資料7

IPA Information-technology Promotion Agency, Japan

制御システムのセキュリティリスク分析ガイド
～リスク分析実施のススメ～
のご紹介

2017年12月20日
独立行政法人 情報処理推進機構
セキュリティセンター
技術ラボラトリー長　金野　千里

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～

IPA

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。　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

① 実効的なリスクの低減の実現
② 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）
③ 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

リスク分析の手法と特徴

項	分析手法			工数	効果
1	ベースラインアプローチ			小	△
2	非形式的 アプローチ			小	×？
3	詳細リスク分析	資産ベース		中	○
		シナリオベース	アタックツリー・アナリシス （ATA）	大	○
			フォールトツリー・アナリシス （FTA）	大	○
4	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

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

2017年10月2日公開

具体的な手順を解説、テンプレート、チェックリスト等を提供

【ガイド本編の目次】

ガイド本編

350頁

別冊
（分析例フルセット）

70頁

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

4章　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　＜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

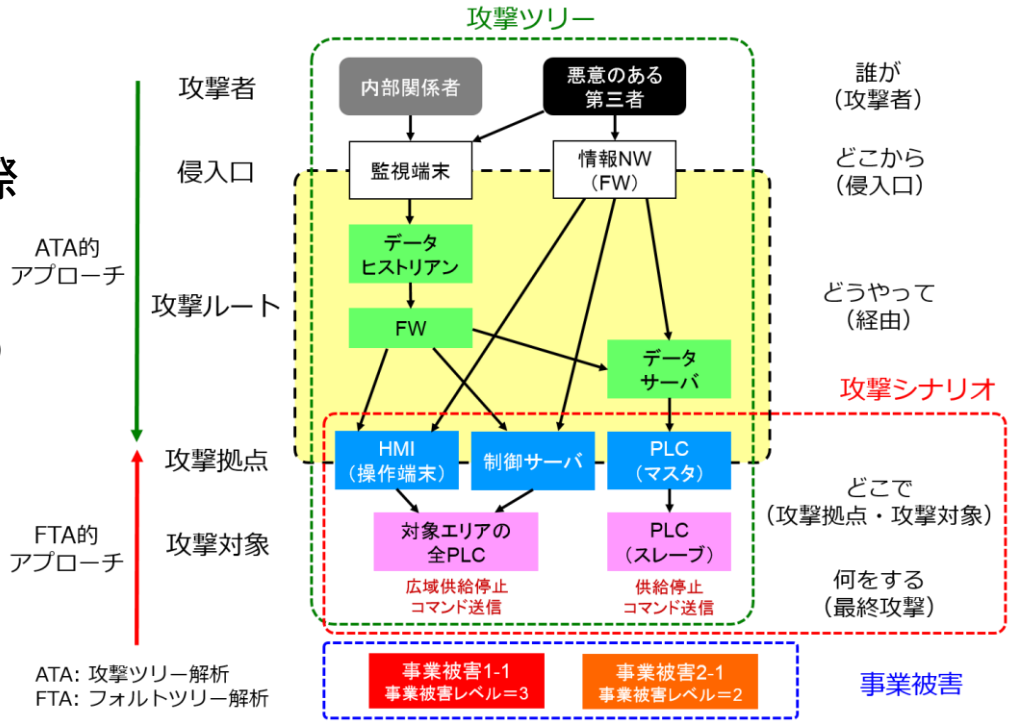
★ 事業被害ベースのリスク分析　＜敵を知る＞

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



事業被害ベースのリスク分析シート
～実例とテンプレートを提示～

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			

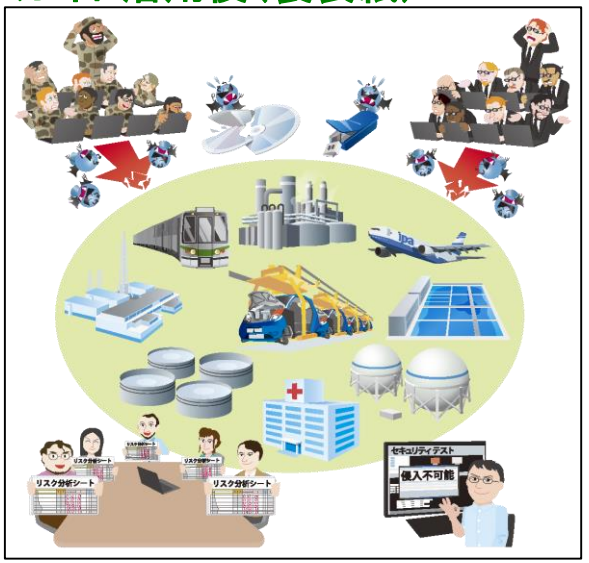
5章　リスク分析結果の解釈と活用方法を解説

- リスク分析結果の解釈及び活用のねらい
  - 制御システムの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。そのため、リスク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）

「制御システムのセキュリティリスク分析ガイド」をご活用下さい

- 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

ガイド活用後（裏表紙）



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

独立行政法人**情報処理推進機構**
Information-technology Promotion Agency, Japan