IPA Better Life with IT

ET & IoT Technology West 2018

制御システムのセキュリティリスク分析ガイド

～詳細リスク分析手法の解説と分析結果の活用～

2018年07月06日（金） 16:00 - 16:20

独立行政法人情報処理推進機構（IPA）

セキュリティセンター

セキュリティ対策推進部

福原　聡

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
p.1-4

【ガイド本編の目次】

- セキュリティ対策におけるリスク分析の位置付け
- リスク分析の全体像と作業手順
- リスク分析のための事前準備
- リスク分析の実施
- リスク分析結果の解釈と活用法
- セキュリティテスト
- 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

【参考資料】

- ガイド別冊：制御システムに対するリスク分析の実施例
- 早分かり　活用の手引き

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

制御システムにおけるリスク分析の必要性

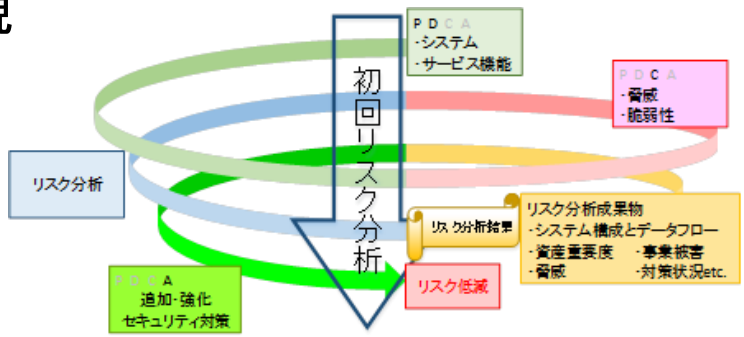
ガイド
p.12-13

- 制御システムの特性
  - 社会基盤、産業基盤を支えており可用性が最重要。停止による社会的な影響・事業継続上の影響が大きい
  - システムのライフサイクルが10-20年と長期間
- セキュリティ対策の必要性
  - インターネット、リモート回線等外部ネットワークとの接続
  - 構成コンポーネントがWindowsやLinux等の汎用品
  - USBメモリの利用
- 制御システムに対するサイバー攻撃
  - 変電所の不正操作による停電（Industroyer/CrashOverride）
  - ランサムウェア感染による生産ラインの停止（WannaCry）

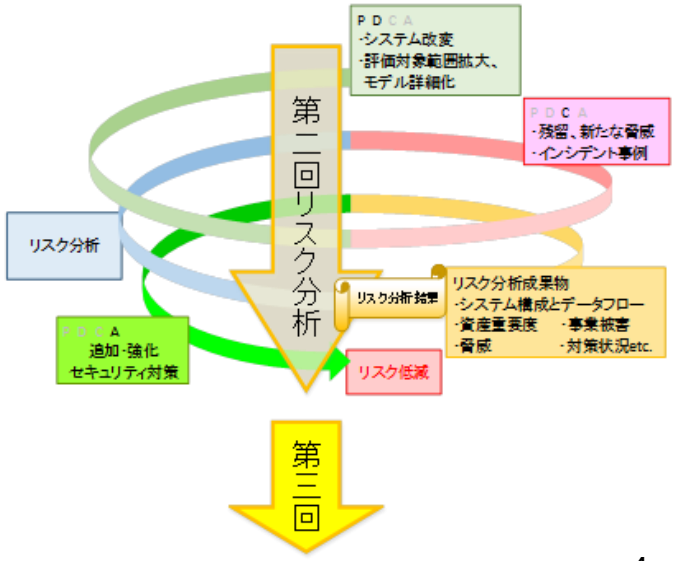
1. セキュリティ対策におけるリスク分析の位置付け

ガイド
p.14-17

- 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（サービス等を含む）に対する脅威と被害のレベル（可能性と大きさ等）を明確化
  - セキュリティ対策上、必要不可欠



- 詳細リスク分析
  - より正確なリスク分析
  - セキュリティ投資の優先順位等、組織として戦略的に検討可能
  - 一度実施するとそれをベースに継続的セキュリティレベルの向上可能

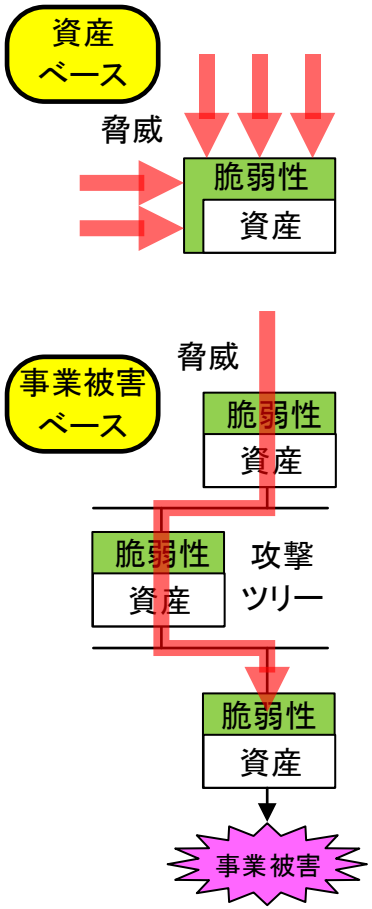


2. 詳細リスク分析の概要

ガイド
p.21-23

ガイドで紹介する2種類の詳細リスク分析

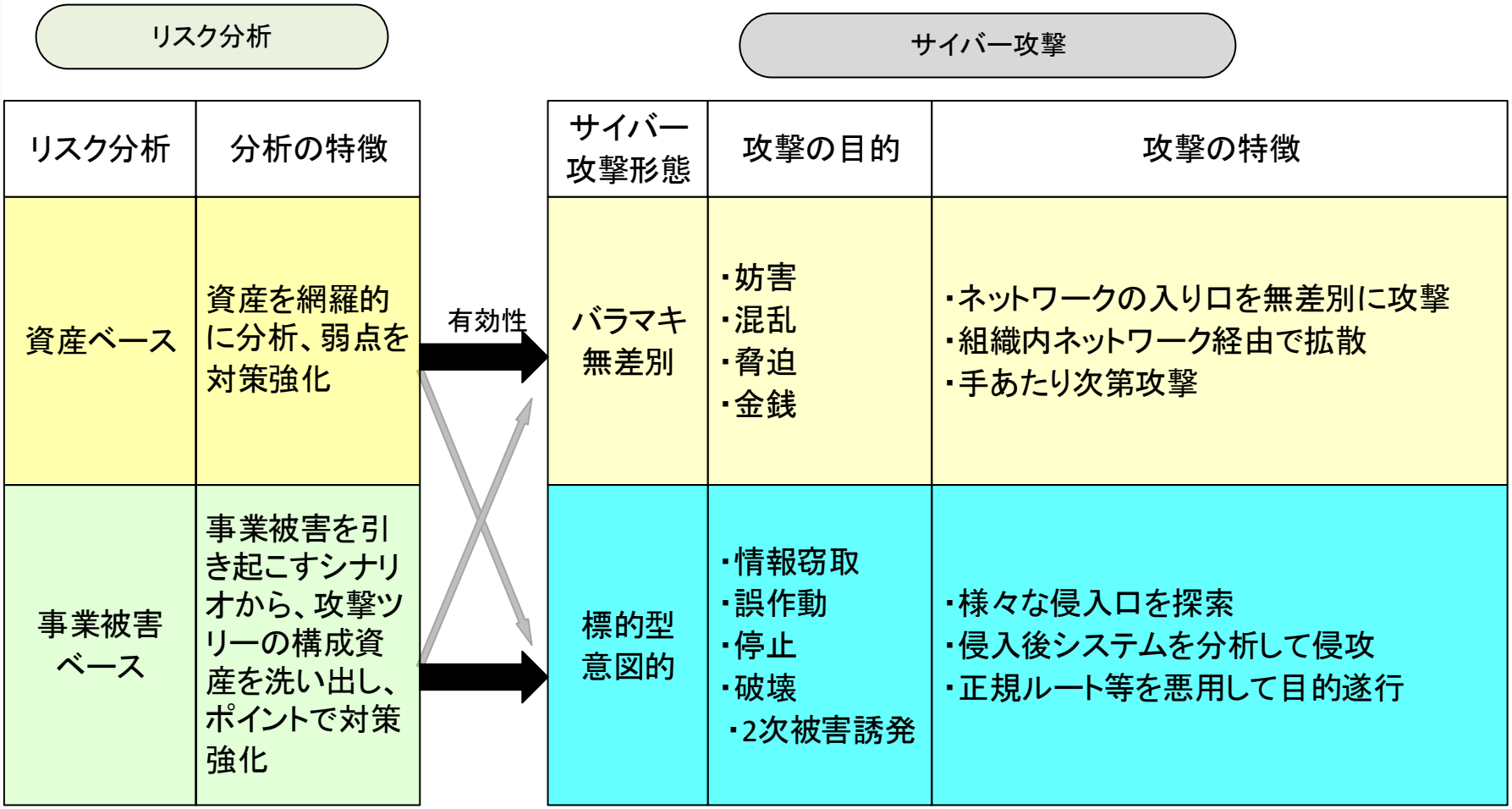
- 資産ベースのリスク分析
  - 保護すべきシステムを構成する資産のリスクを、各資産の重要度（価値）、脅威、脆弱性の3つを指標として評価する
- 事業被害ベースのリスク分析
  - 保護すべきシステムで実現されている事業やサービスの運用が脅かされるシナリオを検討し、それらのシナリオを引き起こす具体的な攻撃ツリー（一連の攻撃手順）が成立するリスクを、各攻撃ツリーの事業被害の大きさ、脅威、脆弱性の3つを指標として評価する



2. 2つのリスク分析の位置づけ

ガイド
p.27

- 相互補完によるリスク分析の有効性向上



2. リスク分析の全体像と作業手順

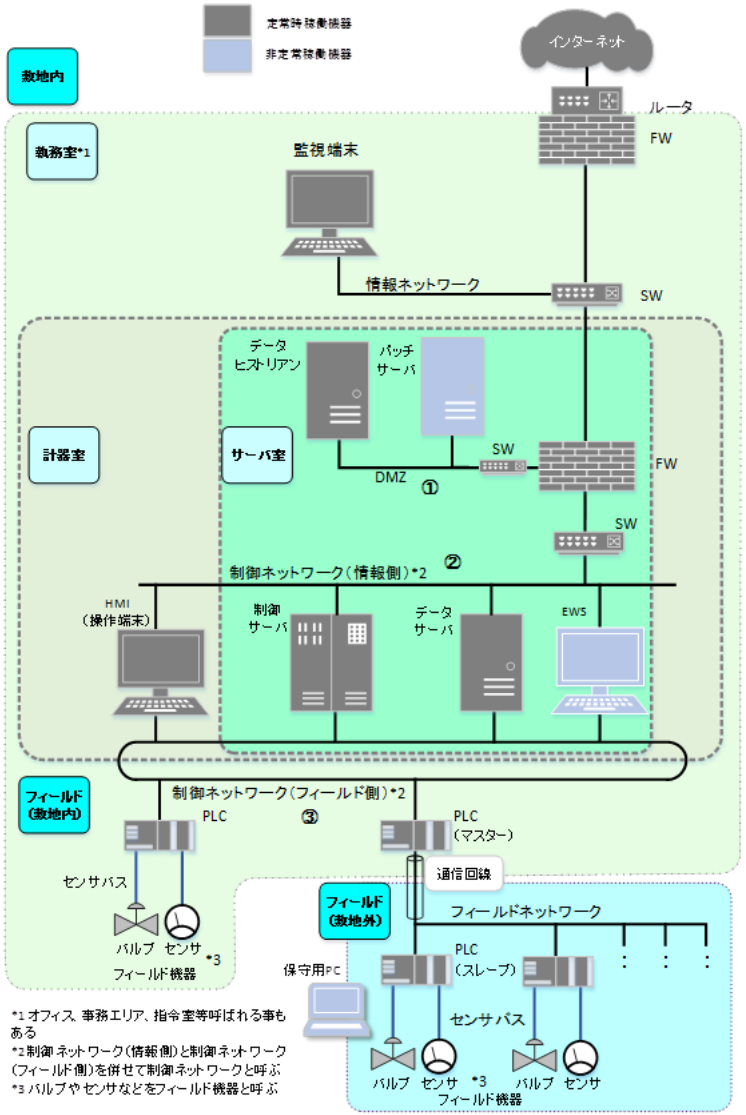
ガイド
p.28-29

*数字は章/節

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
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 資産の重要度の定義と決定

ガイド
p.72-82

- 重要度の判断基準の定義
  - 資産ベースのリスク分析における評価指標
  - 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
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
  - 脅威／攻撃によって生じる事業被害の大きさの評価点（1：小～3：大）
- 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

3. リスク分析のための事前準備
3.4. 脅威レベルの定義と脅威の種類

ガイド
p.88-91

- 脅威レベル
  - 資産ベース／事業被害ベース共通の評価指標
  - それぞれのリスク分析において、
    想定する脅威／攻撃が発生する可能性の評価点（1：低～3：高）
- 脅威（攻撃手法）

【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

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と脆弱性

ガイド
p.94-104

- 脆弱性レベル
  - 資産ベース／事業被害ベース共通の評価指標
  - 各リスク分析における対策内容をもとに算定する、発生した脅威／攻撃を受容する可能性の評価点（レベル1：低～3：高）
- ガイドでは脅威（攻撃手法）と対策候補の一覧を提示

表 3-30 脅威（攻撃手法）と技術的対策／物理的対策の候補一覧（1/3）

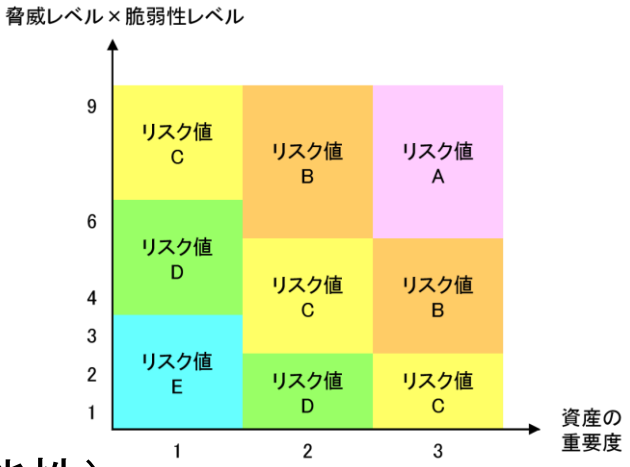
#	資産（機器）に対する脅威（攻撃手法）	技術的／物理的対策候補			
		防御		検知／被害把握	事業継続
		初期侵入段階／内部侵攻・拡散段階	目的遂行段階		
1	不正アクセス	・FW（パケットフィルタリング型）[1] ・FW（アプリケーションゲートウェイ型）[2] ・一方向ゲートウェイ [3] ・プロキシサーバ [4] ・WAF [11] ・通信相手の認証 [7] ・IPS／IDS [5] ・パッチ適用 [15] ・脆弱性回避 [16]		・IPS/IDS [5] ・ログ収集・分析 [35] ・統合ログ管理システム [37]	
2	物理的侵入	・入退管理 [40] ・施錠管理 [43]		・監視カメラ [41] ・侵入センサ [42]	
3	不正操作	・操作者認証 [18]			

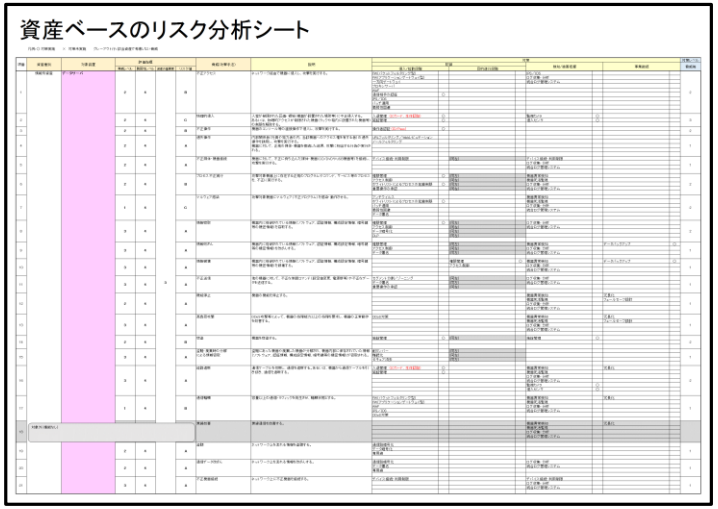
4. リスク分析の実施
4.1. 資産ベースのリスク分析

ガイド
p.106-147

- 事前準備で洗い出し、分析対象として精査した、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(発生した脅威を受容する可能性)

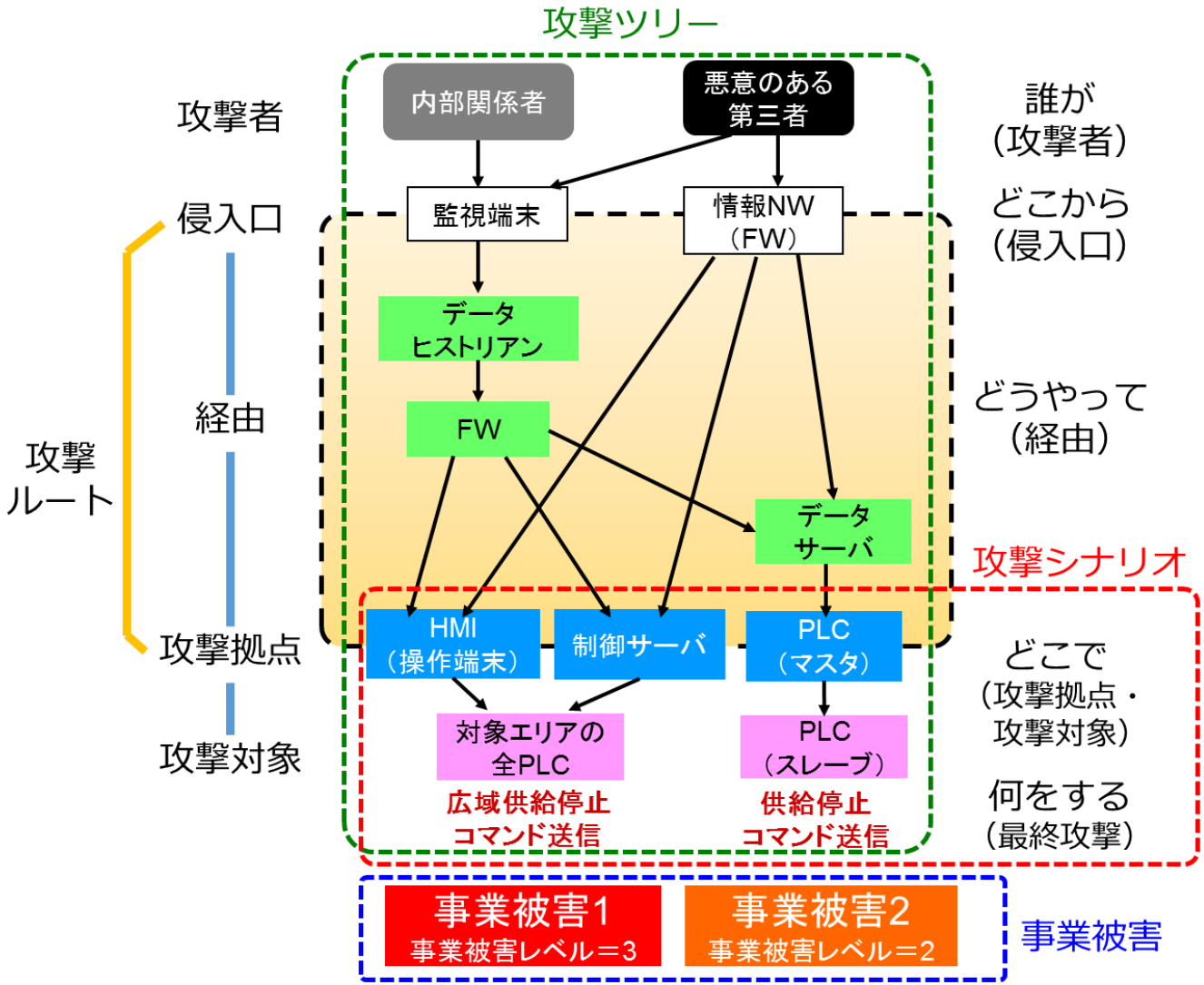
  から算定
- 結果は資産ベースのリスク分析シートに記載





4. リスク分析の実施
4.2. 事業被害ベースのリスク分析：攻撃ツリー

ガイド
p.148-231

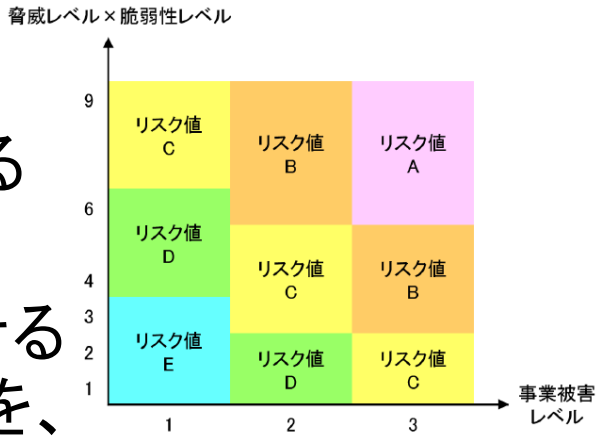


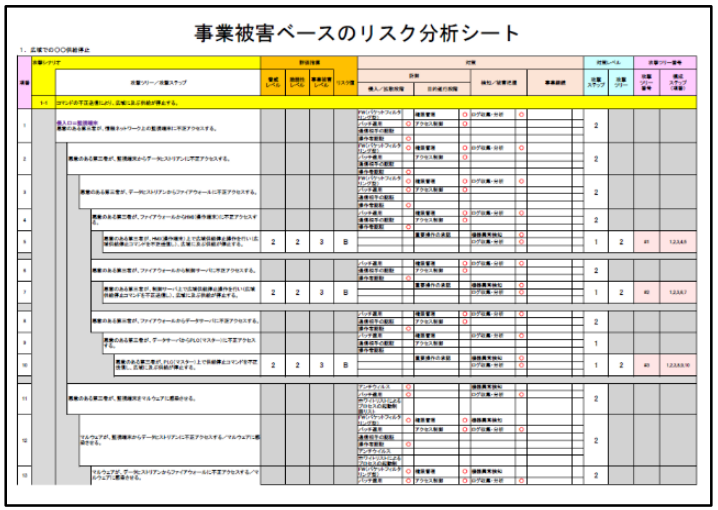
4. リスク分析の実施
4.2. 事業被害ベースのリスク分析

ガイド
p.106-147

- 事前準備で明確化したシステム構成図、データフロー図、事業被害に基づき、
- 保護すべき制御システムで実現されている事業やサービスを対象に、
- 事業被害を引き起こすシナリオを成立させる各攻撃ツリーのリスクの大きさ(リスク値)を、
  - 事業被害レベル
  - 脅威レベル(攻撃の発生可能性)
  - 脆弱性レベル(発生した攻撃を受容する可能性)

  から算定
- 結果は事業被害ベースのリスク分析シートに記載

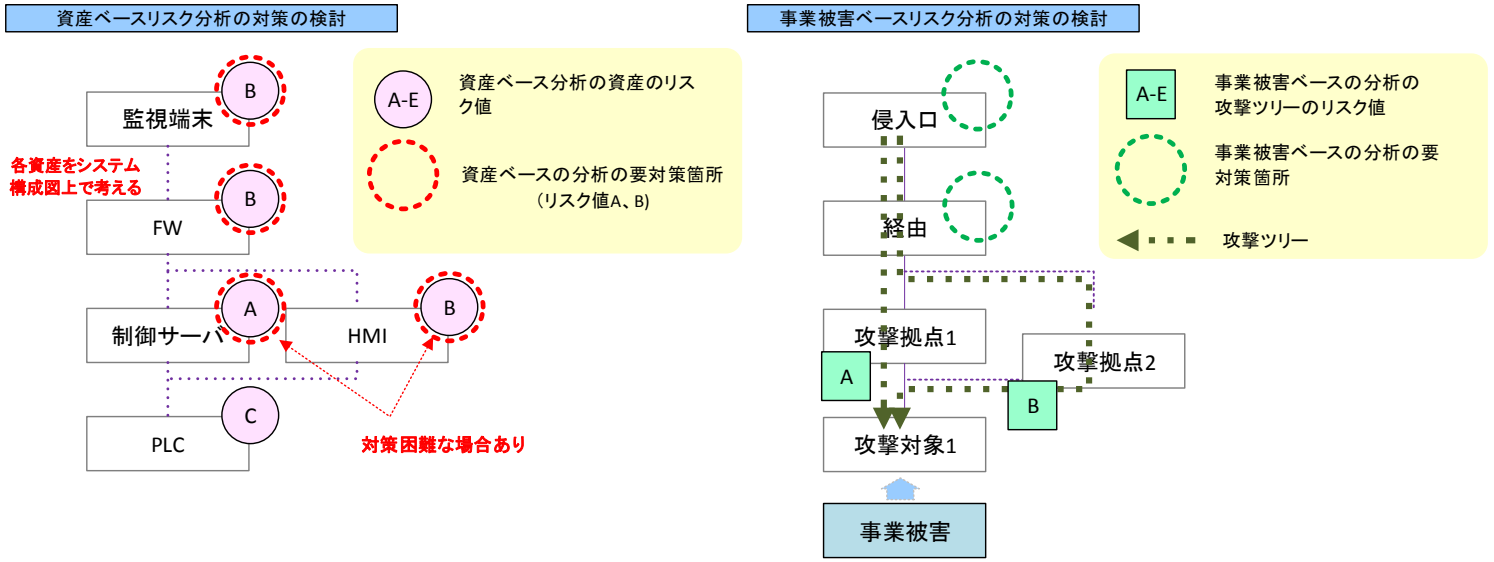




5. リスク分析結果の解釈と活用法

ガイド
p.232-255

- リスク値の活用
  - リスクの把握～改善箇所の抽出、選定
  - リスクの低減と低減効果の確認
  - 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
p.256-275

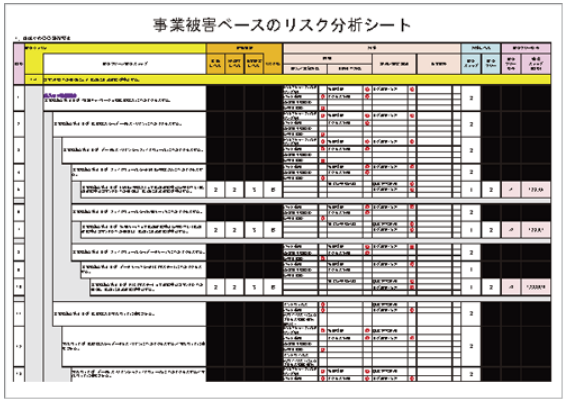
- セキュリティテストの位置付け（実施目的と効果）
  - 制御システムのリスク分析結果の実機での確認
  - 制御システムの現状調査
- セキュリティテストの種類・目的・対象

<table>
<tr><th rowspan="2">目的</th><th colspan="3">テスト対象</th></tr>
<tr><th>ネットワーク</th><th>OS／ミドルウェア</th><th>アプリケーション</th></tr>
<tr><td rowspan="2">既知の脆弱性検出</td><td colspan="2">・脆弱性検査
（システムセキュリティ検査）</td><td>・脆弱性検査
（Webアプリケーション診断）</td></tr>
<tr><td colspan="3">・ファジング</td></tr>
<tr><td>未知の脆弱性検出</td><td colspan="2"></td><td>・ソースコードセキュリティ検査</td></tr>
<tr><td>侵入可否の検証</td><td colspan="3">・ペネトレーションテスト</td></tr>
<tr><td>不審通信の検査</td><td colspan="3">・パケットキャプチャテスト</td></tr>
<tr><td>不正なネットワーク機器の調査</td><td>・ネットワークディスカバリ
・ワイヤレススキャン</td><td colspan="2"></td></tr>
</table>

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

早分かり 活用の手引き

- 制御システムのセキュリティリスク分析ガイド（本体350ページ、別冊70ページ）のエッセンスをまとめた全28ページの紹介資料
- 活用の手引きは、以下のURLからダウンロード可能。
  https://www.ipa.go.jp/security/controlsystem/riskanalysis.html

IPA 制御システムのセキュリティ

- 制御システムに関するセキュリティ情報のポータルサイト

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

- コンテンツ
  - セキュリティ普及啓発
    - 調査報告書、ガイド
  - 脆弱性対策情報(含 ICS-CERT)

展示ブースにもお立ち寄りください。

- 以下の見本を置いています。
  ご自由にお手に取ってご覧ください。
  - ガイド本編
  - ガイド別冊

情報セキュリティ白書2018
― 深刻化する事業への影響：つながる社会で立ち向かえ ―

情報セキュリティ白書2018　目次

2018年7月17日発売予定

◆定価：2,000円（税別）予定
ソフトカバー / A4判

◆入手先：Amazon
全国官報販売組合
IPA　※全国の書店からも購入できます