)に不正アクセスする。					通信相手の認証 パッチ適用 脆弱性回避 権限管理	<input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/>	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			
4	悪意ある第三者が、データベースからHMに不正にアクセスする。					通信相手の認証 パッチ適用 脆弱性回避 権限管理	<input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/>	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、HMからコントローラに広域供給停止操作をして、広域に及び供給が停止する。	2	2	3	B	セグメント分割/ ゾーニング データ署名 重要操作の承認	<input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/>	ログ収集・分析 統合ログ管理システム		1	2	#1	1,2,3,4,5	
1-2 複数コントローラへの供給停止コマンドの送信により、広域で供給が停止する。														
6	[P] 投入口=HM 内部関係者が、計器室に入室する。					入退管理(ICカード) 施設管理	<input type="radio"/> <input type="radio"/>	監視カメラ 侵入センサ ログ収集・分析			1			
7	内部関係者が、HMにログインする。					操作者認証	<input type="radio"/>	統合ログ管理システム ログ収集・分析			1			
8	内部関係者が、過失によりマルウェアに感染したUSB媒体をHMに接続し、HMのマルウェアに感染する。					アンチウイルス(媒体) アンチウイルス(HM) ポートの物理的閉塞 ホワイトリストによるプロセス起動制御 パッチ適用 脆弱性回避 データ署名	<input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/>	統合ログ管理システム 機器異常検知 機器死活監視 ログ収集・分析			1			
9	マルウェアが、HMからコントローラに広域供給停止操作をして、広域に及び供給が停止する。	2	3	3	A	セグメント分割/ ゾーニング データ署名 重要操作の承認	<input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/>	ログ収集・分析 統合ログ管理システム		1	1	#2	6,7,8,9	
1-2 複数コントローラへの供給停止コマンドの送信により、広域で供給が停止する。														
10	[D] 投入口=情報HW 悪意ある第三者が、情報HWからファイアウォールに不正アクセスする。					FW 通信相手の認証 パッチ適用 脆弱性回避 権限管理	<input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/>	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			
11	悪意ある第三者が、ファイアウォールを経由してEWSに不正にアクセスする。					通信相手の認証 パッチ適用 脆弱性回避 権限管理	<input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/>	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			
12	悪意ある第三者が、EWSからコントローラ(マスター)に不正アクセスする。					通信相手の認証 パッチ適用 脆弱性回避 権限管理	<input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/>	IPS/IDS ログ収集・分析 統合ログ管理システム 機器異常検知			1			
13	悪意ある第三者が、コントローラ(マスター)からコントローラ(スレーブ)に供給停止コマンドを送信して、広域に及び供給が停止する。	2	2	3	B	セグメント分割/ ゾーニング データ署名 重要操作の承認	<input type="radio"/> <input type="radio"/> <input type="radio"/> <input type="radio"/>	ログ収集・分析 統合ログ管理システム		1	2	#3	10,11,12,13	

●:実施しているが、有効でないと考えられる

7. リスク分析結果の解釈と活用法

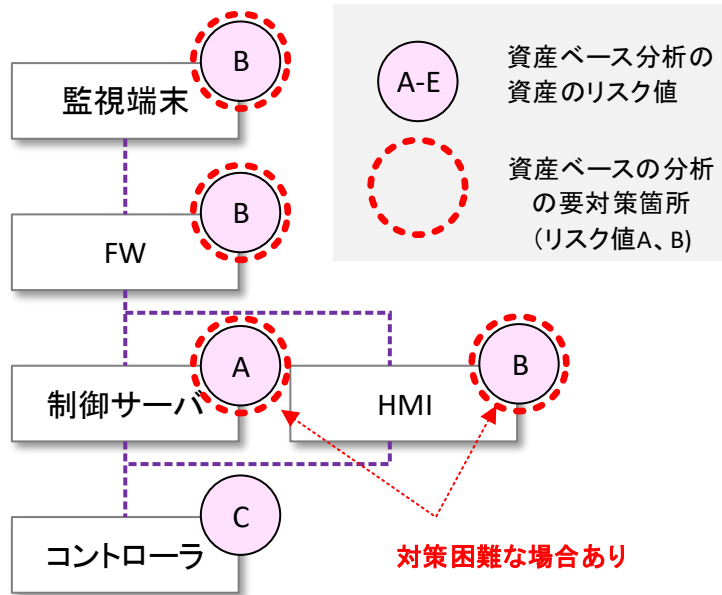
制御システムのセキュリティ向上へ向けた、新たなステップ

- リスク分析結果の解釈及び活用のねらい
 - セキュリティ上の弱点を発見し、サイバー攻撃に対するリスクを低減するため、分析結果として得られたリスク値を可能な限り低減する。
- リスク値の活用
 - リスクの把握
 - 改善箇所の抽出、選定
 - リスクの低減
 - リスクの低減効果の確認
 - セキュリティテストの対策箇所の抽出、特定
- 2種類のリスク分析の活用法の違いと相関
- 継続的なセキュリティ対策の実施(PDCAサイクル)

7. リスク分析結果の解釈と活用法

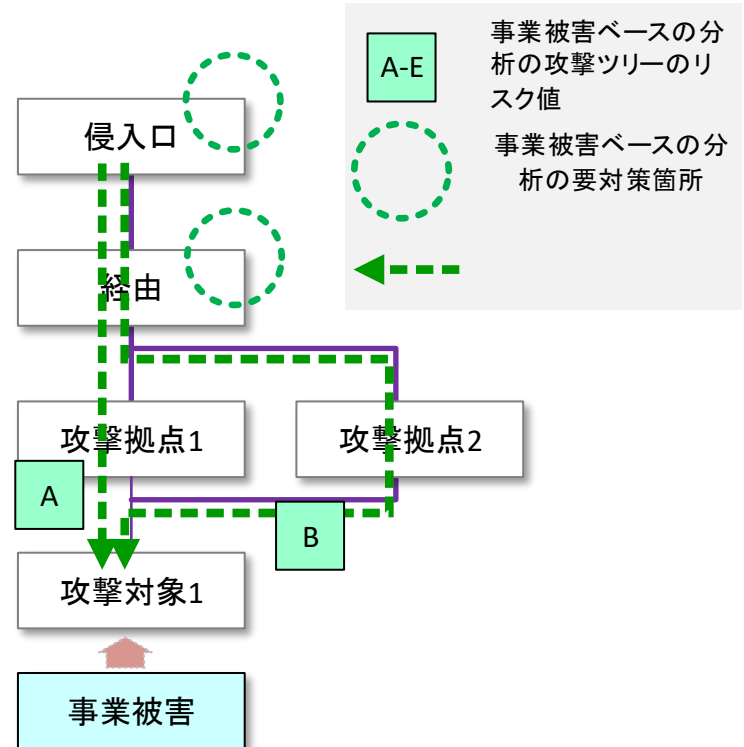
2種類のリスク分析の活用法の違いと相関

資産ベースリスク分析の対策の検討



資産間の接続によらず
すべての資産の対策を検討

事業被害ベースリスク分析の対策の検討



攻撃ツリーを構成する
いずれかの資産の対策を検討

8. セキュリティテスト

対策状況の確実性や有効性、脅威に対する堅牢性の検証

- セキュリティテストの位置付け(実施目的と効果)
 - 制御システムのリスク分析結果の実機での確認
 - 制御システムの現状調査
- セキュリティテストの種類・目的・対象

目的	テスト対象		
	ネットワーク	OS/ミドルウェア	アプリケーション
既知の脆弱性検出	・脆弱性検査 (システムセキュリティ検査)		・脆弱性検査 (Webアプリケーション診断)
未知の脆弱性検出	・ファジング		
			・ソースコードセキュリティ検査
侵入可否の検証	・ペネトレーションテスト		
不審通信の検査	・パケットキャプチャテスト		
不正なネットワーク機器の調査	・ネットワークディスカバリ ・ワイヤレススキャン		

9. 特定セキュリティ対策に対する追加基準

ガイド本編
p.324-329

特定のセキュリティ対策項目の実施状況をより詳細に確認・評価

- 暗号技術の選定と活用基準
- 標的型攻撃対策
- 内部不正対策
- ファイアウォールにおける各種設定
- 外部記憶媒体におけるセキュリティ対策
- 各追加基準における評価項目をチェックリストとして提供
 - 評価項目とセキュリティ要件
 - 「必須」または「推奨」として設定
 - 参照
 - 国際標準・業界標準等の参照箇所
 - 回答想定者／部門（「内部不正対策チェックリスト」のみ）
 - チェックリスト回答欄

制御システムに限定せず
全ての情報システムに活用可能

付録

- ゾーニングにおけるファイアウォールの活用パターン
 - － ファイアウォールの定義
 - － ファイアウォールの分類
 - － ファイアウォールの実装アーキテクチャ
- 特定セキュリティ対策に対するチェックリスト
 - － 暗号技術利用チェックリスト
 - － 標的型攻撃対策チェックリスト
 - － 内部不正対策チェックリスト
 - － ファイアウォール設定チェックリスト
 - － 外部記憶媒体対策チェックリスト
- 制御システムのインシデント事例
- 用語集
- 主な改定内容

	制御システムの境界防壁の詳細項目とセキュリティ要件 (◎必須、○推奨)	検定パターン							参照	チェックリスト管理	
		2	3	4	5	6	7	判定		検定(任意記入欄)	
制御システムのネットワークの分類と分類(他のシステムからの分類)											
1	○送信ドメインはデフォルトでは拒否し、例外許可(全て拒否、例外として許可)することが望ましい。 【全て拒否、例外のみ許可】の送信ドメインポリシーは、承認済みの送信ドメインに限定される。 (これはホワイトリストポリシーとして知られている。)	○	○	○	○	○	○	○	-NST SP800-82.5.2		
2	○プロシキヤは実施し、制御システム環境の情報システムリソース(ファイル、接続、サービス等)に対する、外部からの要求を拒否することが望ましい。		○	○	○	○	○	○	-NST SP800-82.5.2		
3	○提供されていない情報の持ち出しを防止することが望ましい。 例えば、アプリケーションファイアウォール(Deep Packet Inspection、DPI)やXMLゲートウェイ等を用いる。これらのデバイスは、プロトコルのフォーマットや仕様に基づいて、名前をアプリケーション層で検証し、ネットワーク層やトランスポート層で動作するデバイスでは検出できない脆弱性を検出する脆弱性を検出する。	○	○	○	○	○	○	○	-NST SP800-82.5.2		
4	○組織、システム、アプリケーション及び個人(のう)つ(人)または組織による、認可され、認証された送信元と宛先アドレスのペア間の通信のみを許可することが望ましい。	○	○	○	○	○	○	○	-NST SP800-82.5.2		
5	○人選管理を実施し、制御システムの構成要素へのアクセスを制御することが望ましい。	○	○	○	○	○	○	○	-NST SP800-82.5.2		
6	○制御システムの構成要素のネットワークアドレスが分からないように隠蔽し(公開しない、DNSに登録しない等)、知らないアドレスで通信しないことが望ましい。	○	○	○	○	○	○	○	-NST SP800-82.5.2		
7	○管理用やトラブルシューティング用の、特に(製造、攻撃者による)ネットワークの検索に有用な、ブロードキャストメッセージを使うサービス及びプロトコルを無効化することが望ましい。	○	○	○	○	○	○	○	-NST SP800-82.5.2		
8	○セキュリティドメインは、それぞれ別のネットワークアドレスを設定することが望ましい。 【例外: 全て共通なサブネットワークアドレスにする等】。	○	○	○	○	○	○	○	-NST SP800-82.5.2		
9	○プロトコルの検出に失敗した場合に、送信側(フォーマットバグを送らないように)に(詳細表示モード)、攻撃者が検出されないようにすることが望ましい。	○	○	○	○	○	○	○	-NST SP800-82.5.2		
10	○制御ネットワーク及びDMZにインシデント監視システムを設置して異常通信を自動的に検出し、アラートを発報するようにすることが望ましい。 【例】 SP800-82におけるDIS networkは、監視箇所によって検出の意味が異なっていると考えられるが、5.2の記述では、モデルシステムにおける制御ネットワーク及びDMZに相当すると解釈した。	○	○	○	○	○	○	○	-NST SP800-82.5.2		
11	○特に、異なるセキュリティドメインでは、異なるデータフローを実施することが望ましい。					○	○	○	-NST SP800-82.5.2		
12	○制御ネットワーク及びDMZにアクセスしうとする全てのユーザに対して、セキュリティ保護を実施することが望ましい。 【例】には、制御ネットワーク、検出しないコマンド、多段階認証、二重認証、ステータス、ステータス等、様々な方法がある。使用可能な方法を使用するのではなく、保護すべき制御ネットワーク及びDMZの脆弱性を認め、見合った方法を選択する。 【例】には、SP800-82におけるDIS networkは、監視箇所によって検出の意味が異なっていると考えられるが、5.2の記述では、モデルシステムにおける制御ネットワーク及びDMZに相当すると解釈した。	○	○	○	○	○	○	○	-NST SP800-82.5.3		

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

別冊
#1 & #2

典型的なモデルシステムに対するリスク分析の完全な実施事例

- ① 資産一覧
- ② システム構成図
- ③ データフローマトリックス
- ④ データフロー図
- ⑤ 資産の重要度の判断基準
- ⑥ 各資産に対する重要度一覧
- ⑦ 事業被害レベルの判断基準
- ⑧ 事業被害の一覧
- ⑨ 資産レベルの判断基準
- ⑩ 脅威レベルと根拠
- ⑪ 脅威レベルまとめ表
- ⑫ 資産ベースのリスク分析シート
- ⑬ リスク値まとめ表
- ⑭ 攻撃シナリオ一覧
- ⑮ 攻撃ルート一覧
- ⑯ 事業被害ベースのリスク分析シート
- ⑰ リスク値まとめ表
- ⑱ 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)

事業被害ベースのリスク分析シート



リスク分析シート一式(Excelファイル)は、以下のURLからダウンロード可能。

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

制御システム関連のサイバーインシデント事例

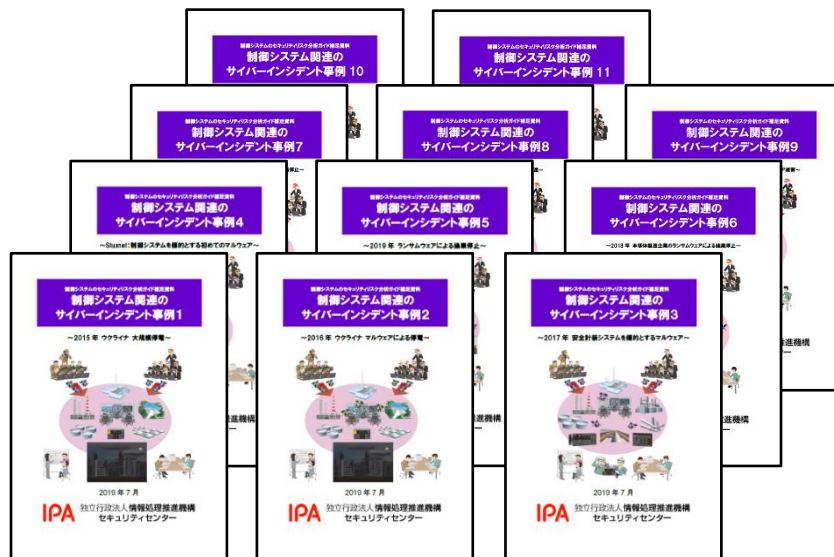
制御システムのセキュリティリスク分析ガイド 参考資料

事例集
#1～#11

「制御システム関連のサイバーインシデント事例」シリーズ

- サイバー攻撃事例の概要と攻撃の流れを紹介
- 事業被害ベースのリスク分析における
攻撃ツリーの作成やセキュリティ対策の策定に活用

#1	2015年 ウクライナ 大規模停電
#2	2016年 ウクライナ マルウェアによる停電
#3	2017年 安全計装システムを標的とするマルウェア
#4	Stuxnet: 制御システムを対象とする初めてのマルウェア
#5	2019年 アルミ製造企業に対する大規模ランサムウェア攻撃
#6	2018年 半導体製造企業のランサムウェアによる操業停止
#7	2020年 医療関連企業のランサムウェアによる操業停止
#8	2021年 水道局への不正侵入と飲料水汚染未遂
#9	2021年 米国最大手のパイプラインのランサムウェア被害
#10	2022年 衛星通信網へのサイバー攻撃
#11	2022年 電力網への攻撃



<https://www.ipa.go.jp/security/controlsystem/incident.html> からダウンロード可能

おわりに

「制御システムのセキュリティリスク分析ガイド 第2版」

制御システムのセキュリティの抜本的向上を可能とするために 重要な位置付けとなるリスクアセスメントの実践的な手引き

- リスク分析の全体像の理解向上と取り組み促進
 - リスク分析を具体的に実施するための手順や手引きの提示
- 2種類の詳細リスク分析の手法を解説
 - 資産ベース、事業被害ベース
- リスク分析のための素材の提供
 - リスク分析シート(フォーマット、実施例)
 - 脅威(攻撃方法)や対策の一覧
 - 特定対策に関する詳細チェックリスト
- リスク分析結果の活用例の提示
 - リスク低減のための対策強化策の検討方法
 - セキュリティテストの解説

