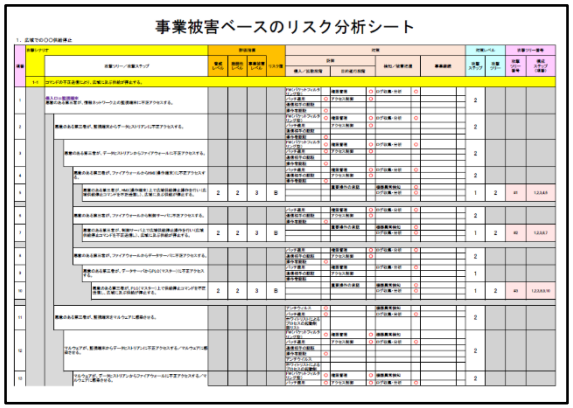
IPA Better Life with IT



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分析実施のススメ～

【活用の手引き】

独立行政法人情報処理推進機構（IPA）
技術本部　セキュリティセンター

2017年12月

制御システムのセキュリティリスク分析ガイド
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

4章　リスク分析の実施

4.1. 資産ベースのリスク分析

4.2. 事業被害ベースのリスク分析

5章　リスク分析結果の解釈と活用法

6章　セキュリティテスト

7章　特定対策に対する追加基準

参考文献、付録

2017年10月2日公開

ガイド本編

350頁

別冊

70頁

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

サイバー攻撃と戦う兵法
～セキュリティリスク分析の重要性～

中国、春秋時代の軍事戦略家、孫武の兵法書『孫子』に示された名句に「彼を知り己を知れば百戦殆うからず」がある。サイバー攻撃時代において、敵＝脅威（攻撃者を含む）、己＝自組織と置き換えてみると、セキュリティ対策において効果的な施策を実施するための教えとなる。 **セキュリティリスク分析**は、

己を知り、敵を知れば、百戦危うからず

を実践する、**サイバーセキュリティ時代の兵法**である。

「リスク分析」 ＝ ①②③を評価指標に、事業リスクを明確にするプロセス

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

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
- 効果的なセキュリティ投資の実現（追加対策、有効なテスト箇所の抽出）
- 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	○
		フォルトツリー解析（FTA）	大	○
組合せアプローチ			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通り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　＜己を知る＞

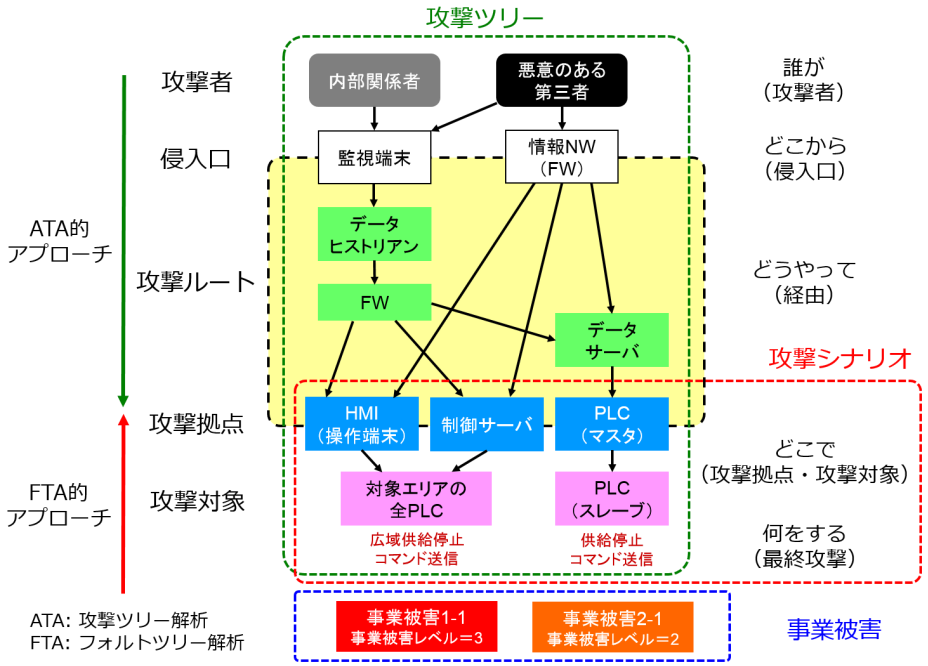
保護すべきシステムを構成する資産を対象に、各資産（サーバ、端末、通信機器等）に対して、その重要度（価値）、想定される脅威、脆弱性の3つを評価指標として、リスク分析を実施。 ⇒ 資産に対して網羅的に脅威と対策状況を評価可能

★ 事業被害ベースのリスク分析　＜敵を知る＞

保護すべき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
（ATAとFTAの利点を融合）

⇒机上でのペネトレーションテスト

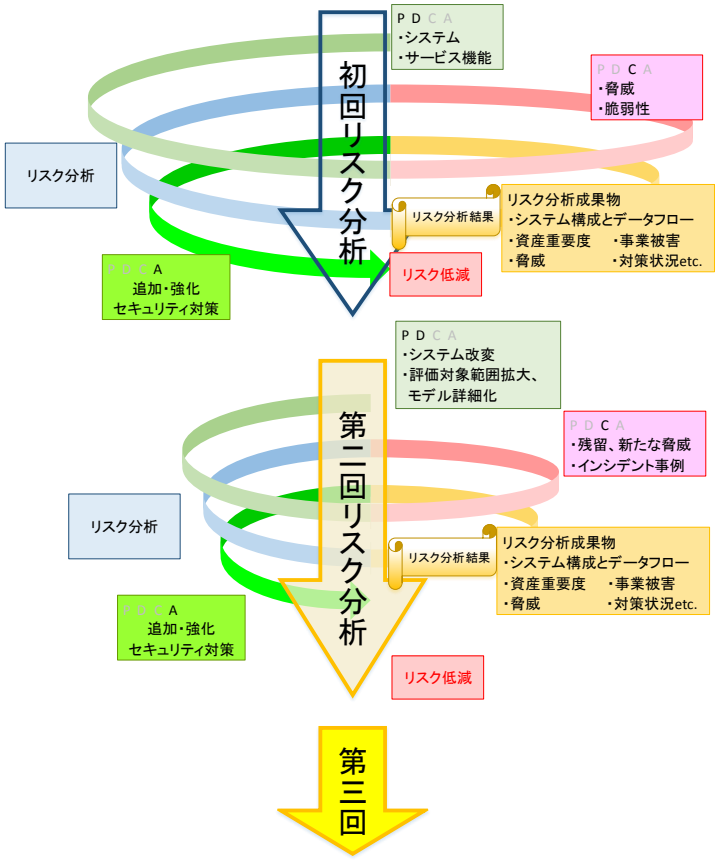


1. セキュリティ対策におけるリスク分析の位置付け

ガイド本編
p.12-17

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

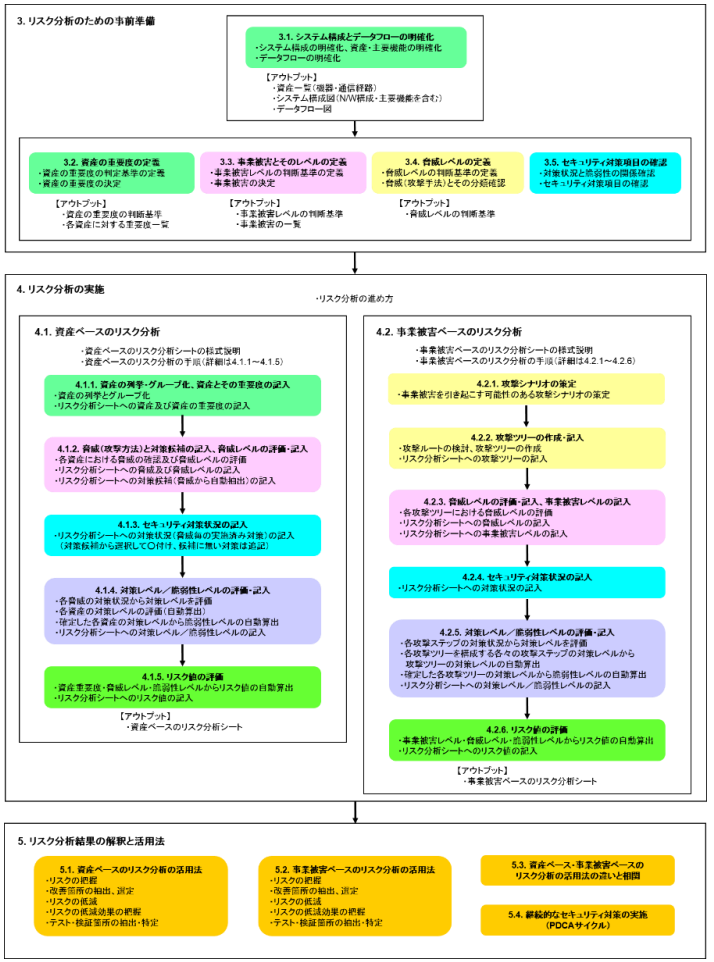


2. リスク分析の全体像と作業手順

ガイド本編
p.18-34

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

ガイド本編
p.35-36

自組織の分析と把握 ＝「己を知る最も重要なステップ」

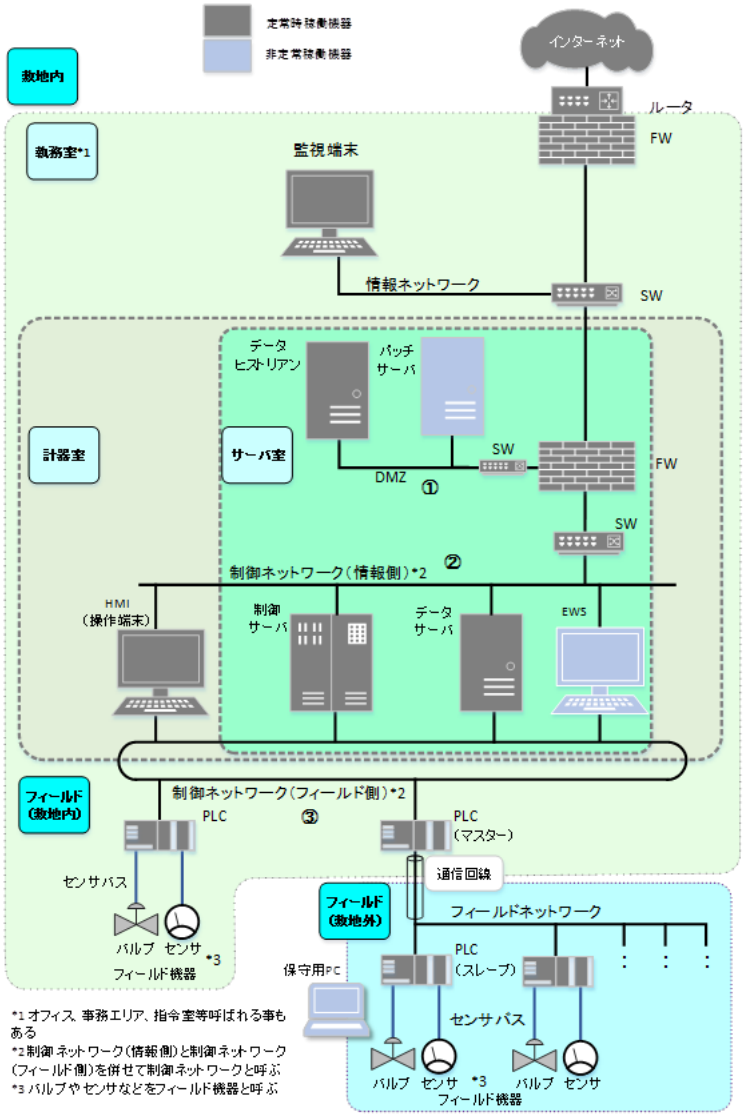
【事前準備作業とそのアウトプット】

節	準備作業	アウトプット
3.1	• システム構成の明確化 • 資産・主要機能の明確化 • データフローの明確化	• 資産一覧 • システム構成図 • データフロー図
3.2	• 資産の重要度の判断基準の定義 • 資産の重要度の決定	• 資産の重要度の判断基準 • 各資産に対する重要度一覧
3.3	• 事業被害レベルの判断基準の定義 • 事業被害の決定	• 事業被害レベルの判断基準 • 事業被害の一覧
3.4	• 脅威レベルの判断基準の定義 • 脅威（攻撃方法）の分類確認	• 脅威レベルの判断基準
3.5	• 対策状況と脆弱性の関係確認 • セキュリティ対策項目の確認	

3. リスク分析のための事前準備
3.1. システム構成とデータフローの明確化

ガイド本編
p.37-71

- 資産の洗い出し
- システム構成の明確化、論理化
  - 分析範囲の決定
  - 分析用アーキテクチャの明確化
  - 資産とその付帯情報の整理
  - 分析対象とする資産の絞り込み（グループ化と除外）
  - ロケーションと資産の配置
  - 各資産の接続情報の記述
- データフローの明確化
  - データの流れのシステム構成図へのマッピング



3. リスク分析のための事前準備
3.2. 資産の重要度の決定

ガイド本編
p.72-82

- 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点（1：低～3：高）

【資産の重要度の判断基準の定義例】

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。

3. リスク分析のための事前準備
3.3. 事業被害とそのレベルの定義

ガイド本編
p.83-87

- 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点（1：小～3：大）

【事業被害レベルの判断基準の定義例】

評価点	判断基準
3	事業上の被害が大きい。 【例】 ・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	事業上の被害が中程度。 【例】 ・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	事業上の被害は小さい。 【例】 ・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。

3. リスク分析のための事前準備
3.3. 事業被害とそのレベルの定義

ガイド本編
p.83-87

- 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

3. リスク分析のための事前準備
3.4. 脅威レベルの定義

ガイド本編
p.88-91

- 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点（1：低～3：高）

【脅威レベルの判断基準の定義例】

評価点	判断基準
3	発生する可能性が高い。 【例】 ・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	発生する可能性は中程度。 【例】 ・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。 ・分析対象システムのライフサイクルにおいて、発生することが想定される。
1	発生する可能性は低い。 【例】 ・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。 ・分析対象システムのライフサイクルにおいては、発生することが想定しがたい。

3. リスク分析のための事前準備
3.4. 脅威レベルの定義

ガイド本編
p.88-91

【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。	● 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。	● 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。	● 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。	● 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。	● 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。	● 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。	● 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。	● 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。	● 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。	● 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。	● 停止命令の不正実行

3. リスク分析のための事前準備
3.5. セキュリティ対策項目の確認

ガイド本編
p.94-104

- 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点（1：低～3：高）

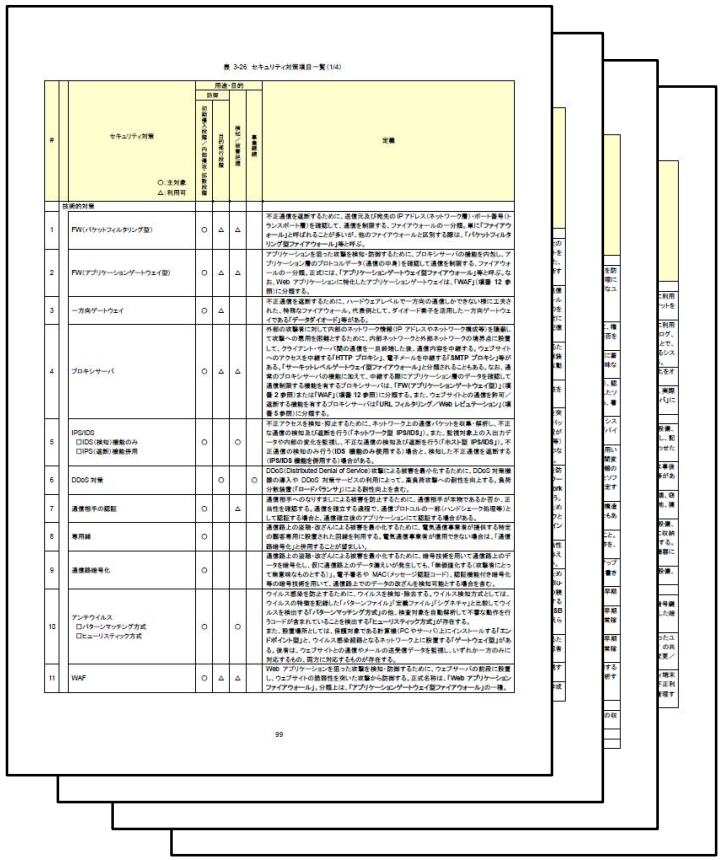
評価点		判断基準
脆弱性レベル	対策レベル	
3	1	脅威が発生した場合、容易に受けいれる可能性が高い。 脅威の対策が実施されておらず、攻撃が成功する可能性が高い。 【例】 ・過去の事例において、脆弱性を利用した攻撃が発生・成功し、被害が生じたことが確認されている。
2	2	脅威が発生した場合、受け入れる可能性が中程度である。 脅威の対策が実施されているが、十分とは言えないため、攻撃が成功する可能性は中程度である。 【例】 ・一般的な対策を実施しており、攻撃が成功するか否かは攻撃者のレベルに依る。 ・過去の事例において、脆弱性を利用した攻撃が発生したが、大きな被害に至らなかったことが確認されている。
1	3	脅威が発生した場合、受け入れる可能性は低い。 脅威の対策が十分実施されている。 【例】 ・効果的な対策や、多層的な対策を実施しており、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。

3. リスク分析のための事前準備
3.5. セキュリティ対策項目の確認

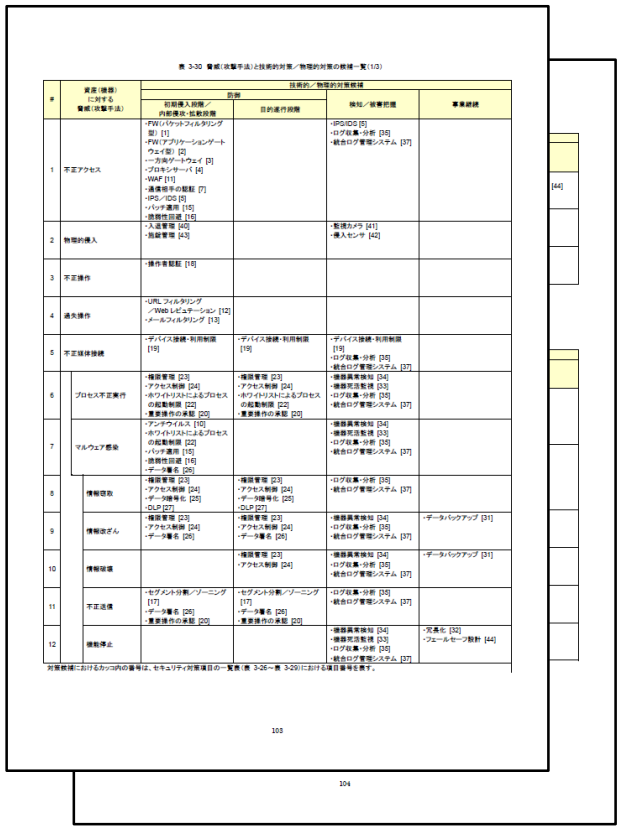
ガイド本編
p.94-104

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47項目）】



【脅威（攻撃手法）と技術的／物理的対策の候補一覧】



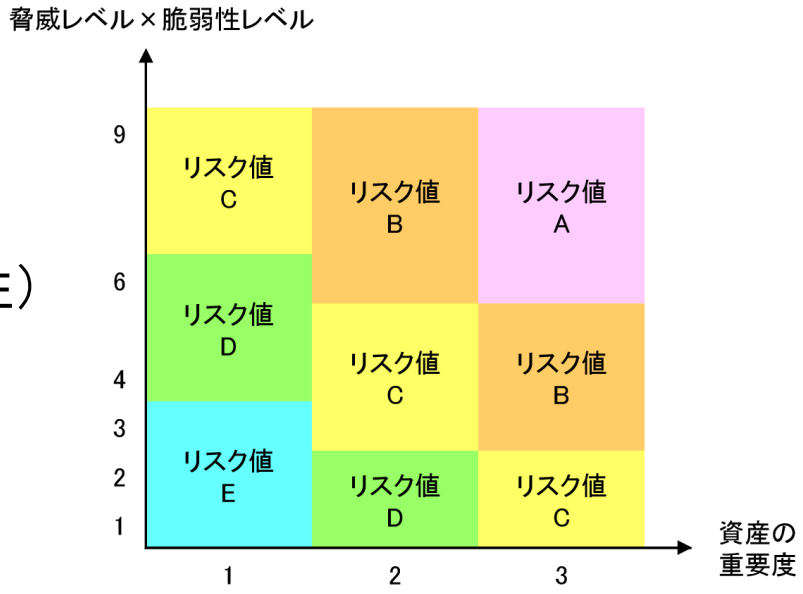
4. リスク分析の実施
4.1. 資産ベースのリスク分析

ガイド本編
p.106-147

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



資産毎のリスク値域の定義

4. リスク分析の実施
4.1. 資産ベースのリスク分析

ガイド本編
p.106-147

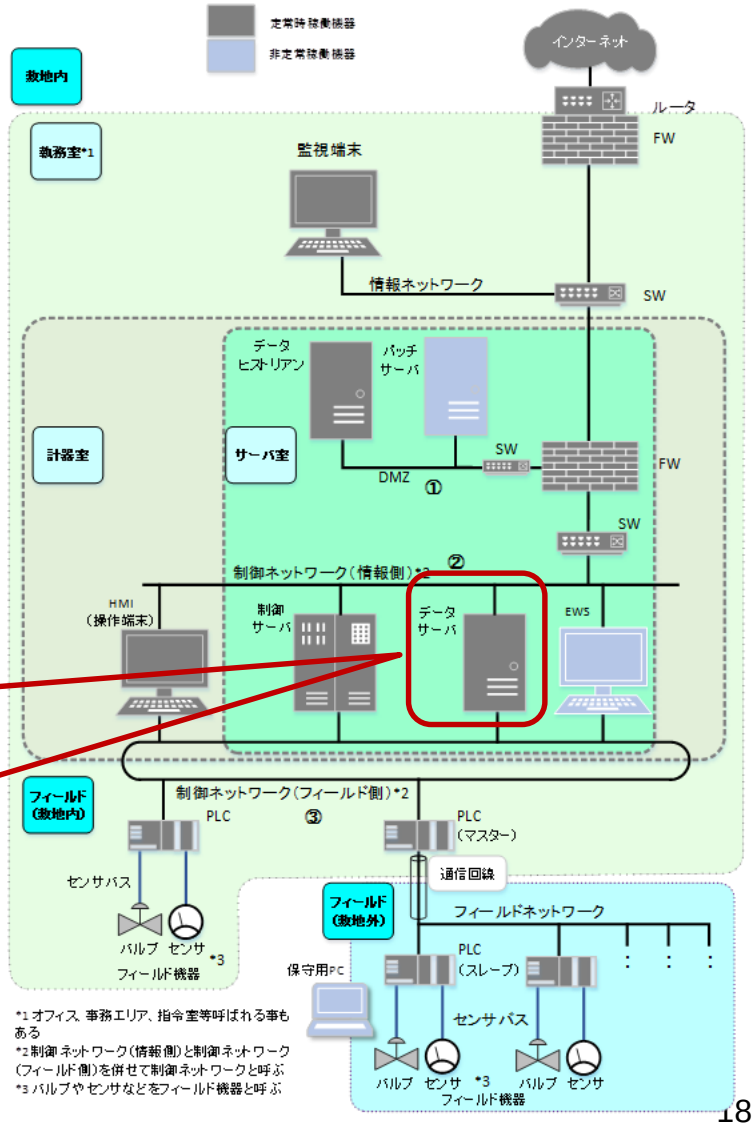
- 保護すべき制御システムを構成する資産群を機能、種別等によってグループ化
- グループ化した資産群を対象に、
  - ★ 脅威(攻撃手法)
  - ★ 対策状況

を記入→脆弱性レベル

脅威(攻撃手法)
不正アクセス
マルウェア感染
情報改ざん
機能停止 etc.

対策状況
通信相手の認証
ホワイトリスト
操作者認証
権限管理 etc.

脅威毎の脆弱性レベル値



4. リスク分析の実施
4.1. 資産ベースのリスク分析

ガイド本編
p.106-147

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

項番	資産種別	対象装置	評価指標				脅威(攻撃手法)	対策								対策レベル
			脅威レベル	脆弱性レベル	資産の重要度	リスク値		防御				検知/被害把握		事業継続		脅威毎
								侵入/拡散段階		目的遂行段階						
1	情報系資産	データサーバ	2	2		B	不正アクセス	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	操作者認証 (ID/Pass)	○							2
4			2	3		A	過失操作	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	デバイス接続・利用制限		(同左)		デバイス接続・利用制限 ログ収集・分析 統合ログ管理システム				1
6			2	2		B	プロセス不正実行	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	2		C	マルウェア感染	アンチウイルス ホワイトリストによるプロセスの起動制限 パッチ適用 脆弱性回避 データ署名	 ○ 			機器異常検知 機器死活監視 ログ収集・分析 統合ログ管理システム				2
8			3	2	3	A	情報窃取	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	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			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		A	不正送信	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	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	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	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

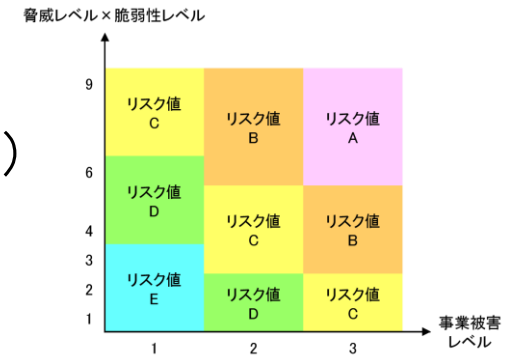
4. リスク分析の実施
4.2. 事業被害ベースのリスク分析

ガイド本編
p.148-231

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

- 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・経由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(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)
  - 事業被害レベル(事業被害の大きさ)

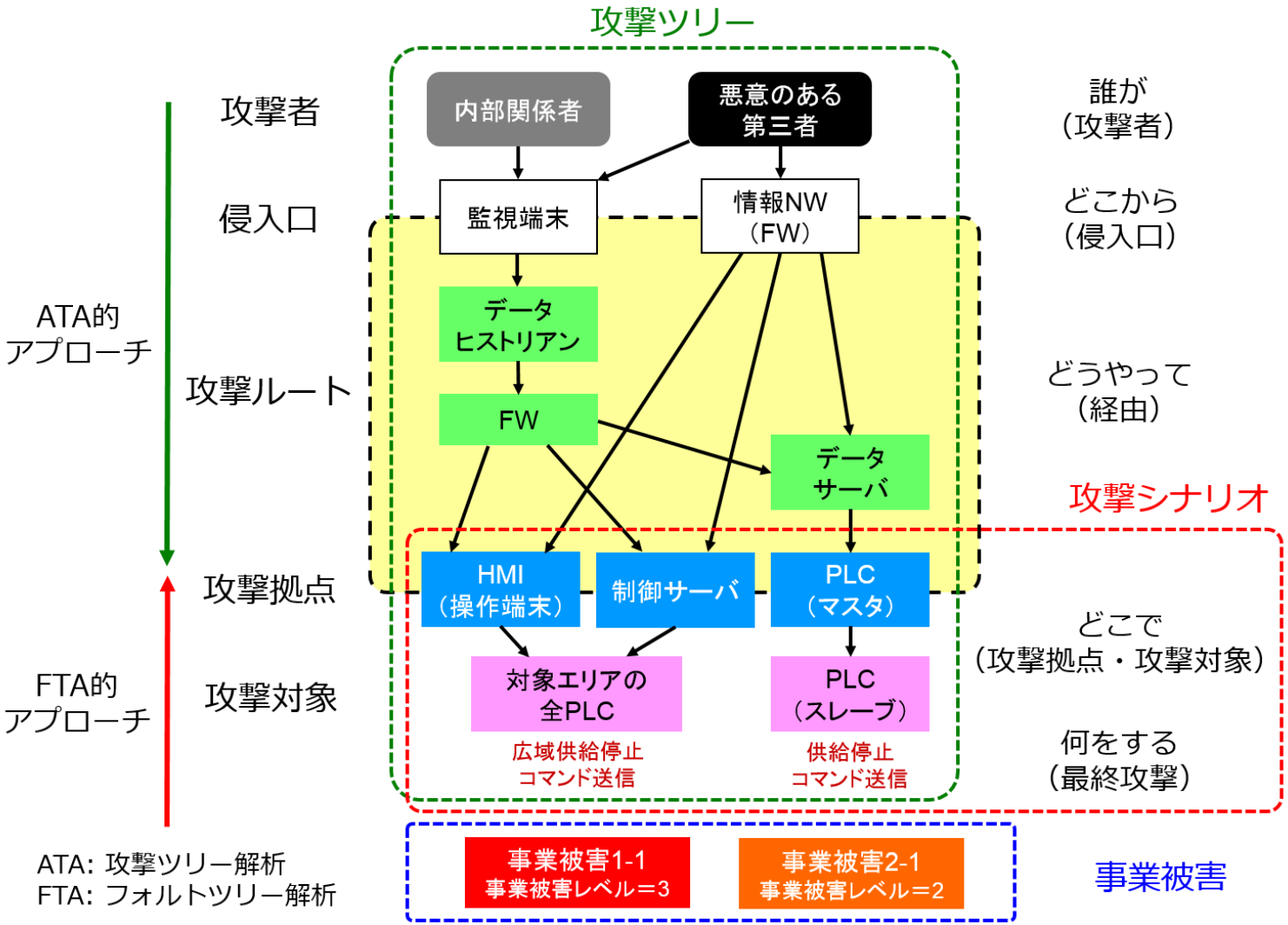
  から算定



攻撃ツリー毎のリスク値域の定義

4. リスク分析の実施
4.2. 事業被害ベースのリスク分析

ガイド本編
p.148-231



4. リスク分析の実施
4.2. 事業被害ベースのリスク分析

ガイド本編
p.148-231

事業被害ベースのリスク分析シート

1．広域での○○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	コマンドの不正送信により、広域に及ぶ供給が停止する。														
1		**侵入口＝監視端末** 悪意のある第三者が、情報ネットワーク上の監視端末に不正アクセスする。					FW（パケットフィルタリング型） パッチ適用 ○ 通信相手の認証 操作者認証 ○		権限管理 ○ アクセス制御 ○		ログ収集・分析 ○		2			
2		悪意のある第三者が、監視端末からデータヒストリアンに不正アクセスする。					FW（パケットフィルタリング型） ○ パッチ適用 通信相手の認証 操作者認証 ○		権限管理 ○ アクセス制御 ○		ログ収集・分析 ○		2			
3		悪意のある第三者が、データヒストリアンからファイアウォールに不正アクセスする。					FW（パケットフィルタリング型） ○ パッチ適用 通信相手の認証 操作者認証 ○		権限管理 ○ アクセス制御 ○		ログ収集・分析 ○		2			
4		悪意のある第三者が、ファイアウォールからHMI（操作端末）に不正アクセスする。					パッチ適用 通信相手の認証 操作者認証 ○		権限管理 ○ アクセス制御 ○		ログ収集・分析 ○		2			
5		悪意のある第三者が、HMI（操作端末）上で広域供給停止操作を行い（広域供給停止コマンドを不正送信し）、広域に及ぶ供給が停止する。	2	2	3	B			重要操作の承認		機器異常検知 ○ ログ収集・分析 ○		1	2	#1	1,2,3,4,5
6		悪意のある第三者が、ファイアウォールから制御サーバに不正アクセスする。					パッチ適用 通信相手の認証 操作者認証 ○		権限管理 ○ アクセス制御 ○		ログ収集・分析 ○		2			
7		悪意のある第三者が、制御サーバ上で広域供給停止操作を行い（広域供給停止コマンドを不正送信し）、広域に及ぶ供給が停止する。	2	2	3	B			重要操作の承認		機器異常検知 ○ ログ収集・分析 ○		1	2	#2	1,2,3,6,7
8		悪意のある第三者が、ファイアウォールからデータサーバに不正アクセスする。					パッチ適用 通信相手の認証 操作者認証 ○		権限管理 ○ アクセス制御 ○		ログ収集・分析 ○		2			
9		悪意のある第三者が、データサーバからPLC（マスター）に不正アクセスする。					パッチ適用 通信相手の認証 操作者認証		権限管理 アクセス制御		ログ収集・分析 ○		1			
10		悪意のある第三者が、PLC（マスター）上で供給停止コマンドを不正送信し、広域に及ぶ供給が停止する。	2	2	3	B			重要操作の承認		機器異常検知 ○ ログ収集・分析 ○		1	2	#3	1,2,3,8,9,10
11		悪意のある第三者が、監視端末をマルウェアに感染させる。					アンチウィルス ○ パッチ適用 ○ ホワイトリストによるプロセスの起動制限リスト				機器異常検知 ログ収集・分析 ○		2			

5. リスク分析結果の解釈と活用法

ガイド本編
p.232-255

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）

6. セキュリティテスト

ガイド本編
p.256-275

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		

7. 特定セキュリティ対策に対する追加基準

ガイド本編
p.276-281

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

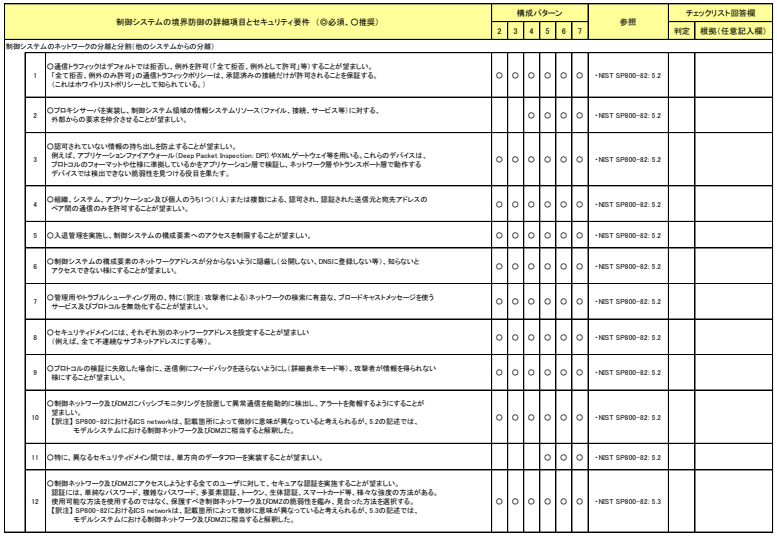
- 各追加基準における評価項目をチェックリストとして提供
  - 評価項目とセキュリティ要件
    - 「必須」または「推奨」として設定
  - 参照
    - 国際標準・業界標準等の参照箇所
  - 回答想定者／部門 （「内部不正対策チェックリスト」のみ）
  - チェックリスト回答欄

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

ガイド本編
p.284-347

- 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



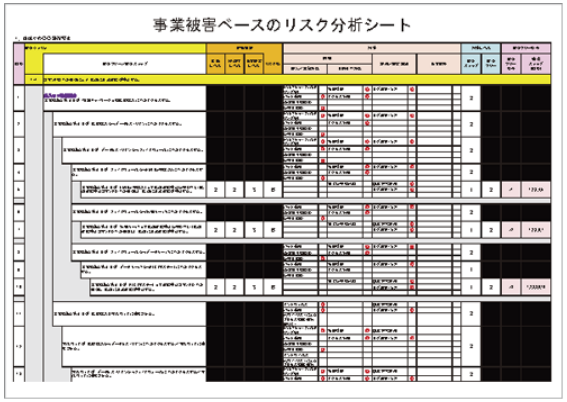
	制御システムの境界防御の詳細項目とセキュリティ要件 （◎必須、○推奨）	構成パターン 2	3	4	5	6	7	参照	チェックリスト回答欄 判定	根拠（任意記入欄）
制御システムのネットワークの分離と分割（他のシステムからの分離）										
1	○通信トラフィックはデフォルトでは拒否し、例外を許可（「全て拒否、例外として許可」等）することが望ましい。 「全て拒否、例外のみ許可」の通信トラフィックポリシーは、承認済みの接続だけが許可されることを保証する。 （これはホワイトリストポリシーとして知られている。）	○	○	○	○	○	○	・NIST SP800-82: 5.2		
2	○プロキシサーバを実装し、制御システム領域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、 外部からの要求を仲介させることが望ましい。			○	○	○	○	・NIST SP800-82: 5.2		
3	○認可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準拠しているか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見つける役目を果たす。	○	○	○	○	○	○	・NIST 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ち1つ（1人）または複数による、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。	○	○	○	○	○	○	・NIST SP800-82: 5.2		
5	○入退管理を実施し、制御システムの構成要素へのアクセスを制限することが望ましい。	○	○	○	○	○	○	・NIST 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）、知らないと アクセスできない様にすることが望ましい。	○	○	○	○	○	○	・NIST SP800-82: 5.2		
7	○管理用やトラブルシューティング用の、特に（訳注：攻撃者による）ネットワークの検索に有益な、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。	○	○	○	○	○	○	・NIST SP800-82: 5.2		
8	○セキュリティドメインには、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 （例えば、全て不連続なサブネットアドレスにする等）。	○	○	○	○	○	○	・NIST SP800-82: 5.2		
9	○プロトコルの検証に失敗した場合に、送信側にフィードバックを送らないようにし（詳細表示モード等）、攻撃者が情報を得られない 様にすることが望ましい。	○	○	○	○	○	○	・NIST SP800-82: 5.2		
10	○制御ネットワーク及びDMZにパッシブモニタリングを設置して異常通信を能動的に検出し、アラートを発報するようにすることが 望ましい。 【訳注】SP800-82における「ICS network」は、記載箇所によって微妙に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。	○	○	○	○	○	○	・NIST SP800-82: 5.2		
11	○特に、異なるセキュリティドメイン間では、単方向のデータフローを実装することが望ましい。				○	○	○	・NIST SP800-82: 5.2		
12	○制御ネットワーク及びDMZにアクセスしようとする全てのユーザに対して、セキュアな認証を実施することが望ましい。 認証には、単純なパスワード、複雑なパスワード、多要素認証、トークン、生体認証、スマートカード等、様々な強度の方法がある。 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の脆弱性を鑑み、見合った方法を選択する。 【訳注】SP800-82における「ICS network」は、記載箇所によって微妙に意味が異なっていると考えられるが、5.3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。	○	○	○	○	○	○	・NIST 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
p.1-70

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 システム構成図
② 資産一覧
③ データフロー図
④ 資産の重要度の判断基準
⑤ 各資産に対する重要度一覧
⑥ 事業被害レベルの判断基準
⑦ 事業被害の一覧
⑧ 資産レベルの判断基準
⑨ 資産ベースのリスク分析シート
⑩ 攻撃シナリオ
⑪ 事業被害ベースのリスク分析シート
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）



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

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」

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セキュリティリスク分析ガイド

- 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通り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